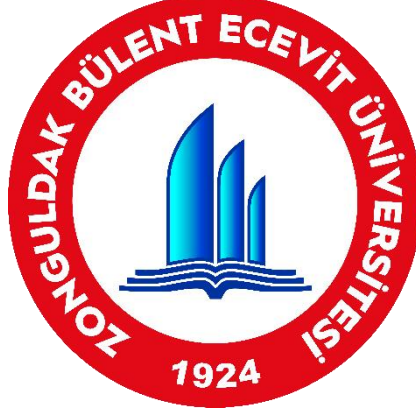




**T.C.
ZONGULDAK BÜLENT ECEVİT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
TÜRKÇE VE SOSYAL BİLİMLER EĞİTİMİ ANABİLİM DALI**

Yüksek Lisans Tezi

**SOSYAL BİLGİLER DERSİ ÖĞRETİM PROGRAMI VE
DERS KİTAPLARININ BİLGİ GÜVENLİĞİ
BAĞLAMINDA DEĞERLENDİRİLMESİ**

Talha Hakan KAYGISIZ

Zonguldak 2025

**T.C.
ZONGULDAK BÜLENT ECEVİT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
TÜRKÇE VE SOSYAL BİLİMLER EĞİTİMİ ANABİLİM DALI**

Yüksek Lisans Tezi

**SOSYAL BİLGİLER DERSİ ÖĞRETİM PROGRAMI
VE DERS KİTAPLARININ BİLGİ GÜVENLİĞİ
BAĞLAMINDA DEĞERLENDİRİLMESİ**

Hazırlayan

Talha Hakan KAYGISIZ

Tez Danışmanı

Doç. Dr. Canan TUNÇ ŞAHİN

Zonguldak 2025

BİLİMSEL ETİK BİLDİRİMİ

Hazırladığım Yüksek Lisans Tezinin bütün aşamalarında bilimsel etiğe ve akademik kurallara riayet ettiğimi, çalışmada doğrudan veya dolaylı olarak kullandığım her alıntıya kaynak gösterdiğimi ve yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, yazımda ve basımda enstitü tez yazım ve basım yönergesine uygun davranıldığını taahhüt ederim.

Talha Hakan KAYGISIZ

18.07.2025

T.C.
ZONGULDAK BÜLENT ECEVİT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

TEZ ONAYI

Enstitümüzün Türkçe ve Sosyal Bilimler Eğitimi Anabilim Dalında 225282125007 numaralı Talha Hakan KAYGISIZ'ın hazırladığı “**Sosyal Bilgiler Dersi Öğretim Programı ve Ders Kitaplarının Bilgi Güvenliği Bağlamında Değerlendirilmesi**” başlıklı YÜKSEK LİSANS tezi ile ilgili TEZ SAVUNMA SINAVI, Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliği uyarınca 18/07/2025 Pazartesi günü saat 14:00’da yapılmış, sorulan sorulara alınan cevaplar sonunda tezinin onayına OY BİRLİĞİYLE karar verilmiştir.

Dr. Öğr. Üyesi Burcu KARAMAN
Başkan

Doç. Dr. Canan TUNÇ ŞAHİN
(Tez Danışmanı)
Üye

Prof. Dr. Oğuzhan KARADENİZ
Üye

Yukarıdaki imzaların, adı geçen öğretim üyelerine ait olduğunu onaylarım.

... / ... / 20...

Prof. Dr. Yücel NAMAL
Enstitü Müdürü

ÖZET

Kurum	: BEUN Sosyal Bilimler Enstitüsü Türkçe ve Sosyal Bilimler Eğitimi Anabilim Dalı
Tez Başlığı	: Sosyal Bilgiler Dersi Öğretim Programı ve Ders Kitaplarının Bilgi Güvenliği Bağlamında Değerlendirilmesi
Tez Yazarı	: Talha Hakan KAYGISIZ
Tez Danışmanı	: Doç. Dr. Canan TUNÇ ŞAHİN
Türü, Yılı	: Yüksek Lisans,
Sayfa Adedi	2025 : 136

Bilgi güvenliği günümüzde insan hayatından ayrılması mümkün olmayan süreçler bütünüdür. Bilişim ve iletişim teknolojilerindeki gelişmeler günümüz toplumunda insan hayatını her alanda etkilediği tartışılmaz bir geçektir. Günlük hayatımızda kullandığımız bilişim cihazlarından artık ekonomik, sosyal, sağlık, e-ticaret gibi kişisel alanımızı da içine alan bir çok konuda iş ve işlemlerimizi de yapabilmekteyiz. Tüm bu konularda insan hayatını bu denli önemli etkileyen dijital etkileşimler birtakım farkındalıkların da bizlerde oluşmasını gerekli kılmaktadır. Bilgi güvenliği bir açıdan yaşamsal davranışlarımızın içinde yer alan ve hayatımızı etkileyen dijital etkileşimlerin önleyici güvenlik sağlamalarının yapılması gereken bir süreçtir.

Bu çalışmada 2024 Sosyal Bilgiler Dersi Öğretim Programı ve Sosyal Bilgiler ders kitaplarında bilgi güvenliği süreçleri açısından farkındalık sağlayıcı önleyici güvenlik önlemlerinin ne derece işlendiği, bahse konu içeriklerin dağılımları ve etkililik düzeyleri açısından incelenmiştir. Bu araştırma nitel araştırma desenlerinden biri olan doküman incelemesi yöntemiyle gerçekleştirilmiştir. Çalışmada, 2024 yılı itibarıyla yayımlanan Sosyal Bilgiler Öğretim Programı ile 2024–2025 eğitim-öğretim yılında Millî Eğitim Bakanlığı tarafından onaylanmış 4., 5., 6. ve 7. sınıf Sosyal Bilgiler ders kitapları veri kaynağı olarak kullanılmıştır. Araştırmanın amacı doğrultusunda, bilgi güvenliği teması; öğrenme alanları, kazanımlar, beceriler, eğilimler ve okuryazarlık bileşenleri kapsamında analiz edilmiştir. Ayrıca, ders kitapları bilgi güvenliğinin üç temel boyutu olan gizlilik, bütünlük ve erişilebilirlik çerçevesinde incelenmiş; içerikler tablolar ve görsellerle desteklenmiştir. Verilerin analizinde betimsel analiz yöntemi kullanılmıştır. Öncelikle ilgili öğretim programı ve ders kitapları taranarak bilgi güvenliği ile ilişkili içerikler belirlenmiş; ardından bu içerikler sınıf düzeylerine göre kategorize edilmiştir. Elde edilen

bulgular, bilgi güvenliği kavramının farklı boyutlarıyla ele alınışını göstermek üzere sınıflandırılmıştır. Çalışmanın sonunda sosyal bilgiler dersi öğretim programında bilgi güvenliği farkındalığı sağlayıcı içeriklerin Teknoloji ve Sosyal Bilimler öğrenme alanında etkili olarak verildiği görülmüştür. 4., 5., 6., ve 7. sınıf ders kitaplarında bilgi güvenliği ile ilgili farkındalık içeren boyutlara doğrudan ve dolaylı olarak yer verildiği görülmüştür. Sosyal mühendislik süreçlerinden ortalama süreci örnekle açıklanmış, dezenformasyon (bilgi çarpıtma) hakkında bilgi verilmiş, internet üzerinden yapılan alışverişlerde gerçek hayattan dolandırıcılık örneği verilmiş, kazanım, beceri, etkinlik ve görsellerin yer aldığı tespit edilmiştir. Bu doğrultuda sosyal mühendislik süreçlerini kullanan kötü niyetli kişilerin insanların teknik bilgi ve farkındalık eksikliklerinden yararlanarak oluşturduğu istenmeyen ve kötü sonuçlar doğuran süreçlerin detaylı teknik ayrıntılarına değinilmediği görülmüştür. Bu kapsamda bu gibi teknik farkındalıkların içeriklerde işlenmesi ile bir çok olumsuz sürecin önüne geçileceği değerlendirilmektedir.

Anahtar Kelimeler: Bilgi Güvenliği, Sosyal Bilgiler Dersi, Öğretim Programı, Ders Kitabı Analizi, Okuryazarlık Becerileri

ABSTRACT

Institution	: BEUN, Institute of Social Sciences, Department of Turkish and Social Sciences Education
Thesis Title	: Evaluation of Social Studies Curriculum and Textbooks in the Context of Information Security
Thesis Author	: Talha Hakan KAYGISIZ
Thesis Adviser	: Assoc. Prof. Dr. Canan TUNÇ ŞAHİN
Type, Year	: MSc Thesis,
Number of Pages	2025 : 136

Information security is a set of processes inseparable from human life today. It is an undeniable fact that advancements in information and communication technologies affect human life in every aspect of today's society. We can now conduct business and transactions in many areas, including economic, social, health, and e-commerce, using the information devices we use in our daily lives. Digital interactions, which significantly impact human life in all these areas, necessitate the development of certain awareness levels within us. Information security is, in a sense, a process that requires preventive security measures to raise awareness of digital interactions that are integral to our daily behaviors and affect our lives.

This study examines the extent to which preventive security measures that raise awareness about information security processes are covered in the 2024 Social Studies Curriculum and Social Studies textbooks, the distribution of these contents, and their effectiveness. This research was conducted using document analysis, a qualitative research design. In this study, the Social Studies Curriculum published as of 2024 and the 4th, 5th, 6th, and 7th grade Social Studies textbooks approved by the Ministry of National Education for the 2024–2025 academic year were used as data sources. In line with the purpose of the research, the theme of information security was analyzed within the scope of learning areas, achievements, skills, dispositions, and literacy components. In addition, the textbooks were examined within the framework of the three basic dimensions of information security: confidentiality, integrity, and accessibility; the contents were supported with tables and visuals. Descriptive analysis was used in the analysis of the data. First, the relevant curriculum and textbooks were scanned to identify content related to information security; then, these contents were categorized according to grade levels.

The findings were classified to demonstrate how the concept of information security was addressed in different dimensions. At the end of the study, it was observed that the content that raises information security awareness in the social studies curriculum was effectively provided in the field of Technology and Social Sciences learning. It was observed that the 4th, 5th, 6th, and 7th grade textbooks directly and indirectly address aspects of information security awareness. The social engineering process of phishing is explained with examples, information is provided on disinformation (information distortion), real-life examples of fraud in online shopping are provided, and the objectives, skills, activities, and visuals are included. Consequently, it was observed that the technical details of the processes that malicious individuals using social engineering processes exploit people's lack of technical knowledge and awareness to create undesirable and harmful outcomes are not addressed. Therefore, it is believed that incorporating such technical awareness into the content will prevent many negative consequences.

Keywords: Information Security, Social Studies, Curriculum Analysis, Textbook Evaluation, Digital Literacy

ÖN SÖZ

Bu çalışma da 2024 Sosyal Bilgiler öğretim programı ve güncel ders kitaplarının bilgi güvenliği (siber güvenlik) ve alt başlıkları açısından etkililik durumlarının değerlendirilmesi, dijital vatandaşlık ve dijital okuryazarlık kapsayıcılığı açısından güvenli bilgiye ulaşma, bilginin güvenlik ve bütünlüğünü sağlama, bilgi güvenliği farkındalığının sağlanmasında SBÖP ve ders kitaplarının içerik verilerinin değerlendirilmesi ve etkililik durumunun yorumlanarak analiz edilmesi ifade edilmeye çalışılmıştır. Çalışma boyunca dijital dünyanın bizlere etkisi üzerinde ki olumsuz durumlardan kaçınmak için sahip olmamız gereken önleyici güvenlik bilgi ve farkındalığının sağlanmasının önemi belirtilmeye çalışılmıştır.

Bu çalışma süresince bana desteklerini her zaman hissettiren aileme başta kıymetli eşim Tülin'ime, bal küpüm Gökçe'me ve aramıza yeni katılan bal oğlum Gökalp'e her zaman yanımda oldukları için çok teşekkürler, varlıklarına çok şükür.

Severek başladığım yüksek lisans sürecimde bana yol göstericiliğini ve desteklerini her zaman hissettiren değerli hocalarım Prof. Dr. Oğuzhan KARADENİZ'e ve Doç. Dr. Canan TUNÇ ŞAHİN'e çok teşekkürler.

Yüksek lisans sürecinde tanıdığım süreç boyunca yardımlaştığımız ve arkadaşlığımızın daim olduğu Yavuz KORKMAZ' a çok teşekkürler.

İÇİNDEKİLER

ÖZET	iv
ABSTRACT	vi
ÖN SÖZ	viii
İÇİNDEKİLER	ix
TABLolar LİSTESİ	xi
ŞEKİLLER LİSTESİ	xii
RESİMLER LİSTESİ	xiii
KISALTMALAR LİSTESİ	xvii
GİRİŞ	1
1. PROBLEM DURUMU	4
1.1. Araştırmanın Amacı	10
1.2. Araştırmanın Önemi	11
1.3. Varsayım	11
1.4. Sınırlılıklar	11
1.5. Tanımlar	12
2. KURAMSAL ÇERÇEVE	15
2.1. Bilgi ve Bilişim	15
2.1.1. Bilgi Kapsamında Veri ve Bilişim Teknolojileri	15
2.1.2. İnternet ve Dijital	17
2.2. Bilgi Güvenliği ve Süreçleri	23
2.3. Bilgi Güvenliğinin Temel Unsurları	24
2.3.1. Gizlilik	26
2.3.2. Bütünlük	26
2.3.3. Erişilebilirlik (Kullanılabilirlik)	27
2.4. Bilgi Güvenliği Tehditleri	27
2.4.1. Sosyal Mühendislik	30
2.4.2. En Çok Kullanılan Sosyal Mühendislik Türleri	32
2.4.3. Kötücül (Kötü Niyetli) Yazılım Türleri	36
2.5. Eğitimde Bilgi Güvenliği	41
2.6. Sosyal Bilgiler Dersi ve Bilgi Güvenliği	43
3. YÖNTEM	45
3.1. Araştırmanın Modeli	45
3.2. Örneklem Seçimi	45
3.3. Verilerin Toplanması ve Analizi	46
4. BULGULAR	48
4.1. 2024 Sosyal Bilgiler Dersi Öğretim Programının Genel Amaçlarında Bilgi Güvenliğine İlişkin Bulgular	48

4.2. 2024 Sosyal Bilgiler Öğretim Programında ve Ders Kitaplarında Bilgi Güvenliği Bağlamında Öğrenme Alanı, Beceri ve Kazanım ile İlgili Bulgular	50
4.2.1. 2024 Sosyal Bilgiler Öğretim Programında Bilgi Güvenliği Boyutu ile İlgili Bulgular	51
4.2.2. 2024 Sosyal Bilgiler 4.Sınıf Ders Kitabında Bilgi Güvenliği Boyutu ile İlgili Bulgular	51
4.2.3. 2024 Sosyal Bilgiler 5.Sınıf 1.Ders Kitabında Bilgi Güvenliği Boyutu İle İlgili Bulgular	66
4.2.4. 2024 Sosyal Bilgiler 5.Sınıf 2.Ders Kitabında Bilgi Güvenliği Bağlamında Kazanım (Öğrenme Çıktısı) ile İlgili Bulgular	71
4.2.5. 2024 Sosyal Bilgiler 6.Sınıf Ders Kitabında Bilgi Güvenliği Bağlamında Kazanım (Öğrenme Çıktısı) ile İlgili Bulgular	95
4.2.6. 2024 Sosyal Bilgiler 7.Sınıf Ders Kitabında Bilgi Güvenliği Bağlamında Kazanım (Öğrenme Çıktısı) ile İlgili Bulgular	108
SONUÇ	124
KAYNAKÇA	126
ÖZ GEÇMİŞ	135

TABLÖLER LİSTESİ

Tablo 3.1: Analiz Değerlendirme Kriterleri	46
Tablo 4.1: 2024 Sosyal Öğretim Programında ve Ders Kitaplarında Bilgi Güvenliği ile İlgili Bulgular Tablosu	50
Tablo 4.2: 4.Sınıf SBD Kitabında “Bilgi Güvenliği” Boyut ve Alt Kategorilerine İlişkin Bulgular	52
Tablo 4.3: Sosyal Bilgiler 5.Sınıf 2.Ders Kitabında Bilgi Güvenliği Bağlamında Kazanım (Öğrenme Çıktısı) ile İlgili Bulgular	72
Tablo 4.4: Sosyal Bilgiler 6.Sınıf Ders Kitabının Bilgi güvenliği Açısından Değerlendirilmesi	96
Tablo 4.5: Sosyal Bilgiler 7.Sınıf Ders Kitabı Bilgi Güvenliği Açısından Değerlendirilmesi	109



ŞEKİLLER LİSTESİ

Şekil 2.1: McCumber Bilgi Güvenliği Modeli (McCumber, 1991). (Özdemir, Uluyol, 2021).....	25
Şekil 2.2: Sosyal Mühendislik Süreci	32



RESİMLER LİSTESİ

Resim 2.1: Dijital Büyüme	18
Resim 2.2: Ulusal Sosyal Medya Kullanım Oranı	19
Resim 2.3: Global İnternet Kullanım Oranı	20
Resim 2.4: Türkiye'de İnternet Kullanım Oranı	20
Resim 2.5: Türkiye'de İnternet Kulanım Oranı	21
Resim 2.6: Türkiye'de İnternet Kulanım Oranı	22
Resim 2.7: TCMB Konulu Phishing Denemesi Esnasında Kullanılan E-Posta Örneği	33
Resim 4.1: Türkiye'de Kimlik Belgesi Tarihçesi	53
Resim 4.2: Türkiye Cumhuriyeti Kimlik Kartı Arka Yüzü	54
Resim 4.3: Bilgi Notu Kutucuğu	54
Resim 4.4: Öneri Kutucuğu	55
Resim 4.5: Etkinlik Kutucuğu	56
Resim 4.6: Etkinlik Kutucuğu	56
Resim 4.7: Öneri Kutucuğu	57
Resim 4.8: Deneyelim Kutucuğu	57
Resim 4.9: Çinçan Oynayan Çocuklar	58
Resim 4.10: Hasan Tahsin Bilgi Kutucuğu	58
Resim 4.11: Milli Mücadele Cepheler Haritası	59
Resim 4.12: Bilgi Kutucuğu	59
Resim 4.13: Etkinlik Kutucuğu	60
Resim 4.14: Neler Öğreneceğiz Kutucuğu	60
Resim 4.15: Nedir, Ne Yapar? Kutucuğu	61
Resim 4.16: Teknolojik Ürünler	61
Resim 4.17: Teknolojik Ürünlerin Kullanımı	62
Resim 4.18: Eğitim Alanında Kullanılan Teknolojik Ürünler	63
Resim 4.19: Teknolojinin Zararları	63

Resim 4.20: Teknolojinin Öyküsü	64
Resim 4.21: Kullanma Kılavuzu Örneği	65
Resim 4.22: E-Ticaret	66
Resim 4.23: Genel Ağdan Alınan Haber Örneği	67
Resim 4.24: Örnek Olay Kutucuğu	67
Resim 4.25: Elektronik Posta Açılımı	68
Resim 4.26: Performans Görevi	69
Resim 4.27: Bilgi Kutucuğu	70
Resim 4.28: Haber Örneği	70
Resim 4.29: Kaynak Örneği	70
Resim 4.30: Haber örneği	73
Resim 4.31: Etkinlik Örneği	74
Resim 4.32: Metin Kutucuğu	75
Resim 4.33: Dilekçe Örneği	75
Resim 4.34: Bilgi Kutucuğu	76
Resim 4.35: Düşünelim Kutucuğu	76
Resim 4.36: Bilgi Kutucuğu	77
Resim 4.37: Öğrenelim Kutucuğu	77
Resim 4.38: EBA Kullanımı Bilgi Kutucuğu	78
Resim 4.39: Teknolojik Aletlerin Kullanımı Bilgi Kutucuğu	78
Resim 4.40: E-Nabız Bilgi Kutucuğu	79
Resim 4.41: Bilgi Kutucuğu	80
Resim 4.42: Etkinlik Kutucuğu	80
Resim 4.43: Teknolojinin Etkileri	81
Resim 4.44: Teknolojik Ürünlerin Bilinçli Kullanımı	83
Resim 4.45: Öğrenelim Kutucuğu	84
Resim 4.46: Bilgi Kutucuğu	85
Resim 4.47: Bilgi Kutucuğu	86
Resim 4.48: Bilgi Notu Kutucuğu	87

Resim 4.49: Bilgi Kutucuğu	87
Resim 4.50: Dijital Okuryazarlık Yeterlilikleri	88
Resim 4.51: Teknoloji Kullanımı Bilgi Kutucuğu	889
Resim 4.52: Bilgi Kutucuğu	90
Resim 4.53: Çalışma Yaprağı Örneği	91
Resim 4.54: Değerlendirelim Kutucuğu	92
Resim 4.55: Etkinlik Örneği	93
Resim 4.56: Örnek Olay Kutucuğu	94
Resim 4.57: Bilgi Kutucuğu	97
Resim 4.58: Bilgi Kutucuğu	97
Resim 4.59: Örnek Olay Kutucuğu	98
Resim 4.60: Bilgi Kutucuğu	99
Resim 4.61: Bilgi Kutucuğu	99
Resim 4.62: Bilgi Kutucuğu	99
Resim 4.63: Bilgi Kutucuğu	99
Resim 4.64: Bilgi Kutucuğu	100
Resim 4.65: Düşünelim Kutucuğu	101
Resim 4.66: İnceleyelim Kutucuğu	102
Resim 4.67: Bilgi Kutucuğu	103
Resim 4.68: Bilgi Kutucuğu	104
Resim 4.69: Örnek Olay Kutucuğu	104
Resim 4.70: Bilgi Kutucuğu	105
Resim 4.71: Bilgi Kutucuğu	105
Resim 4.72: Etkinlik Zamanı Kutucuğu	106
Resim 4.73: Bilgi Kutucuğu	106
Resim 4.74: Bilgi Kutucuğu	106
Resim 4.75: Bilgi Kutucuğu	1077
Resim 4.76: Bilgi Kutucuğu	1077
Resim 4.77: Etkinlik Kutucuğu	110

Resim 4.78: Etkinlik Kutucuđu	111
Resim 4.79: Bilgi Kutucuđu	112
Resim 4.80: Örnek Olay Kutucuđu	113
Resim 4.81: Bilgi Kutucuđu	114
Resim 4.82: Bilgi Kutucuđu	115
Resim 4.83: Bilgi Kutucuđu	116
Resim 4.84: Bilgi Kutucuđu	1177
Resim 4.85: Bilgi Kutucuđu	1177
Resim 4.86: Bilgi Kutucuđu	1188
Resim 4.87: Bilgi Kutucuđu	1199
Resim 4.88: Örnek Olay Kutucuđu	120
Resim 4.89: Etkinlik Kutucuđu	121
Resim 4.90: Bilgi Kutucuđu	122
Resim 4.91: Bilgi Kutucuđu	122
Resim 4.92: Etkinlik Kutucuđu	123

KISALTMALAR LİSTESİ

APWG	: Ortalama Önleme Çalışma Grubu
BİT	: Bilgi ve İletişim Teknolojileri
BTK	: Bilgi Teknolojileri Kurumu
ICANN	: Internet Corporation for Assigned Names and Numbers
IoT	: İnternet Of Things
MEB	: Milli Eğitim Bakanlığı
NCSS	: Ulusal Sosyal Bilimler Konseyi
NIST	: National Institute of Standards and Technology
OECD	: Ekonomik Kalkınma ve İşbirliği Örgütü
SBÖP	: Sosyal Bilgiler Öğretim Programı
TDK	: Türk Dil Kurumu
TÜİK	: Türkiye İstatistik Kurumu
URL	: Uniform Resource Locator
WASD	: We Are Social Digital (2024 Küresel Dijital Bakış Raporu)

GİRİŞ

Bilişim ve iletişim teknolojilerindeki gelişmeler her geçen gün hızla artmaktadır. Bilişim teknolojilerinin kullanıldığı cihazlar da bu gelişmelerden hızlı bir şekilde etkilenmekte bu cihazların kullanım oranı da artmaktadır. Teknolojinin hayatımızın içinde yer almasıyla günümüz toplumlarının teknolojinin meydana getirdiği bu gelişim ve değişimlere uyum sağlamaya çalışması ile ortaya çıkan dijital vatandaşlık kavramı da teknolojinin toplum hayatına girmesi sonucunda ortaya çıkan vatandaşlığın yeni bir boyutudur (Turan & Avcı 2018). Farmer (2010) dijital vatandaşlığı, çevrimiçi alandaki bilgilere etkin ve eleştirel bir şekilde ulaşarak bu bilgileri hem kişisel hem de toplumsal fayda sağlamak amacıyla kullanabilen bireylerin yetiştirilmesine olanak sağlayan eğitim şeklinde tanımlamaktadır. Çubukçu ve Bayzan (2013) ise dijital vatandaşlığı teknoloji ve iletişim kaynaklarını etkin kullanabilen, eleştirebilen, dijital sorumluluklarının bilincinde olan teknolojiyi ve bilişim sistemlerinden yararlanırken başkalarına zarar vermeyen ve bütün bunları vatandaşlık hak ve sorumluluklarının farkında olarak değerlendirebilen bireyler yetiştirmeyi hedeflediğini belirtmişlerdir. Bu tanımlamalara göre Karaduman ve Öztürk (2014) ise dijital vatandaşlık tanımlarının ortak noktalarının incelendiğinde ilk başta çevrim içi ortama etkin katılımın ön plana çıktığını ve dijital vatandaşların bilgi iletişim teknolojilerinin, etik, yasal, güvenli ve sorumlu bir biçimde kullandıklarını vurgulamışlardır. Aynı zamanda bu kavram, bireylerin bilgiye erişim, bilgiyi üretme ve paylaşma süreçlerinde karşılaşılabilecekleri etik, güvenlik ve mahremiyet temelli sorunlara yönelik farkındalık geliştirmelerini hedefler (Jones & Mitchell, 2016).

Temel eğitimde okuma ve yazma eğitimlerinin verilmesinin yanında insanlara bilgiye erişme, bilgiyi kullanma, yeni bilgi üretebilme gibi beceriler kazanabilmesinin temeli oluşturulmaktadır (Önal, 2010). Talan ve Aktürk (2021) ise teknolojinin de gelişmesiyle birlikte insanın içinde bulunduğu çevreyi anlamlandırması ve kendi ifadelerini oluşturabilmesi için en temel bileşenlerden meydana gelen çeşitli okuryazarlık kavram ve becerilerine ek olarak medya okuryazarlığı, dijital okuryazarlık gibi yeni kavramların ortaya çıkması ile çeşitli

ortamları kullanabilme becerileriyle bilgiye erişme ve yeni bilgiler üretebilmenin bir sonucu olarak bu kavram ve becerilerin de farklılaştığını belirtmişlerdir.

Medya ve dijital okuryazarlık kuramı ise bireyin dijital içerikleri analiz edebilme, değerlendirme ve güvenilir bilgiye erişme becerilerini vurgular (Livingstone, 2004). Bu kapsamda öğrencilerin bilgi güvenliği farkındalıkları; medya içeriklerini eleştirel biçimde değerlendirme, kişisel verileri koruma ve dijital ayak izi gibi konularda bilinçlenmeleri ile doğrudan ilişkilidir (Voogt et al., 2013). Bu nedenle çalışmada, bilgi güvenliği teması bu üç kuramsal çerçeve içinde değerlendirilmiştir.

Bilgi, günümüz toplumlarının ekonomik, sosyal ve kültürel gelişiminde en önemli belirleyici bir unsuru haline gelmiştir. Dijital teknolojilerin hızla gelişmesiyle birlikte bilgiye erişim kolaylaşmış; ancak bu durum, bilginin güvenliği, gizliliği ve doğruluğu gibi yeni sorunları da beraberinde getirmiştir (Özdemir & Uluyol, 2021; Talan & Aktürk, 2021). Özellikle çocuklar ve gençler, dijital ortamlarda karşılaşabilecekleri güvenlik tehditleri karşısında bilinçli farkındalık oluşturmali ve donanımlı bireyler olarak yetiştirilmelidir.

Bilgi güvenliği; bilginin yetkisiz erişime, kullanıma, ifşaya, bozulmaya veya yok olmaya karşı korunmasını ifade eder. Bu bağlamda bireylerin bilgi güvenliği farkındalığı, hem dijital vatandaşlık hem de medya ve teknoloji okuryazarlığının temel bileşenlerinden biridir (Talan & Aktürk, 2021). Özellikle erken yaşta verilen bilgi güvenliği eğitimi, çocukların çevrim içi risklere karşı korunmasına ve eleştirel dijital farkındalık geliştirmelerine katkı sağlamaktadır (Ünal Peker, 2015).

Sosyal Bilgiler dersi, bireylerin toplumsal yaşam becerilerini geliştirmeyi ve demokratik değerlerle donatılmasını amaçlayan disiplinler arası bir yapıya sahiptir. Son yıllarda bu ders kapsamında bilgi okuryazarlığı, dijital vatandaşlık ve etik bilişim kullanımı gibi konulara daha fazla yer verilmeye başlanmıştır (Derin & Gençoğlu, 2020). Ancak müfredat ve ders kitaplarının bu içerikleri ne düzeyde ve hangi biçimlerde sunduğu sorusu önem kazanmaktadır. Türkiye’de yapılan bazı araştırmalar, müfredatların bilgi güvenliği konularını yeterince açık biçimde

iřlememesi nedeniyle ğrencilerde kavramsal karmařa oluřabildiğini gstermektedir (elik & Kılıođlu, 2022; Ateř & Kk, 2023).

Bu bađlamda, bu arařtırmanın temel amacı; 2024 yılı Sosyal Bilgiler đretim Programı ve 2024–2025 eđitim–đretim yılına ait 4., 5., 6. ve 7. sınıf ders kitaplarında bilgi gvenliđi konusunun nasıl yer aldıđı, hangi boyutlarda iřlendiđi ve đrencilere kazandırılmak istenen bilgi gvenliđi farkındalıđının ieriđe nasıl yansıtıldıđı sorularına yanıt aramaktadır.



1. PROBLEM DURUMU

Bilgi günümüz çağında en kıymetli ve dinamik araçsal iletkenidir. İletken özellikli işlenmemiş en küçük bilgi birimini genel olarak veriler oluşturur. Bilişim teknolojileri kapsamında veri temelde bu iletkenliğin içeriğini dolduran sayısal sinyaller olarak tanımlanabilir. Bu sayısal ifadeler veri parçalarının iletimini sağlayan bir enerjidir. Dijital enerjinin işlenmesiyle oluşan veriler anlamsal bütünlük ile bilgi varlığını oluşturur. (Savaş, Topaloğlu ve Yılmaz 2012)'ın aktardığına göre bilgi belli bir hedef doğrultusunda işlenen veridir. İnsanlığın bilinen tarihinden itibaren bilgi bazen bir ses bir yazı ve işaret ile sembolize edilmiş ve iletişimin temel kaynağını oluşturmuştur. Bu doğrultuda birtakım anlamsal belirteçlerin yanında bilgi ve iletişim teknolojilerindeki veriler, bilginin varlığını ve yokluğunu belirten temel unsurlar olmuş, aynılık veya farklılık oluşturarak insan hayatında hem amaç hem de araç olarak son derece kıymetli bir varlık halini almıştır. Günümüzde gelişen teknoloji ile güvenli ve doğru bilgiye ulaşmak okuryazarlık becerilerinin geliştirilmesiyle mümkün olmaktadır. Dijital vatandaşlık özelliklerinin kazanılması ve dijital okuryazarlık becerilerinin önemi bilgi güvenliğinin sağlanmasında günümüzde oldukça önem kazanmaktadır. Dijital vatandaşlık, bireyin çevrim içi ortamlarda haklarını kullanırken sorumluluklarını da yerine getirmesini ifade eder (Ribble, 2011). Bilgi güvenliği, dijital vatandaşlığın temel boyutlarından biri olarak değerlendirilmektedir (İnce & Akbaş, 2020). Aynı zamanda bu kavram, bireylerin bilgiye erişim, bilgiyi üretme ve paylaşma süreçlerinde karşılaşılabilecekleri etik, güvenlik ve mahremiyet temelli sorunlara yönelik farkındalık geliştirmelerini hedefler (Jones & Mitchell, 2016).

Medya ve dijital okuryazarlık kavramı ise bireyin dijital içerikleri analiz edebilme, değerlendirme ve güvenilir bilgiye erişme becerilerini vurgular (Livingstone, 2004). Bu kapsamda öğrencilerin bilgi güvenliği farkındalıkları; medya içeriklerini eleştirel biçimde değerlendirme, kişisel verileri koruma ve dijital ayak izi gibi konularda bilinçlenmeleri ile doğrudan ilişkilidir (Voogt et al., 2013). Bu nedenle çalışmada, bilgi güvenliği teması bu üç kuramsal çerçeve içinde değerlendirilmiştir.

En küçük bir bilgi parçası çağlar boyunca insanoğluna yeni bilgiler için temel oluşturmuş ve dinamik yaşamı destekleyerek insanlığı hayatın her alanında etkilemiştir. Bu ilerlemeci ve etki edici özelliği günümüzde de artarak devam etmektedir. Dolayısıyla bilginin içinde bulunduğumuz çağın en önemli varlığı olduğu tartışılmaz bir gerçektir (Canberk & Sağiroğlu,2006). Bu bakımdan iletilen her bir bilginin özgün değerinin korunması gerekmektedir. Düzenlenen bir bilgi biriminin bir noktadan başka bir noktaya iletilmesi bir takım güvenlik önlemlerinin yansira önemli ölçüde bilişsel farkındalık gerektirir. Bilgi güvenliğinin sağlanmasının başlıca bileşenleri arasında “gizlilik, bütünlük ve erişilebilirlik” yer alır (Baykara & Karadoğan & Daş 2013). Bu kavramlara karşı kullanıcılar farklı düşünce ve buna bağlı olarak farklı davranışlar ortaya koyabilirler (Akay, 2014). Belirtilen bu üç özellik dışında günümüzde son derece önem kazanan bir faktör daha eklemek gerekir ki bu da son kullanıcı olan insanın Bilgi ve İletişim Teknolojilerini (BİT) kullanırken sergilediği bilinçli farkındalıktır. Çağın en kıymetli iletkeni olan bilgi varlığının değerlendirilmesini sağlayan dijital bilinç (İnsan) bilgiye ulaşım, kullanım, değiştirme araçları bakımından kendini sürekli güncel tutmalı ve farkındalık sağlamalıdır. (Schlienger ve Teufel, 2002) ın aktardığına göre; bilgi güvenliği konusunda insan faktörü genellikle göz ardı edilerek yoğunlaşılın kısmın bilgi güvenliğinin sağlanmasında kullanılan bir takım teknik güvenlik önlemlerinin üzerine olduğudur. Bu önlemlerin bilgi güvenliğini sağlamada memnun edici sonuçlar vermediği, yapılan çalışmada “kullanıcı benim düşmanımdırdan, kullanıcı benim güvenlik varlığımdıra” yönelik bir düşünce değişikliği hedeflenerek belirtilmiştir.

Bilgi ve İletişim Teknolojileri alanındaki sürekli artan değişim ve yenilikler günümüz toplumunun yadsınamaz bir gerçeği olmuştur. Ayrıca Teknolojik cihazların sürekli yenilenme ve gelişmelerinin yanında herkes tarafından ulaşılabilir ve kullanılabilir olması birçok kurum, kuruluş ve son kullanıcılar açısından çeşitli iş süreçlerinde dijital araçlardan fazlaca yararlanmayı da zorunlu kılmıştır. 1990’lı yılların sonuna doğru başlayan “İnternet Çağı” oldukça önemli değişimlere neden olmuş internet kullanımının artarak yaygınlaşmasıyla birlikte bilgiye erişim kolaylaşmış, iş ve işlemlerde hız ve pratiklik sağlanmıştır. (Değirmenci & Demiral 2023)

We Are Social şirketinin belirttiği rapora göre “Dijital 2025: Dijitalin küresel durumuna ilişkin temel rehber- Digital 2025 Global Overview Report” 2025 yılı için raporun önemli belirtileri arasında 2025 yılının dijital alanda oldukça dinamik olması ve yapay zeka alanındaki hızlı gelişmeler, gelişen sosyal medya ortamı ve genişleyen çevrimiçi davranışların hayatımızda daha belirgin bir şekilde yer alacağını gösteriyor. Global anlamda internet kullanıcı sayısı 5,56 milyar ile toplam dünya nüfusunun yüzde 67,9’unu oluşturuyor. Kullanıcılar 2025 yılı başlarında internete girmenin en büyük sebebinin “bilgi bulma” olduğunu belirtmiş, yetişkin kullanıcıların yüzde 62,8’i interneti kullanmalarının başlıca nedenlerinden birinin “bilgiyi bulma” amacını taşıdığını ifade etmiştir. Ülkemizde günlük internette geçirilen zaman olarak 7 saat 13 dakika ile dünya genelinde 18.sırada yer alarak dünya ortalamasının (6 saat 38 dakika) üzerinde yer aldığımız görülmüş. Ayrıca mobil telefonların internete erişim için kullanılmasında yüzde 96,3 oranla dünya genelinde 12.sırada yer aldığımız belirtilmiş ve dünya ortalamasının (yüzde 96,3) üzerinde yer aldığımız görülmüştür. Ülke olarak mobil cihazlarda internet kullanımına ayrılan zaman 4 saat 4 dakika ile dünya genelinde 18.sırada yer alarak dünya ortalamasının (3 saat 46 dakika) üzerinde yer almıştır. Ülkemizde kullanıcıların bilgisayardan internete erişim oranı ise yüzde 63,5 ile 43.sırada yer alarak dünya ortalamasının (%61,5) üzerinde yer almış, bilgisayardan internet kullanımına ayrılan zaman 3 saat 9 dakika ile 23. sırada yer alarak dünya ortalamasının (2 saat 52 dakika) üzerinde yer almıştır.

Ülkemiz dijital mesajlaşma uygulamalarının kullanımında yüzde 97,2 oranla dünya genelinde 22.sırada yer alarak dünya ortalamasının (%94,5) üzerinde yer almıştır. E-posta kullanım oranı yüzde 90,2 ile 21.sırada yer alarak dünya ortalamasının (%75) üzerine çıkmıştır. Yine ülkemizde haftalık olarak çevrimiçi (online) alışveriş sitelerinde internet kullanım oranı yüzde 61,0 ile dünyada 6.sırada yer alarak yüzde 55,8 olan dünya ortalamasının üzerinde kalmıştır.

Ayrıca raporda bir önceki yıla göre (2024) sosyal medya kullanıcı sayısının yüzde 4,1 artarak 5,24 milyara ulaşarak sosyal medyayı kullanmanın birincil nedenini arkadaşlar ve aileyle iletişim halinde olmak şeklinde belirtmiştir. Bunun yanında boş zamanları doldurmak ikinci sırada yer alırken 3’te 1’inden fazlası sosyal platformları ziyaret etme nedenlerinden birinin haber okumak olduğunu

belirtmiş. Bununla birlikte bir sosyal medya kullanıcısının günde ortalama 2 saat 21 dakikaya yakın sosyal medyada zaman geçirdiğini ortaya çıkartıyor.

Yine aynı raporda (WASD, 2025) Ülkemizde en çok ziyaret edilen web sitesi türleri ve kullanılan uygulamaların sıralaması ise;

1.sırada sosyal ağ uygulamaları,

2.sırada sohbet ve mesajlaşma uygulamaları,

3.sırada arama motorları ve web portalları,

4.sırada ise E-posta uygulamaları yer almıştır.

Yine aynı (We are social dijital, 2025) raporda ayrıca nüfusa göre sosyal medya kullanım oranı olarak Türkiye %66,7 ile 58,5 milyon sosyal medya kullanıcı kimlik sayısı ile 47. sırada yer alarak yüzde 63'lük dünya ortalamasının üzerinde yer alıyor. Sosyal medyada geçirilen süre olarak Türkiye 2 saat 43 dakika ile dünya ortalamasının üzerinde yer alarak 16.sırada bulunduğu belirtilmiştir. Ülkemizde en çok kullanılan sosyal medya uygulamaları ise yüzde 92,2'lik oran ile Instagram, yüzde 90,6'lık oran ile WhatsApp, yüzde 71,1'lik oran ile Facebook, yüzde 60,5'lik oran ile ise X uygulaması yer almıştır.

Yerelde ise TÜİK (Hane halkı Bilişim Teknolojileri Kullanım Araştırması, 2024) raporuna göre internet kullanıcı sayısı 2023 yılında %87,1 iken 2024 yılında %88,8 oldu. Belirtilen raporun yayınlanma tarihinden itibaren son 12 ay içinde özel amaçla resmi makamların web sitelerini ve uygulamalarını kullanan ve İnternet üzerinden kamu hizmetlerinden yararlanan bireylerin oranı %73,7 oldu. Bu erişim içerisinde önemli yeri E-devlet hizmetlerinin aldığı belirtilmiştir.

Ayrıca internet üzerinden mal ve hizmet alımı %49,5 iken 2024 yılında %51,7 olarak artış göstermiştir. Bunun yanında bireylerin en fazla kullandıkları sosyal medya ve mesajlaşma uygulamaları %86,2 ile WhatsApp, %71,3 ile YouTube ve %65,4 ile Instagram olduğu belirtilmiştir (TÜİK 2024).

Bu raporlar doğrultusunda bilginin ulaşılması ve kullanılmasında bilişim teknolojilerindeki gelişmeler ile internetin kullanım oranının sürekli arttığı gözlenmiştir. İnternet günlük hayatımızın önemli bir parçası olarak kullanıcı sayısı her geçen gün artmakta, bilgi ve iletişim teknolojileri alanındaki ilerleme ve bu alandaki ulaşılabilirliğin artmasıyla daha fazla veri üretilerek bilgiyi kullanım ve ulaşım da artmıştır. Bu durum bilgi güvenliği açısından yeni tehditler oluşturarak önemli güvenlik sorunlarını ortaya çıkarmıştır (Taha, Dahabiyeh 2021). Belirtilen çalışmalarda görüldüğü üzere günlük hayatımızda internet ortamında yaptığımız iş ve işlemler bize zaman ve emek olarak tasarruf sağlamıştır. Bunun yanında son kullanıcı olan bireyin internet ortamında dikkat etmesi gereken birçok farkındalık bulunmaktadır. Genel olarak bilgi güvenliği farkındalığı bireylerin güvenli bilgi uygulamalarına ilişkin algılarını, değerlerini, tutumlarını, davranışlarını, normlarını, çalışma alışkanlıklarını ve kurumsal kültür ve yapılarını değiştirmeyi amaçlayan bir süreçtir (Tsohou & Karyda & Kokolakis & Kiountouzis 2015). Bilgi güvenliğindeki bu süreç, bilginin güvenliğinin sağlanmasında devamlılık ve sürekliliğin yanında aynı zamanda güncellikte gerektirmektedir. Belirtilen farkındalığın önemi bireylerin internet ortamında birtakım tehditler karşısında önem kazanmaktadır. Kullanıcılar virüs, kimlik avı, oltalama (yemleme) gibi çeşitli saldırılara maruz kalmakta, hatta kullanıcı hesaplarının veya kredi kartı, bankacılık ve kimlik verilerinin kötü amaçlı kişilerin eline geçmesi gibi siber suçların mağduru olmaktadır (Talan & Aktürk 2021).

Yukarıda belirtilen durumlara göre günümüz toplumunun ihtiyacı olan bireylerin hayat boyu öğrenme becerilerine sahip bilgisini güncelleyebilen, bilgiyi güvenli bir biçimde üretebilen, değiştiren ve anlamlandıran bir dijital bilince sahip olması gerekmektedir. Bilgi güvenliğini sağlamada internet ve veri kullanımının artmasına bağlı olarak siber dünyadaki güvenlik farkındalıklarının artırılması gerekmektedir (Ateş & Küçük 2024). Yapılan araştırmalar bilgi güvenliğinin sağlanması ve siber dünyada güvenli erişimlerin birtakım olumsuzluklar ve tehditlere maruz kalınmasında teknolojik sistemlerin yetersizliği ve zayıflığı değil bireylerin neden olduğunu önemli ölçüde göstermektedir. Toplumumuzda yer alan kullanıcıların (Bireylerin) çoğunun bilgi güvenliği ihlalinin nihai kaynağının olduğu ve dolayısıyla siber güvenlik zincirindeki en zayıf halka oldukları sürekli gözlemlenen bir olgu olarak tanımlanmıştır (Yan vd, 2018). İçinde bulunduğumuz

çağda bireylerin büyük bir fayda sağladığı teknoloji yüzyıllar boyunca korunmaya çalışılan doğru bilgiye hızlı ve zamanında ulaşılması adına bireyler için son derece kıymetli iken, tehdit yaratabilecek unsurları da beraberinde getirmiştir. Bu unsurların başında insan faktörü güvenliğin sağlanmasında kilit durumdadır (Derin & Gençoğlu 2020). Genel olarak bilgi güvenliği araştırmaları bilgi güvenliğinin sağlanmasında teknik yönlelere odaklanmış ve çoğunlukla insan boyutunu göz ardı etmiştir (Stanton vd. 2003).

Belirlenen bu tespitlere göre günümüz çağındaki bireylerin bilişim teknolojileri ve interneti kullanmadan önce sahip olması gereken bilgi ve beceriler bulunmaktadır. Bireylerin herhangi bir bilişim malzemesini kullanırken ve bu malzemeler aracılığı ile internet ortamında çevrim içi olmadan önleyici güvenlik sağlamaları yapması gerekmektedir. Bu sağlamaların yapılabilmesi için kullanılan dijital dünya malzemelerine ait terim ve anlamların öğrenilmiş olması önemlidir. Genellikle bilgi güvenliği ve dijital vatandaşlıkla ilgili verilen bilgiler birtakım tespitler olmuştur. Ancak geline nokta nasıl dijital vatandaş olunur ve bilginin güvenliği nasıl sağlanır sorusuna bireyi etkin kılan bilgi ve becerilerin anlamsal kılavuzları aranmaktadır. Bu doğrultuda bilgi güvenliği ve dijital vatandaşlık etkililiği hususunda önleyici bilgi ve beceriler sosyal bilgiler öğretim programı ve ders kitaplarında ne kadar yer alıyor sorusuna cevap aranmaktadır. Örnekle açıklamak gerekirse sosyal bilgiler ders kitabında belirtilen E-Devlet hizmeti ve nasıl ulaşılacağı bilgisi (<https://www.turkiye.gov.tr/>) verilirken E-Devlete ulaşacağımız web sitesi uzantısının güvenli bir site olup olmadığını nasıl anlayabiliriz, web site linkinin güvenilir olduğunu nasıl yorumlayabiliriz gibi bilgilerin yer almadığı görülmüştür. Burada güvenli web site uzantısında bulunması gereken özellikler nelerdir ve bir bilgiye ulaşmak için yukarıda da belirtilen uygulamaları kullanırken farkındalık sağlamamız gereken önleyici güvenlik bilgi ve becerileri nelerdir sorularına cevap aranmaktadır. Bu gereksinimleri sağlayan kişileri yetiştirme sorumluluğunu üstlenen eğitim kurumlarının odağına alması gereken son derece önemli bilgi, beceri ve yeterlilikler vardır (Akkoyunlu & Kurbanoglu 2003).

Tüm bunlarla birlikte Sosyal Bilgiler Dersi toplum içinde etkin ve uyum içinde yaşayabilen, toplum kurallarına uyan, etik ve ahlaki ilkelere uyum gösteren,

karşılaştığı problemlere eleştirel bakabilmeyi amaçlayan bireyler yetiştirmeyi amaç edinmektedir. Sosyal bilgiler, öğrencileri yerel, ulusal ve küresel vatandaşlık yaşamına hazırlayan, zaman ve mekân içindeki bireyleri, toplulukları, sistemleri ve bunların etkileşimlerini inceleyen bir bilimdir (NCSS 2023). Öğretim programında belirtilen kural ve ilkeler günümüzde dijital alanda da geçerliliğini sağlamaktadır. Dijital alandaki yaptığımız iş ve işlemler gerçek hayatımızı etkilemekte ve hukuki sorumluluk oluşturmaktadır. Sosyal bilgiler ders kitaplarında bu kural, ilke ve becerilerin kazanılmasında önemlidir. Burada hem günlük hayatımızda hem dijital alanda etkin ve bilgi sahibi bir dijital vatandaş olmamız gerekli görülmektedir.

1.1. Araştırmanın Amacı

Araştırmanın amacı; 2024 yılı itibarıyla güncellenen Sosyal Bilgiler Dersi Öğretim Programı ile 2024-2025 eğitim-öğretim yılında okutulan ortaokul (4., 5., 6. ve 7. sınıf) Sosyal Bilgiler ders kitaplarında "bilgi güvenliği" konusunun ne şekilde ele alındığını incelemektir. Bu kapsamda öğretim programındaki genel ve özel amaçlar, öğrenme alanları, kazanımlar, beceriler ve eğilimler bağlamında bilgi güvenliğine yönelik doğrudan veya dolaylı yansımalar analiz edilmiştir. Aynı zamanda ders kitaplarında bilgi güvenliği kavramının gizlilik, bütünlük ve erişilebilirlik boyutları çerçevesinde nasıl işlendiği sınıf düzeylerine göre sistematik biçimde incelenerek önleyici güvenlik farkındalığı oluşturma açısından değerlendirmektedir.

Sosyal Bilgiler öğretim programının bilgi güvenliği bağlamında öğrencilere kazandırdığı bilgi ve becerilerin yeterliliği değerlendirilecek, geliştirilmesi gereken alanlar belirlenmeye çalışılacaktır.

Belirtilen genel amaç doğrultusunda cevap aranan sorular şunlardır;

1-Sosyal Bilgiler öğretim programı ve ders kitaplarında bilgi güvenliği unsurlarını hatırlatıcı bilgilere yer verilmiş mi?

2-Sosyal Bilgiler öğretim programı ve ders kitaplarında bilgi güvenliğinin sağlanmasında etik ilkelere yer verilmiş mi?

3-Sosyal Bilgiler öğretim programı ve ders kitaplarında sosyal mühendislik hakkında farkındalık oluşturacak bilgilere verilmiş mi?

4-Sosyal Bilgiler öğretim programı ve ders kitaplarında siber suç ve tehdit yöntemlerine ait önleyici farkındalık bilgileri yer almış mı?

5-Sosyal Bilgiler öğretim programı ve ders kitaplarında dijital okuryazarlık ve bilgi güvenliği farkındalığını arttıracak terimlere ve açıklamalarına yer verilmiş mi?

6-Sosyal Bilgiler öğretim programı ve ders kitaplarında dijital bilgiye ulaşım araçlarındaki uygulamaları eleştirel bir şekilde doğruluğunu yorumlayabilme bilgilerine yer verilmiş mi?

7-Sosyal Bilgiler öğretim programı ve ders kitaplarında bilginin kaynak doğrulamasını yapabilecek bilgiler yer almış mı?

1.2. Araştırmanın Önemi

Bireylerin Dijital Vatandaşlık etkililiği için çevrimiçi dünyada bilgiye ulaşırken ve kullanırken önleyici güvenlik sağlamalarını yapması amacıyla sosyal bilgiler öğretim programı ve ders kitaplarının içerik olarak gerekli rehberliği yapabilmesi son derece önemlidir. Bilgi güvenliği farkındalığının geliştirilmesi ve dijital birey olma sürecinde gerekli bilgi ve becerilerin kazandırılmasının yanında eleştirel bakış ve analiz süreci farkındalığa katkı sağlayacaktır. Tüm bunların SBÖP ve ders kitaplarında yer alması dijital vatandaş olan bireyin önleyici güvenlik rehberi oluşturmasında oldukça önemlidir.

1.3. Varsayım

Çalışmanın herhangi bir varsayımı bulunmamaktadır.

1.4. Sınırlılıklar

Çalışma 2024 Sosyal Bilgiler öğretim programı ve 2024-2025 Sosyal Bilgiler ders kitaplarını kapsamaktadır.

1.5. Tanımlar

Algoritma: Belirli bir problemi çözmek veya belirli bir işlemi gerçekleştirmek için çeşitli adımlardan oluşan yönergeler dizisidir.

URL (Uniform Resource Locator): İnternet üzerindeki bir kaynağın adresini tanımlayan bir formattır. URL'ler, bir web sayfasını, bir dosyayı, bir resim dosyasını veya başka bir kaynağı bulmak ve erişmek için kullanılır. Yapısı “protokol://alanadı/yol/parametreler/” şeklindedir.

Alan Adı (Domain Name): İnternet üzerindeki bir web sitesinin adresini tanımlayan ve kullanıcıların bir web sitesine kolayca erişmesini sağlayan isimdir. Alan adları, IP adreslerinin (192.168.1.1) yerine kullanılır, çünkü IP adreslerini hatırlamak güç olduğundan daha anlaşılır ve akılda kalıcı bir yol sunar. İnternet adresleri **com**, **edu**, **gov**, **net**, **org** gibi daha alt bölümlere ayrılmaktadır. Bu ifadeler üst düzey (top-level) alan adlarına karşılık gelmektedir. Üst düzey alan adlarında; **com**: Ticari kuruluşları, **edu**: Eğitim kurumlarını, **org**: Ticari olmayan, hükümete de bağlı bulunmayan kurumları, **net**: İnternet omurgası işlevini üstlenen ağları, **gov**: Hükümete bağlı kurumları göstermektedir (BTK, 2022). Bu isimlere Son yıllarda ICANN (Internet Corporation for Assigned Names and Numbers) tarafından onaylanan ve piyasaya sürülen yeni alan adları da eklenmiştir. Bunlar; **tech**: Teknoloji şirketleri için, **.store**: E-ticaret siteleri için, **.blog**: Blog siteleri için, **.app**: Uygulama geliştiricileri için, **.design**: Tasarımcılar için, **xyz**: Genel kullanım için.

Bilişim: Bilgi ve iletişim teknolojilerinin bir araya gelmesiyle oluşan, bilginin toplanması, işlenmesi, depolanması ve iletilmesi süreçlerini kapsayan bir alandır.

Veri: Ham ve işlenmemiş bilgi parçalarıdır. Bir olay, gözlem, ölçüm veya işlem hakkında elde edilen sayısal, metinsel veya sembolik göstergeler olabilir.

Bilgi: Verilerin işlenmiş, anlamlandırılmış ve organize edilmiş hâlidir. Verilerin belirli bir bağlama oturtulması, analiz edilmesi ve yorumlanması sonucunda elde edilir.

Siber Güvenlik: Dijital sistemleri, ağları, verileri ve cihazları kötü amaçlı saldırılardan, yetkisiz erişimden ve hırsızlıktan korumayı amaçlayan bir dizi

teknoloji, süreç ve uygulamayı ifade eder. Siber güvenlik, internet tabanlı tehditlere ve saldırılara karşı savunma sağlar ve bireylerin, kurumların, devletlerin dijital varlıklarını güvenli bir şekilde korumalarını sağlar.

Bilgi Güvenliği: Bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini korumayı amaçlayan yöntemler, stratejiler ve süreçler bütünüdür. Bilgi güvenliği, bilginin yetkisiz erişim, bozulma veya kötüye kullanılma gibi tehditlerden korunmasını sağlar.

Dijital Vatandaşlık: Bireylerin dijital ortamda güvenli, etik ve sorumlu bir şekilde hareket etmelerini sağlayan beceriler ve davranışlar bütünüdür. İnternet, sosyal medya, mobil uygulamalar ve diğer dijital teknolojilerde aktif olan bireylerin, çevrimiçi hak ve sorumluluklarını bilinçli bir şekilde yerine getirmesini amaçlar.

Dijital Okuryazarlık: Bireylerin dijital teknolojileri etkili ve bilinçli bir şekilde kullanma becerisinin yanında dijital araçları ve platformları anlama, kullanma, değerlendirme ve üretme yeteneğidir.

SSL (Secure Socket Layer): SSL bireysel olarak ağ üzerinde bilgiye erişim ve iletim esnasında gizlilik, güvenilirlik ve bütünlüğü sağlayarak web sunucuları ile istemci (bireysel kullanıcıların) arasındaki iletişimin şifrelenmiş şekilde yapılabilmesine imkân veren kriptografik güvenlik protokolüdür.

Bilgisayar: Kullanıcılardan aldığı verilerle aritmetik ve mantıksal işlemleri yapabilen ve yaptığı işlemlerin sonuçlarını saklayabilen, saklanan bilgilere istenildiğinde ulaşılabilen elektronik bir makinedir.

Bilgisayar Programı: Bir bilgisayar sisteminin özel bir işlem veya görev yapmasını sağlayacak düzene konulmuş komut dizilimidir.

TCP/IP Protokolü: “Bilgi ağı” üzerindeki bilgi iletimi ve paylaşımı bazı kurallar dâhilinde yapılmaktadır. Bu kurallara, internet protokolleri ya da TCP/IP (Transmission Control Protocol/ Internet Protocol) protokoller ailesi denmektedir. Bu protokoller birbirleriyle iletişim kuran milyonlarca bilgisayardan oluşan bir ağda yer alan farklı yapıdaki bilgisayarların birbirleriyle iletişim kurabilmeleri için oluşturulan bir anlaşma dilidir. Transport Control Protokol sözcüklerinin

kısaltılmış hali olan “TCP” iletim kontrol protokolü anlamına gelir ve mesajların doğru yere ulaştırılmasından; “IP” ise internet protokolü anlamına gelir ve adresleme sisteminden sorumludur.

World Wide Web (www) Kısaca Web: Birçok internet hizmetini birleştiren bir araç olarak; yazı, resim, ses, video, animasyon gibi pek çok farklı nitelikteki verilere etkileşimli olarak ulaşmamızı sağlayan çoklu hiper ortam sistemidir.

Web Browser (Web Tarayıcısı): İnternet üzerindeki tüm bilgilere bakabilme ve bu bilgilerle etkileşim halinde olabilme imkânı veren bir uygulama programıdır. Web tarayıcısı ile web adreslerine erişilebilmektedir.

Botnet: Çeşitli dolandırıcılık ve siber saldırıları gerçekleştirmek için kullanılan ele geçirilmiş bilgisayar cihazlarından oluşan ağlardır. "Botnet" terimi "robot" ve "ağ" kelimelerinden üretilmiştir. Bir botnet'in kurulması genellikle çok katmanlı bir planın sızma aşamasıdır. Botlar, veri hırsızlığı, sunucu çökertme ve kötü amaçlı yazılım dağıtımı gibi kitlesel saldırıları otomatikleştirmek için bir araç görevi görür (Kaspersky, 2025).

2. KURAMSAL ÇERÇEVE

Burada bilgi, bilişim, bilgi güvenliği gibi kavramlar detaylı bir şekilde ele alınacaktır.

2.1. Bilgi ve Bilişim

Bilgi güvenliğinin tam olarak anlaşılabilmesi ve farkındalık oluşturarak önleyici güvenlik sağlamasını etkin olarak yapabilmesi için günümüz teknolojilerinin temel bilgilerine sahip olmak gerekir.

Bilgi; insanın çevresindeki nesneleri ve varlıkları yorumlaması, açıklaması veya anlamlandırması sonucu oluşan bir üründür. İnsan ile nesne arasında kurulan ilişkiden doğan bilgi, insanlık tarihinin en kıymetli sermayesi olarak görülmektedir. Bu sermayeyi gelecek nesillere sağlıklı biçimde aktarırken gizliliklerini korumak kurumsal ve kişisel bağlamda sorumluluk isteyen önemli bir ihtiyaçtır. Bu nedenle veri ve bilgilerin gizlilik, bütünlük ve erişilebilirlik unsurları çerçevesinde korunması önemlidir (Kavak & Odabaş, 2023).

Bilişim; “İnsanların teknik, ekonomik ve toplumsal alanlardaki iletişimde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla düzenli ve akılcı biçimde işlenmesi, bilginin elektronik cihazlarda toplanması ve işlenmesi bilimi” olarak açıklanmaktadır. Bilişim; bilginin aktarılması, organize edilmesi, saklanması, tekrar elde edilmesi, değerlendirilmesi ve dağıtımı için gerekli kuram ve yöntemlerdir. Bilişim sistemlerinin en yaygın unsuru, verilerin saklanması, işlenmesi ve aktarılmasını sağlaması bakımından bilgisayarlardır. Ancak bilgisayarlar dışında da bilişim sistemi olarak nitelendirilebilecek aygıtlar mevcuttur (Btk, 2022).

2.1.1. Bilgi Kapsamında Veri ve Bilişim Teknolojileri

Günümüz dünyasında internet kullanım oranının her geçen gün daha da artması ve dijital cihazlara ulaşımın kolaylaşmasıyla birlikte bilgiye ulaşma ve kullanma oranı da artmıştır. Bilgi bireyler ve kurumlar için hayati öneme sahiptir. Bu kapsamda bilginin güvenliğinin sağlanması da son derece önem kazanmıştır. Bilgi güvenliği, dijital ortamlarda verilerin veya bilgilerin işlenmesi ve iletilmesi

sırasında bütünlüğünün korunarak, izinsiz ve yetkisiz erişimlerin engellenmesinin amaç edinildiği süreç ve işlemler bütünüdür (Canbek & Sağıroğlu, 2006).

Bilgi kavramını incelediğimizde Türk Dil Kurumu tanımlamasına göre; öğrenme, araştırma veya gözlem yoluyla elde edilen gerçeğin yanı sıra verinin anlam kazanmış halidir şeklinde ifade edilmektedir. Bilgiyi oluşturan veriler Günlük hayatımızda çeşitli durumlarda farklılığa neden olabilecek dijital işleyişin kaynak olgusu olan ham belirteçlerdir (Eravcı, 2020). Bu bakımdan veriler tek başına anlam ifade etmezler. Veri, işlenmemiş sinyal parçacıklarıdır (Durna & Demirel, 2008). Günlük hayatımızda veriler ekonomi, sağlık, eğitim, güvenlik gibi çeşitli alanlarda, kamu kurum ve kuruluşlarında, özel firmalarda birçok alanda kullanılmakla beraber önemli bilgilere temel oluşturmaktadır. Bir araya getirilen ve hedefler doğrultusunda anlam kazanan veriler bilgiyi oluşturur. Veri bilinen bir işleme sürecine dâhil olmayan, gözlenebilir ve ölçülebilir usuller ile çevreden edinilen kıymetli niteliklerdir (Şeker, 2013). Veriler birleşerek anlamlı bütünlükler ortaya çıkardıkça bilginin değişmesi ve gelişmesi de söz konusu olmakta, alanlarına göre farklılaşan veri tipleri insan hayatında sürekli bir şekilde yer almakla birlikte yaşam içindeki süregelen gerçekliğini korumaktadır (Şeşen & Kuzucuoğlu, 2021)

Veriler geçmişten günümüze yaşam içerisinde son derece önemli olan bilgi kavramının temel yapısını sağlayan birçok anlamlı ve anlamsız bildirim parçacıkları olarak yine günümüzde Bilgi ve İletişim Teknolojileri içerisinde hedef anlamı gerçekleştiren sinyal ve işaretler olarak yer almaktadır. Bütünü oluşturan anlamsal verilerin bilgi üretiminden sonra güvenliğinin sağlanması da son derece hayati bir önem taşımaktadır.

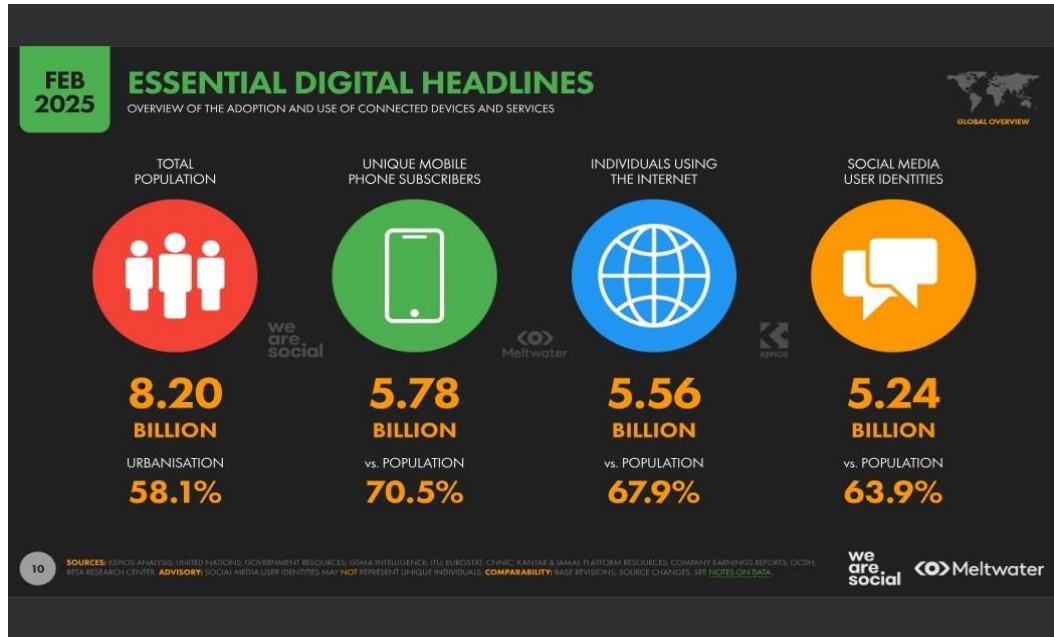
TDK tanımlamasına göre bilişim; insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişimde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi olarak tanımlanmaktadır. Bilişim teknolojileri kavramı bilginin ulaşılması, işlenmesi, depolanması ve gerektiği zaman istenilen yerlere gönderilmesi bunun yanında herhangi bir yer ve zamanda ihtiyaç duyulan bilgiye ulaşma durumu sağlayan teknolojiler olarak belirtilmiştir (Ceyhun ve Çağlayan, 1997). BT, bilişimin elektronik fiziksel bileşenlerinin (donanımların) çeşitli

yazılımlar vasıtası ile çevrimiçi dünyaya açılması sonrasında bilgi ağlarının oluşturulması, geliştirilmesi ve denetlenmesinde etkindir (Ersöz & Özmen, 2020).

2.1.2. İnternet ve Dijital

Günümüz dünyasında üretim, dağıtım, kontrol, güvenlik, eğitim ve sağlık sistemleri ve teknolojileri oldukça süratli bir şekilde gelişip değişmekte bununla birlikte günümüzde kullanılan ve yaşamımızı etkileyen tüm modern sistemlerin odak noktasında teknoloji yer almaktadır (Kamber & Bolatan, 2019). Tarih boyunca insan yaşamını etkileyen temelinde bilginin yer aldığı birçok endüstriyel sıçrama meydana gelmiştir. Bunlardan endüstri 4,0 olarak adlandırılan süreç ise günümüzün önemli bir gerçeğidir. Endüstri 4.0 ile bilgi ve iletişim teknolojileri ve kullanıldıkları alanlar ile internetin de etkisiyle otomasyon, üretim sistemleri, büyük veri, veri transferleri alanları da hızla gelişmektedir (Kağnıcıoğlu ve Özdemir, 2017). Endüstri 4.0 küresel ölçekte büyük bir hızla artan veri miktarları ve bunların işlenmesi, depolanma süreçleri internet kullanım oranında hızla artması, mobil teknolojilerin sürekli gelişmesi insanların daha fazla çevrimiçi ortamda kalmalarını sağlamıştır. Son derece önemli olan internet kullanımı beraberinde bilgi güvenliği kavramını da ortaya çıkarmış WEB tabanlı iş ve işlemlerde kişisel ve kıymetli bilgilerin paylaşılması zaman zaman kaçınılmaz olmuştur (Değirmenci & Demiral 2023). Uluslararası ölçekte bakıldığında WAS şirketinin belirttiği rapora göre “Dijital 2025: Dijitalin küresel durumuna ilişkin temel rehber- Digital 2025 Global Overview Report” 2025 yılı için raporda önemli bulgular yer almaktadır.

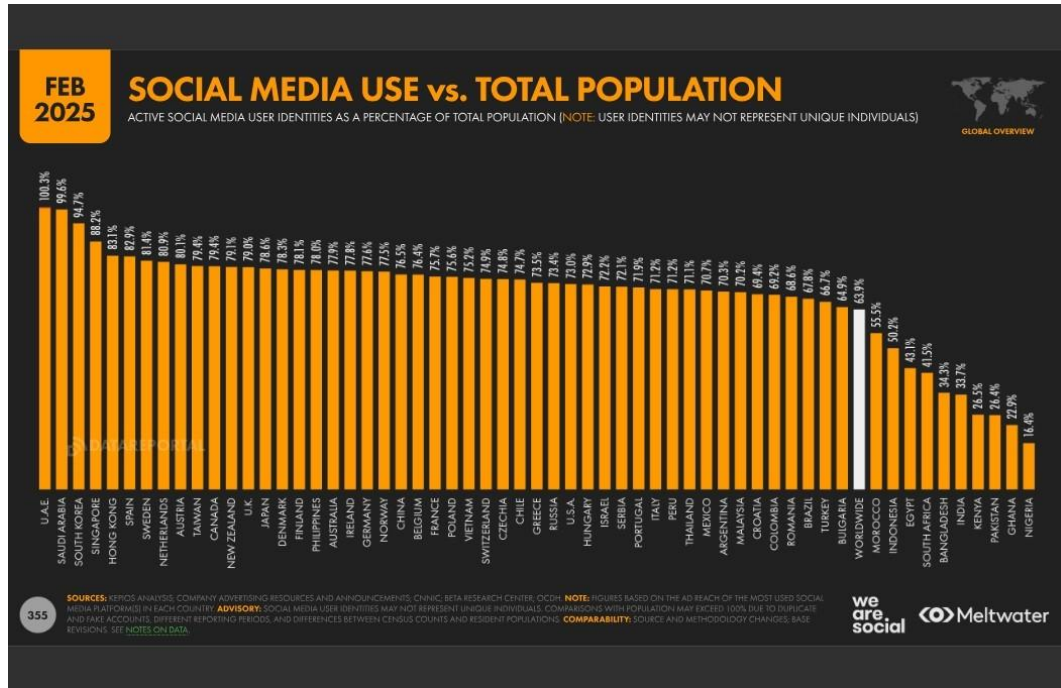
Resim 2.1: Dijital Büyüme



Kaynak: We Are Social Dijital 2025 raporu, Haziran 15, 2025 tarihinde <https://wearesocial.com/uk/blog/2025/02/digital-2025/> adresinden alındı.

- Birleşmiş Milletler'in nüfus verilerine göre, bugün Dünya'da 8,20 milyar insan yaşadığını ve bu toplamın geçen yılın aynı dönemine göre 70 milyon kişi (+%0,9) arttığını gösteriyor. Dünya çapında, yaklaşık 4,8 milyar insan - küresel nüfusun %58,1'i- artık kent merkezlerinde yaşarken, 3,4 milyar insan kırsal alanlarda yaşıyor.
- Raporda belirtilen verilere göre 5,78 milyar kişi cep telefonu kullanıyor, bu da dünya nüfusunun %70,5'ine denk geliyor. Tekil mobil aboneler son 12 ayda 112 milyon artarak yıllık %2,0 büyüme sağladı. Ayrıca veriler akıllı telefonların artık dünya genelinde kullanılan mobil cihazların yaklaşık %87'sini oluşturduğunu gösteriyor.

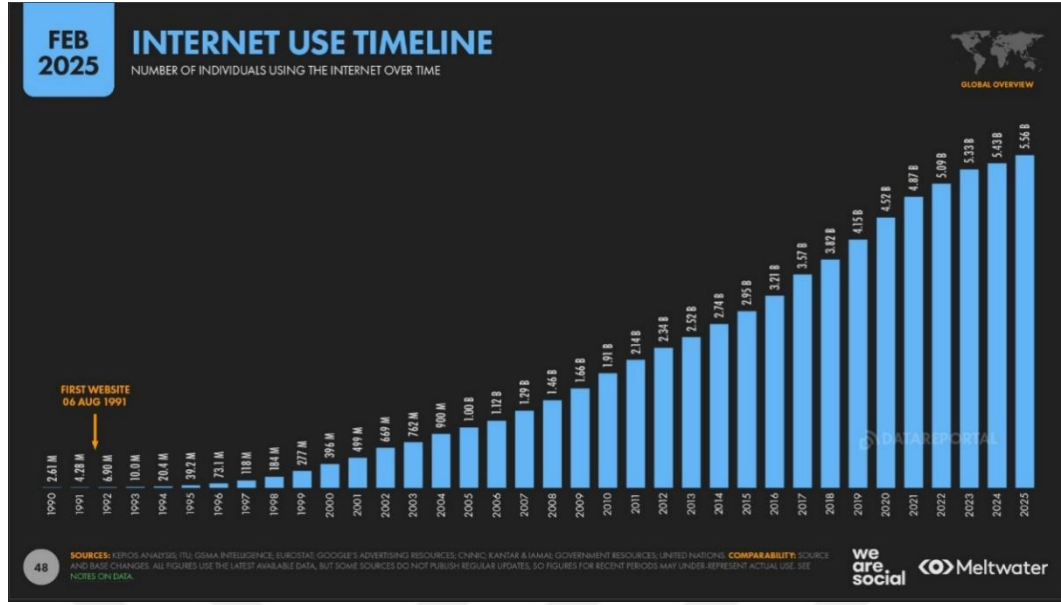
Resim 2.2: Ulusal Sosyal Medya Kullanım Oranı



Kaynak: We Are Social Dijital 2025 raporu, Haziran 15, 2025 tarihinde <https://wearesocial.com/uk/blog/2025/02/digital-2025/> adresinden alındı.

- Sosyal medya kullanım oranları bakımından yüzde 66,7 ile Türkiye 47. sırada yer alıyor.
- Ülkemizin sosyal medya kullanım süresi olarak ortalamanın üzerinde kalarak günlük 2 saat 43 dakika ile dünyada 16. sırada yer alıyor.

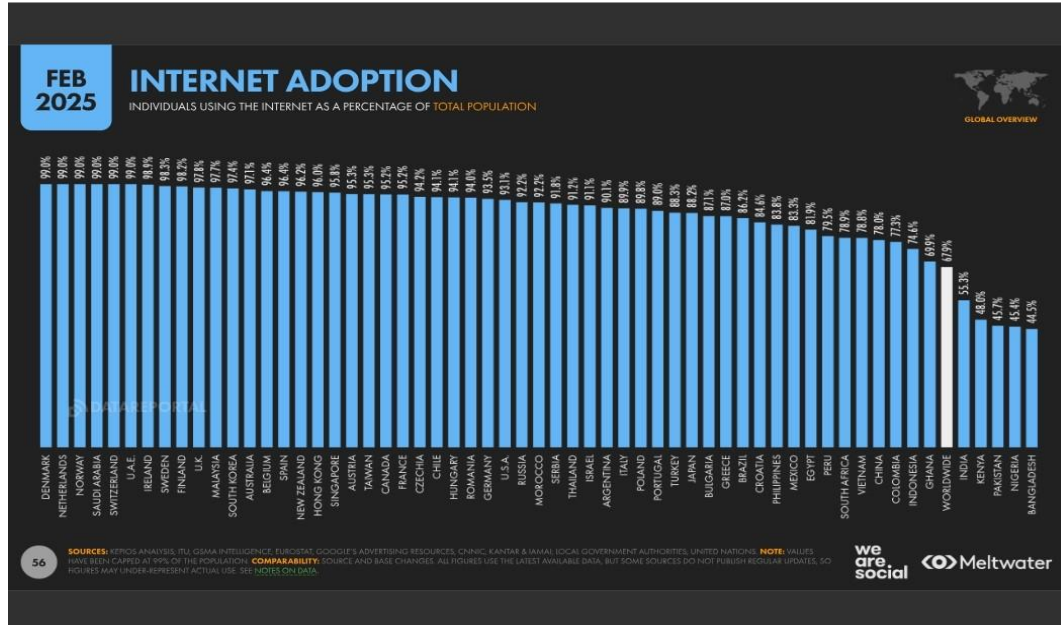
Resim 2.3: Global İnternet Kullanım Oranı



Kaynak: We Are Social Dijital 2025 raporu, Haziran 15, 2025 tarihinde <https://datereportal.com/reports/digital-2025-global-overview-report> adresinden alındı.

- Raporda 2025 yılı başında toplam 5,56 milyar kişi interneti kullanıyor ve bu da %67,9'luk bir oran oluşturuyor. İnternet kullanıcıları küresel toplamda, ek 206 milyon yeni kullanıcı kimliği sayesinde son 12 ayda %4,1 arttı.

Resim 2.4: Türkiye'de İnternet Kullanım Oranı

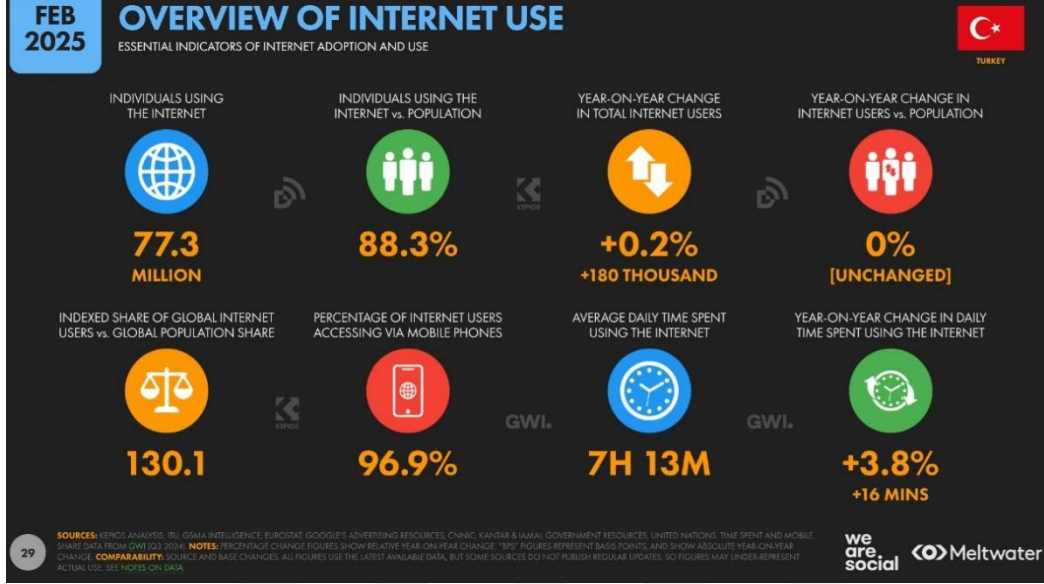


Kaynak: We Are Social Dijital 2025 raporu, Haziran 15, 2025 tarihinde <https://www.clicksus.com/we-are-social-2025-global-ve-turkiye-verileriyle-dijital-dunya> adresinden alındı.

- Türkiye 2025 yılında toplam nüfusa göre internete sahip olma bakımından yüzde 88,3 oranıyla dünyada 38. sırada bulunduğu,

- Türkiye’de interneti kullanılarak geçirilen süre 7 saat 13 dakikayla dünyada 18. Sırada yer aldığı belirtilerek dünya ortalamasının 35 dakika üzerinde olduğu,

Resim 2.5: Türkiye'de İnternet Kullanım Oranı



Kaynak: We Are Social Dijital 2025 raporu, Haziran 15, 2025 tarihinde <https://www.clicksus.com/we-are-social-2025-global-ve-turkiye-verileriyle-dijital-dunya> adresinden alındı.

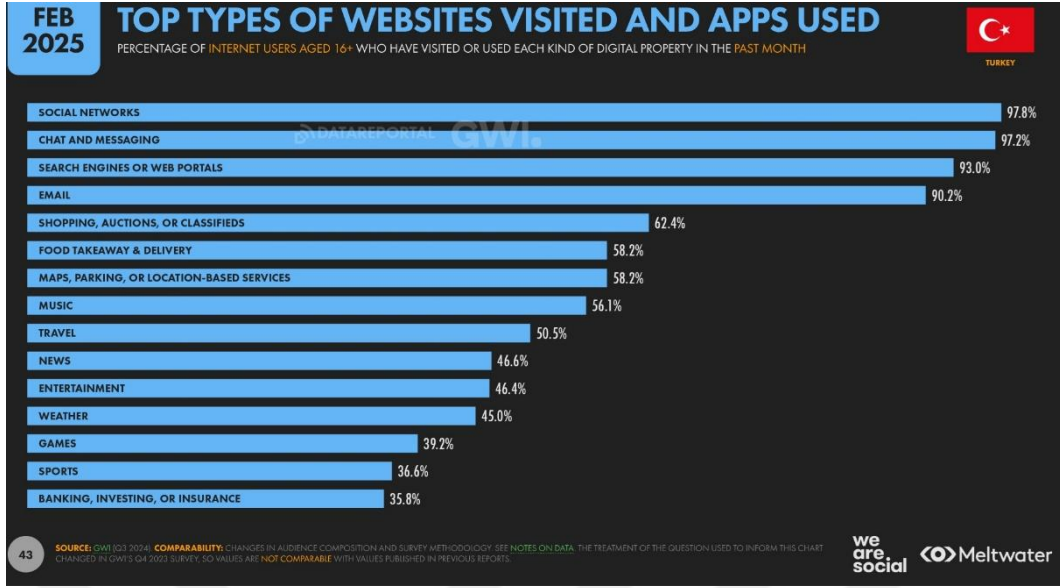
Raporun devamında;

- İnterneti kullanmanın ana nedeni olarak “bilgiyi bulmak, bilgiye ulaşmak” yüzde 76,2’lik oranla 1.sırada yer almıştır.

En çok ziyaret edilen web sitesi türleri ve kullanılan uygulamalar olarak;

- 1- Sosyal ağ siteleri ve uygulamaları
- 2- Sohbet ve mesajlaşma uygulamaları
- 3- Arama motorları ve web portalları
- 4- E-posta siteleri ve uygulamaları
- 5- Alışveriş siteleri ve uygulamaları

Resim 2.6: Türkiye'de İnternet Kullanım Oranı



Kaynak: We Are Social Dijital 2025 raporu, Haziran 15, 2025 tarihinde <https://www.clicksus.com/we-are-social-2025-global-ve-turkiye-verileriyle-dijital-dunya> adresinden alındı.

- İnternette geçirilen süre yaşlara göre sıralandığında en yüksek kullanımı 16 – 24 yaş arasının aldığı,
- Sohbet ve mesajlaşma uygulamalarının 16 – 64 yaş arasında 1.sırada yer aldığı,
- Sosyal ağ olarak 16 – 64 yaş arası kullanıcıların çoğunun en az bir sosyal medya uygulamasını kullandığı,
- Arama motorlarının da yüzde 80,7 olan kullanım oranıyla 3.sırada yer aldığı,
- İnterneti alışveriş amacıyla kullanım oranının 5. sırada yer alarak internet kullanıcılarının yüzde 62,4'e yaklaşan kısmı e-ticaret hizmetini kullandığı belirtilmiştir (WASD, 2025).

Yerelde ise TÜİK hanehalkı bilişim teknolojileri (BT) kullanım araştırması raporuna (27 Ağustos 2024) göre;

- İnternet kullanan bireylerin yüzde 88,8 olduğu,
- E- Devlet hizmetini kullanan kişilerin yüzde 73,3 olduğu,
- İnternet üzerinden mal veya hizmet satın alma oranının yüzde 51,7 olduğu,
- E-ticaret yapan bireylerin yüzde 76,7'si giyim, ayakkabı ve aksesuar kategorisinde satın alma gerçekleştirdiği,

- Sosyal medya ve mesajlaşma uygulamaları yüzde 86,2 ile WhatsApp, yüzde 71,3 ile YouTube ve yüzde 65,4 ile Instagram olduğu belirtilmiştir (TÜİK, 2024).

2.2. Bilgi Güvenliği ve Süreçleri

İnternet ve bilişim teknolojilerinin yukarıda belirtilen rapor ve araştırmalardan da anlaşılacağı üzere günlük hayatımız içinde önemli bir yer aldığı anlaşılmaktadır. Nesnelerin interneti (Internet of Things, IoT), yapay zekâ, artırılmış gerçeklik gibi yeni gelişmeler ile biçimlenen içerisinde yaşadığımız dijital çağ, bilgi ve iletişim teknolojileri öncülüğünde ilerleme göstermektedir. İnternetin süratli ve baş döndürücü şekilde gelişmesiyle birlikte, veri ve bilgi alışverişlerine ilişkin süreçlerde dijital iletişim ortamlarının kullanımı giderek artmıştır (Solichin & Ramadhan, 2017). Birçok alanda kullandığımız internet ve dijital teknolojilerin günlük iş ve işlemlerimizin büyük kısmını doğrudan etkilediği görülmektedir. Bu kapsamda hayati öneme sahip birçok verimiz internet ve dijital teknolojilerde kullanılmaktadır. Çevrimiçi ortamda önemli birçok veri kullanılmaktadır. Verilerimizin güvenliğinin sağlanmasında bilinçli farkındalık kapsamında sahip olamamız gereken önleyici güvenlik önlemleri bulunmaktadır. Bunların büyük bir kısmı bilgi güvenliği kapsamında değerlendirilmektedir.

Bilgi güvenliği, bir varlık türü olarak bilginin izinsiz veya yetkisiz bir biçimde erişimini, kullanımını, değiştirilmesini, açığa çıkarılmasını, yok edilmesini, transferini ve hasar verilmesini önlemek olarak tanımlanabilir; gizlilik, bütünlük ve erişilebilirlik olarak üç temel unsurdan meydana gelir (Puhakainen, 2006).

Bilgi güvenliğinin en temel unsurları; “Gizlilik, (confidentiality), bütünlük (integrity), kullanılabilirlik (availability), kimlik kanıtlama (authentication) ve inkâr edememe (non-repudiation) şeklinde belirtilmiş bunların yanında sorumluluk (accountability), erişim denetimi (access control), güvenilirlik (reliability) ve emniyet (safety)” etkenleri de bilgi güvenliğini destekleyen unsurlar oldukları belirtilmiştir (Canberk & Sağıroğlu, 2006).

Ulusal Standartlar ve Teknoloji Enstitüsüne (National Institute of Standards and Technology - NIST) göre bilgi güvenliği tanımı; gizlilik, bütünlük ve kullanılabilirlik hedefinin sağlanması amacıyla bilgilerin ve bilgi sistemlerinin

yetkisiz erişim, kullanım, ifşa, kesinti, değişiklik veya imhaya karşı korunması şeklindedir (NIST 2024).

Bilgi güvenliği, bilginin çevrimiçi ortamda ulaşılabilirliğin sağlandığı, bilginin kaynağından alıcısına doğru gizliliğe bağlı olarak, bozulmadan, değişikliğe uğramadan ve başkaları tarafından yetkisiz olarak ele geçirilmeden bütünlüğünün korunması ve güvenli bir şekilde aktarılması süreci olarak tanımlanmaktadır (Vural, 2007)

Bilgi güvenliği genel olarak kurumlar, kuruluşlar ve özelde bireylerin günümüz dünyasında çevrimiçi ve dijital ortamlarda bulunan verilerin bilgi güvenliği tehditlerine karşı bütünlüğüne, gizlilik ve kullanılabilirliğe karşı oluşabilecek olumsuzluklara karşı önleyici güvenlik farkındalığının kazanılması süreci veya farkındalığın oluşması şeklinde açıklanabilir.

2.3. Bilgi Güvenliğinin Temel Unsurları

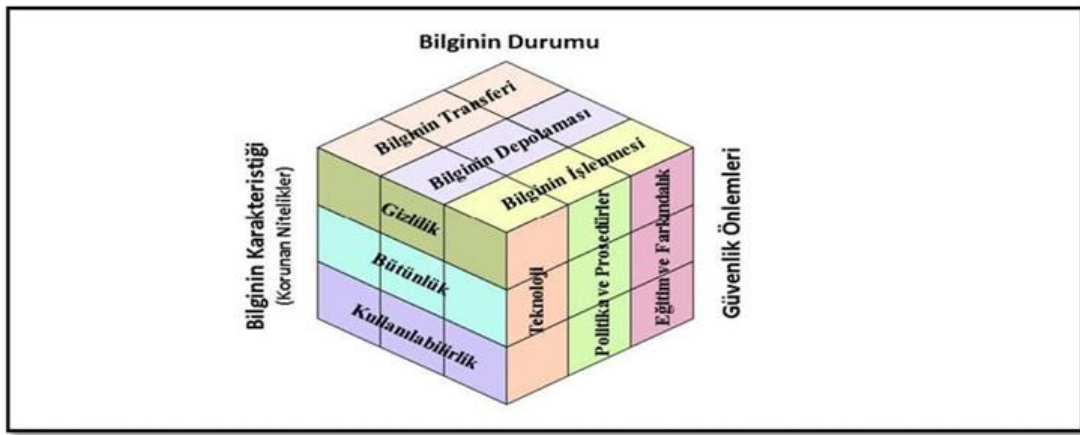
Bilişim teknolojilerinin eğitimden ticarete, ulaşımdan iletişime, kamu hizmetlerinden özel sektöre kadar hemen her alanda köklü değişiklikler yaparak hayatı ciddi anlamda etkiler hale gelmesi, bilişim teknolojilerinin kanunları ihlal etme fırsatı veren ve ortaya yeni art niyetli fiilleri çıkartan bir etkiye sahip olmasını da beraberinde getirmiştir. Bu sebeple, özellikle bu teknolojilerin kaynağını oluşturan ülkeler başta olmak üzere, pek çok devlet bilişim alanında yasal düzenlemelere gitmiş, mevzuatlarını teknolojinin gerektirdiği biçimde değiştirme çabasına girmişlerdir (BTK, 2022). Bu bakımdan bilginin güvenliğinin sağlanmasında bazı temel unsurlar bulunmaktadır.

Bilgi güvenliği; bilginin bütünlüğünün, gizliliğinin ve erişilebilirliğinin sağlanmasıdır. Bu ilkelerinin bir kısmı teknik olarak sağlanırken bir kısmı ise bilgi güvenliği bilinci oluşturularak gerçekleştirilebilir. Bilgi güvenliği kapsamında varlık, varlıkta bulunan açıklık ve bu açıklığı kullanacak tehdit unsurları çok önemlidir. Bu üç faktörün bir araya gelmesi bilginin gizliliğinin, bütünlüğünün veya erişilebilirliğinin zarar görmesine sebep olabilmektedir (Gündüz & Daş, 2021).

Bilgi güvenliğinin daima korunması gereken özellikleri bir diğer ifadeyle korunması gereken ilkeleri bulunmaktadır. Bilgi güvenliği Solomon'un (Solomon

ve Chapple, 2005) bilgi güvenliği üçgeninde anlattığı gibi gizlilik, bütünlük ve erişilebilirlik olmak üzere bu üç faktörün bileşimi kabul edilir ve bu üç faktör üzerine inşa edilir. Şekil 1’de gösterilen McCumber Bilgi Güvenliği modeli bilgi güvenliği alanında hem ulusal hem de uluslararası boyutta bilgi güvenliği politikası geliştirebilmek ve bilgi güvenliğini gerçekten tüm yönleriyle ele alabilmek için temel alınabilecek en uygun ve anlamlı modellerden biridir (Özdemir & Uluyol, 2021).

Şekil 2.1: McCumber Bilgi Güvenliği Modeli (McCumber, 1991). (Özdemir, Uluyol, 2021)



Kaynak: McCumber Bilgi Güvenliği Modeli (McCumber,1991), Haziran 29, 2025 tarihinde <https://images.app.goo.gl/HEzArcKyjnbScG9d8> adersinden alındı.

Bilgi güvenliğini tüm unsurlarıyla birlikte farklı boyutlarda gruplandırarak gösteren McCumber modeli uzun yıllar önemini korumuş ve halen geçerliliğini devam ettirmektedir (Özdemir & Uluyol, 2021). McCumber (2005), bilgi güvenliğini, bilgi ve bilgi sistemlerine yetkisiz erişim, bilginin kullanımı, ifşa edilmesi, bozulması, değiştirilmesi veya bilginin gizlilik, bütünlük ve kullanılabilirliğine zarar vermek için yapılan kötü niyetli girişimlere karşı sağlanacak koruma olarak tanımlamıştır. Kısaca, bilginin kullanım hakkı kimde ise, o kişi dışında kullanımı durumunda bilgi güvenliğinden söz edilemez. Şekil 2.1’de belirtilen McCumber’in geliştirmiş olduğu bilgi güvenliği modeli, uygulanabilirliği olan en güncel ve en temel yaklaşımdır. Bilgi güvenliğinden söz edebilmek için, gizlilik, bütünlük ve kullanılabilirlik birbirini tamamlamalı ve ayrılmaz bir bütün olmalıdır (Değrimenci & Demiral, 2023).

2.3.1. Gizlilik

Çeşitli veri türlerinin kullanımı ve depolanması gibi süreçlerde bu veriler üzerindeki çeşitli kısıtlamalardır (Khidzir vd. 2018). Veri iletimi ve kullanımı dijital ortamın doğası gereği birtakım güvenlik açıklarına sahiptir. Bu süreçte kullanıcıların gizlilik farkındalığı oluşturularak kimlik doğrulama yöntemlerini etkili kullanmaları sağlanmalı ancak yeterli güvenlik seviyesini oluşturmadığı için süreç içerisinde gerekli erişim kontrolü yetkisi belirlenerek gizliliğe yönelik tehditler engellenebilir (Yee & Zolkipli, 2021). Bilgiye ulaşma ve kullanma sürecinde gizliliğin sağlanmasında yönetim süreci ve farkındalık oldukça önemlidir. Microsoftun belirttiğine göre gizliliğin bilgi güvenliğinin önemli bir bileşeni olduğu kurumların, yalnızca yetkili kullanıcıların bilgilere erişmesine izin veren önlemleri geçerli kılmasını belirterek verileri şifreleme, çok faktörlü kimlik doğrulama gibi kuruluşların veri gizliliğini sağlamada etkili olabilmesi için kullanabileceği yöntemlerden bazıları olduğuna dikkat çekmiştir (Microsoft, 2024).

Gizlilik; bilginin yetkisiz kişilerin erişimine kapalı olması ve bilginin yetkisiz kişilerce açığa çıkarılmasının engellenmesidir (Yılmaz, 2014). Yapılan çalışmalar kapsamında bakıldığında bilgi dijital ortamlarda ileti ve saklama süreçlerinde birtakım korunma kısıtlarına sahip olmalıdır. Bu kısıtların etkililiğini yönetsel süreçlerin verimliliği ve güncelliğinin yanında kullanıcı farkındalığı ve bilgisi etkilemektedir.

2.3.2. Bütünlük

Bütünlük: Verilerin veya kaynakların güvenilirliğini ifade eder ve genellikle uygunsuz veya yetkisiz değişikliği önleme, veri bütünlüğünü, verinin içeriğini ve köken bütünlüğünü, bilginin veri kaynağının bozulmadan ve değiştirilmeden kalmasını sağlamak şeklinde ifade edilir (Singh vd, 2014).

Bilgi güvenliğinde bütünlük; verilerin yetkilendirme olmadan değiştirilememesi şeklinde adlandırıldığı gibi kullanıcının çeşitli hatalar veya kötü niyetli bir şekilde verilere zarar verdiğinde, zararlı bir virüs sistem etkinliğini bozduğunda, bir web sitesi tahrip edildiğinde bütünlük ihlal edilmiş olur (Alhassan & Adjei-Quaye, 2017).

Samanos ve Coss (2014)'e göre ise bütünlük kavramını etik kavramıyla ilişkilendirmiş bilgi güvenliği ve denetiminde etikliği çeşitli uygulama standartları ve yeterlilikleri bakımından genel kabul görmüş ilke ve değerleri içerdiğini belirtmiştir.

Bütünlük; bilginin yetkisiz bir şekilde değiştirilmesi, yok edilmeli ya da herhangi bir şekilde zarar görmesi tehditlerine karşı içeriğinin korunmasının yanında doğruluğunun ve eksiksizliğinin sağlanmasıdır (Yılmaz, 2014). Bu kapsamda bilginin son derece kıymetli oluşu dijital ve çevrimiçi ileti ve depolama alanlarında veri kaybının olmaması için yüksek düzeyde önleyici güvenlik farkındalığı oluşturmamız gerektiğine işaret etmektedir.

2.3.3. Erişilebilirlik (Kullanılabilirlik)

Kullanılabilirlik; yetki sahibi kişilerin gerek duyulduğunda bilgi ve ilişkili varlıklara ulaşma yetkisinin olması şeklinde tanımlanmaktadır (Canberk & Sağıroğlu, 2006). Bilginin her ihtiyaç anında kullanıma hazır durumda olmasının yanında bir sorun ya da problem karşısında bilgiye ulaşılabilir olması kullanılabilirlik özelliğinin etkililiğinin önemini gösterir (Yılmaz, 2014).

Kullanılabilirlik; herhangi bir bilgi sisteminin amacına hizmet edebilmesi için, bilginin ihtiyaç duyulduğunda kullanılabilir olması gerektiği anlamına gelir. Kullanılabilirlik bilgiyi depolamak ve işlemek için kullanılan bilgi işlem sistemlerinin, onu korumak için kullanılan güvenlik kontrollerinin ve ona erişmek için kullanılan iletişim kanallarının doğru bir şekilde çalışmasını sağlayarak etkililiğini gösterir. Kullanılabilirliğin önemi bilginin kullanımı, depolaması ve geri çağırımı esnasında yüksek öneme sahip olan güvenlik süreçlerinin etkililiğidir.

2.4. Bilgi Güvenliği Tehditleri

Bilişim teknolojilerinin gelişmesiyle birlikte günümüzde bilgi ve bilişim güvenliği konusunda en ciddi tehditlerin başında zararlı ve kötü niyetli yazılımlar gelmektedir (Canbek & Sağıroğlu, 2007). Bilginin iletilmesi ve depolanmasında önemli bir güvenlik sorunu olarak karşımıza çıkan kötü niyetli yazılımlara karşı dijital ortamda kullandığımız her türden bilgi ve uzantılarının kaynağına karşı eleştirel yaklaşmamız gerekmekte bunun yanında kaynağın doğruluğunu ve

güvenilirliğini kontrol etmemiz son derece önemlidir. “Bilişim teknolojilerinin hızlı bir şekilde gelişmesi sonucunda internet faydalarının yanı sıra art niyetli kişilerin ulaşması kolay, izlerinin diğer suçlara göre daha zor bulunacağı, sanal bir suç işleme ortamı sunmuştur. Teknolojiye bağlı olarak bilişim alanına kazandırılan her türlü araca bağlı olarak işlenen suç şekilleri de sürekli gelişmektedir. İnternetin özellikle hukuksal alanda pek çok davranış şekilleriyle birlikte yeni sorunları da beraberinde getirdiği yaşanan bir gerçek haline gelmiştir. Siber suçlar ya da Bilişim suçları yaygın olarak; sahte internet siteleri (phishing, pharming amaçlı) oluşturma, kişilerin şifreleri ve kullanıcı bilgilerini ele geçirme, web sitelerine ve sunucularına yönelik saldırılar düzenleme (defacement-bozma), virüs taşıyan e-postalar (spam mail) yollayarak elektronik saldırılar yapma gibi çeşitli şekillerde gerçekleştirilmektedir. Kullanıcının bilgisi ve rızası dışında ele geçirilen şifre, kullanıcı adı, resim, görüntü gibi bilgi ve dokümanlar kullanıcıya karşı çeşitli tehdit unsuru olarak kullanılmaktadır. Bilişim suçlarının kendine özgü niteliği nedeniyle suçu işleyen kişi (fail) ile suç mağduru kişi fiziksel olarak uzaktadır. Aynı zamanda işlenen fiilin suç olup olmadığı geleneksel suçlarda olduğu gibi siyah ve beyaz ayrımından ziyade gri alan içerisinde kalmaktadır. Kötü niyetli kullanıcılar bu eylemi gerçekleştirirken kasıtlı hareket etmektedirler ve belirli bir amaçları vardır” (BTK, 2022).

Temel olarak güvenlik kavramı TDK sözlüğünde; toplum yaşamında yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu; emniyet olarak tanımlanmaktadır (TDK). Güvenlik tanımlaması yapılırken farklı türden etkenlerin göz önünde bulundurulması ve farklı durumlara göre kavram yapısının yeniden belirlenmesi herkesçe onaylanmış bir tanımın ortaya çıkmasını engellemiştir (Sancak, 2013). Bununla birlikte güvenliğe ilişkin “tehlikelerden ve korkulardan uzak kalma, bir tehdidin olmaması” gibi ifadelerin birçok tanımda kullanılmış olması ortak bir anlayışın olduğunu da göstermektedir (Özcan, 2011). Genel olarak güvenlik kavramına bakıldığında “koruma, tehditleri algılama ve uzak tutma, sürekli tetikte olma, riskleri göz önünde bulundurma” gibi çeşitli anlamlar içermektedir.

Siber güvenlik ise; siber saldırıları önlemek veya etkilerini azaltmak için kullanılan tüm teknolojiler, uygulamalar ve politikalar anlamına gelir. Siber

güvenlik, bilgisayar sistemlerini, uygulamaları, cihazları, verileri, finansal varlıkları ve kişileri fidye yazılımlarına ve diğer kötü amaçlı yazılımlara, kimlik avı dolandırıcılıklarına, veri hırsızlığına ve diğer siber tehditlere karşı korumayı amaçlar (IBM, 2025). Burada güvenliğin sağlandığı bilgi varlıklarının yer aldığı çevrimiçi internete bağlı olan ve birçok bilgi varlığı içeren siber kavramına bakacak olursak, Siber kavramı; bilişim ortamları ve bilişim ağlarını içeren varlıkları tanımlamak için kullanılır (Korucu, 2021). Bu varlıkların birbirleri ile olan iletişimleri ve bulunduğu ortam ise siber uzay kavramı ile ifade edilebilir. Siber uzay kavramı ise; İnternet, telekomünikasyon ağları, bilgisayar sistemleri ve gömülü işlemciler ve denetleyiciler dâhil olmak üzere bilgi teknolojisi altyapılarının birbirine bağlı ağından oluşan bilgi ortamı içindeki küresel bir alan olduğu gibi bilginin oluşturulduğu, iletildiği, alındığı, depolandığı, işlendiği ve silindiği elektronik çevrimiçi ortam olarak tanımlamaktadır (Mbanaso & Dandaura, 2015).

İçinde bulunduğumuz dijital bilgi çağında siber uzay, çevrimiçi alan, bilişim sistemleri, nesnelerin interneti ve internet olarak da adlandırılan dijital çevrimiçi alan artık günlük iş ve işlemelerimizi hayati ölçüde etkilemektedir. Bu kapsamda dijital alanda birçok istenmeyen durum yaşanmaktadır. Kurum veya kullanıcıların yukarıda belirtilen bilgi güvenliği unsurları doğrultusunda bilgi güvenliği tehditlerine maruz kalmaması birtakım önleyici güvenlik önlemleri gerektirmektedir. Önleyici güvenlik; bir kurumun, bireyin veya sistemin karşılaşılabileceği potansiyel risk ve tehditleri önceden tespit edilerek, bu olası tehditlerin analizlerinin yapılarak gerçekleşmesini engellemeye yönelik alınan önlem ve uygulamalardır. Önleyici güvenlik, olayların meydana gelmeden önce önlenmesini hedefler ve risk kategorilendirmesi yapılarak analiz ve eleştirel değerlendirme neticesinde risk ve tehditlerin bertarafı için gerekli kılavuzlama süreci ve bilişsel tecrübenin oluşmasını sağlar.

Bilişim suçu en genel anlamıyla; bilişim alanındaki gelişmelere paralel artış gösteren, kendini yenileyen ve teknolojinin yardımı ile genellikle sanal bir ortamda kişi veya kurumlara maddi veya manevi zarar verecek davranışlarda bulunmaktır. Başka bir tanım, bilişim sistemine yönelik olarak bilişim sistemlerinin kullanılarak işlendiği suç olduğu söylenmektedir. Diğer bir tanımda

ise “bir bilgisayarda ya da bilgisayar olarak nitelendirilememesine rağmen veri-iletişimi sağladığı için bilişim alanının unsurlarından olduğu kabul edilmesi gereken diğer elektronik, manyetik, mekanik araçlar üzerinde (örneğin, cep telefonları, üzerindeki web paneli sayesinde ağa bağlanıp bilgi aktarımı yapabilen elektronik ev aletleri, üzerinde yüklü programlar aracılığıyla şifreli yayınları alan, bunları işleyen ve bunlardan sonuç çıkaran çözücüler) veya bunları veri-iletişimi için birbirine bağlayan soyut veya somut bir ağ üzerinde gerçekleştirilebilir eylemler” bilişim suçu olarak nitelendirilmektedir(BTK, 2022).

“Bilişim suçu veya bilgisayar (dijital) suçu terimi bir bilgisayar ve bilgisayar ağı (Bilgisayar, çevre birimleri, pos makinesi, cep telefonu gibi her türlü teknoloji) kullanılarak işlenen herhangi bir suçu ifade etmek için kullanılmaktadır. Bilgisayar, bir suçun işlenmesinde kullanılmış olabileceği gibi bir suçun hedefi de olabilmektedir. Bilişim (siber) suçları: Bireylere veya birey gruplarına yönelik, mağdurun onurunu zedelemeye veya mağdura fiziksel veya zihinsel olarak doğrudan veya dolaylı olarak zarar verme suçu kastı ile İnternet (görüşme odaları, epostalar, sosyal medya uygulamaları, ilan sayfaları) ve cep telefonu (SMS/MMS) gibi çağdaş iletişim araçları kullanarak zarar verme amaçlı saldırıların yapılmasıdır” (BTK, 2022).

Bilgi güvenliği kapsamında suç konusunun ve istenmeyen durumların ortaya çıkmasını sağlayan siber tehdit unsurlarının başında son yıllarda oldukça artan sosyal mühendislik gelmektedir.

2.4.1. Sosyal Mühendislik

Sosyal mühendislik, kullanıcıların bilgi sistemlerini tehlikeye atmasına yönelik davranışlar sergilemesine etki etme sürecidir. Dijital sistemlere yönelik teknik saldırıların yerine, bilgiye erişimi veya bilginin sahibi olan insanları hedef alarak, onları gizli bilgileri açığa çıkarmaları doğrultusunda etkileyerek aynı zamanda ikna yoluyla kötü niyetli saldırılarını gerçekleştirmeye yönlendirir (Krombholz, vd, 2015). Sosyal mühendislik; etkileme, zorlama, aldatıcı ilişkiler geliştirme, sorumluluğu, etik değerleri, dürüstlüğü ya da bağlılığı azaltma amacını güden yöntemler kullanarak kişileri gizli bilgi vermeleri veya erişim sağlamaları için aldatma sürecidir (Bağcı, 2009). Hassas, önemli bilgilere ve ağ sistemlerine, yasal kullanıcılar üzerinden erişim sağlama amacıyla saldırganlar tarafından

kullanılan düşük teknolojili ve insan zafiyetlerine dayalı yöntemlerin tamamıdır (Gündüz & Daş, 2016). Bu kapsamda bakıldığında sosyal mühendislik süreci insan zafiyetleri ve bilgi eksikliği kullanılarak dijital sistemler üzerinde kötü niyetli ve casus yazılımlarında kullanılmasıyla yasadışı denetim sahibi olmak şeklinde görülebilir. Burada ortaya çıkan önemli bir hususta sosyal mühendislik hakkında farkındalık ve bilgi sahibi olmanın önemli olduğudur. 2003 yılında kurulan Anti-Phishing Çalışma Grubu (APWG), siber suçlarla mücadele eden kişiler, adli soruşturmacılar, kolluk kuvvetleri, teknoloji şirketleri, finansal hizmetler şirketleri, üniversite araştırmacıları, STK'lar ve çok taraflı antlaşma örgütlerinden oluşan, kâr amacı gütmeyen bir kuruluş olarak faaliyet gösteren uluslararası bir koalisyondur. Kimlik hırsızlığı ve dolandırıcılıklarının giderek arttığını kimlik avı, suç yazılımları ve e-posta sahteciliğinden kaynaklanan sorunları ortadan kaldırmaya odaklanan bu kuruluş ve bünyesindeki uluslararası kuruluşlar “DUR, DÜŞÜN, BAĞLAN” (STOP, THINK, CONNECT) kampanyasını yürütmektedir. APWG’ ye göre Kimlik Avı Tanımı, tüketicilerin kişisel kimlik verilerini ve finansal hesap bilgilerini çalmak için hem sosyal mühendislik hem de teknik hileler kullanan bir suç türüdür. Sosyal mühendislik planları, aldatıcı e-posta adresleri ve mesajları, sahte web siteleri ve aldatıcı alan adları kullanarak, güvenilir ve meşru bir tarafla iş yaptıklarına inandırarak dikkatsiz veya bilinçsiz kurbanları avlamak şeklindedir. Kötü niyetli bu kişiler, kullanıcı adları ve parolalar gibi finansal verileri ele geçirmek için bireyleri kandıran sahte web sitelerine tasarlarlar. Teknik hileler ile doğrudan kimlik bilgilerini çalmak için bilgisayarlara kötü amaçlı yazılımlar yerleştirir ve çoğunlukla kullanıcıların hesap adlarını ve parolalarını ele geçiren veya kullanıcıları sahte web sitelerine yönlendiren sistemler kullanılırlar.

Şekil 2.2: Sosyal Mühendislik Süreci



Kaynak: Yazar tarafından oluşturulmuştur.

2.4.2. En Çok Kullanılan Sosyal Mühendislik Türleri

1- Phishing (Oltalama): Kullanıcıların kişisel kimlik verilerini, finansal hesap bilgilerini, kişiye özel şifre bilgilerini yetkisiz olarak ele geçirmek için hem sosyal mühendislik hem de teknik hileler yoluyla oluşan suçtur. Sosyal mühendislik planları yoluyla, kullanıcıların aldatıcı e-posta adresleri ve mesajları, sahte web siteleri ve sahte alan adları kullanarak, güvenilir ve meşru bir tarafla iş yaptıklarına inandırılarak kişilerin kandırılması süreci (APWG, 2024). Yine aynı rapora göre 932.923 kimlik avı saldırısı olduğu görülmüş buna göre sosyal medya platformları, tüm kimlik avı saldırılarının yüzde 30,5'inde kullanılmıştır. Bunun yanında SMS ve kısa mesajlarla oluşturulan kimlik avı türü olan smishing 2024 yılında yüzde 22'den fazla artış göstermiş, e-posta dolandırıcılıklarının yüzde 83,1 Gmail hesapları üzerinden gerçekleştiği APWG raporunda belirtilmiştir. Phishing, sosyal mühendislik teknikleri kullanarak, kurbanın şifreleri, banka hesap numaraları, kredi kartı bilgileri gibi özel ve yüksek güvenliğini bilgilerini, kurbanı aldatarak elde etme yöntemi olarak tanımlanabilir (Alataş & Atan, 2007). Phishing yöntemi balık tutmaya benzetilebilir. Öncelikli bilinirliği yüksek olan bir Kurum, kuruluş veya özel firma, e-ticaret sitesi seçilerek internet sitesi gözlemlenir ve sistemi tespit edilir. Burada şifre ve kullanıcı adı kullanımı

analizleri yapılır, bu noktadan sonra hedef sitenin bir kopyası ya da bir benzeri oluşturulur ve sahte sunucuda sistem çalıştırılır buradan sonra kötü niyetli kişi veya kişiler zararlı e-postaları hazır olan listedeki e-postalara SPAM olarak yollar. Belirtilen bu e-postalarda bir senaryo kurgulanır ve kullanıcıdan bazı kişisel bilgiler istenir, bu isteklerin altına gizlenen daha önceden hazırlanmış sahte site bilgileri girilir ve kullanıcı kendi kişisel bilgilerini bilmeden isteyerek girmiş olur (Alataş & Atan, 2007). Burada önemli olan bize gönderilen e-posta, sms ve sosyal medya uzantılarına eleştirel bir bakıştır. Genel senaryolara bakıldığında çevrimiçi dünyada herhangi bir işlem öncesinde önleyici farkındalığın ve bilginin önemli olduğu görülmektedir. Burada taklit tarzı saldırı tiplerinde URL (internet adresi) sahteciliği senaryosu oluşturulmaktadır.

Resim 2.7: TCMB Konulu Phishing Denemesi Esnasında Kullanılan E-Posta Örneği



Kaynak: Alataş, Ş., & Atan, M. (2007)

Merkezbanka.org alan adı üzerinden alınan alt alan adı olarak <http://tcmb.gov.tr.teyit.merkezbanka.org> adresi sayesinde kullanıcılar kandırılmaya çalışılmaktadır. Burada dikkat edilmesi gereken genel önleyici

güvenlik davranışımız TCMB'nin resmi internet sitesinin <http://www.tcmb.gov.tr> olduğu analizini yapmak ve bilmektir.

2- *Baiting (Yemleme)*: Kurbanı belirlenen tuzağa çekmek için merak uyandırıcı ve cazip hale getirilen bir dijital materyalin örneğin USB bellek gibi genellikle kolay bulunmasını sağlayacak halka açık kalabalık alanlara bırakılarak üzerine “gizli”, “ödeme”, “banka bilgileri” gibi etiketler eklenerek bırakılır. Kurban cihazı kendi bilgisayarına taktığı anda kötü amaçlı yazılım otomatik olarak yüklenir ve saldırganın kurbanın sistemine ulaşmasına olanak tanır. Bununla birlikte yemleme dijital biçimler de alabilir. Örneğin, saldırganlar gizlice kötü amaçlı kod içeren ücretsiz yazılım indirmeleri veya medya dosyaları sunabilir. “Gerçek olamayacak kadar iyi” fırsatlar veya “ürün hediyeleri” sunan çevrimiçi reklamlar da kurbanları kötü amaçlı yazılım indirmeye yönlendirmek için kullanılabilir. Yemlemede bir vaat vardır. Karşılığında müzik, telefon, ödül parası vaat eder, kurbanın sadece giriş yapması ve bazı kişisel bilgileri paylaşması gerekir. Bu yöntemde genellikle e-posta ve reklamlar kullanılır (Lohani, 2019).

3- *Spear Phishing (Mızraklı Kimlik Avı)*: Çok fazla kişiyi hedef almak yerine odak noktası belirli bir kişi olan saldırı türüdür. Diğer Phishing saldırı türlerine kıyasla daha zordur. Bunda saldırgan, kurbanın özellikleri, beğenileri, beğenmedikleri vb. hakkında tam bilgi edinmek zorundadır. Bu, hedefe bağlı olarak bir haftadan birkaç aya kadar sürebilir. Etkili bir şekilde yapılırsa diğer yollara kıyasla çok daha etkili ve verimli bir sosyal mühendislik yoludur. Örneğin, bir saldırgan hedeflenen BT şirketinin veya kurumunun çalışanına kritik bir güncelleme içeren bir e-posta gönderir. E-posta, saldırganın hazırlamış olduğu kötü amaçlı yazılımı içerir. Bu yazılım indirilerek yazılım güncellemesi yapılır ancak saldırganın hazırladığı kötü amaçlı sayfanın kendisinden parolalarını değiştirmelerini istediği bir sayfaya yönlendirilir burada kötü amaçlı bir bağlantı gerçekleştirilerek şirketin veya kurumun güvenliği tehlikeye atılır. Bir varlığa içeriden saldırı yapıldığı için onları tespit etmek ve meşru kullanıcılardan ayırt etmek zordur, bu da bu saldırıların diğer sosyal mühendislik saldırılarına kıyasla yüksek başarı oranını açıklar (Salahdine & Kaabouch, 2019).

4- *Whaling Phishing (Balina Avcılığı)*: Mızraklı kimlik avının bir alt türüdür. Büyük balıklar adlı şirketlerdeki yüksek görünümlü çalışanları hedef alan bir mızrak kimlik avı saldırısıdır. Bu kişiler genellikle son derece hassas bilgilere

veya büyük finansal işlemleri yetkilendirme yetkisine sahiptir ve bu da onları saldırganlar için birincil hedefler haline getirir. Balina avcılığı saldırılarında, riskler genellikle çok daha yüksektir ve saldırganlar son derece özel bir saldırı oluşturmak için ayrıntılı bilgi toplamaya daha fazla zaman harcarlar. Balina avcılığı saldırılarında kullanılan e-postalar veya mesajlar genellikle yasal sorunlar, şirket genelinde acil durumlar veya finansal krizler gibi yüksek riskli durumları simüle eder. Aciliyet duygusu, hedefi sahte bir havaleyi onaylamak veya hassas kurumsal verileri ifşa etmek gibi hızlı bir şekilde harekete geçmeye zorlamak için tasarlanır. Burada kullanılan yöntem günlük hayatımızda bireysel olarak bizlerde de etkili olduğu görülmektedir.

5- *Vishing (Sesli Oltalama)*: Kişilerin hassas bilgilerini doğrulamalarını sağlayarak ele geçirmek amacıyla manipüle etmek ve hesap ayrıntıları veya kişisel kimlik numaraları gibi hassas bilgileri almak için bankalar veya hükümet kurumları gibi meşru kurumları taklit ederek arama yapmayı içerir. Saldırganlar genellikle kurbanın hesabının tehlikeye atıldığını veya yasal sonuçlardan kaçınmak için hızlı hareket etmeleri gerektiğini iddia ederek aciliyet veya korku hissi oluştururlar.

6- *Smishing (Kısa Mesaj Oltaması)*: Kullanıcılara bankalar veya resmi kurumlardan ve servis sağlayıcılar gibi güvenilir kaynaklardan geliyormuş gibi görünen kısa mesajlar göndermeyi içerir. Mesajlar genellikle kurbanların hassas bilgilerini girmelerini sağlayan sahte web sitelerine bağlantılar içerir. Kullanıcılar bu sahte web site uzantılarına tıkladıkları anda hassas bilgileri ifşa etmek için gizlenen kötü niyetli yazılım çalışmış olur.

Sosyal mühendislik süreçlerinde yukarda da görüldüğü üzere güvenliğin sağlanması için yapılacak en etkili yöntem süreçte en zayıf halka olan insanın farkındalık kazanarak bilgilendirilmesidir (Gündüz & Daş, 2016). En yüksek güvenlik düzeyine sahip sistemler bile insan zaaflarının faydalanılarak ele geçirilen şifrelerden dolayı kolaylıkla geçilebilmektedir (Mouton vd, 2014, Abraham & Chengalur-Smith, 2010). Bilgi güvenliğinin daha verimli olmasını sağlamak için süreç, insan ve teknoloji birlikteliğinin “eğitim” etkeni ile desteklenmesi daha verimli olacak ve bu durum sosyal mühendislik karşısındaki algımızı güçlendirecektir (Gündüz & Daş, 2016).

2.4.3. Kötücül (Kötü Niyetli) Yazılım Türleri

Bilgi güvenliğinin sağlanması günümüzde oldukça önemli bir olgudur. Yukarıda belirtilen ulusal ve uluslararası raporlarda da görüldüğü üzere teknoloji günümüzde her geçen gün daha da gelişmektedir. Bunun için bilgi ve iletişim teknolojilerinde güvenlik tartışılmaz bir gerçeklik halini almıştır. Yaşamımızın hemen hemen her alanında bilgiye ulaşma ve diğer hizmetler için interneti kullanırız. Bundan dolayı kötü amaçlı yazılımların yarattığı olumsuz sonuçlardan kaçınılabilmek için bu tür yazılımları mümkün olduğunca erken tespit etme ve devre dışı bırakma ihtiyacı her geçen gün daha önemli hal almaktadır (Tahir, 2018). Kötü amaçlı yazılımlar, hassas verileri çalmak ve bulunduğu kaynaklara zarar vermek ve bunlara gerektiğinde erişmek amacıyla uzak bilgisayarları hedef alan türlü zararlı yazılımlardır. Bu türden yazılımlar, .exe dosyaları, betikler, dll'ler vb. olmak üzere sistemin arka planında birçok farklı şekilde çalışabilir. Ağa yasadışı erişim sağlayarak kötü amaçlı kodun bilgisayar ve ağ güvenliğini etkileyecek şekilde sisteme yayılması sağlanır. Güncel verilere göre, günümüzde kullanılan küresel kötü amaçlı yazılım, siber saldırıların %80'inden sorumludur (Chandy, 2022). Sıradan kullanıcıları ve sistemleri tehdit eden kötü niyetli yazılım türleri, son zamanlarda internet ve ağ teknolojilerinin gelişmesi ve kullanımının getirdiği kolaylık ile artarak yaygınlaşmaktadır (Canbek, 2005). Başlıca kötü amaçlı yazılım türleri;

1- *Polimorfik Virüs (Polymorphic Virus)*: Bu kötü amaçlı yazılım türü otonom olarak çoğalma ve polimorfik kod gibi tespit edilmekten kaçınmak için çeşitli stratejiler kullanma yeteneğine sahiptir ve kendini kodlayarak çoğaltır. Sonuç olarak, anti-virüs ve güvenlik duvarı uygulamaları bunları ortadan kaldırmaya çalışırken önemli zorluklarla karşılaşır. Temel özellikleri tespit edilmekten kaçınmak ve güvenlik araçlarını atlatmak için sisteme uyum sağlamaktır (Vasani vd, 2023). Bu yazılım türü her saldırı sırasında şifrelenir ve her kendini kodlayıp kopyalayarak çoğaldığında yeni bir şifreleme ile kendini şifreler. Polimorfik bir virüs saldırısı genellikle öngörülebilir bir yol izler. İlk olarak, siber suçlu virüs kodunu şifreler ve antivirüs yazılımı aracılığıyla fark edilmeden geçmesini sağlayacak şekilde maskeler. Virüs güvenliği aşıldıktan sonra, belirli bir algoritma aracılığıyla bilgisayar ağına yüklenir. Yazılım sisteme enfekte olduktan sonra bir düzen oluşturarak kendini değiştirir ve tamamen farklı bir

dosya gibi görünerek güvenlik araçları tarafından farkedilemez hale gelir. Bir tür şekil değiştiren virüs haline gelir. Bundan sonra virüs enfekte olduğu sisteme kalıcı ve büyük zarar verebilir hale gelecektir. Polimorfik bir virüsü engellemek için sistem güvenlik araçlarımızı sürekli güncel halde tutmak önemlidir. Bunun yanında oldukça önemli olan çeşitli web sitelerinde açılan reklamlara tıklamaktan, e-postalara eklenen şüpheli dosyaları açmaktan ve güvenli görünmeyen ücretsiz yazılımları indirmekten kaçınmaktır.

2- *Solucanlar (Worms)*: En yaygın görülen kötü amaçlı kod türünü temsil eden solucanlar bireysel kullancılardan ve çeşitli kuruluşların veri güvenliği için önemli bir risk oluşturur. Virüslerden farklı olarak solucanlar insan davranışlarından bağımsız olarak çoğalabilir. Birincil amaçları hızla yayılmak ve kaynak hedefleri yok ederek bilgisayarları etkisiz kılmaktır (Vassani vd, 2023). Bir solucan yazılımının yayılmasında kullanılan yaygın yöntemler arasında, e-posta, FTP ve HTTP gibi internet hizmetleri bulunmaktadır. Genellikle solucan yayılımında hedef sistemlerin açıklarından veya kullanıcıların solucanları aktif etmesini sağlayacak olan çeşitli sosyal mühendislik yöntemlerinden yararlanılır. Solucanlar mevcut dosyalarda değişiklik yapmayarak bellek üzerinde aktif bir şekilde yer alarak kendilerini kopyalarlar. Bilgisayar solucanları; e-posta, IM (İnternet Messaging), internet ve ağ solucanları olarak dört gruba ayrılabilir. E-posta solucanları, kötücül yazılımlar arasında en çok tercih edilen türdür (Canbek & Sağiroğlu, 2007). Bunların yanında sosyal ağlar, dosya paylaşımları, usb bellek gibi cihazlar aracılığı ile de sisteme enfekte olurlar.

3- *Truva Atı (Trojan Horse)*: Sistemlere doğrudan zarar vermek amacıyla saldırganların ana bilgisayara erişmeye çalıştığı zararlı yazılım türüdür. Truva atının faaliyetlerinin sonucu yıkıcıdır. Bilgisayarlara ve sistemlere sızmak için internet üzerinden indirilebilen dosyalar içine saklanırlar (Vassani vd, 2023). Truva atı virüsü, meşru bir program içerisine gizlenerek bilgisayara indirilen bir kötü amaçlı yazılım türüdür. Dağıtım yönteminde, saldırgan genellikle kötü amaçlı kodu meşru veya güvenilir gibi görünen yazılım içinde gizlemek için sosyal mühendislik yöntemlerinden yararlanır ve tasarladıkları kötü amaçlı yazılım ile kullanıcıların sistem erişimini ele geçirmeye çalışırlar. Genellikle e-posta veya ücretsiz indirilebilen bir yazılım içerisine gizlenir. Yazılım bilgisayar veya sistem içerisine indirildiğinde bu sistemlerin arka kapı erişimlerini elde

etmek amacıyla çalışmaya başlar ve bu süreçte kullanıcıların çevrimiçi etkinliklerini izleyerek, hassas verilerini ele geçirmeye çalışır.

Yaygın olarak kullanılan kötü amaçlı Truva atı yazılım türleri;

Arka Kapı Truva Atı (Backdoor Trojan): Bir saldırganın bilgisayar ve sistemlerine uzaktan erişmesini ve bir arka kapı kullanarak kontrolü ele geçirmesine olanak tanır. Bu türden bir kötü niyetli yazılımın amacı kurban bilgisayarlardan oluşan bir botnet ağı oluşturmaktır.

Banker Truva Atı (Bankacı): Bu zararlı yazılım türü, kullanıcıların banka hesaplarını ve finansal bilgilerini ele geçirmek için tasarlanmıştır. Kredi ve banka kartları bilgilerini, e-ödeme sistemleri ve çevrimiçi bankacılık sistemleri için hesap verilerini çalmaya çalışır.

Dağıtılmış Hizmet Reddi (DDoS): Bu zararlı program, bir ağı genellikle bir web sitesine, diğer virüs bulaşan birçok bilgisayardan birden fazla istek göndererek ağı aşırı yükleyen saldırılar gerçekleştirir. Hedef adrese aşırı yüklenilerek hizmet kesintisine ve reddine neden olunur.

İndirici Truva Atı (Trojan Downloader): Kötü amaçlı yazılımlarla enfekte olmuş programları bilgisayarlara yüklemeyi hedefler. Bu virüs reklam uyarıları ve diğer güvenilir görünen programlar içine saklanabilir.

Exploit Trojan (İstismar): Bu zararlı yazılım türü bir uygulama veya bilgisayar sistemindeki belirli güvenlik açıklarından faydalanan kod veya veri parçaları içerir. Siber suçlu, kullanıcıları kimlik avı saldırısı gibi bir yöntemle hedef alır ve ardından programdaki kodu bilinen bir güvenlik açığından faydalanmak için kullanır.

Sahte Antivirüs Truva Atı: Sahte bir antivirüs Truva Atı, meşru antivirüs yazılımlarının eylemlerini taklit eder. Zararlı yazılım, normal bir antivirüs programı gibi tehditleri tespit edip kaldırmak ve ardından var olmayan tehditleri kaldırmak için kullanıcılardan veri sızdırmak üzere tasarlanmıştır.

Anlık Mesajlaşma (IM) Truva Atı: Bu tür zararlı yazılım, kullanıcıların oturum açma bilgilerini ve parolalarını çalmak için IM servislerini hedef alır. Messenger, Skype vb. gibi programlardan oturum bilgilerini ve verilerini çalmayı hedefler.

Fidye Truva Atı: Fidye Truva Atları, bir bilgisayarın performansını düşürmeyi veya cihazdaki verilere ulaşmayı engellemeyi amaçlar, böylece kullanıcı artık bu verilere ulaşamaz ve kullanamaz. Saldırgan daha sonra, cihaz ve sistemdeki olumsuzluğu gidermek ve etkilenen verilerin kilidini açmak için bir fidye ücreti ödeyene kadar kullanıcıyı veya kuruluşu baskı altında tutar.

Uzaktan Erişim Truva Atı: Arka kapı Truva atına benzer şekilde bu kötü amaçlı yazılım bir kullanıcının saldırganın bir kullanıcının bilgisayarı üzerinde tam kontrol sağlamayı amaçlar. Siber suçlu, bilgi çalmak veya bir kullanıcıyı gözetlemek amacıyla kullandıkları uzak bir ağ bağlantısı aracılığıyla cihaza erişimi sürdürebilir (Fortinet & Kaspersky, 2025)

4- *Spyware (Casus Yazılım):* Bu zararlı yazılım türü ana bilgisayar ve sistemdeki iş ve işlemleri gözetleyerek, saldırganlar için verileri çalmayı ve onları dışarı sızdırmayı amaç edinir (Vassani vd, 2023). Casus yazılım, bir kullanıcının bilgisayarına girerek, cihazdan ve kullanıcıdan veri toplayan ve bunları kullanıcının izni olmadan üçüncü taraflara gönderen kötü amaçlı yazılım türüdür. Casus yazılım, kişisel ve hassas bilgileri reklam şirketlerine, veri toplama şirketlerine veya kötü niyetli aktörlere kar amacıyla gönderir. Saldırganlar, kullanıcıların internet kullanımı, kredi kartı ve banka hesap bilgileri gibi kullanıcı verilerini izlemek, çalmak ve satmak için bu zararlı yazılım türünü kullanır. Casus yazılımlar kullanıcılar, işletmeler ve kurumlar için tespit edilmesi zor olabilen ve ağlara ciddi zararlar verebilen en yaygın kullanılan siber saldırı yöntemlerinden biridir.

En sık kullanılan casus yazılım türleri;

Reklam Yazılımı: Bu zararlı yazılım türü cihazlarda yer alarak kullanıcıların faaliyetlerini izleyerek elde ettiği verileri reklam şirketlerine ve kötü niyetli kişilere satar. Kullanıcının cihazında istenmeyen reklamlar oluşur.

Tuş Kaydediciler: Tuş vuruşlarını kaydeden bu zararlı yazılım türü, bir tür bilgi sızdırma amacıyla geliştirilen casus yazılım türüdür. Enfekte olmuş bir

kullanıcının bilgisayarındaki tuş vuruşlarını kaydederek verileri şifrelenmiş olan günlük dosyalarına kaydeder. Bu zararlı yazılım türü kullanıcının cihazında yazdığı e-posta verilerini, parolaları, kısa mesajları ve kullanıcı adları gibi tüm bilgileri toplar ve kaydeder.

Rootkit'ler: Bu zararlı yazılım türünde saldırganlar cihaz ve sistemlerin güvenlik açıklarını istismar ederek hedef sistem ve cihazlarda yönetici olarak giriş yaparlar. Sistem ve cihazlara derinlemesine sızma yaparlar. Bu zararlı yazılım türünün tespit edilmesi oldukça zordur.

5- *İzleme Çerezleri (İnternet Çerezleri):* Web siteleri tarafından cihazlara bırakılarak kullanıcının çevrimiçi etkinliğini izlemek için kullanılır (Fortinet, 2025).

Adware (Reklam Yazılımı): Reklam destekli yazılım olarak da bilinen bu tür genellikle bir web tarayıcısı içinde bilgisayarınızda otomatik olarak reklamlar oluşturur. Bazı reklam yazılımı türleri son derece manipülatif olup kötü amaçlı diğer programlara bir arka kapı oluşturur (Kaspersky, 2025).

6- *Rootkit:* Siber suçluların tespit edilmeden makinelere erişmesini ve verilere sızmasını sağlayan bir kötü amaçlı yazılım programıdır. Bu zararlı yazılım türü bir sisteme yüklendikten sonra, siber suçlunun potansiyel olarak yönetici erişimi olabilir ve bu da dosyaları yürütmesine, sistem yapılandırmalarını değiştirmesine, etkinlikleri ve süreçleri izlemesine ve etkinlikleri gizlemesine olanak tanır.

7- *Ransomware (Fidye Yazılımı):* Bu zararlı yazılım türü siber suçlular fidye yazılımını verileri çalmak ve esasen rehin tutmak için bir araç olarak kullanırlar. Verileri yalnızca fidye ödemesi aldıklarında serbest bırakırlar. En çok fidye yazılımı saldırılarına maruz kalan kuruluşlar, kamu ve özel sektör kurumlarının yanında, kişisel bilgiler, finansal veriler ve fikri mülkiyet gibi hassas veriler yer alır.

Yukarıda belirtilen sosyal mühendislik ve türleri, zararlı yazılım ve türleri gibi süreç ve programlar internet ile birlikte oldukça gelişen bilgi iletişim teknolojilerinin yanında hayatımızın son derece önemli bir parçası haline geldiği açıkça görülmektedir. Günlük yaşantımızın önemli bir bölümü artık çevrimiçi dünyada bilgiye ulaşarak fayda sağlamakla geçmektedir. Dolayısıyla gerçek hayatta yaptığımız ve istediğimiz her şey dijital dünyadaki davranışlarımızı önemli ölçüde etkilemektedir. Gerek çalışma hayatımız gerek kişisel hayatımız

olsun birçok gereklilikleri çevrimiçi dünya olan internet üzerinden karşılanmaktadır. Bundan dolayı internet üzerinden yaptığımız her işlemin yasal ve davranışsal bir sonucu olduğunun farkındalığını kazanmak da artık yadsınamaz bir gerçektir. Belirtilen çalışma ve raporlar kapsamında dijital dünyada güvenliğin sağlanması konusunda en zayıf halka olan insanın gerekli farkındalıklar kazandırılarak birçok sorunun çözümünde başat bir rol üstleneceği tartışmasız bir gerçektir. Bunun için eğitim de bilgi güvenli ve bilgi güvenliği konusunun eğitimdeki güncelliği oldukça önemlidir.

2.5. Eğitimde Bilgi Güvenliği

Bilgi güvenliğinin sağlanmasında istenmeyen süreç ve durumlardan korunmak için bilgi güvenliği farkındalık eğitimlerini ve etkili güvenlik stratejilerini kullanabilmek oldukça önemlidir (Puhakainen, 2006; Siponen, 2001). Yapılan çalışmalar bilgi güvenliğini sağlama konusunda oldukça önemli bir etkiye sahip olan bilgi güvenliği farkındalığının eksikliği durumunda güvenlik tehditlerinin olumsuzluklarını ve güvenlik problemlerini arttırdığını belirtmektedir (Alkalbani, Deng & Kam, 2015; Chandarman & Van Niekerk, 2017; Hanus & Wu, 2016). Bu doğrultuda oldukça fazla güvenlik önlemleri de alınsa sistemlerin geliştirilmesi için oldukça fazla para harcansa bile en önemli yatırım, insanların bilinçlendirilmesi, doğru güvenlik çözümlerinin ve stratejilerinin doğru yerde ve doğru zamanda kullanılmasıdır. Bilgi güvenliği sürecini sadece teknik olarak tedbir alınan bilgisayar güvenliği süreci olarak algılanması doğru değildir. Bilgi güvenliği; insan, süreç ve teknolojinin birlikte etkili ve uyumlu bir şekilde çalışmasını gerektiren bir olgudur (Eminağaoğlu & Gökşen, 2009). Teknoloji ve internetin bilinçsiz kullanımı, insanların maddi veya manevi zararlar görmesine neden olabilecek kadar büyük tehditler taşımaktadır. Bu tehditlerin ortadan kaldırılması için bilişim teknolojilerinin doğru bir şekilde kullanılabilmesi amacıyla gerekli eğitimlerin alınması ve bu konuda kullanıcılarda yeterli bir bilinç oluşturulması oldukça önemlidir (Talan & Aktürk, 2021). Bu doğrultuda İnsan unsurunun, bilgi güvenliğinin sağlanması açısından anahtar noktası olma ihtimali ve bilgi güvenliğinin en zayıf halkası olabileceği göz önünde bulundurulmalıdır (Wagner & Brooke, 2007). Bu kapsamda yukarıda belirtilen raporlar ve çalışmalar ile bilginin kullanımı ve ulaşımında dijital dünyadaki birçok istenmeyen durum ve yazılım bizleri birtakım önleyici güvenlik önlemleri almaya zorunlu kılmaktadır.

Bunun için kaçınılmaz olan gerçek bu istenmeyen durum ve yazılımlara karşı bilişsel ve davranışsal farkındalıktır. Çoğunlukla insan davranışına bağlı olabilen (Wagner & Brooke, 2007) bilgi ve bilişim güvenliği tehditlerini en düşük seviyeye indirebilmek kullanıcıların bilgi ve bilişim güvenliği ilkelerine uygun farkındalık kazanarak buna uygun davranması ile sağlanabilir (Şahinaslan & Kaantürk, Şahinaslan & Borandağ, 2009). Bu doğrultuda eğitim kurumları bilişim güvenliği farkındalığının ve bilgisinin oluşturulmasında son derece önemli görülmektedir (Akgün, Topal, 2015). Bilginin önemli olması bilgiye erişim izni olmayan kişilerin tehditlerine ve bu tehditlerin oldukça fazla çeşitliliği, bilgi güvenliğinin sağlanması konusunda son derece etkili tedbirler almayı gerektirmektedir. En hızlı ve etkili yöntemlerden biri eğitim programları vasıtasıyla bilgi güvenliğini sağlamak konusunda farkındalık oluşturmaktır (Canbek & Sağiroğlu, 2007; Öğün & Kaya, 2013; Peltier, 2005). Bilgi güvenliği farkındalığının eğitim yolu ile kazandırılması bununda çok genç iken ve çocukların teknolojiye ilk merak duydukları yıllarda oluşturulmaya başlaması oldukça önemlidir (Avcı & Oruç, 2020).

Eğitim ortamlarında bilgi ve iletişim teknolojileri araçları ve İnternet hizmetlerine erişimdeki artış ve öğrencilerin mobil cihaz sahip olma oranlarındaki sürekli artış bilgi güvenliği konusundaki endişeleri arttırmaktadır. İnternet hizmetinin eğitim-öğretim süreçlerini geliştirmek amacıyla kullanılmasını olumsuz yönde etkilemekte ve özellikle beraberinde çeşitli bilgi güvenliği sorunları oluşturmaktadır. Ayrıca öğrencilerin mobil telefonlarından her an ulaşabildikleri hücresel veri, bilgi güvenliğini eğitim ortamları açısından da önemli bir inceleme alanı haline getirmektedir (Gökçearslan & Günbatar & Sarıtepeci, 2021). Böyle bir ortamda öğretmen, öğrenci, yönetici ve okul bilgi güvenliği bağlamında genel olarak zarar görebilecek unsurlar olarak ele alınabilir. Bilgi güvenliği tehditlerinin hem birey hem de kurum için önemi her geçen gün artmakta ve bu sorunları azaltmak için işe kokuşacak en yeni ve en ileri teknolojilerin dahi bireyler doğru davranışları sergilemedikleri sürece başarılı olması oldukça güçtür (Stanton, Stam, Mastrangelo & Jolton, 2005).

Dünyada bilgi güvenliği farkındalığını kazandırmak için uygulanan çalışmalar incelendiğinde, bilgi güvenliği unsurlarının ders içeriklerinin

müfredatlarına eklenmesi, bilgi güvenliği konusunda komisyonlar kurulması ve bilgi güvenliğine dikkat çekecek günler düzenlenmesi gibi etkinlikler yer alır. Daha önceden yalnızca ortaokul çağındaki öğrencilere verilen internetin güvenli kullanımı eğitimi günümüzde tüm ilköğretim çağındaki öğrencilere ders olarak verilmektedir (Ulaşanoğlu & Yılmaz ve Tekin, 2010).

Belirtilen hususlar kapsamında toplumun insan kaynağının, önleyici güvenlik davranışları kapsamında farkındalık kazanarak daha bilinçli, bilgili bir şekilde güven ve huzur içinde yaşaması eğitimin bir parçasıdır. Kişilerin bu gibi yeterlilikleri kazanabilmelerinin en doğru yolu nihai olarak bilginin üretildiği, öğretildiği, sunulduğu yerler olan eğitim örgütleridir (Can, 2002). Bilgi toplumunun vazgeçilmez kurumları olan eğitim örgütleri kişileri bilgi toplumuna hazırlamayı ve onları bu toplumun nitelikli birer üyesi olarak yetiştirmeyi kendilerine amaç edinmişlerdir (Can, 2002). Toplumsal değişim ve gelişimlere gerekli öncülüğü sağlayan eğitim kurumları, toplumun gelişimine katkı sağlayan tüm teknolojik gelişmeleri izlemek, kullanmak ve bunların nasıl etkin kullanıldığını öğretmek durumundadır (Vardal, 2009).

2.6. Sosyal Bilgiler Dersi ve Bilgi Güvenliği

Sosyal Bilgiler, öğrencileri yerel, ulusal ve küresel vatandaşlık yaşamına hazırlayan, zaman ve mekân içindeki bireyleri, toplulukları, sistemleri ve bunların etkileşimlerini inceleyen bir bilimdir (NCSS, 2025). Günümüzde ulusal ve küresel düzeyde zaman ve mekân içindeki bireyin artık çevrimiçi dijital dünya ile zaman ve mekandan bağımsız hale gelerek tüm sistemin bilgisine ulaşabilir hale gelmesi sosyal bilgiler dersine önemli bir görev yüklemiştir. Sosyal bilgiler dersinin bilgiye erişim ve kullanımda bireye nitelikli okuryazarlık ve nitelikli çevrimiçi vatandaşlık özelliklerinin kazandırılmasında önemi tartışılmaz bir gerçektir. Çağımızda teknolojinin oldukça hızlı geliştiği ve toplum hayatını etkilediği bilinen bir saptamadır. Teknolojinin toplumsal hayat ile bütünleşmesi ile artık toplumlar teknolojinin ortaya çıkardığı bu gelişim ve değişimlere uyum sağlamaya çalışmaktadır. Dijital vatandaşlık kavramı da teknolojinin toplum hayatına etkisi sonucunda ortaya çıkan vatandaşlığın yeni bir boyutudur (Turan & Karasu-Avcı, 2018). Sosyal bilgiler dersi, sahip olduğu zengin konu ve içerikleri sayesinde, bireyleri toplumsal yaşama hazırlar, toplumsal yaşamda sahip olması

gereken temel bilgi ve beceriler aktarılmasında etkin rol oynayarak eleştirel ve problem çözme becerisine sahip, dijital ve bilgi teknolojilerini etkin kullanan, toplumsal sorunlarla başa çıkan, değerleri içselleştirmiş bireyleri yetiştirmeyi hedefler (Yalçın, 2022). Sosyal bilgiler dersinde dijital okuryazarlık beceresine sahip olmak bilgiye ulaşmada kolaylıklar sağlar. Teknolojik okuryazarlığın bir bileşeni diyebileceğimiz dijital okuryazarlık, sosyal bilgiler dersi ve öğretim programı ile uyumlu özelliklere sahiptir. Sosyal bilgiler dersinde teknolojik araç ve gereçlerin kullanılması bilgiye ulaşma, bilgiyi düzenleme ve bilginin tasarlanması konusunda destekleyici bir rol üstlenir (Lee, Doolittle ve Hicks 2006; Crowe, 2006). Dijital iletişimin etkililiği ve kalitesi dijital okuryazarlıkla ilişkilidir. Dijital okuryazarlık, birtakım karmaşık, bilişsel, sosyolojik ve duygusal becerileri ve farkındalıkları içermektedir. Bu beceriler ve farkındalıklar kullanıcıların dijital ortamdaki etkinlik ve hedefe ulaşma derecesini belirlemektedir. Ekranlardaki grafiksel yönergeleri okumak, dijital ortamda yeni işlevsel içerikler oluşturmak, bilginin niteliğini ve geçerliliğini değerlendirmek dijital okuryazarlık etkinlikleri kapsamındadır (Altun & Alpan, 2021).

Bu doğrultuda sosyal bilgiler dersi kapsamında sosyal hayatımızda bilişsel ve duyuşsal bilgi güvenliği farkındalığı kazanmak için önemli materyallerin olması gerektiği bir gerçektir. Bilgiye ulaşmak ve bilgiyi doğru şekilde kullanabilmek açısından günümüzde karşımıza çıkan okuryazarlık becerilerinin son derece etkin olduğu anlaşılmaktadır (Demirezen & Hasgöl, 2022). Dijital okuryazarlık, çevrimiçi alandan bilgiye ulaşma ve bilgiyi analiz ve değerlendirme becerisi olarak tanımlanır. Dijital okuryazarlık dijital materyallerin farkında olma, onlara ulaşma ve organize etme, değerlendirme, yeni bilgiler ve içerikler oluşturabilme ve diğer bireyler ile iletişim kurabilme becerisidir (Martin, 2005).

3. YÖNTEM

Çalışmanın bu bölümünde araştırmanın modeli, örneklem grubu, veri toplama teknikleri ve verilerin analizine yer verilmiştir.

3.1. Araştırmanın Modeli

Bu araştırma, nitel araştırma yaklaşımına uygun olarak desenlenmiş ve nitel araştırma yöntemlerinden biri olan doküman analizi yöntemi kullanılarak gerçekleştirilmiştir. Nitel araştırmalar, önceden belirlenmiş hipotezleri test etmekten ziyade, verilerin detaylarına inerek, tümevarım yoluyla kavram ve temalara ulaşmayı hedefler. Bu bağlamda nitel araştırmacılar, anlamlı bir bütün oluşturmak amacıyla verileri gruplayarak yorumlamaya yönelirler (Özden & Saban, 2019). Christensen, Burke ve Turner'a (2015) göre, "Nitel araştırma, öncelikli olarak kelimeler, resimler ve imgeler gibi sayısal olmayan verilerin toplanmasına dayalı ampirik bir yaklaşımdır".

Araştırma sürecinde kullanılan doküman analizi yöntemi, araştırılması amaçlanan olgu ve kavramlara ilişkin bilgi içeren yazılı, görsel ya da elektronik materyallerin sistematik biçimde incelenmesini kapsar (Yıldırım & Şimşek, 2013). Bu yöntem, incelenen konuya ilişkin mevcut belgeler üzerinden analiz yapmaya olanak sağladığı için, araştırma konusunun geniş çerçevede ele alınmasını mümkün kılar (Yıldırım & Şimşek, 2018). Wiersma'ya (2000) göre, "doküman analizi, verilerin toplanması, düzenlenmesi, sistematik olarak incelenmesi ve değerlendirilmesinde kullanılan önemli bir tekniktir".

3.2. Örneklem Seçimi

Bu araştırmanın dokümanlarını 2024-2025 Sosyal Bilgiler Öğretim Programı ve ders kitabı olarak kullanılan MEB basımlı 2024 yılı 4, 5, 6, 7. Sınıf güncel ders kitapları oluşturmaktadır. Doküman incelemesine dayalı araştırmalarda Yıldırım ve Şimşek'in (2008, s. 197) belirttiği gibi "tüm doküman verisinin bir bütün olarak analize konu olması mümkün olmayabilir. Bu nedenle çoğu zaman araştırmacılar, eldeki veri setinin içinden bir örneklem oluşturmaya çalışır".

3.3. Verilerin Toplanması ve Analizi

Verilerin analizinde betimsel analiz yöntemi kullanılmıştır. Öncelikle ilgili öğretim programı ve ders kitapları taranarak bilgi güvenliği ile ilişkili içerikler belirlenmiş; ardından bu içerikler sınıf düzeylerine göre kategorize edilmiştir. Elde edilen bulgular, bilgi güvenliği kavramının farklı boyutlarıyla ele alınışını göstermek üzere sınıflandırılmıştır. Bilgi güvenliği boyutuna ait tema McCumber (1991)'ın bilgi güvenliği modeli “Bilginin karakteristiği, korunan nitelikleri” *Gizlilik, Bütünlük, Erişilebilirlik ve Bilginin durumu olarak nitelendirilen; Bilginin Transferi, Bilginin Depolanması ve Bilginin İşlenmesi süreçleri bunun yanında teknoloji, politika ve prosedürler ile eğitim ve farkındalık alanları güvenlik önlemleri başlığı altında toplanmıştır.* Ulusal Standartlar ve Teknoloji Enstitüsü (NIST, 2025)'nün 3 temel boyutu olan “*Gizlilik, Bütünlük, Erişilebilirlik*” boyutları göz önünde bulundurularak Sosyal Bilgiler Öğretim Programı (2024) ve SBD kitaplarının analiz çerçevesi belirlenmiştir.

Bu aşamada 4, 5, 6 ve 7. Sınıf SBD kitaplarının bilgi güvenliği boyutunda analiz edilen veriler alt problemler doğrultusunda tasnif edilmiş, tanımlanmış, tablolar şeklinde çerçeve oluşturulmuş ve doğrudan alıntılarla desteklenmiştir.

Veri toplama ve analiz sürecinde araştırmacı tarafından geliştirilen bir analiz formu kullanılmış; bu form aşağıdaki ölçütleri içerecek şekilde yapılandırılmıştır:

Tablo 3.1: Analiz Değerlendirme Kriterleri

İnceleme Kriteri	Alt Boyutlar/Açıklamalar
Sınıf Düzeyi	4, 5, 6, 7
Öğrenme Alanı	Örneğin: Teknoloji ve Sosyal Bilimler, Birlikte Yaşamak vb.
Kazanım (Varsa)	MEB kazanım kodu ve ifadesi
Bilgi Güvenliği Boyutu	Gizlilik / Bütünlük / Erişilebilirlik
Okuryazarlık Becerisi	Bilgi / Dijital / Görsel / Vatandaşlık vb.
Etkinlik Türü	Yazılı metin, görsel, haber, karikatür, soru, etkinlik
Teknik Kavram Kullanımı	Örneğin: URL, e-ticaret, dijital ayak izi, telif, veri güvenliği vb.
Günlük Yaşamla İlişkilendirme Durumu	Var / Yok
Açıklık ve Anlaşılabilirlik Düzeyi	Açık – Kısmen Açık – Belirsiz
Bilgi Güvenliği Bilinci Geliştirme Potansiyeli	Düşük / Orta / Yüksek

Kaynak: Yazar tarafından oluşturulmuştur.

Tablo: 3.1’de verilen inceleme kriterleri belirlenmiş alt boyutlar ile ilgili gerekli analizlerin yapılması amaçlanmıştır. Öğretim programı ve öğrenme alanlarında Bilgi Güvenliği farkındalığını arttıran bilgi, beceri, etkinlik kriterlerinde etkililiği alt boyutlar açısından değerlendirilmiştir. Bu doğrultuda farkındalık ve denetim artırıcı becerilerden en az birine yer verilip verilmediği, önleyici bilgi güvenliği bilinci geliştirme potansiyeline ne kadar öncülük ettiği analiz edilmeye çalışılmıştır.

2024-2025 Sosyal Bilgiler Dders kitapları ve 2024 Sosyal Bilgiler öğretim programında bilgi güvenliği farkındalığını artırıcı niteliklerin araştırıldığı bu çalışmada “Sosyal Bilgiler Dersi Öğretim Programının” bilgi güvenliği farkındalığını artıran amaçlar, programda yer alan kazanımlar (öğrenme çıktıları), değerler ve beceriler, Sosyal Bilgiler ders kitaplarında ise öğrenme alanı kapsamında bilgi güvenliği boyutunda öğrenme çıktıları, beceriler, etkinlikler açısından analiz edilmiş ayrıca bilgi güvenliği, dijital, bilişim, veri, internet, ağ, eleştirel düşünce, kaynak, uzantı, erişim gibi anahtar kelimeler kullanılarak içerik analizine tabi tutulmuştur. Yıldırım ve Şimşek (2008)’e göre “betimsel analiz, veri toplama unsurlarından elde edilen verilerin daha önceden belirlenen çerçeveye göre analiz edilmesidir”. Analizin belirleyici faktörlerini bilgi güvenliğinin temel unsurları olan “Gizlilik, Bütünlük, Erişilebilirlik” (ISO/IEC 27001, 2025) oluşturmaktadır. Bu çalışmada betimsel analiz Ulusal Standartlar ve Teknoloji Enstitüsüne (National Institute of Standards and Technology - NIST), (NIST, 2024) ve McCumber modelinde belirtilen üç temel boyuta göre “Gizlilik, Bütünlük, Erişilebilirlik” yapılmıştır. Bilgi güvenliği sürecini baltalayan uygulamalar içerisinde en etkilisi olan sosyal mühendislik kategorilerinde ise Anti-Phishing Çalışma Grubu (APWG) raporları dikkate alınmıştır.

4. BULGULAR

Bulgular bölümünde Sosyal Bilgiler Dersi Öğretim Programında (2024) ve Sosyal Bilgiler Ders kitaplarında (2024-2025) yer alan Bilgi Güvenliği ile ilgili beceri ve eğilimler sınıf düzeylerine göre tablolar halinde sunulmuştur. Bununla birlikte ortaokul Sosyal Bilgiler ders kitaplarında (2024-2025) yer alan bilgi güvenliğine yönelik beceri ve eğilimler yayınevi ve sınıf düzeyine göre incelenmiştir.

4.1. 2024 Sosyal Bilgiler Dersi Öğretim Programının Genel Amaçlarında Bilgi Güvenliğine İlişkin Bulgular

1739 sayılı Milli Eğitim Temel Kanununa göre Türk Milli Eğitiminin amaçlarından biri “Her derece ve türdeki ders programları ve eğitim metotlarıyla ders araç ve gereçleri, bilimsel ve teknolojik esaslara ve yeniliklere, çevre ve ülke ihtiyaçlarına göre sürekli olarak geliştirilir. Eğitimde verimliliğin artırılması ve sürekli olarak gelişme ve yenileşmenin sağlanması bilimsel araştırma ve değerlendirmelere dayalı olarak yapılır. Bilgi ve teknoloji üretmek ve kültürümüzü geliştirmekle görevli eğitim kurumları gereğince donatılıp güçlendirilir; bu yöndeki çalışmalar maddi ve manevi bakımından teşvik edilir ve desteklenir” (Md.13). “Bu madde Türk Milli Eğitiminin temel ilkeleri kısmında yer almış ders ve eğitim metotlarının teknolojik gelişmeler ve yeniliklere uyum sağlaması ülke olarak bu yeniliklerin özümsemesi, yakından takip edilmesi için gerekli beceri ve donanımın sağlanmasının önemi üzerinde durulmuştur” (MEB, 2024).

“Öğrencilerin ihtiyaç duyabilecekleri bilgiler, öğretim programında uygun becerilerle bütünleştirilerek öğrenme çıktısı olarak sunulmuştur. Bu tasarıma dayalı öğrenme sürecinin etkili bir şekilde uygulanabilmesi için konu içeriği sadeleştirilmiştir. Öğrenme çıktılarında işe koşulan beceriler arasında hiyerarşik veya taksonomiye dayalı bir yaklaşım yerine becerilerin birbirini destekleyen ve tamamlayan özellikleri benimsenmiştir” (MEB, 2024).

“Sosyal Bilgiler Dersi Öğretim Programı ile öğrencilere kavramsal beceriler (temel, bütünsel, üst düzey düşünme), alan becerileri (zamanı algılama ve kronolojik düşünme, kanıta dayalı sorgulama ve araştırma, tarihsel empati,

değişim ve sürekliliği anlama), sosyal ve duygusal öğrenme becerileri (benlik, sosyal yaşam, ortak/birleşik), okuryazarlık becerileri (bilgi, dijital, finansal, görsel, kültür, vatandaşlık, veri, sürdürülebilirlik, sanat), eğilimler (benlik, sosyal, entelektüel) ve değerlerin (adalet, aile bütünlüğü, çalışkanlık, dostluk, duyarlılık, özgürlük, sorumluluk) kazandırılması amaçlanmaktadır. Program içerisinde günlük yaşam ile köprü kurulması ve öğrencilerin gerekli becerileri gerçek yaşamla bağlantılı bir şekilde deneyimleyerek edinmeleri amaçlanmıştır” (MEB, 2024).

“Sosyal Bilgiler Dersi Öğretim Programı’nın temel öğelerinden biri de toplumsal hayat için vazgeçilmez olarak ifade edilebilecek değerlerdir. Sosyal Bilgiler Dersi Öğretim Programı doğası gereği değerler eğitiminin işe koşulduğu bir yapıya sahiptir. Bu minvalde “erdem-değer-eylem” çerçevesinde yer alan değerler, öğrenme yaşantıları sürecinde işe koşulmuştur. Öğretim programında sosyal-duygusal öğrenme becerileri, okuryazarlık becerileri ve değerler gibi programlar arası bileşenler öğrenme-öğretme uygulamaları ile ilişkilendirilerek verilmiştir. Tüm bu süreçle sosyal bilgiler derslerinin bütüncül, dikkat çekici, anlaşılır ve günlük hayat ile bağlantılı bir biçimde öğretilmesi amaçlanmıştır” (MEB, 2024).

1739 sayılı Millî Eğitim Temel Kanunu’nun 2. maddesinde ifade edilen “Türk Millî Eğitimi’nin Genel Amaçları ile Temel İlkeleri” esas alınarak hazırlanan Sosyal Bilgiler Dersi Öğretim Programı’yla öğrencilerin:

1.Bilimsel ve teknolojik gelişmelerin toplumsal hayata etkilerini değişim ve süreklilik açısından yorumlayabilmeleri,

2.Öğrenme ve araştırma süreçlerinde bilişim teknolojilerini etkin bir şekilde kullanmaları ve dijital ortamlarda güvenlik ve gizliliğe ilişkin farkındalık kazanmaları amaçlanmaktadır.

“Burada ifade edilen özel amaçların her birinin öğrenme çıktılarında karşılığı yer almaktadır. Öğrenme etkinliklerinin planlanmasında ve öğretim materyallerinin hazırlanmasında özel amaçlar ve öğrenme çıktıları bir bütün olarak değerlendirilmelidir”.

4.2. 2024 Sosyal Bilgiler Öğretim Programında ve Ders Kitaplarında Bilgi Güvenliği Bağlamında Öğrenme Alanı, Beceri ve Kazanım ile İlgili Bulgular

2024 Sosyal Bilgiler Öğretim Programında “Programlar arası bileşenler Sosyal-Duygusal öğrenme becerileri, değerler, okuryazarlık becerileri şeklinde ifade edilmiştir” (MEB, 2024).

2024 Sosyal Bilgiler Öğretim Programı’nda kavramsal beceriler ve alan becerilerinin yanı sıra sosyal-duygusal öğrenme ve okuryazarlık becerileri ile değerlere de yer verilmiştir (MEB, 2024).

“Sosyal Bilgiler dersinde öğrencilerin bilgi teknolojilerinde ve yaşam koşullarında meydana gelen değişimlere ayak uydurabilmeleri bağlamında ihtiyaç duyacakları birtakım sosyal yaşam becerilerinin geliştirilmesi amacı güdülmektedir. Bu amaçla Sosyal Bilgiler Dersi Öğretim Programı’nda yeni durumlara uyum sağlamayı, değişimi fark etmeyi ve gelişen teknolojik yenilikleri günlük hayatta uygulamayı sağlayan okuryazarlık becerilerine de yer verilmiştir” (MEB, 2024). “Sosyal Bilgiler Dersi Öğretim Programı’nda öğrencilerin vatandaşlık okuryazarlığı, bilgi okuryazarlığı, görsel okuryazarlık, dijital okuryazarlık, sanat okuryazarlığı, kültür okuryazarlığı, sürdürülebilirlik okuryazarlığı, finansal okuryazarlığı ve veri okuryazarlığı becerilerine yer verilmiştir. Öğretim uygulamalarında söz konusu okuryazarlık becerilerinin desteklenmesi için öğrencilere farklı fırsatlar sağlanmalıdır” (MEB, 2024).

Tablo 4.1: 2024 Sosyal Öğretim Programında ve Ders Kitaplarında Bilgi Güvenliği ile İlgili Bulgular Tablosu

İnceleme Kriteri	Alt Boyutlar/Açıklamalar
Sınıf Düzeyi	4, 5, 6, 7
Öğrenme Alanı	Örneğin: Teknoloji ve Sosyal Bilimler, Birlikte Yaşamak
Kazanım (Varsa)	MEB kazanım kodu ve ifadesi
Bilgi Güvenliği Boyutu	Gizlilik / Bütünlük / Erişilebilirlik
Okuryazarlık Becerisi	Bilgi / Dijital / Görsel / Vatandaşlık
Etkinlik Türü	Yazılı metin, görsel, haber, karikatür, soru, etkinlik
Teknik Kavram Kullanımı	Örneğin: URL, e-ticaret, dijital ayak izi, telif, veri güvenliği
Günlük Yaşamla İlişkilendirme Durumu	Var / Yok
Açıklık ve Anlaşılabilirlik Düzeyi	Açık – Kısmen Açık – Belirsiz
Bilgi Güvenliği Bilinci Geliştirme Potansiyeli	Düşük / Orta / Yüksek

Kaynak: Yazar tarafından oluşturulmuştur.

Tablo: 4.1’de verilen inceleme kriterleri belirlenmiş alt boyutlar ile ilgili gerekli analizlerin yapılması amaçlanmıştır. Öğretim programı ve öğrenme alanlarında Bilgi Güvenliği farkındalığını arttıran bilgi, beceri, etkinlik kriterlerinde etkililiği alt boyutlar açısından değerlendirilmiştir. Bu doğrultuda farkındalık ve denetim artırıcı becerilerden en az birine yer verilip verilmediği, önleyici bilgi güvenliği bilinci geliştirme potansiyeline ne kadar öncülük ettiği analiz edilmeye çalışılmıştır.

4.2.1. 2024 Sosyal Bilgiler Öğretim Programında Bilgi Güvenliği Boyutu ile İlgili Bulgular

Bu bölümde 2024 Sosyal Bilgiler Öğretim Programı Öğrenme Alanına ilişkin bulgular incelenmiştir. 2024 Sosyal Bilgiler Öğretim Programı bilgi güvenliğini doğrudan içine alan öğrenme alanının “Teknoloji ve Sosyal Bilimler” öğrenme alanı olduğu görülmüştür.

“Teknoloji ve Sosyal Bilimler öğrenme alanında dijital ortamlarda güvenlik ve gizliliğe, teknolojik ürünlerin bilinçli kullanımına, buluşlar ve teknolojik ürünlerin toplum hayatına etkilerine, teknolojinin kültürel değişime etkisine; telif, patent ve fikrî mülkiyet haklarına, bilimsel ve teknolojik gelişmelerin toplumsal hayata etkilerine, toplumsal hayatta karşılaşılabilecek problemlerin çözüm yollarına değinilmiştir” (MEB, 2024).

“Teknoloji ve Sosyal Bilimler öğrenme alanında öğrencilerin çevrim içi ortamları güvenli bir biçimde kullanabilmeleri için almaları gereken önlemlerin neler olduğunu belirleyerek çevrim içi ortamlarda güvenlik ve gizliliğe ilişkin farkındalık kazanmalarının amaçlandığı” (MEB, 2024) belirtilmiştir.

4.2.2. 2024 Sosyal Bilgiler 4.Sınıf Ders Kitabında Bilgi Güvenliği Boyutu ile İlgili Bulgular

İncelenen 4. sınıf sosyal bilgiler ders kitabında “Teknoloji ve Sosyal Bilimler” öğrenme alanında doğrudan “çevrim içi ortamda uyulması gereken güvenlik kurallarını eylemlerine yansıtır” şeklinde öğrenme çıktısı verilmiştir.

4. sınıf Sosyal Bilgiler ders kitabı bilgi güvenliği açısından değerlendirildiğinde;

Her öğrenme alanında “Genel Ağ” haberine yer verilmiş, ayrıca öneri kısımlarında ilgili etkinliğin bulunduğu genel ağ adresi uzantısı belirtilmiş ve bu ağ adresine gidilerek yapılan etkinliklerin incelenmesi istenmiştir. Bu kapsamda ağ adreslerinin yer aldığı alan adlarındaki anlamlarının belirtilmediği görülmüştür.

Tablo 4.2: 4.Sınıf Sosyal Bilgiler Ders Kitabında “Bilgi Güvenliği” Boyut ve Alt Kategorilerine İlişkin Bulgular

İnceleme Kriteri	Alt Boyutlar
Sınıf Düzeyi	4.Sınıf
Öğrenme Alanı	Teknoloji ve Sosyal Bilimler
Kazanım	1.Çevrim içi ortamda uyulması gereken güvenlik kurallarını eylemlerine yansıtabilme 2.Çevrim içi ortamdaki deneyimleri güvenlik kuralları çerçevesinde gözden geçirir. 3.Çevrim içi ortamda uyulması gereken güvenlik kurallarına ilişkin çıkarım yapar.
Bilgi Güvenliği Boyutu Etkiliği	Gizlilik, Bütünlük ve Erişilebilirlik
Okuryazarlık Becerisi	Dijital okuryazarlık
Etkinlik Türü	Yazılı Metin, Görsel, İnternet Bağlantı linki, Karekod
Teknik Kavram Kullanımı	Çip (Yonga), Barkod, Teknoloji, Genel Ağ, E-ticaret
Günlük Yaşamla İlişkilendirme Durumu	“Genel ağ haberi örneği”
Açıklık ve Anlaşılabilirlik Düzeyi	Kısmen açık http://www.meb.gov.tr/baglantilar/okullar/ adresi örneğinde belirtilen http://, meb.gov.tr gibi uzantıların ne anlama geldiği gibi
Bilgi Güvenliği Bilinci Geliştirme Potansiyeli	Orta

Kaynak: Yazar tarafından oluşturulmuştur.

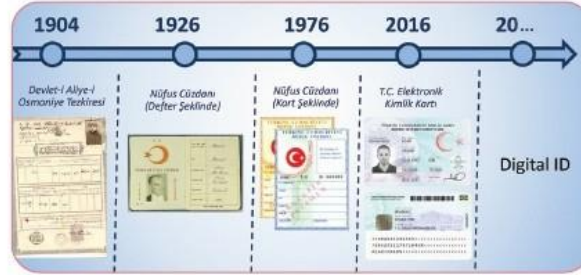
Tablo 4.2’de görüldüğü gibi 4.Sınıf SBD kitabında “Farklıyız Arkadaşız” öğrenme alanında Bilgi Güvenliği boyutlarında gizlilik, bütünlük, erişilebilirlik boyutlarına rastlanmaktadır.

Yukarıda SBD kitabındaki bulgular “*Bilgi Güvenliği Boyutlarının her birinde ayrı ayrı olarak Bilginin Transferi, Bilginin Depolanması, Bilginin İşlenmesi kategorilerinde yazılı bilgi, haber, teknik kavram ve açıklaması, fotoğraf, ölçme amaçlı soru ve etkinlik*” kısımlarına yer verilip verilmediği VAR/YOK şeklinde daha açık olarak ifade edilmeye çalışılmış ve bu açıklama kitaptan görsel ve açıklamalarla desteklenmiştir.

Tablo 4.2’de “*Farklıyız Arkadaşız*” Ünitesi incelendiğinde kimlik bilgilerimiz örneğinden yola çıkarak bilginin gizliliğine vurgu yapılmış gelişen teknoloji ile birlikte kişisel gizli bilgilerin çiplere aktarılarak güncellendiği ve ihtiyaca göre yenilendiği belirtilmiştir. Bilginin geliştirilen çip teknolojisiyle depolandığı belirtilmiştir. Kişisel bilgilerin çip içerisinde işlendiğine değinilmiş ve bunun gizliliğinin kişiye özgü olduğu belirtilmiş. Bu kişiselliğin kişiye ait olan kimliğin ve bu kimliğe özgü olan barkot kısmının bilginin gizliliğini ve güvenilirliğini sağladığı farkındalığı öğrencilerde oluşturulmaya çalışılmıştır.

Resim 4.1: Türkiye'de Kimlik Belgesi Tarihçesi

Aşağıda Türkiye'de kimlik belgesinin tarihçesine ilişkin bir zaman çizelgesi verilmiştir. Çizelgeyi inceleyiniz ardından gelecekte kimlik kartlarının ne gibi teknolojiler kullanılarak geliştirilebileceğini tartışınız.



Görsel 1.1 Türkiye'de kimlik belgesi tarihçesi

Kaynak: MEB. (2025). 4.Sınıf. S.12

Resim 4.1’de kişisel bilgilerin teknolojik olarak gelişim şeridi gösterilmiş ve bilgilerin saklandığı çeşitli teknolojilerin yıllara göre gelişimi gösterilmiştir. Burada teknolojik gelişmenin günlük hayatımıza etkisinden yola çıkarak gelecekteki değişimler hakkında eleştirel düşünme farkındalığı geliştirilmeye çalışılmıştır.

Resim 4.2: Türkiye Cumhuriyeti Kimlik Kartı Arka Yüzü



Görsel 1.4 Türkiye Cumhuriyeti kimlik kartı arka yüzü

Kaynak: MEB. (2025). 4.Sınıf. s.13

Resim 4.2’de kişiye ait bilgilerin kaydedildiği çip teknoloji gösterilmiş kimlik ve kişiye özgü olan barkot görseli verilmiştir. Taklit edilmesinin zor olduğu anlatılmaya çalışılmış ve kişiye özgü olan vurgusu yapılarak gizliliğin günlük hayatımızda dijital alanda nasıl olduğu anlatılmaya çalışılarak farkındalık oluşturulmaya çalışılmıştır.

Resim 4.3: Bilgi Notu Kutucuğu

Bilgi Notu

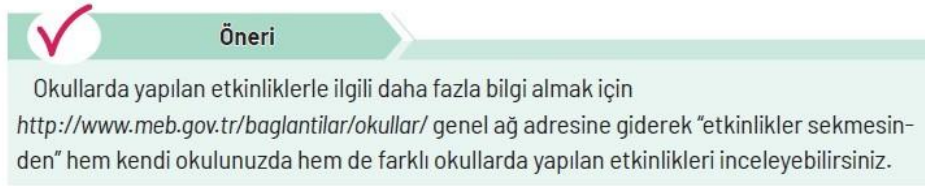
Yeni kimlik kartlarımız, 2017'nin Ocak ayından itibaren tüm Türkiye'de dağıtılmaya başlanmıştır. Yeni kimlik kartlarımız, taklit edilemeyecek şekilde tasarlanmıştır. En az on yıl dayanabilecek bir maddeden üretilmiştir. Bu yüzden yeni kimlik kartlarımız, güvenli ve dayanıklıdır. Ayrıca, boyutları nedeniyle kullanışlı bir kart özelliğindedir. Küçük olduğu için de çantamızda ya da cüzdanımızda çok yer kaplamamaktadır.

Kartta bulunan çip (yonga) sadece eşleştirilmiş olduğu T.C. kimlik numarasıyla ilgili bilgilere yönelik hazırlanmıştır. T.C. kimlik numaramız tıpkı parmak izimiz gibi benzersizdir. Bu nedenle kimlik numaramızla ilişkilendirilen bilgiler de bize özgüdür. Çipin içindeki bilgiler; kişinin varsa önceki soyadı, doğum yeri, medeni hâli yani bekâr ya da evli olması, dinî inancı, kan grubu, nüfusa kayıtlı olduğu il, ilçe, kimlik kartının verilmiş nedeni ve verilmiş tarihi gibi bilgilerdir. Çipe, gerekli görülebilecek farklı bilgilerin eklenmesinde de bir engel yoktur. Yeni kimlik kartları, nüfus müdürlüklerinden alınabilmektedir.

Kaynak: MEB. (2025). 4.Sınıf. s.14

Resim 4.3'te dijital gelişmelerin hayatımızı kolaylaştırmasından bahsedilmiş kişiye özgü olan bu kartların taklit edilememesi kişisel bilgilerimizin güvende olduğunu, içerisinde bulunan çip teknolojisinin benzersiz olan T.C. Kimlik numaramızla eşleştiği vurgulanmış burada gerekli görüldüğünde farklı bilgilerinde eklenebileceği belirtilerek fonksiyonelliği belirtilmiştir.

Resim 4.4: Öneri Kutucuğu



Kaynak: MEB. (2025). 4.Sınıf. s.21

Resim 4.4 incelendiğinde <http://www.meb.gov.tr/baglantilar/okullar/> (URL internet erişim adresi) verilmiş bu adresin; ...gov.tr alan adının sadece devlet kurumlarının kullandığı belirtilmemiş ancak belirtilen genel ağ adının Millî Eğitim Bakanlığı genel ağ adı olduğu belirtildiği için farkındalık oluşturu olduğu değerlendirilmiştir. Burada ...gov.tr uzantılarının sadece devlet kurumlarına ait olduğunun belirtilmesi sosyal mühendislik süreçlerinin olumsuz yanlarından örneğin oltalama, internet dolandırıcılığı, sahte web adresleri üzerinden dolandırma gibi olumsuz durumlara karşı önleyici güvenlik farkındalığı oluşturmaya sağlar. “.com ticari amaçlı siteler için, .org sivil toplum kuruluşları, .net teknoloji ve internet hizmetleri için, .gov devlet kurumları için, .edu eğitim kurumları için, .tr Türkiye’ye özgü alan adları” için kullanılır gibi açıklamalar ile farkındalık oluşturulabilir. Bu sayede bilgi güvenliğinin gizlilik, bütünlük, erişilebilirlik unsurlarının etkililiği sağlanabilir.

Resim 4.5: Etkinlik Kutucuğu

**4. Etkinlik**

Aşağıda verilen özelliklerden sizinle ilgili olanların yanına (✓) işareti koyunuz. Ardından arkadaşlarınızın hangi özelliklere (✓) işareti koyduğuna bakınız. Böylelikle arkadaşlarınızla aranızdaki ortak ve farklı ilgi alanlarını belirleyebilirsiniz.

1. Çizgi film izlemeyi seviyorum. (....)	6. Boş zamanlarımda gezerim. (....)
2. Futbol oynamayı biliyorum. (....)	7. Macera filmlerini seviyorum. (....)
3. Müzik dinlemekten hoşlanıyorum. (....)	8. Voleybol oynamayı seviyorum. (....)
4. Satranç oynamayı biliyorum. (....)	9. Robotik yapboz yapmayı seviyorum. (....)
5. Bilgisayar oyunları oynuyorum. (....)	10. Boş zamanlarımda kitap okurum. (....)

Kaynak: MEB. (2025). 4.Sınıf. s.23

Resim 4.5'te robotik ve bilgisayar oyunlarının günlük hayatta kullanımlarına işaret edilmiş ilgi duyulan bu alanlarda bağımlılık ve güvenlik gibi kısımlara vurgu yapılmadığı görülmüştür.

Resim 4.6: Etkinlik Kutucuğu

**6. Etkinlik**

Aşağıda verilen genel ağ haberini okuyunuz. Konya Büyükşehir Belediyesi sizce neden böyle bir çalışma yapmıştır? Düşüncelerinizi arkadaşlarınızla paylaşınız.



GENEL AĞ HABERİ

Konya Büyükşehir Belediyesi ve İl Millî Eğitim Müdürlüğü iş birliğiyle, "Suriyeli Çocukların Türk Eğitim Sistemine Entegrasyonunun Desteklenmesi Projesi" kapsamında, 29 okulda kurulan geçici eğitim merkezlerindeki öğrencilere, üç bin adet kitap seti hediye edildi.

Konya'nın Karatay ve Meram ilçelerinde, Genç Komek Yaz Okulu eğitimlerinin verildiği 29 okulda kurulan geçici eğitim merkezlerinde eğitim gören savaş mağduru Suriyeli çocukların, Türkçe dil seviyelerini geliştirmeleri amacıyla 3 bin adet kitap dağıtıldı.

Genel ağ / Erişim Tarihi: 11.12.2021 (Özetlenmiştir.)

Kaynak: MEB. (2025). 4.Sınıf. s.28

Resim 4.6'da Genel ağ haberine yer verilmiş ancak internet adresi uzantı kısmına GENEL AĞ HABERİ yazılmış, bunun yerine ulaşılan haberin internet web adresi uzantısının kullanılması bir güvenli erişim farkındalığı oluşturacağı

değerlendirilmektedir. Bununla birlikte genel ağ haberi kısmı internet tarayıcı kısmına benzetilmiş ve ileri, geri ve yenile işaretlerine yer verilmiştir.

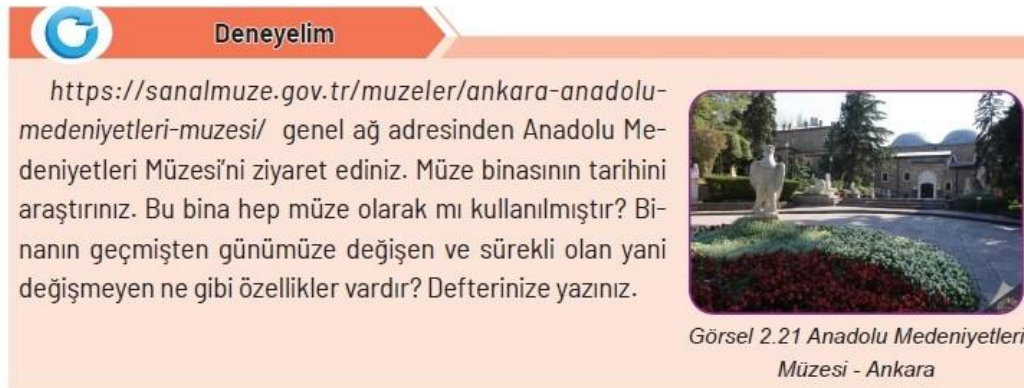
Resim 4.7: Öneri Kutucuğu



Kaynak: MEB. (2025). 4.Sınıf. s.41

Resim 4.7’de karekod ibaresine yer verilmiş ancak karekod kullanımı konusunda bilgi verilmemiştir. Karekodların kullanımında kimlik avı tehditlerinin olduğu ve bu tehditlerin çoğunda kullanıcıların kişisel bilgilerinin ele geçirilebileceği belirtilmelidir. Sahte karekod kullanımında istenmeyen sonuçların ortaya çıkabileceği ve sahte internet sitelerine yönlendirme yapılarak veri ihlallerine sebebiyet verebileceği belirtilmemiştir.

Resim 4.8: Deneyelim Kutucuğu



Kaynak: MEB. (2025). 4.Sınıf. s.45

Resim 4.8’de Anadolu Medeniyetleri müzesinin internet erişim adresi verilmiş <https://sanalmuze.gov.tr/muzeler/ankara-anadolu-medeniyetleri-muzesi/> uzantısında (https:) protokolünün açıklaması verilmemiş ve güvenli bağlantı erişimine sahiplik özellikleri belirtilmediği görülmüştür. Https: protokolünün SSL sertifikası eklenerek sitenin güvenli olduğu belirtilmemiştir. Bu sertifika “Secure Socket Layer” yani “Güvenli Giriş Katmanı” olarak bilinir ve sitenin güvenli olduğunu teyit eder.

Resim 4.9: Çinçan Oynayan Çocuklar



Kaynak: MEB. (2025). 4.Sınıf. s.51

Resim 4.9’da belirtilen etkinlikte yine karekod güvenliğinin ve karekod uzantı bilgilerinden bahsedilmediği görülmüştür.

Resim 4.10: Hasan Tahsin Bilgi Kutucuğu

HASAN TAHSİN (1888-1919)

İzmir’in Yunanlılarca işgal edilmesinin ardından şehri Yunanlara teslim etmek istemeyenler tarafından bir dernek kurulmuştu. 14 Mayıs’ı 15 Mayıs’a bağlayan gece binlerce İzmirli eski mezarlıkta toplanmıştı. Bu esnada İngiliz, Fransız, Amerikan, İtalyan ve Yunan zırhlıları İzmir Körfez’inde bulunuyordu. Kalabalığa hitap eden önemli bir isim Hukuk-u Beşer gazetesinin başyazarı olan Hasan Tahsin’di (Görsel 2.45). Halkı direnmeye çağırıyordu.

15 Mayıs 1919 sabahı saat 08.55 sıralarında Yunan askerleri gemilerden inerek karaya çıktı. Askerler yaya olarak Hükümet Konağı, kışla, Kokaryalı istikâmetinden Karantina’ya doğru yürüyüşe geçmişti. Hasan Tahsin, Konak Meydanı Kordonboyu’nda koyu renkli takım elbisesi ile bekliyordu.

Düşman askerlerinin geldiğini gören Hasan Tahsin, kalabalığın arasından sıyrılarak öne geçti. Sesli bir şekilde “Olamaz, olamaz, böyle ellerini sallaya sallaya giremezler.” dedi. Hasan Tahsin, daha sonra yanında bulunan silahla düşmana ilk ateşi açtı ve iki düşman askerini öldürdü. Hasan Tahsin’in tabancasındaki tüm fişeklerin bitmesi üzerine Yunan askerleri Hasan Tahsin’e ateş açmış, ardından süngüleyerek onu şehit etmişlerdir.

Genel ağdan alınmıştır.

Görsel 2.45 Gazeteci Hasan Tahsin

Kaynak: MEB. (2025). 4.Sınıf. s.52

Resim 4.10’da Genel ağdan alınan bir bilgi verilmiş ancak bu bilginin kaynak doğrulamasının hangi internet sitesinden alındığı belirtilmemiş. Bu türden bilgilerin güvenilirliğinin sağlanması konusunda hangi internet erişim sitelerinin güvenilir olduğu örneklenilmemiş olduğu görülmüştür.

**D. Aşağıda verilen haritayı inceleyiniz. Haritada renklerle boş bırakılan yerlere cephe-
lerin ismini yazınız. Genel ağdan ve öğretmeninizin önereceği kaynaklardan araştır-
ma yaparak verilen soruları cevaplayınız.**



Harita 2.1 Millî Mücadele Cepheler Haritası

Kaynak: MEB. (2025). 4.Sınıf. s.63

Resim 4.11’de verilen etkinlikte genel ağdan araştırma yapılması istenmiş, bilginin ulaşılması gereken güvenilir internet siteleri örneklendirilmemiş olduğu görülmüştür. Bununla birlikte bilgiye ulaşılması için genel ağ içeriğinin kullanılması beceri olarak önemli bir farkındalık sağlamıştır.

Resim 4.12: Bilgi Kutucuğu

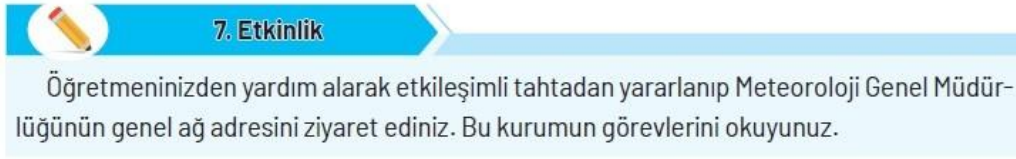
Teknoloji geliştikçe yön bulmak ya da gideceğimiz bir yere ulaşmak daha kolay hâle gelmiştir. Örneğin akıllı telefonlarda yer alan GPS teknolojisi yön bulmamızı sağlayabilir (Görsel 3.7). Bu teknoloji yoluyla GPS alıcısı bulunan cihazın uydulara gönderdiği sinyaller sayesinde o cihazın dünya üzerindeki yeri net bir şekilde saptanabilmektedir. Ardından bize yakın ve uzakta olan doğal ve beşerî unsurları ve hangi yönlerde olduklarını görebiliriz. Bu teknoloji araçlara takılan navigasyon cihazında da kullanılır. Cihaz, bulunduğumuz konumu tespit ederek gitmek istediğimiz üzerinden elde edilebilen uydu görüntülerinin de bulundu unsurları tanımamızda önemi büyüktür. Yakın çevremizi ta mada da bunu fark etmişizdir.



Görsel 3.7 GPS alıcısı

Kaynak: MEB. (2025). 4.Sınıf. s.69

Resim 4.13: Etkinlik Kutucuğu



Kaynak: MEB. (2025). 4.Sınıf. s.81

Resim 4.12 ve 4.13'te teknolojinin günlük hayatta bizlere sunduğu imkanlardan bahsedilmiş, akıllı telefon kullanımında GPS uygulamasının kullanılması ve teknik olarak nasıl çalıştığı ile ilgili bilgi verilmiştir. Resim 4.12'de konum güvenliği ve her uygulama ile konum paylaşmamız gerektiği belirtilmemiştir. Ayrıca güvenilir uygulama ve genel ağ adreslerinden doğru bilgiye ulaşma ve bilginin doğruluğunu teyit etme bilgisi verilmemiştir. Buna ek olarak uydu görüntülerinin yakın çevremizi tanımamızda önemli katkılarının olduğu söylenmiş ancak güncel bilgilere ulaşılmasının öneminin belirtilmediği görülmüştür. Bu doğrultuda Resim 4.13'te bulunan etkinlikte Meteoroloji Genel Müdürlüğü internet sitesinin ziyaret edilmesi istenmiş ancak Web bağlantı uzantısı (Url) belirtilmemiştir. Meteoroloji Genel Müdürlüğünün bağlantı adresi belirtilip ve bu bağlantı adresi üzerinden güvenilir bir devlet kurumunun internet erişim adresine nasıl ulaşılacağı konusunda farkındalık kazandırılabilir. Bu doğrultuda bilgi güvenliğinin “erişilebilirlik” özelliği farkındalık olarak kazandırılabilir olduğu değerlendirilmiştir.

Resim 4.14: Neler Öğreneceğiz Kutucuğu

Nedir, Ne Yapar? Geçmişte ve Şimdi Teknolojinin Öyküsü	Benim Ürünüm Teknolojiyi Kullanıyorum
--	--

Neler Öğreneceğiz?

- Çevremizdeki teknolojik ürünleri, kullanım alanlarına göre sınıflandırmayı,
- Teknolojik ürünlerin geçmişteki ve bugünkü kullanımlarını karşılaştırmayı,
- Kullandığımız teknolojik ürünlerin mucitlerini ve bu ürünlerin zaman içerisindeki gelişimini araştırmayı,
- Çevremizdeki ihtiyaçlardan yola çıkarak kendimize özgü ürünler tasarlamaya yönelik fikirler geliştirmeyi,
- Teknolojik ürünleri kendimize, başkalarına ve doğaya zarar vermeden kullanmayı öğreneceğiz.

Kaynak: MEB. (2025). 4.Sınıf. s.99

Resim 4.14'te “Zaman İçinde Teknoloji” Ünitesinin kazanımlarına yer verilmiştir. Günlük hayatımızda kullanılan teknolojilerden ve bunların doğru kullanımlarından bahsedilmiştir.

Resim 4.15: Nedir, Ne Yapar? Kutucuğu

4.1. NEDİR, NE YAPAR?

**Hazırlanalım**

İletişim ve ulaşım teknolojileri olmasaydı yaşamımız nasıl olurdu? Teknolojik ürünlerin günlük yaşamımızdaki yeri ve önemi nedir? Fikirlerinizi söyleyiniz.

Teknolojik ürünler, çok çeşitli alanlarda hayatımızı kolaylaştıran ve işlerimizi hızlandıran insan yapımı araçlardır. Teknolojik ürünler; günlük yaşamımızda haberleşme (Görsel 4.1), eğitim, sağlık (Görsel 4.2), sanayi, ulaşım (Görsel 4.3), güvenlik, eğlence (Görsel 4.4), bankacılık, ticaret, iletişim, mühendislik vb. birçok alanda kullanılır.

Kaynak: MEB. (2025). 4.Sınıf. s.100

Resim 4.16: Teknolojik Ürünler



Görsel 4.1 Çocuklarına telefon eden bir anne baba



Görsel 4.2 MR cihazına giren bir vatandaş



Görsel 4.3 Kalkış saatini bekleyen yüksek hızlı tren



Görsel 4.4 Sanal gerçeklik gözlüğüyle oyun oynayan bir çocuk

Kaynak: MEB. (2025). 4.Sınıf. s.100

Resim 4.15 ve resim 4.16’da teknolojik ürünlerin olmaması durumunda nasıl bir durumla karşılaşacağımız konusunda fikir üretilmesi istenmiş, bu ürünlerin hayatımızda hangi alanlarda kullanıldığı konusunda bilgi ve görsellerle desteklenerek farkındalık oluşturulmaya çalışılmıştır.

Resim 4.17: Teknolojik Ürünlerin Kullanımı

Teknolojik ürünlerin kullanım alanlarından biri iletişimdir. İletişim kurma ihtiyacı insanlar için her zaman önemli olmuştur. Günümüzde iletişim farklı teknolojik araçlar aracılığıyla kolaylıkla sağlanmaktadır (Görsel 4.5). Ayrıca birçok insan genel ağ bağlantılı cep telefonlarını kullanmayı tercih ederek sosyal medya üzerinden de yakınları ile iletişim kurabilmektedir (Görsel 4.6).



Görsel 4.5 Telefon kullanan bir insan



Görsel 4.6 Cep telefonu kullanan bir insan

Kaynak: MEB. (2025). 4.Sınıf. s.101

Resim 4.17’de teknoloji ve genel ağ kullanımına günlük yaşamımızdan alıntılara yer verilerek “erişilebilirlik” unsuruna yer verilmiştir. Ancak güvenli kullanımın önemi sosyal medyanın olumsuz yanlarına değinilmemiştir.

Resim 4.18: Eğitim Alanında Kullanılan Teknolojik Ürünler

Eğitim alanında da teknolojik ürünleri kullanmaktayız. Eğitim alanında kullanılan teknolojik ürünler daha iyi bir öğrenim ortamı sunmaktadır. Örneğin bilgisayarlar (Görsel 4.7), araştırma yapmak isteyen her kullanıcı için iyi bir eğitim aracıdır. Aynı zamanda genel ağ üzerinden çevrim içi olarak ulaşılabilecek ders materyalleri, dünyanın her yerindeki öğrenciler için verimli bir eğitim ortamı sağlamaktadır. Projeksiyon cihazı, etkileşimli tahta (Görsel 4.8) gibi ürünler de eğitim alanında kullanılan teknolojik ürünlerdir. Bu ürünler, eğitim faaliyetlerinin kolaylıkla yapılmasını sağlar. Örneğin birçok öğrenci, araştırma ödevlerini yaparken kütüphanelerden yararlanır. Kütüphanelerde binlerce kitap bulunur. Bu kitaplar içinden kendilerine uygun olanları bilgisayar teknolojisi sayesinde kolayca bulabilirler.



Görsel 4.7 Dizüstü bilgisayarda ders çalışan öğrenci



Görsel 4.8 Etkileşimli tahta ile ders işlenen bir sınıf

Kaynak: MEB. (2025). 4.Sınıf. s.101

Resim 4.18’de teknoloji kullanımında eğitim ve araştırma faaliyetlerinde bilgiye ulaşma ve daha kolay bir şekilde öğrenme faaliyetlerinin gerçekleştirilmesinin öneminden bahsedilmiştir.

Resim 4.19: Teknolojinin Zararları

Cep telefonlarının yaygınlaşması ve teknolojinin gelişmesi, haberleşmeyi kolaylaştırmış ancak insanlar arasındaki sosyal etkileşime olumsuz etkilerde bulunmuştur. Misafirliğe gittiğinizde insanların sohbet etmekten çok telefonlarıyla ilgilendiklerini görmüşsünüzdür. Bu durum sosyal bağları zayıflatmaktadır. Bilgisayar ve genel ağ teknolojilerinin gelişimi, öğrencilerin araştırma yapmaları için katkı sağlamış ancak bu gelişmeler aynı zamanda kitap okuma ve kütüphaneleri ziyaret etme kültürünü olumsuz yönde etkilemiştir.



Görsel 4.31 Bilgisayarda araştırma yapan öğrenci

Teknolojinin belki de en büyük zararlarından biri insanlarda bağımlılık oluşturmaktır. Teknolojik ürünlere vaktimizin önemli bir kısmını ayırıyoruz. Teknolojinin getirdiği kolaylıklar, insanların hareketsizleşmesine ve toplumdan soyutlanmasına neden oluyor. Dünya çapında obezite ile mücadele eden yaklaşık 700 milyon insanın önemli bir kısmının teknolojik ürünlere bağımlı olduğu düşünülüyor. Bu insanların obez olmasında hareketsiz bir yaşama sahip olmalarının büyük bir etkisi vardır. Ayrıca dünya çapında kanser vakalarının artışında teknolojik ürünlerin bilinçsiz kullanımından doğan zararların etkisi olduğu düşünülmektedir.

Kaynak: MEB. (2025). 4.Sınıf. s.107

Resim 4.19’da günümüzde kullanılan cep telefonlarının yaygın olması ve gelişen teknoloji ile insanların gün içinde teknoloji ürünleriyle daha fazla zaman harcamalarına sebep olduğu yönünde olumsuzluğa değinilmiştir. Ayrıca bilgisayar ve genel ağ teknolojilerinin gelişmesi bilgiye ulaşmanın kolay olmasından dolayı kütüphane ziyaretlerini olumsuz etkilediği belirtilmiş. Bu doğrultuda doğru ve güvenilir bilgiye ulaşmak amacıyla genel ağ üzerinden kütüphanelerin arşivlerine ulaşılabilirdiği belirtilmemiştir.

Resim 4.20: Teknolojinin Öyküsü

4.3. TEKNOLOJİNİN ÖYKÜSÜ

**Hazırlanalım**

Tablet bilgisayar ile masaüstü bilgisayar arasında ne gibi farklılıklar vardır? Fikirlerinizi söyleyiniz.

Teknolojik ürünler günümüzdeki görünüm ve işlevlerine ulaşmaya kadar pek çok aşamadan geçmiştir. Örneğin ilk bilgisayar bir oturma odası büyüklüğündeyken günümüz bilgisayar teknolojileri cebimizde taşıyabileceğimiz kadar küçülmüştür. Zamanla teknolojik ürünlerin insanların komutlarını yerine getirmesi de istenmiştir.

Günümüzde ise teknolojik ürünlerin insan komutlarına ihtiyaç duymadan özellikle yapay zeka kullanarak faaliyet göstermesi ön plandadır. Bu durum bize teknolojik ürünlerin birer öyküye sahip olduğunu göstermektedir.

Kaynak: MEB. (2025). 4.Sınıf. s.109

Resim 4.20’de teknoloji gelişiminin birikimli olarak ilerlediği ve zaman içerisinde bu gelişmenin devam ettiği ve günümüzde de oldukça hızlı bir şekilde gelişme gösterdiğinden bahsedilerek hayatımızı oldukça etkilediği belirtilmiştir. Burada ayrıca yapay zekâ teknolojilerine değinilmiş ve bu gelişimin bir parçası olduğu belirtilmiştir.

Resim 4.21: Kullanma Kılavuzu Örneği

Kullanma kılavuzu, teknolojik ürünleri amaçlarına uygun olarak kullanmamızda yardımcı olur. Kullanma kılavuzunda cihazları tanıtan görseller de yer almaktadır. Cihaz pille çalışıyorsa bu pilin nasıl şarj edileceği bilgisi de anlatılır. Cihazda bir problem oluştuğunda başvurulacak merkezlerin listesi de sunulan bilgiler arasındadır.

Aşağıda bir kullanım kılavuzunda bulunması gereken bölümler verilmiştir. İnceleyiniz.

MY Tablet Bilgisayar Kullanma Kılavuzu	Bakım Bilgileri
İÇİNDEKİLER Genel Bilgiler Tabletin Kurulumu Tabletin Kullanımı Bakım Bilgileri Sorun Giderme Sık Sorulan Sorular İletişim	Genel ağı bağlıyken aygıt yazılımı güncellemesi olduğunda kontrol edip yazılımı güncelleyin.
Genel Bilgiler	Sorun Giderme
Bu tablet PC yalnızca setle birlikte verilen şebeke adaptörü ile çalıştırılabilir.	Tabletinizi bilgisayarınıza usb kablo ile bağlayın. "Sorun Giderme" butonunu tıklayın. Bu işlem 3-5 dakika sürecek ve işlem bittiğinde tabletiniz kendi kenide kapanıp açılacaktır.
Tabletin Kurulumu	Sık Sorulan Sorular
Bilgisayarınızı başlatın ve tableti USB kabloyu kullanarak bilgisayarınıza bağlayın. Güç açık modunda 3 saniye boyunca "Güç düğmesine" uzun basın. Yaklaşık 100 sn. sonra sistem otomatik olarak cihazı açacaktır.	Tam dolum şarj süresi ne kadardır? En iyi sonuçlar için tam gücü doğrulamak ve ardından cihazı kullanmak üzere ilk kullanım öncesinde yaklaşık 7 ila 8 saat şarj ediniz.
Tabletin Kullanımı	İşletim sistemi nedir? General F. 7.1.2 işletim sistemine sahiptir.
Kurulum tamamlandıktan sonra modül menü simgesine tıklayın. "Tamamla" butonunu tıklayın.	İletişim
	... Elektronik İşletmesi ... Mah. ... Cad. No:... İvedik/ANKARA

Kaynak: MEB. (2025). 4.Sınıf. s.121

Resim 4.21’de en çok kullanılan teknolojik ürünlerden biri olan tablet bilgisayar kullanım kılavuzuna yer verilmiş ve kurulum aşamaları örneklendirilmiştir.

Resim 4.22: E-Ticaret

Günümüzde ürünlerin üretimi ve bizlere sunulması, farklı aşamalara sahip büyük bir küresel organizasyon şeklindedir. Örneğin bir ürünün hazırlanması için gereken teçhizatlar ve ham madde farklı ülkelerden sağlanabilmektedir. Ürünün üretildiği fabrikaların bulunduğu ülkeler ve tüketiciye sunulduğu ülkeler de farklılaşabilmektedir. Tüm bu büyük organizasyon ve ekonomik ağ yeni mesleklerin doğmasına yol açmıştır. E-ticaret uzmanlığı bunlardan biridir (Görsel 5.17).



Görsel 5.17 E-ticaret (temsili)

Günümüzde daha önce hiç duymadığımız mesleklerin ortaya çıktığı görülmektedir. Örneğin giyilebilir teknoloji tasarımcısı, sosyal medya uzmanlığı ve veri güvenliği uzmanlığı bunlardan birkaçıdır. Bazı meslekler yavaş yavaş öncelikli konumunu kaybetmektedir. Örneğin ahşap oymacılığı (Görsel 5.18), bakırcılık (Görsel 5.19) ve çömlekçilik bunlardan birkaçıdır.

Kaynak: MEB. (2025). 4.Sınıf. s.137

Resim 4. 22’de E-ticaret hakkında genel bir bilgi verilmiş teknolojinin yeni meslek alanlarını ortaya çıkardığından bahsedilmiş. Ancak E-ticaret sitelerinin güvenli olmasından ve verileri şifreli olarak saklamasından ve iletilmesinden sorumlu olduğu belirtilmemiştir. Kimlik avı saldırılarının sahte e-ticaret siteleri üzerinden gerçekleştiği kullanıcıların kişisel ve finansal verilerinin kimlik avı saldırıları ile ele geçirilebileceği belirtilmemiştir. Küresel ve ulusal e-ticaret sitelerinin güvenli ödeme altyapısı ve kişilerin veri güvenliğini sağlaması konusunda sorumlu olduğu belirtilmemiştir.

4.2.3. 2024 Sosyal Bilgiler 5.Sınıf 1.Ders Kitabında Bilgi Güvenliği Boyutu İle İlgili Bulgular

Sosyal Bilgiler 5.sınıf 1.ders kitabı bilgi güvenliği boyutu ile ilgili incelendiğinde; birçok kurum ve kuruluşun genel ağ erişim adresleri etkinlik ve genel bilgi şeklinde aktarıldığı görülmüştür. Doğrudan bilgi güvenliği ile ilgili aktarım yapan ünite veya bulguya rastlanılmamıştır. Aşağıda belirtilen görsellerde kurum ve kuruluşların genel ağ erişim adresleri verilmiş genel bilgi ve etkinliklerin yapılması istenmiştir.

Resim 4.23: Genel Ağdan Alınan Haber Örneği

Aşağıdaki haber başlıklarını inceleyiniz. Soruyu cevaplayınız.



MSB'den Kıbrıs Barış Harekatı'nın 50'nci yıl dönümü paylaşımı
"... Milli Savunma Bakanlığı (MSB), Kıbrıs Barış Harekatı'nın 50'nci yıl dönümünü kutladı..."
(Genel ağdan alınmıştır.)



Kuzey Kıbrıs Türk Cumhuriyeti'nde, Türkiye Cumhuriyeti'nin kuruluşunun 100. yıl dönümü ve 29 Ekim Cumhuriyet Bayramı törenlerle kutlandı
(Genel ağdan alınmıştır.)

Kaynak: MEB. (2025). 5.Sınıf. 1.Kitap. s.24

Resim 4.24: Örnek Olay Kutucuğu

Merhaba, ben Uğur Öğretmen (Görsel 1.30). Asrın felaketinde halkımızın gösterdiği birliktelik örneğine öğrencilerimle destek olmak istedik. Deprem bölgesine ne tür yardımlar yapabiliriz ve bu yardımları nasıl ulaştırabiliriz, diye düşüncelerimizi söyledik. Öğrencilerimle birlikte sosyal sorumluluk projesi hazırlamaya karar verdik. Proje için öncelikle öğrencileri gruplara ayırdım. Grup üyelerinin yönetici, ihtiyaç saptama, kampanya sorumlusu, kaynak belirleyici ve faaliyet yürütücü görevlerinden birini seçmelerini istedim. Grupların yapması gereken çalışmaları belirlemeden önce afet ve acil durumlarda süreci etkin bir şekilde yürüten AFAD ile sivil toplum kuruluşlarının çalışmalarını öğrencilerimden incelemelerini rica ettim. Ayrıca T.C. Millî Eğitim Bakanlığına bağlı kurum ve kuruluşların deprem bölgesinde yaptığı çalışmalara yönelik bakanlığın genel ağ sitesindeki açıklamaları okumalarını istedim. Böylece bakanlığın deprem bölgesinde yaptığı çalışmaların hazırlayacağımız sosyal yardımlaşma projesine örnek teşkil etmesini hedefledim.

Kaynak: MEB. (2025). 5.Sınıf. 1.Kitap. s.36

Resim 4.23'te genel ağdan alınan habere yer verilmiş ve kaynak belirtilmediği görülmüştür. Resim 4.24'te belirtilen bilgi kısmında Türkiye Cumhuriyeti Millî Eğitim Bakanlığına bağlı kurum ve kuruluşların deprem bölgelerinde yaptıkları çalışmaların incelenmesi istenmiştir. Burada doğrudan bilgi güvenliği ile ilgili süreçlere yer verilmemiş ancak genel ağdan araştırma ve inceleme yapmanın farkındalığı kazandırılmak istenmiştir.

Resim 4.25: Elektronik Posta Açılımı

Gruplarla yaptığımız fikir alışverişi sonrasında zayıf yönlerimizi güçlendirmek için kararlar aldık. Grup içinde iletişimi güçlendirmek adına ebeveynlerimizin izniyle elektronik posta (e-posta) adresi açtık. Basında yer alan yardım haberlerinde çanta ve boya kalemlerine de ihtiyaç olduğunu öğrendik. İhtiyaç listesine bu malzemeleri de ekledik. Sadaka kutumuza kurumsal bir güven kazandırmak için Türk Kızılay ile iletişime geçmeye karar verdik. Okulda düzenleyeceğimiz kermes için okul idaresine dilekçe ile başvurup okul idaresinden izin aldık. Kermes davetiyelerini dağıtmak üzere arkadaşlarımızdan ebeveynleri gündüz çalışanların yerine öğretmenlerimizden yardım isteme kararı aldık. Kermesin görevli listesini ve görev paylaşımını önceden belirledik. Bir taraftan etkinlik planımızı hazırlarken diğer taraftan da yapacağımız faaliyetlerle ilgili yasal izin işlemlerimizi başlatma kararı aldık. Türk Kızılaya dilekçe vererek okulumuza bağış kutusu koymalarını istedik (Görsel 1.36).

Kaynak: MEB. (2025). 5.Sınıf. 1.Kitap. s.40

Resim 4.25’te gerekli izinlerin alınarak e-posta hesabının açtırıldığı belirtilmiştir. Bu kapsamda güvenli internet kullanımı ve erişim farkındalığı sağlanarak ebeveyn kontrolünün farkındalığı sağlanmıştır.

Resim 4.26: Performans Görevi



PERFORMANS GÖREVİ

Adı: Afetlere Hazır mıyız?

Amacı: Yaşadığınız ilde meydana gelebilecek afetlerin etkilerini azaltmaya yönelik etkinlik oluşturma

Beceri: Sosyal katılım

Süre: 2 ders saati

Yönerge:

- Öğretmeniniz rehberliğinde altı grup oluşturunuz.
- Yaşadığınız ilde meydana gelebilecek iki afet belirleyiniz.
- Afet bilincine sahip olmanın afetlerin etkilerini azaltmadaki rolünü göz önünde bulundurarak bir etkinlik hazırlayınız.
- Etkinlikleri afet öncesinde evde, okulda ve çevrede alınacak tedbirler olacak şekilde gruplara dağıtınız.

..... AFETİ

1. GRUP Afet öncesi evde alınması gereken tedbirlere yönelik etkinlik hazırlayacaktır.

2. GRUP Afet öncesi okulda yapılması gerekenlere yönelik etkinlik hazırlayacaktır.

3. GRUP Afet öncesi çevrede yapılması gerekenlere yönelik etkinlik hazırlayacaktır.

..... AFETİ

4. GRUP Afet öncesi evde alınması gereken tedbirlere yönelik etkinlik hazırlayacaktır.

5. GRUP Afet öncesi okulda yapılması gerekenlere yönelik etkinlik hazırlayacaktır.

6. GRUP Afet öncesi çevrede yapılması gerekenlere yönelik etkinlik hazırlayacaktır.

- Belirlediğiniz etkinlikler için bir plan hazırlayınız ve grup içinde görev dağılımı yapınız.
- Gerekli hazırlıkları yaptıktan sonra etkinliklerinizi sunum, resim, afiş, poster olarak sınıf ortamı, çevrim içi ortamlar, okul panoları, okul bahçesi veya koridorunda paylaşınız.
- Alınacak tedbirleri belirlerken bilgi kirliliğini önlemek ve güvenilir bilgilere ulaşmak için T.C. İçişleri Bakanlığı, AFAD ve Türk Kızılay genel ağı adresinden faydalanabilirsiniz.

Kaynak: MEB. (2025). 5.Sınıf. 1.Kitap. s.80

Resim 4.26’da “Alınacak tedbirleri belirlerken bilgi kirliliğini önlemek ve güvenilir bilgilere ulaşmak için T.C. İçişleri Bakanlığı, AFAD, ve Türk Kızılay genel adreslerinden faydalanabilirsiniz” şeklinde bilgi yer almıştır. Burada doğru ve güvenilir bilgiye ulaşmanın önemi belirtilmiş ve bilgi güvenliğinin temel alanlarından birine değinilmiştir.

Resim 4.27: Bilgi Kutucuğu

Bilgi Kutusu

UNESCO Ortak Miras Listesi'ne alınma kriterleri

- İnsanlık tarihinde önemli bir aşamayı veya aşamaları gösteren bir öge olmalıdır.
- Yaşayan ya da ortadan yok olmuş bir kültürel geleneğe veya bir medeniyete yönelik tanıklık üstlenmelidir.
- Bir zaman zarfı içinde veya dünyanın bir kültürel alanında, mimarlık ya da teknoloji, anıtsal sanatlar, şehir planlama alanlarındaki gelişmeler ile ilgili insani değerler arasında önemli bir alışverişi sergilemelidir.
- Evrensel öneme sahip olaylar veya yaşayan gelenekler, fikirler, inançlar, sanatsal ve edebî eserler ile doğrudan veya somut bir biçimde ilgili olmalıdır.
- Herhangi bir özelliğiyle dikkat çeken, kitleleri etkileme gücü olan, farklı bir doğal güzelliğe ve estetik öneme sahip alanları içermelidir.

kvmgm.ktb.gov.tr

Kaynak: MEB. (2025). 5.Sınıf. 1.Kitap. s.102

Resim 4.28: Haber Örneği

**Duyarlı vatandaşın CİMER'e başvurusu ile Mardin'deki höyük koruma altına alındı**

Mardin'deki Hayırlı Höyüğü, bir vatandaşın Cumhurbaşkanlığı İletişim Merkezine (CİMER) yaptığı başvuru üzerine "1. derece arkeolojik sit alanı" ilan edildi.

Bu kapsamda, bölgede sadece bilimsel çalışmalara izin verilecek, yapılaşma söz konusu olamayacak.

(Genel ağdan alınmıştır.)

Kaynak: MEB. (2025). 5.Sınıf. 1.Kitap. s:115

Resim 4.29: Kaynak Örneği

Kaynak 8

Hititler, diğer medeniyetlerle olan ilişkilerini ve imzaladıkları belgeleri kayıt altına almıştır. Kadeş Antlaşması da bu belgelerden biridir. Mısırlılar ile Hititler arasında yapılan bu antlaşmanın bir nüshası Boğazköy kazılarında bulunmuş olup günümüzde İstanbul Arkeoloji Müzesinde sergilenmektedir (Görsel 3.42). Kadeş Antlaşması, tarihteki ilk uluslararası barış antlaşması olarak kabul edilmektedir. Modern diplomasinin temeli olan antlaşmanın bir nüshası da günümüzde New York'taki Birleşmiş Milletler Binası'nda sergilenmektedir.

ktb.gov.tr

Görsel 3.42



Kaynak: MEB. (2025). 5.Sınıf. 1.Kitap. s.134

Resim 4.27, 4.28 ve 4.29’da K lt r ve Turizm Bakanlıđı genel ađ adresinden alınan bilgiler ve g rseller ile genel ađ adresleri verilerek kurumsal bilgiye ulařma farkındalıđı sađlanmıřtır. Belirtilen genel adresleri k lt r varlıklarının sorumluluđuunda olan kurumdan dođrudan bilgi almayı i ermektedir.

4.2.4. 2024 Sosyal Bilgiler 5.Sınıf 2.Ders Kitabında Bilgi G venliđi Bađlamında Kazanım ( đrenme  ıktısı) ile İlgili Bulgular

İncelenen 5. Sınıf sosyal bilgiler ders kitabında “Teknoloji ve Sosyal Bilimler”  đrenme alanında dođrudan;

- 1- Teknolojik geliřmelerin toplum hayatına etkisi
 - 2- Teknolojik  r nlerin bilin li kullanımı adında
- Toplam 2 konuya,

Ayrıca bu  đrenme alanında dođrudan bilgi g venliđi farkındalıđı oluřturan;

- 1- Teknolojik geliřmelerin toplum hayatına etkilerini tartıřabilecek,
 - 2- Teknolojik  r nlerin bilin li kullanımının  nemine iliřkin  r n oluřturabileceksiniz řeklinde;
- Toplam 2  đrenme  ıktısı verilmiřtir.

Bu  đrenme alanında verilen anahtar kelimeler;

- 1- Dijital ayak izi
- 2- E-ticaret
- 3- Genel ađ
- 4- Teknoloji

Toplam 4 bilgi g venliđi farkındalıđı oluřturabilecek okuryazarlık geliřtirici kelimeye yer verilmiř ve tanımı yapılmıř.

Tablo 4.3: Sosyal Bilgiler 5.Sınıf 2.Ders Kitabında Bilgi Güvenliği Bağlamında Kazanım (Öğrenme Çıktısı) ile İlgili Bulgular

İnceleme Kriteri	Alt Boyutlar
Sınıf Düzeyi	5.Sınıf (2.Kitap)
Öğrenme Alanı	Teknoloji ve Sosyal Bilimler
Kazanım	1- “Teknolojik gelişmelerin toplum hayatına etkilerini tartışabilecek” 2- “Teknolojik ürünlerin bilinçli kullanımının önemine ilişkin ürün oluşturabileceksiniz” şeklinde öğrenme çıktılarına yer verilmiştir.
Bilgi Güvenliği Boyutu	Gizlilik, Bütünlük ve Erişilebilirlik boyutlarında farkındalık sağlayıcı içerikler yer almıştır. (Bakınız Görsel 15 “Teknolojik ürünlerin bilinçli kullanımı başlığı altında 3 örnek olay verilmiştir (Gizlilik, Oltalama, Şifre güvenliği) ve bu içerikler günlük yaşamdan örneklerle desteklenmiştir. Bunların yanında dijital vatandaşlık ve dijital hak ve sorumluluklar konusunda da bilgi verilmiştir.
Okuryazarlık Becerisi	Dijital okuryazarlık, Eleştirel Düşünme, Dijital Vatandaşlık
Etkinlik Türü	Yazılı Metin, Görsel, İnternet Bağlantı linki, Karekod, Genel Ağ Haberi, Etkinlik
Teknik Kavram Kullanımı	Güvenli Web, Güvenli Çocuk, Dijital ayak izi, Güvenli Web, e-ticaret
Günlük Yaşamla İlişkilendirme Durumu	Var “Genel ağ haberi örneği”, Görsel 15’te teknolojik ürünlerin bilinçli kullanımı başlığı altında 3 örnek olay verilmiş bu 3 örnek olay (Gizlilik, oltalama, şifre güvenliği) ile ilgili olduğu görülmüştür ve günlük yaşamdan örneklerle açıklanmıştır.
Açıklık ve Anlaşılabilirlik Düzeyi	5.Sınıf 2. ders kitabında hemen hemen her ünite de genel ağ haberine yer verildiği görülmüş, etkinlik ve web ulaşım adresleri için karekod kullanımı istenmiş, haklarımızı kullanma konusunda yol gösterilerek etkililik sağlanmıştır. Bu kapsamda AÇIK olarak nitelendirilebilmektedir.
Bilgi Güvenliği Bilinci Geliştirme Potansiyeli	Teknolojik ürünlerin bilinçli kullanımı başlığı (Görsel 15) altında örnekler verilmiştir. Bilgi güvenliği geliştirme potansiyeli oldukça yüksektir.

Bilgi Güvenliđi Gerektiren Dijital Teknolojiler Varlıđı	e-ticaret, e-devlet
--	---------------------

Kaynak: Yazar tarafından oluşturulmuştur.

Resim 4.30: Haber örneđi



CİMER'e (Cumhurbaşkanlıđı İletişim Merkezi) 2023'te 7 milyon 650 bin başvuru yapıldı

"... Vatandaşların dilekçe ve bilgi edinme haklarının kullanımını kolaylaştırmayı amaçlayan CİMER'e başvuru sayısı 2023'te yüzde 23 artışla 7 milyon 650 bine ulaştı.

CİMER'e istek, şikâyet, bilgi edinme, teşekkür, görüş ve öneri türlerinde başvuru yapılabilmektedir. Bu alanlarda 2023'teki başvuruların yüzde 98'i genel ağ üzerinden yapılırken yüzde 2'si posta ve şahsen müracaat yoluyla gerçekleşti..."

(Genel ağdan alınmıştır.)

Kaynak: MEB. (2025). 5.Sınıf. 2.Kitap. s.27

Resim 4.31: Etkinlik Örneği

**UYGULAYALIM**

ETKİNLİK
Adı: Siz Olsaydınız Ne Yapardınız?
Amacı: Etkin vatandaş olmanın toplum düzeni açısından önemini kavrama ve çıkarımda bulunma
Beceri: Çıkarım yapma
Süre: 2 ders saati

Yönerge:

- Kartlarda verilen toplumsal sorun örneklerini okuyunuz.
- Öğrenci listesindeki sıraya göre söz alınız.
- Kartlardaki örneklerden birini seçiniz.
- Etkin vatandaş ve etkin olmayan vatandaş olarak bu örnek durum veya olayda nasıl davranacağınızı empati yaparak söyleyiniz.
- Etkinlik sonunda vatandaşların sorumluluk değerine sahip olması ve topluma karşı görevlerini yerine getirmesinin toplumsal düzene nasıl katkıda bulunduğunu tartışınız.
- Etkinlik sürecinin kontrol listesi ile değerlendirilecektir.

Yaşadığımız ilde bir salgın hastalık ortaya çıkmıştır. İl genelinde karantina uygulanmasına karar verilmiştir. Ailenizin bazı üyeleri karantinaya uyma konusunda kararsız kalmışlardır.

Sosyal medyada görülen bir şaka, çocuklar ve gençler arasında yayılmaya başlamıştır. Ancak yapılan bu şaka gençlerin fiziki yaralanmalar yaşamasına, hatta hayati tehlikenin ortaya çıkmasına sebep olabilmektedir.

Yaşadığınız çevrede okuma yazma bilmeyen büyükleriniz bulunmaktadır. Bireysel çabalarınız, bu kişilerin okuma yazma bilmesine yeterli olmamıştır.

Mahallenizde marketler zincirinin bir şubesi bulunmaktadır. Bu markette bazı ürünlerin raf fiyatları ile ödeme noktasında ortaya çıkan fiyatlar farklılık göstermektedir. Bu durumun marketin diğer şubelerinde de yaşandığını haberlerden öğrenmişsinizdir.

Yaşadığımız şehir son yıllarda çok göç aldı ve hızla büyüdü. Yerleşme alanlarının genişlemesi sebebiyle sanayi tesisleri yerleşim alanlarının içinde kaldı. Tesislerden kaynaklanan hava ve ses kirliliği, sağlık sorunlarının artmasına sebep olmaya başladı.

Çevrenizdeki yol kenarlarına belediye ve trafik ekiplerince bisiklet yolları yapılmıştır. Ancak park edecek yer bulamayan komşularınız araçlarını bisiklet yollarına park etmektedir. Bu durum bisiklet sürücülerinin kaza yapma ihtimalini artırmaktadır.

Kaynak: MEB. (2025). 5.Sınıf. 2.Kitap. s.30

Resim 4.30 ve resim 4.31 incelendiğinde CİMER (Cumhurbaşkanlığı İletişim Merkezi) üzerinden yapılan başvurular belirtilerek vatandaşların genel ağ üzerinden oldukça yüksek oranlı yüzde 98 ile kullandıkları belirtilmiştir. Burada insanların sorunlara ve diğer isteklerine yaklaşımlarından genel ağı etkin bir şekilde kullandıkları görülmektedir.

Resim 4.32: Metin Kutucuğu

 **Metni okuyunuz. Salgın dönemiyle ilgili verilen bilgileri ve geçmiş yaşantılarınızı dikkate alarak tabloda istenen bilgileri yazınız.**

Dünyayı etkileyen bir sağlık sorunu olarak karşımıza çıkan COVID-19 (KOVİT-19) salgını, bireysel ve sosyal hayatımız üzerinde ani ve beklenmedik etkiler oluşturmuştur. COVID-19 salgını sürecinde uluslararası uçak seferleri iptal edilmiş, ülkelere giriş ve çıkışlar sınırlandırılmıştır. Aile ve akraba ziyaretleri gibi sosyal ilişkiler uzaktan yürütülmüştür. Bu durum, sosyal yaşamın kısıtlanmasına neden olmuştur. Örneğin misafirlğe gitme, arkadaşlarla buluşma gibi etkinlikler azalmış, toplantı ve konferanslar genel ağ üzerinden yapılmıştır. Ülkemizde okulların kapanmasıyla öğretmen ve öğrenciler arasındaki iletişim EBA (Eğitim Bilişim Ağı) üzerinden yapılan uzaktan eğitim ile sağlanmıştır. Herkesin evlere kapandığı bu süreçte genel ağ ve sosyal medyada geçirilen süre artmıştır. İş yerleri devlet tarafından desteklenmiş ve bazı iş yerleri de genel ağ üzerinden müşterilerine hizmet vermiştir.

Kaynak: MEB. (2025). 5.Sınıf. 2.Kitap. s.35

Resim 4.33: Dilekçe Örneği

 **Muhtarlık, belediye ve kaymakamlıklara giderek dilekçe verebiliriz. Ayrıca ülkemizdeki belediyelerin tamamına “<https://www.belediye.gov.tr>” adresinden “e-dilekçe” ile ulaşabiliriz. Aşağıdaki dilekçeyi inceleyiniz.**

... KAYMAKAMLIĞINA

İlçeniz mahallelerinden Alparslan'da ikamet eden bir mahalle sakiniyim.

Mahallemizdeki bisiklet yollarına park edilen araçlar nedeniyle bisiklet kullanırken güçlük yaşamaktayız. İlgili yerlere uyarı levhaları koyularak tedbirlerin alınmasını istiyorum.

Gereğinin yapılmasını arz ederim.

Adres:
.....
.....
e-posta:@...mail.com.tr
Telefon:

Tarih
İmza
Adı SOYADI

Kaynak: MEB. (2025). 5.Sınıf. 2.Kitap. s.55

Resim 4.32 ve 4.33'te doğrudan bilgi güvenliğiyle alakalı bilgi sunulmamış ancak toplumu ilgilendiren geniş çaplı olayların (COVID-19) meydana getirdiği olumsuzluklardan genel ağ ve dijital cihazlar ile çözüldüğü aktarılmıştır. Görsel 4.33'te ayrıca “e-dilekçe” ile belediyelere ulaşabileceğimiz

belirtilmiştir. Burada mevcut başvurular yapılırken genel ağ adresi kontrolü sağlanması şeklinde bir uyarı verilip bilgi güvenliği farkındalığı artırılır.

Resim 4.34: Bilgi Kutucuğu

Bireysel ve toplumsal ihtiyaçların karşılanması ve sorunların çözülmesinde bizlere bir takım sorumluluklar düşmektedir. Aşağıda verilen yöntemlerle sorunların çözülmesine ve ihtiyaçların karşılanmasına katkıda bulunabiliriz.

CİMER'e (Cumhurbaşkanlığı İletişim Merkezi) "ALO 150" hatından, genel ağ üzerinden, posta yoluyla veya şahsen başvuru yapabiliriz.

Yaşadığımız sorunları ifade edip sorunlarımızı çözmek ve haklarımızı arayabilmek için kolayca başvuru yapabileceğimiz kuruluşlardan biri de "Kamu Denetçiliği Kurumu"dur. Sorunlarınızın çözümü için KDK Çocuk (kdkcocuk.gov.tr) genel ağ sayfasını ziyaret etmeniz yeterli olacaktır. Kamu Denetçiliği Kurumu başvuru yapılan sorunu inceler, araştırır ve gerekirse sorunun çözümü için ilgili kurum idaresine önerilerde bulunarak sorunun çözümünü sağlar.

Görsel 4.56

KDK Çocuk tanıtımı

2 | Yakın çevrenizde veya ülkede yaşanan sorunların çözümünde ne gibi sorumluluklarınız bulunmaktadır? Söyleyiniz.

Kaynak: MEB. (2025). 5.Sınıf. 2.Kitap. s.56

Resim 4.34'te bilgi güvenliği farkındalığı doğrudan işlenmemiştir. Ancak resmi kurum dijital adresleri belirtilmiş ve kısa zamanda sorun çözümü için başvuru yapılabileceği belirtilmiştir. Bu tip içeriklerde resmi sitelerin genel ağ adreslerinin erişim öncesinde kontrol edilmesinin gerekliliği belirtilmelidir.

Resim 4.35: Düşünelim Kutucuğu

DÜŞÜNELİM

KAYNAKLARIMIZIN VERİMLİ KULLANIMI

Kaynak

- Toprağı işleyen, ekmeği dişler.
- Bir avuç altının olacağına bir avuç toprağın olsun.
- Bakarsan bağ olur, bakmazsan dağ olur.

sozluk.tdk.gov.tr

Kaynak: MEB. (2025). 5.Sınıf. 2.Kitap. s.68

Resim 4.35'te “sozluk.tdk.gov.tr” genel ağ adresi verilerek kaynak belirtilmiş ve doğru bilgiye ulaşma konusunda farkındalık sağlanmıştır.

Resim 4.36: Bilgi Kutucuğu



Kaynak: MEB. (2025). 5.Sınıf. 2.Kitap. s.105

Resim 4.36'da ekonomi alanı içerisinde dijital ve çevrimiçi faaliyetlerin yer aldığı ekonomik kategori belirtilmiştir.

Resim 4.37: Öğrenelim Kutucuğu



Kaynak: MEB. (2025). 5.Sınıf. 2.Kitap. s.122

Resim 4.37’de teknoloji tanımı yapılarak insan hayatı üzerindeki etkilerine değinilmiştir. Doğrudan bilgi güvenliği sürecinde farkındalık oluşturacak bilgiye yer verilmemiştir.

Resim 4.38: EBA Kullanımı Bilgi Kutucuğu



The image shows a graphic titled 'EBA Kullanımı Bilgi Kutucuğu'. On the left, there is a circular inset showing a hand holding a smartphone displaying a bookshelf, with colorful papers and books scattered below it. Below this, the EBA logo is displayed with the tagline 'Eğitim, daima...'. To the right, there is a text box with a book icon and the title 'EBA dijital dünyada üst sıralarda yer aldı'. The text inside the box discusses the benefits of EBA for students and researchers, mentioning its 24/7 availability and the large number of users. A quote from the Ministry of National Education (MEB) is included, stating that EBA is one of the most visited websites in Turkey and the world. The source is cited as 'Kaynak: MEB. (2025). 5.Sınıf. 2.Kitap. s.124'.

İnsanlar, genel ağ teknolojisinin sağladığı kolaylıklar sayesinde mesafe, mekân ve zaman sınırı olmaksızın istedikleri eğitimlere kolayca katılabilmektedir. Öğrenciler ve araştırmacılar, genel ağ ile dünyanın her yerinden birçok kütüphanenin dijital arşivine, sanal ansiklopedilerine erişim sağlayabilmektedir (Görsel 6.10). Bu erişim kolaylığı, farklı ülkelerden insanlarla etkileşim hâlinde birçok yabancı dil öğrenmek için geniş bir imkan sunmaktadır.

EBA dijital dünyada üst sıralarda yer aldı

"... Türkiye’de koronavirüs tedbirleri kapsamında eğitime ara verilmesinin ardından uzaktan eğitim sürecinde Eğitim Bilişim Ağı (EBA) 18 milyon öğrenci için 7 gün 24 saat kullanılabilir altyapıya kavuştu. Uzaktan eğitimde aktif kullanılan EBA, 16 milyar 348 milyon 941 bin tıklanma ile Türkiye’de ve dünyada en çok ziyaret edilen siteler arasında üst sıralarda yer aldı..."

(Genel ağdan alınmıştır.)

Görsel 6.10

eba
Eğitim, daima...

Kaynak: MEB. (2025). 5.Sınıf. 2.Kitap. s.124

Resim 4.39: Teknolojik Aletlerin Kullanımı Bilgi Kutucuğu



The image shows a graphic titled 'Teknolojik Aletlerin Kullanımı Bilgi Kutucuğu'. On the left, there is a text box with a question mark icon and the title 'Teknolojik eğitim araçlarını kullanırken nelere dikkat etmeliyiz? Düşüncelerinizi söyleyiniz.' Below this, there is a text box with the title 'Eğitim amacıyla kullanılan teknolojik araçlar sosyal hayatınızı nasıl etkiliyor? Örnekler veriniz.' On the right, there is a circular inset showing two people sitting at desks using computers. The person on the left is sitting correctly with good posture, indicated by a green checkmark. The person on the right is sitting incorrectly with poor posture, indicated by a red X. Below the inset, the text 'Görsel 6.12' is visible. The source is cited as 'Kaynak: MEB. (2025). 5.Sınıf. 2.Kitap. s.125'.

Eğitim sektöründe kullanılan bilgisayar, etkileşimli tahta, hoparlör, haricî bellek, fotokopi makinesi, yazıcı, tarayıcı, çizim tableti ve projeksiyon makinesi gibi teknolojik aletler öğrenme ve bilgiye ulaşmada kolaylık sağlamaktadır. Ancak eğitim amacıyla kullanılan tablet ve bilgisayar gibi teknolojik ürünlerin kontrolsüz kullanımı bireylerde bağımlılık yapabilmektedir. Sosyal becerilerin gelişimini engelleyerek bireylerin yalnızlaşmasına yol açabilen bu teknolojik aletler, aşırı ve kontrolsüz kullanım sonucu öğrenme ve dikkat toplamayı güçleştirerek zihinsel performansı olumsuz etkileyebilmektedir. Sağlık açısından ise duruş, işitme ve görme bozuklukları yaşanmasına yol açabilmektedir (Görsel 6.12).

2 Teknolojik eğitim araçlarını kullanırken nelere dikkat etmeliyiz? Düşüncelerinizi söyleyiniz.

Eğitim amacıyla kullanılan teknolojik araçlar sosyal hayatınızı nasıl etkiliyor? Örnekler veriniz.

Görsel 6.12

Kaynak: MEB. (2025). 5.Sınıf. 2.Kitap. s.125

Resim 4.38 ve 4.39’da genel ağ ve dijital teknolojilerin kullanımının eğitimde sağladığı faydalara değinilmiştir. Burada doğrudan bilgi güvenliği ile

ilgili süreçlere yer verilmemiş ancak bilgiye ulaşma ve paylaşma da EBA programı üzerinden olumlu aktarımlar yapılmıştır. Ayrıca dijital teknolojilerin aşırı kullanımının sağlık üzerinde olumsuz etkilerine değinilerek farkındalık oluşturulmaya çalışılmıştır.

Resim 4.40: E-Nabız Bilgi Kutucuğu

Sağlık ve iletişim alanında teknolojik ürünlerin kullanımının toplumsal hayata etkileri ile ilgili verilen kaynak metinleri okuyunuz ve soruları cevaplayınız.

Kaynak 2

Ateşölçer, ultrason, tomografi, MR (emar) cihazı, röntgen cihazı, stetoskop, diyaliz makinesi, gözlük ve işitme cihazı gibi teknolojik aletler sayesinde hastalıklar daha hızlı teşhis ve tedavi edilebilmektedir.

"e-nabız" mobil uygulaması; tüm sağlık bilgilerinizi yönetebildiğiniz, tıbbi özgeçmişinize tek bir yerden ulaşabildiğiniz bir kişisel sağlık kaydı sistemidir.

Günümüzde genel ağdan hastalıklar ve tedavi yöntemleri hakkında bilgilere ulaşılabilir. Ancak genel ağdaki her bilginin doğru olmadığı dikkate alınarak mutlaka doktora danışılmalıdır. Ayrıca röntgen, ultrason gibi cihazların yaydığı zararlı ışınlar, hem hastalara hem de bu cihazları kullanan sağlık çalışanlarına zarar verdiği için dikkatli bir kullanım gerektirmektedir.

sanayi.gov.tr

Görsel 6.13

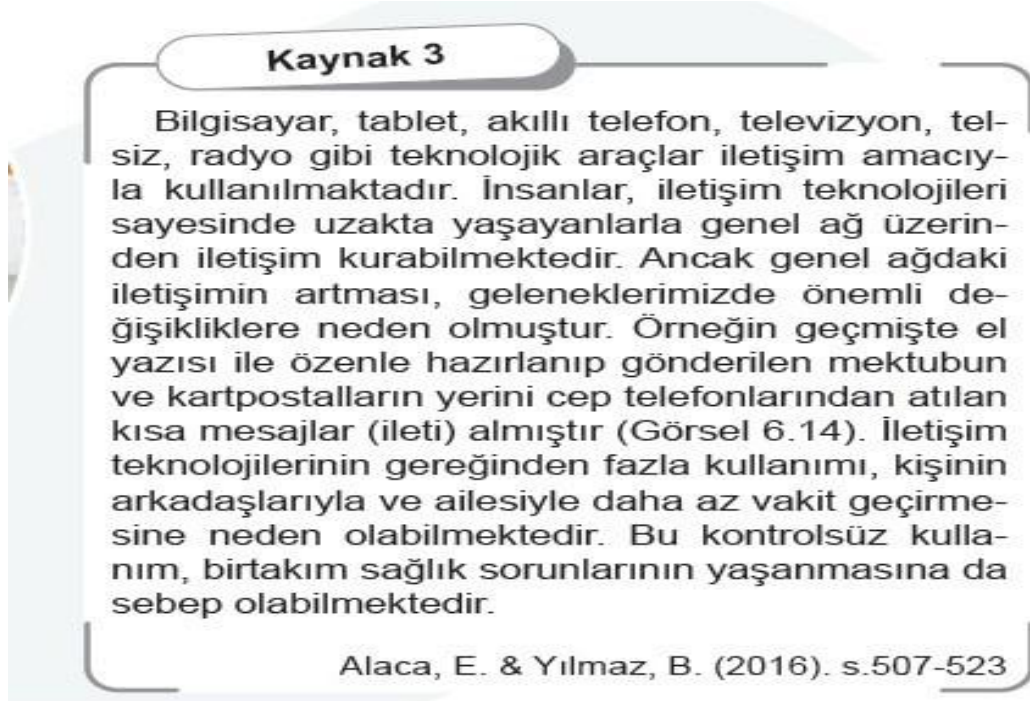
2 | "e-nabız" uygulamasının sağladığı kolaylıklar nelerdir? Örnekler veriniz.

Kaynak: MEB. (2025). 5.Sınıf. 2.Kitap. s.125

Resim 4.40'ta sağlık alanındaki özellikle e-nabız mobil uygulamasının sağladığı hayatımızı kolaylaştıran yanları aktarılıyor. Bu görsel doğrudan bilgi güvenliği farkındalığı oluşturmaya da dolaylı bir katkı sağlar. Burada kişilerin sağlık verilerinin dijital ortamlarda saklanması bilgi güvenliği açısından kritik bir konudur. Kişisel ve hassas sağlık verilerinin korunması, yetkisiz erişimlerin engellenmesi ve veri gizliliğinin sağlanması oldukça önemli bir konudur. Bu tür veriler siber saldırı ve veri sızıntısı risklerini de taşır, bu nedenle iki faktörlü kimlik doğrulama ve güvenli giriş yöntemleri gibi farkındalık sağlayıcı bilgilerin verilmesi oldukça önemlidir. Ayrıca, genel ağda bulunan sağlık bilgilerine erişirken, kaynağın güvenilirliğine dikkat edilmesi ve yanlış bilgilere karşı

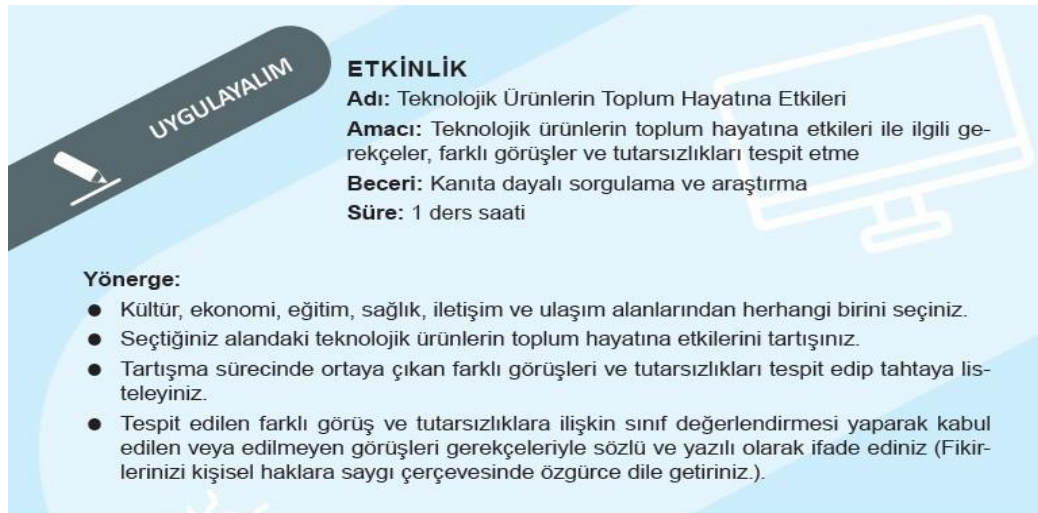
dikkatli olunması gerektiği belirtilmiş; bu da dolaylı olarak dijital okuryazarlık ve bilgi güvenliği farkındalığını destekleyici nitelik kazanmıştır.

Resim 4.41: Bilgi Kutucuğu



Kaynak: MEB. (2025). 5.Sınıf. 2.Kitap. s.126

Resim 4.42: Etkinlik Kutucuğu



Kaynak: MEB. (2025). 5.Sınıf. 2.Kitap. s.127

Resim 4.41 ve 4.42’de teknolojik ürünlerin toplum hayatı üzerindeki etkisine değinilmiş ve yaşamımızda ne gibi değişikliklere sebep olduğu üzerine

fikir üretilmesi istenmiştir. Doğrudan bilgi güvenliği farkındalığı içermese de bakış açısı kazandırmaya ve düşünmeye yönelik bir aktarım olmuştur.

Resim 4.43: Teknolojinin Etkileri

Aşağıda kültür, ekonomi, eğitim, sağlık, iletişim ve ulaşım gibi alanlardaki teknolojik gelişmelerin toplumsal hayat üzerindeki olumlu ve olumsuz etkileriyle ilgili cümleler verilmiştir. Bu cümleleri okuyunuz ve cümle numaralarını ilgili alanlara yazınız.

1. COVID-19 salgını sürecinde bilgisayar ve tablet gibi iletişim teknolojilerinin uzaktan eğitimde derslere katılımı sağlaması
2. Günlük hayatta kullandığımız cep telefonu gibi elektronik cihazların yaydığı radyasyonun insan sağlığını etkilemesi
3. İnsanların bir yerden başka bir yere ulaşmasını sağlayan uçak ve hızlı tren gibi ulaşım araçlarının yolculuk süresini kısaltması
4. Anadolu uygarlıklarına ait önemli eserlerin yer aldığı Anadolu Medeniyetleri Müzesi gibi birçok müzenin "Sanal Müze" uygulaması ile gezilmesi
5. Bilgisayar başında geçirilen sürenin artmasıyla insanlarda görme bozukluğu gibi sağlık sorunlarının yaşanması
6. Elektrikli araçların yaygınlaşması ile hava kirliliğinde azalmanın yaşanması
7. Cep telefonu, tablet ve bilgisayarın aşırı kullanımının insanları teknolojiye bağımlı hâle getirmesi
8. Eğitimde kullanılan akıllı tahtaların video oynatma, yazı yazma, şekil çizme gibi işlevlere sahip olması
9. Cep telefonundan T.C. Sağlık Bakanlığı Merkezi Hekim Randevu Sistemi ile istenilen gün ve saatte randevu alınması
10. Sosyal medyadaki bazı paylaşımların insanları şiddet ve saldırganlığa yönlendirmesi
11. Dünyadaki sosyal, ekonomik ve kültürel gelişmeler hakkında bilgi almak için televizyonun takip edilmesi
12. E-ticaretin yaygınlaşmasıyla kişisel banka hesaplarının çalınması vakalarında artış yaşanması
13. E-devlet gibi teknolojik uygulamaların hayata geçirilmesiyle vatandaşın resmî işlerinin kolayca yapılması
14. Elektrik süpürgesi, buzdolabı, bulaşık ve çamaşır makinesi gibi aletlerin ev işlerini kolaylaştırması
15. Otomobillerden çıkan egzoz gazlarının hava kirliliğine yol açması

OLUMLU ETKİLER	OLUMSUZ ETKİLER

Kaynak: MEB. (2025). 5.Sınıf. 2.Kitap. s.129

Resim 4.43'te bilgi güvenliği ile alakalı doğrudan iki önemli vurgu bulunuyor.

- 12. madde: "E-ticaretin yaygınlaşmasıyla kişisel banka hesaplarının çalınması vakalarında artış yaşanması. Bu madde dijital ortamlarda yaygınlaşan kişisel verilerin ve banka bilgilerinin çalınmasına değiniyor. Çevrimiçi ortamlarda bilgi güvenliği önlemlerinin alınmasına dikkat çekiyor.

- 13. madde: “E-devlet gibi çevrimiçi uygulamaların hayata geçirilmesiyle bireylerin resmî işlerini zaman ve emek tasarrufu sağlayarak kolayca yapabilmesi.” Bu madde dijital alanda yapılan önemli ve resmi işlemlerimizde kişisel veri güvenliği farkındalığını sağlamada etkili bir örnek sunmuş. Ancak burada e-devlet web sitesinin taklit edilerek kişisel verilerin web sitesine önce web sitesi kontrolünün yapılması sağlanmalıdır. Bu farkındalık içeriklerde sunulursa kişiler sahte web sitelerin olumsuzluklarından korunacaktır.



Resim 4.44: Teknolojik Ürünlerin Bilinçli Kullanımı

**DÜŞÜNELİM**

TEKNOLOJİK ÜRÜNLERİN BİLİNÇLİ KULLANIMI

▶ Aşağıda verilen örnek olayları okuyunuz. Öğrencilerin yaptıkları hataları yazınız ve soruları cevaplayınız.

**Örnek Olay 1**

Ezgi, fotoğraflarını sosyal medya hesabına herkesin erişebileceği bir şekilde yüklemiştir. Bir süre sonra bu fotoğrafların tanımadığı bir kişiye ait hesaptan paylaşıldığını fark etmiştir.

Hata

2 Ezgi, dijital ortamı güvenli kullanmak için nasıl davranmalıydı? Açıklayınız.

**Örnek Olay 2**

Serdar, e-postasına gelen "Hakkında şikâyet var, verilen linki tıklarsan bu sorunu çözeceğiz." mesajını görünce paniklemiş, gelen e-postaya tıklamıştır.

Hata

2 Tanımadığınız kişi ve kuruluşlardan gelen mesajları görünce ne yapmanız gerekir? Açıklayınız.

**Örnek Olay 3**

Ecem, sosyal medya hesaplarının şifrelerini kolay hatırlamak için kendi doğum tarihi, adını veya sıralı sayıları kullanmaktadır. Hatta şifrelerini unutursa hatırlatsınlar diye birkaç arkadaşına da şifrelerini söylemektedir.

Hata

2 "Dijital vatandaşlık" hakkında neler biliyorsunuz? Söyleyiniz.

2 Dijital ortamda hangi temel hak ve hürriyetlerimizi kullanabiliriz? Yazınız.

Kaynak: MEB. (2025). 5.Sınıf. 2.Kitap. s.130

Resim 4.44 incelendiğinde bilgi güvenli farkındalığı oluşturması açısından oldukça başarılıdır. Görsel de “Teknolojik Ürünlerin Bilinçli Kullanımı” başlığı altında üç örnek olay verilmiş öğrencilerin bu görselleri değerlendirmeleri istenmiştir. Her üç örnek de bilgi güvenliğiyle doğrudan ilgili temel konular (gizlilik, ortalama saldırıları, şifre güvenliği) günlük yaşamdan örneklerle açıklanmış. Öğrencilerin hatalarını tespit edip doğru olanları yazmaları istenmiş ve farkındalık oluşması sağlanmış. Dijital vatandaşlık ve dijital ortamlarda hak ve

özgürlük kavramlarına yer verilerek bilgi güvenliğine bütüncül bir bakış sağlanmıştır.

Resim 4.45: Öğrenelim Kutucuğu

ÖĞRENELİM

Teknolojinin olumlu veya olumsuz etkileri, insanların teknolojiyi kullanma biçimleriyle ilgilidir. Teknolojik ürünlerin yapım amacını ve kullanımında dikkat edilecek hususları bilmek; bu ürünleri doğru zamanda, miktarda ve yerde kullanmak, kullandığımız ürünün verimliliğini artırır. Bunun tersini düşünecek olursak kullandığımız teknolojik ürünün olumsuz sonuçları ile karşı karşıya kalırız. Bu yüzden teknolojik araçları kullanırken kendimize “Hangi cihaz ne yapmaya yarıyor, neyi yaparsam daha kullanışlı hâle getiririm, hangi amaçla kullanırsam faydası dokunur, kullanırken nelere dikkat etmeliyim?” sorularını sormalyız.

Cep telefonu, tablet ve dizüstü bilgisayar taşınabilir teknolojik ürünler olduğundan genel ağ kullanımı ile birlikte artan rolleriyle hayatımızın her alanında yer almaktadır (Görsel 6.22). Evde, okulda ve iş hayatında taşınabilir teknolojilerin kullanım alanı her geçen gün artmaktadır.

Taşınabilir teknolojik ürünlerin kullanımı ile ilgili aşağıdaki metinleri okuyunuz. Analiz kartına uzman görüşlerinin bakış açısını ve kendi görüşünüzü yazınız.

Uzman Görüşü 1

Sadece bir telefon deyip de geçmemek gerek. Akıllı telefonlar hayatımızın merkezine yerleşmiş durumda. Bu küçük aletler sayesinde hayatımız o kadar kolaylaştı ki... Tüm bilgiler elimizin altında artık. İstedığımız yeri sanal ortamda gezebiliyor, mağaza mağaza dolaşmadan alışveriş yapabiliyoruz... Daha neler neler... Son derece kaliteli fotoğraflar çekebiliyor, banka işlemlerini bir tuşla halledebiliyor, çeşitli uygulamalarla hiç bilmediğimiz yerleri kolayca bulabiliyoruz. Akıllı telefonlar çoktan bizden biri olmuş durumda. Onlar olmadan dışarıya adım bile atamıyoruz. Bize bir nefes kadar yakın bu küçük aletlere sıkı sıkıya sarılıp hayatın hızına ayak uydurmalyız.

Uzman Görüşü 2

Teknoloji insanın hayatını kolaylaştırır. Bulaşık makinesi, ütü veya çamaşır makinesinin hayatımızda olmadığını bir düşünün. Hayatımız ne kadar zorlaşırdı. Kendi küçük ama etkileri çok büyük olan akıllı telefonlar ise bizim hayatımızı kolaylaştırmak bir yana dursun âdeta hayatımızı esir almış durumda. İnsanları yalnızlaştıran bu teknolojik ürün, göz sağlığımız başta olmak üzere fiziki sağlığımızı etkilemekle beraber ruh sağlığımıza da zarar vermektedir. Yanımızdan bir an bile ayırmadığımız bu küçük aletin bağımlılığından bir an önce kendimizi ve yakınlarımızı kurtarmalyız.

Yazarlar tarafından düzenlenmiştir.

Kaynak: MEB. (2025). 5.Sınıf. 2.Kitap. s.132

Resim 4.45’te doğrudan bilgi güvenliğiyle alakalı bilgi verilmemiştir. Burada taşınabilir teknolojik ürünlerin kullanımı anlatılmış, taşınabilir teknolojik cihazların hayatımızdaki merkezi işlevi aktarılırken bilgi güvenliği süreçleri ile ilgili durumlardan bahsedilmemiştir.

Resim 4.46: Bilgi Kutucuğu

2 | Görsellerdeki çocuklardan hangisinin bilgisayar kullanırken duruş şekli doğrudur? Diğer görsellerdeki yanlışlar nelerdir? Açıklayınız.

Sahip olduğunuz veya kullandığınız taşınabilir teknolojik ürünler var mı? Varsa bunlar nelerdir? Açıklayınız.

Bu teknolojik ürünleri ne zaman, ne kadar süre, hangi ortamlarda ve hangi amaçlarla kullanıyorsunuz? Söyleyiniz.

Cep telefonu, günümüzde pek çok insan için taşınabilir, akıllı ve farklı birçok işlevi olan bir teknolojik üründür. Cep telefonları artık arama yapmak veya yazılı mesaj göndermekten daha çok şeye yarar durumdadır. Cep telefonu; genel ağa erişim aracı, fotoğraf makinesi, günlük etkinlikleri düzenleme aracı, e-postaların okunabileceği bir cihaz olarak da kullanılabilir. Bu işlevlere daha birçoğu eklenebilir.



AFAD Acil Çağrı Mobil Uygulaması hayat kurtarıyor

"... Kahramanmaraş merkezli, 7,7 büyüklüğündeki depremin ardından geliştirilen ve acil yardım çağrısı yapma imkânı veren 'AFAD Acil Çağrı Mobil Uygulaması' hayat kurtarıyor. Uygulama, telefon şarjı bitse de konum bilgileri sisteme işlendiği için afetzedelere ulaşma imkânı sağlıyor..."

(Genel ağdan alınmıştır.)



Görsel 6.26



Seyir hâlinde cep telefonu kullanımı kazalara yol açıyor

"... Sürücülerin seyrir hâlinde cep telefonu ile uğraşmaları, kazalara ve can kayıplarına yol açabilmektedir. Oysaki telefona birkaç saniyelik bir bakış bile büyük risk taşıyor. Türkiye'de günde ortalama 20-25 kişi trafik kazaları nedeniyle hayatını kaybederken bu trafik kazalarının büyük çoğunluğuna ise cep telefonu kullanımı yol açıyor..."

(Genel ağdan alınmıştır.)



Görsel 6.27

2 | Haberlerde olduğu gibi günlük hayatınızda cep telefonunun bilinçli veya bilinçsiz kullanımına verilebilecek örnekler nelerdir? Söyleyiniz.

Kaynak: MEB. (2025). 5.Sınıf. 2.Kitap. s.133

Resim 4.46'da Günlük hayatımızda çokça kullandığımız cep telefonu ile ilgili bilgi verilmiş, cep telefonundan internete erişim sağlanabileceği ve genel ağda birçok işlemin yapılabilmesi belirtilmiştir. Doğrudan bilgi güvenliğiyle alakalı bilgiler verilmese de cep telefonun etkili kullanımı anlatılmıştır.

Resim 4.47: Bilgi Kutucuğu



Görsel 6.28

Görsel 6.29

Tablet; ortalama bir kitap büyüklüğünde, birçok bilgisayar işlemini gerçekleştirebilen, kablosuz ve akıllı bir cihazdır. Tabletler, akıllı telefon ve bilgisayarda yapılabilecek hemen her şeyi yapmamıza imkân sunmaktadır. Aşağıdaki haberleri okuyunuz ve soruları cevaplayınız.



Tablet kullanımı çocukların dil gelişimini etkiliyor

"... Bir çocuğa çok küçük yaşta tablet kullanırmak, çocuk için bazı becerilerin gelişmesini geciktirebilir. Örneğin küçük yaşta yoğun bir şekilde tablet kullanmaya başlayan bir çocuğun konuşma becerileri, yaşıtlarının gerisinde kalabilir. Çünkü çocuklar, tabletle oynarken konuşma ihtiyacı hissetmezler..."

(Genel ağdan alınmıştır.)



Uzaktan eğitime tablet desteği

"... T.C. Milli Eğitim Bakanlığı, uzaktan eğitim sürecinde eğitime evinden ulaşamayan çocuklara tablet dağıtıyor. Öğrenciler, tabletler aracılığı ile derslerde daha aktif olup anlatılanları daha kolay öğrenme imkânına kavuşuyor. Ayrıca öğrenciler, TRT EBA kanallarının yanında uzaktan eğitimin önemli bir ayağı olan "EBA"ya genel ağdan ulaşabiliyorlar..."

(Genel ağdan alınmıştır.)



Tabletlerin bilinçli kullanılmasının öğrencilere ve eğitime sunacağı katkılar nelerdir? Örnekler veriniz.

Kaynak: MEB. (2025). 5.Sınıf. 2.Kitap. s.134

Resim 4.47'ye bakıldığında doğrudan bilgi güvenliği farkındalığı oluşturacak içerik olarak yeterli değildir. Tabletlerin bilinçli kullanımı aktarılırken, bilgi güvenliğiyle ilgili temel önlemler (güçlü şifre kullanımı, güvenli sitelerden içerik indirme, kişisel bilgilerin paylaşılması) de belirtilmemiştir.

Resim 4.48: Bilgi Notu Kutucuğu



Kaynak: MEB. (2025). 5.Sınıf. 2.Kitap. s.134

Resim 4.48’de “dijital ayak izi” kavramının tanımı yapılarak internet ortamındaki verilerin izlenebildiği ve kötü niyetli kişilerin eline geçmesinin mümkün olabileceği vurgulanıyor. Ayrıca çeşitli gelişmiş yazılımlar ile kişilerin internetteki etkinliklerinin takip edilebileceği ve kişilere özel teklifler sunabileceği belirtiliyor. Görsel, bilgi güvenliği farkındalığı oluşturma açısından oldukça başarılıdır. Dijital ayak izi, kişisel veri güvenliği ve çevrim içi gizlilik konularına doğrudan değinilmektedir. Bu görsel, bilgi güvenliğiyle ilgili temel kavramları (dijital ayak izi, veri güvenliği, gizlilik, bilinçli paylaşım) açık ve anlaşılır şekilde aktarmış ve bilgi güvenliği farkındalığı oluşturma açısından oldukça etkilidir.

Resim 4.49: Bilgi Kutucuğu

Dijital okuryazarlık, yazılı ve görsel kitle iletişim araçları tarafından verilen mesajların doğru algılanıp değerlendirilmesidir (Görsel 6.38). Dijital okuryazar bir çocuk, sosyal medyayı kullanmanın sadece özçekim yaparak bunları her fırsatta paylaşmak olmadığını bilir. Genel ağ hesaplarının gizliliğini ayarlar, güçlü şifreler oluşturur, hangi tür paylaşımlar yapacağı hakkında fikir sahibidir.

Çocukların kullandıkları teknolojiyi anlaması, onu güvenli ve etkili şekilde kullanabilmesi dijital okuryazarlık becerisini kazanmaları açısından önemlidir.



Kaynak: MEB. (2025). 5.Sınıf. 2.Kitap. s.137

Resim 4.50: Dijital Okuryazarlık Yeterlilikleri

Dijital okuryazarlığın hangi yeterliliklerine sahip olduğunuzu “✓” ile işaretleyiniz.

Arama motorlarını kullanabilirim, e-posta gönderebilirim, çevrim içi toplantılara katılabilirim.	☐
Genel ağda yer alan bilginin doğruluğunu farklı kaynakları inceleyerek araştırabilirim.	☐
Dijital verilere, bilgilere, içeriğe ulaşabilir ve kullanabilirim.	☐
Dijital teknolojileri kullanırken güvenlik tedbirlerini alırım.	☐
Dijital teknolojiler vasıtasıyla toplumsal faaliyetlere katılabilirim.	☐
Dijital teknolojilerin kişisel ve çevresel etkilerinin ve kullanımlarının farkındayım.	☐

Kaynak: MEB. (2025). 5.Sınıf. 2.Kitap. s.137

Resim 4.49 ve 4.50’de bilgi güvenliği farkındalığı oluşturması açısından oldukça etkili olduğu görülmektedir. Burada dijital okuryazarlık kavramı ve çocukların teknolojiyi güvenli ve etkili şekilde kullanabilmesinin önemi vurgulanıyor. Dijital okuryazarlık kavramı açıklanarak sosyal medyayı verimli kullanım, genel ağ hesaplarının gizliliğini ayarlayabilme, güçlü şifreler oluşturma gibi farkındalıkların önemi belirtiliyor. Her iki görsel de dijital okuryazarlığın bilgi güvenliğiyle ilişkili olduğunu önemli ölçüde ortaya koyuyor. Görsel 21’de dijital okuryazarlığın çeşitli yeterlilikleri listelenmiş ve bireylerden sahip oldukları yeterlilikleri işaretlemeleri istenmiş. Yeterlilikler arasında arama motoru kullanımı, e-posta gönderme, bilgi doğrulama, dijital verilere erişim, güvenlik tedbirleri alma, toplumsal faaliyetlere katılım ve dijital teknolojilerin etkilerinin farkında olma gibi başlıklar yer alıyor. “Dijital teknolojileri kullanırken güvenlik tedbirlerini alırım.” ifadesi, bilgi güvenliği farkındalığının doğrudan vurgulandığı bir yeterliliktir. Bu, şifre güvenliği, kişisel veri koruma, güvenli internet kullanımı gibi temel bilgi güvenliği davranışlarını içerir. Bilgiye erişim, bilginin kaynağını doğrulama ve dijital verilerin kullanımı gibi diğer yeterlilikler de dolaylı olarak bilgi güvenliğiyle ilişkilidir. Çünkü güvenilir bilgiye ulaşmak ve dijital ortamda bilinçli hareket etmek, bilgi güvenliği risklerini azaltır.

Resim 4.51: Teknoloji Kullanımı Bilgi Kutucuğu

Bilinçli teknoloji kullanımı ile ilgili devlet kurumları ve sivil toplum kuruluşları tarafından birçok proje ve kamu spotu hazırlanmıştır. Bunlardan bazıları şunlardır:



Güvenli Web
www.guvenliweb.org.tr
Görsel 6.39

Genel ağın güvenli, etkin ve bilinçli kullanımı konusunda başta çocuklar ve gençler olmak üzere genel ağ kullanıcılarını bilgilendirmek, eğitim çalışmaları ve bilinçli genel ağ kullanımı konusunda farkındalık oluşturmak amacıyla kurulmuştur.

Güvenli Web

Güvenli Çocuk
www.guvenlicocuk.org.tr
Görsel 6.40

Çocuklara yönelik birçok bilgi, oyun, e-kitap içerikleri ile bilinçli genel ağ ve bilgisayar kullanımını eğlendirerek öğretmek amacıyla kurulmuştur.

Genel ağı nasıl kullanmalıyım?

Türkiye Bağımlılıkla Mücadele Eğitim Programı
YESİLAY
Görsel 6.41

Türkiye Bağımlılıkla Mücadele Eğitim Programı (TBM); teknoloji bağımlılığı ile sağlıklı yaşam bölümlerinden oluşan, başta çocuklar ve gençler olmak üzere toplumun tamamını bu konularda bilgilendirmeyi ve farkındalıklarını artırmayı hedefleyen birincil önleme programıdır.

Türkiye Bağımlılıkla Mücadele Eğitim Programı

RTÜK
Radyo ve Televizyon Üst Kurulu
Görsel 6.42

İletişim teknolojileri arasında yer alan televizyon, tablet, cep telefonu ve genel ağın doğru kullanımı için birçok çalışma yapmaktadır. Akıllı İşaretler, Uyarıcı Sembol Sistemi, Medya Okuryazarlığı Projesi bu çalışmalardan bazılarıdır.

Akıllı işaretler

Karekodlarda verilen kurum ve sivil toplum kuruluşlarının genel ağ sayfalarından birini ziyaret ediniz. Sahip olduğunuz teknolojik ürünlerin bilinçli kullanımına dair edindiğiniz bilgileri yazınız.

Kaynak: MEB. (2025). 5.Sınıf. 2.Kitap. s.138

Resim 4.51’de belirtilen projeler ve kurumlar, bireyleri ve toplumu internetin güvenli ve bilinçli kullanımı konusunda bilgilendirmeyi ve farkındalık oluşturmayı amaçlıyor. “Güvenli Web” ve “Güvenli Çocuk” gibi platformlar, genel ağda güvenli davranışlar, kişisel bilgilerin korunması, zararlı içeriklerden uzak durma ve dijital ortamda karşılaşılabilecek riskler hakkında rehberlik sağlıyor. TBM, teknoloji bağımlılığı ve sağlıklı dijital yaşam konularında insanları bilinçlendiriyor; bu da dolaylı olarak bilgi güvenliği farkındalığını destekliyor.

Resim 4.52: Bilgi Kutucuğu

İzmir’deki bir ilkokulda “eTwinning” projesi kapsamında farklı illerden ve ülkelerden katılan öğrencilere yönelik çevrim içi “Genel Ağın Bilinçli ve Güvenli Kullanımı” semineri verildi (Görsel 6.45).

Gerçekleştirilen seminerde, genel ağın faydaları olduğu kadar zararlarının da olduğu ve bilinçli kullanılmadığında istenmeyen sonuçlara yol açabileceği farklı örneklerle anlatıldı. Ayrıca genel ağ ile sosyal medyanın bilinçli ve güvenli kullanımı, genel ağ ve sosyal ağların doğru kullanımı, dijital oyunların olumlu ve olumsuz etkileri, genel ağ yardım merkezi konuları da detaylı bir şekilde işlendi.



Kaynak: MEB. (2025). 5.Sınıf. 2.Kitap. s.139

Resim 4.52’de “Genel ağın bilinçli ve verimli kullanımı” semineri anlatılıyor. Anlatılan seminerin ana teması, internetin ve sosyal medyanın güvenli ve bilinçli kullanımı olarak belirlenmiş bu da bilgi güvenliği farkındalığının temelini oluşturuyor. İnternetin doğru kullanımı ve dijital ortamlarda dikkat edilmesi gerekenler anlatılmış ve bilinçlendirme sağlanmaya çalışılmıştır. Sosyal ağlar ve dijital oyunlarda kişisel bilgilerin korunması, güvenilmeyen ve kaynağı doğrulanamayan içeriklerden uzak durulması gibi konular bilgi güvenliği farkındalığını destekleyicidir.

Resim 4.53: Çalışma Yaprağı Örneği

Yönerge:

- Öğretmeninizin rehberliğinde gruplara ayrılınız.
- Teknolojik ürünlerin bilinçli kullanımı konusunda farkındalık oluşturmaya yönelik verilen video, kamu spotu veya proje örneklerini inceleyiniz.
- Verilen çalışma yaprağı yardımıyla bir teknolojik ürün belirleyiniz.

TEKNOLOJİNİN BİLİNÇLİ KULLANIMI ÇALIŞMA YAPRAĞI	
Teknolojik ürün	
Teknolojik ürünün hatalı kullanım örnekleri	
Teknolojik ürünün hatalı kullanımının yol açtığı olumsuz durumlar	
Teknolojik ürünün bilinçli kullanımı için dikkat edilmesi gereken hususlar	
Teknolojik ürüne dair farkındalık oluşturmak için tasarlanacak (kısa film, kamu spotu, afiş, karikatür, hikâye, şiir, şarkı, diyalog, kullanım kılavuzu) ürünler	

- Grubunuz tarafından geliştirilen teknolojik ürünün bilinçli kullanımına yönelik farkındalık oluşturmayı amaçlayan ürün fikirlerini sınıfta sunarak bunlara yönelik dönüt alınız.
- Dönütler doğrultusunda son şeklini verdiğiniz ürün fikirlerini, performans görevi kapsamında estetik unsurlarla zenginleştirilmiş ürünlerden birine (kısa film, kamu spotu, afiş, karikatür, hikâye, şiir, şarkı, diyalog veya kullanım kılavuzu) dönüştürünüz.
- Grubunuzun teknolojik ürünlerin bilinçli kullanımına ilişkin hazırladığı ürünleri sınıfta sununuz veya okul koridorundaki panolarda sergileyiniz.
- Ürünleriniz bütüncül dereceli puanlama anahtarı ile değerlendirilecektir.

Kaynak: MEB. (2025). 5.Sınıf. 2.Kitap. s.140

Resim 4.53'te teknolojik ürünlerin bilinçli kullanımına yönelik farkındalık kazandırmayı amaçlayan bir etkinlik bulunuyor. Teknolojik ürün ve bu ürünlerin kullanımı, yol açtığı olumsuz durumlar, bilinçli kullanım için farkındalık oluşturacak çalışmalar gibi başlıklar yer almıştır. Görsel doğrudan bilgi güvenliği ile ilgili bir bilgi ve uyarı içermiyor; ancak teknolojik ürünlerin bilinçli kullanımı bilgi güvenliği farkındalığı için önemli bir temel oluşturuyor. Bu içerikte güvenli internet kullanımı, kişisel verilerin korunması gibi bilgiler ve önlemlerin vurgulanabileceği bir alandır.

Resim 4.54: Değerlendirelim Kutucuğu

DEĞERLENDİRELİM

Aşağıda teknolojinin kullanımı ile ilgili ifadeler verilmiştir. Verilen ifadeleri bilinçli kullanım veya bilinçsiz kullanım olarak "✓" ile işaretleyiniz.

Verilen İfade	Bilinçli Kullanım	Bilinçsiz Kullanım
Sabah kalkar kalkmaz cep telefonundan gelen bildirimleri kontrol eden Hakan, kontrollere gereğinden fazla zaman harcamaktadır.	☐	☐
Sosyal medya paylaşımlarını kontrollü yapan Ecem, mevcut dostluklarını pekiştirdiği gibi arkadaşlarıyla ilişkilerinin kalitesini de artırmaktadır.	☐	☐
Bilgisayarda uzun süre vakit geçiren Serdar, derslerinde dikkat dağınıklığı yaşadığı için odaklanmada sorun yaşamaktadır.	☐	☐
Sema'nın ailesi, kızlarının uygunsuz içeriklere maruz kalma ihtimaline karşı genel ağda ebeveyn denetim araçlarını kullanmaktadır.	☐	☐
Fatih, sosyal medya hesaplarına baktıktan sonra yaptığı işe dönme süresinin uzadığını ifade etmektedir.	☐	☐
Derya bilgisayarını oyun oynamak, müzik dinlemek, araştırma veya ödev yapmak gibi amaçlarla kullanmaktadır.	☐	☐
Tunahan evinin aydınlatmasında düşük maliyet ile yüksek aydınlatma sağlayan led ampuller tercih etmektedir.	☐	☐
Yakup bilgisayara eğilerek baktığında boynunun ağrdığını ve çok yorgun hissettiğini söylemiştir.	☐	☐
Adem cep telefonunu az kullanıp ailesiyle daha fazla zaman geçirmeye özen göstermektedir.	☐	☐
Zeynep gece yatarken cep telefonunun alarmini kurmuş, cep telefonunu uçak moduna alarak yatağından uzak bir yere koymuştur.	☐	☐

Kaynak: MEB. (2025). 5.Sınıf. 2.Kitap. s.141

Resim 4.54 incelendiğinde teknolojinin bilinçli ve bilinçsiz kullanımı yönünde farkındalık oluşturulmaya çalışılmış, bilgi güvenliği ile ilgili doğrudan bir içerik yer almamıştır. Günlük hayatımızda teknoloji ve sosyal medya kullanımının bilinçli olarak kullanımına yönelik davranışların önemine dikkat çekilmiş ve dijital okuryazarlık farkındalığı kazandırılmaya çalışılmıştır.

Resim 4.55: Etkinlik Örneği

6. ÖĞRENME ALANI - DEĞERLER

Aşağıdaki tabloda değerler numaralandırılarak verilmiştir. Verilen soruları tablodaki değer numaralarını kullanarak ilgili alana cevaplayınız (Bir numarayı birden fazla cevap alanında kullanabilirsiniz.).

1 Çalışkanlık	2 Duyarlılık	3 Sorumluluk
4 Mahremiyet	5 Yardımseverlik	6 Saygı
7 Tasarruf	8 Özgürlük	9 Adalet

- "Ecem, sosyal medya hesaplarının güvenliği için doğum tarihi, sıralı sayılar gibi kolay tahmin edilebilen şifreler belirlememektedir. Ayrıca şifrelerini başkaları ile paylaşmamaktadır."

Yukarıdaki metinde hangi değerlere vurgu yapılmıştır?

- "Hüseyin, led ampullerin düşük maliyetle yüksek verimlilik sağladığı bilgisini babası ile paylaşmıştır. Bu bilgi üzerine Hüseyin ve babası evlerinin aydınlatmasında led ampul kullanmaya karar vermişlerdir."

Yukarıdaki metinde hangi değerlere vurgu yapılmıştır?

- "Defne, seyir hâlinde telefona bakan otobüs şoförünü "Seyir hâlinde cep telefonu ile uğraşmak kazalara ve can kayıplarına yol açabilir. Telefona birkaç saniyelik bir bakış bile büyük risk taşır. Lütfen trafik kurallarına uyunuz. Benim yaşama hakkımı tehlikeye atıyorsunuz." diyerek uyarmıştır."

Yukarıdaki metinde hangi değerlere vurgu yapılmıştır?

Kaynak: MEB. (2025). 5.Sınıf. 2.Kitap. s.142

Resim 4.55'te verilen etkinlikte "Ecem, sosyal medya hesaplarının güvenliği için doğum tarihi, sıralı sayılar gibi kolay tahmin edilebilen şifreler belirlememektedir. Ayrıca şifrelerini başkaları ile paylaşmamaktadır." Şeklinde

ifade paylaşılmış ve hangi değere vurgu yapıldığı sorulmuştur. Burada Ecem'in kolay tahmin edilebilen şifreler kullanmaması ve şifrelerini başkalarıyla paylaşmaması bilgi güvenliği farkındalığının temel unsurlarını içeriyor. Bu farkındalık dijital hesapların korunması, kimlik hırsızlığı ve hesap ele geçirme gibi risklere karşı alınabilecek temel ve etkili önlemler arasında yer alır.

Resim 4.56: Örnek Olay Kutucuğu

Aşağıdaki örnek olayı okuyunuz ve soruları cevaplayınız.

Gümüşhane'de yaşayan Leyla ve ailesi, üniversite sınav sonuçlarının açıklandığını televizyondan öğrenince büyük bir heyecan yaşadılar. Leyla, bilgisayar üzerinden öğrenci sistemine giriş yaparak Afyonkarahisar Sağlık Bilimleri Üniversitesi Eczacılık Bölümünü kazandığını öğrendi. Leyla, beş yıl Afyonkarahisar'da yaşayacağı için barınma sorununu çözmesi gerekiyordu. Bu sorunu çözmek isteyen Leyla, genel ağ üzerinden devlet yurduna başvurdu. Ailesinin göndereceği parayı alabilmek için çevrim içi bankacılık hesabı açtırdı. Bir süre sonra devlet yurdu çıktığını öğrenen Leyla, kalacağı yurt ve eğitim göreceği okul arasındaki ulaşımın nasıl sağlandığını araştırmaya başladı. Genel ağdan ulaştığı Afyonkarahisar Belediyesinin iletişim numarasını aradı. Belediye otobüslerini kullanarak okuluna gidebileceğini ve belediye otobüslerinde kullanmak üzere bir ulaşım kartı çıkartması gerektiğini öğrendi.

Okulu için hazırlıklarını tamamlayan Leyla, üniversitenin açılma vakti geldiğinde ailesiyle Afyonkarahisar'a gitti. Eşyalarını yurduna bırakıp önce ailesiyle birlikte üniversiteye giderek öğrenci işlerine gerekli belgeleri teslim etti. Sonra belediye otobüsünde kullanmak üzere bir ulaşım kartı çıkarttı. Daha sonra hep birlikte Afyonkarahisar mutfağının geleneksel lezzetlerinden olan haşhaşlı bükme ve Afyon sucuğunun tadına baktılar. Afyonkarahisar'a 16 km mesafede bulunan Büyük Taarruz Şehitliği ve Atatürk Anıtı'nı da ziyaret ettiler. Fotoğraf makinesiyle çok güzel kareler çeken Leyla, son olarak ailesini memleketine uğurlayıp kalacağı yurda döndü.

Kaynak: MEB. (2025). 5.Sınıf. 2.Kitap. s.144

Resim 4.56'da verilen örnek olay incelendiğinde doğrudan bilgi güvenliği ile ilgili içerik yer almamış, genel ağ üzerinden öğrenci sistemine giriş yapılması, banka hesabı açılması, belediye iletişim numarasını arayarak bilgi alması gibi süreçler dijital işlem ve kişisel bilgi paylaşımı açısından önemli noktalar barındırıyor. Burada belirtilen örnekte çevrimiçi bankacılık işlemleri, kurumların alınan iletişim bilgilerinin sahte sitelerden olmadığı teyit edilmelidir. Bu tip içerikler bilgi güvenliği farkındalığını oluşturması açısından oldukça önemlidir.

4.2.5. 2024 Sosyal Bilgiler 6.Sınıf Ders Kitabında Bilgi Güvenliđi Bađlamında Kazanım (Öđrenme Çıktısı) ile İlgili Bulgular

İncelenen 6. Sınıf sosyal bilgiler ders kitabında “4. Ünite Bilim ve Toplum Hayatı” öđrenme alanında doğrudan;

- 1- Bilimsel ve teknolojik gelişmelerin gelecekteki yaşam üzerine etkilerine ilişkin fikirler ileri sürebileceđi,
 - 2- Telif ve patent hakları saklı ürünlerin yasal yollardan temin edilmesinin gerekliliđini savunulabileceđi,
- Toplamda 2 adet bilgi güvenliđi farkındalıđını geliştirici öđrenme çıktıısına yer verilmiştir.

Ayrıca;

- 1- Bilişim,
- 2- Teknoloji,
- 3- Patent,
- 4- Telif olarak toplamda 4 ilgili anahtar kelimeye yer verilmiştir.

Sosyal Bilgiler 6.Sınıf ders kitabı incelendiđinde bilgi güvenliđi açısından;

Tablo 4.4: Sosyal Bilgiler 6.Sınıf Ders Kitabının Bilgi güvenliği Açısından Değerlendirilmesi

İnceleme Kriteri	Alt Boyutlar
Sınıf Düzeyi	6.Sınıf
Öğrenme Alanı	Tüm Öğrenme Alanları
Kazanım	1- “Bilimsel ve teknolojik gelişmelerin gelecekteki yaşam üzerine etkilerine ilişkin fikirler ileri sürebileceği” 2- “Telif ve patent hakları saklı ürünlerin yasal yollardan temin edilmesinin gerekliliğini savunulabileceği”
Bilgi Güvenliği Boyutu	Gizlilik, Bütünlük ve Erişilebilirlik boyutlarında farkındalık sağlayıcı içerikler yer almıştır.
Okuryazarlık Becerisi	Dijital okuryazarlık, Eleştirel Düşünme
Etkinlik Türü	Yazılı Metin, Görsel, İnternet Bağlantı linki, Karekod, Genel Ağ Haberi,
Teknik Kavram Kullanımı	İnternet/sanal dolandırıcılık, “...gov”, “...edu” uzantıları belirtilerek daha güvenli bilgiye ulaşılacağı açıklanmış. PARDUS işletim sistemi, Çip kullanımı ve görselleştirmesi, Yapay Zekâ, Otonom Sürüş, Kuantum Bilgisayar,
Günlük Yaşamla İlişkilendirme Durumu	Var “Genel ağ haberi örneği”, Bakınız Görsel 3 İnternet Dolandırıcılığı Haberi, kurumların güncel bağlantı adresleri ve hizmetleri,
Açıklık ve Anlaşılabilirlik Düzeyi	6.Sınıf ders kitabında hemen hemen her ünite de genel ağ haberine yer verildiği görülmüş, etkinlik ve web ulaşım adresleri için karekod kullanımı istenmiş, haklarımızı kullanma konusunda yol gösterilerek etkililik sağlanmıştır. Bu kapsamda AÇIK olarak nitelendirilebilmektedir.
Bilgi Güvenliği Bilinci Geliştirme Potansiyeli	İnternet dolandırıcılığı haberine yer verilerek bilgi güvenliği farkındalığı somutlaştırılmıştır. Bilgi güvenliği geliştirme potansiyeli oldukça yüksektir.
Bilgi Güvenliği Gerektiren Dijital Teknolojiler Varlığı	Yapay Zekâ, Kuantum Bilgisayarlar, Otonom Araçlar, Küresel İnternet Erişimi, PARDUS işletim Sistemi, İnsansız Hava Araçları,

Kaynak: Yazar tarafından oluşturulmuştur.

Resim 4.57: Bilgi Kutucuğu



6 Şubat 2023 tarihinde yaşanan Kahramanmaraş merkezli depremler ve bu depremler sonrası yardım faaliyetleri hakkında ayrıntılı bilgi için www.afad.gov.tr genel ağ adresini ziyaret edebilirsiniz.



AFAD

Kaynak: MEB. (2025). 6.Sınıf. s.25

Resim 4.58: Bilgi Kutucuğu



Türk Kızılay ile benzer çalışmalar yapan resmi ve sivil toplum kuruluşları hangileridir?



Türk Kızılayın faaliyetleri hakkında daha ayrıntılı bilgi edinmek için www.kizilay.org.tr genel ağ adresini ziyaret edebilirsiniz.



Kızılay

Kaynak: MEB. (2025). 6.Sınıf. s.26

Resim 4.57 ve 4.58’de AFAD ve Türk Kızılay’ı Web bağlantı uzantılarına (URL) yer verilmiş kurumsal web farkındalığı oluşturulmuştur. Burada doğrudan bilgi güvenliği farkındalığı oluşturacak site uzantı açıklamalarına yer verilmemiştir.

Resim 4.59: Örnek Olay Kutucuğu

Alışverişlerimizle ilgili bir sorun çıktığında çözüm aramak hem hakkımız hem de özgürlüğümüzdür.

? Satın aldığımız ürünlerle ilgili sorunlarımızın çözümü için haklar, sorumluluklar ve özgürlükler çerçevesinde neler yapabiliriz?

İnternette pulluk alan çiftçi hayatının şokunu yaşadı

Manyas ilçesinde çiftçilik yapan M. M. (58), internet üzerinden pazarlaması yapılan pulluğu almak için anlaştığı kişi tarafından dolandırıldığını iddia ederek Cumhuriyet Savcılığına başvurduğunu söyledi.

M. M. olayı şöyle anlattı: "Bizim pulluk ihtiyacımız vardı. Oğlum internette dolaşırken bir reklam görmüş. Reklamı veren Aydın-Söke ilçesinden Ö. C. ile telefonla görüştük. Beğli pulluğa 20 bin lira fiyat koymuştu. Biz pazarlık ile 19 bin liraya anlaştık. Bize nakliye için yardımcı olacağını söyledi, daha sonra arayarak Bandırma'ya yük çıktığını, pulluğu da bu araçla göndereceğini ancak nakliyeciyi M. A.'nın 2 bin lira istediğini söyledi. Ben de 'Sen pullukları bize 18 bine bırak, nakliye ile 20 bin liraya bize mal olsun.' dedim, nazlanarak kabul etti. Çünkü normalde pullukların piyasa değeri 35-40 bin lira, biz de 'Sıkışık herhâlde, bu fiyata satıyor.' diye düşündük. Biz Ö. C. IBAN numarasını gönderdi, oğlum bana 'Baba belki hastası vardır, hemen gönderelim.' dedi. Biz de parayı gönderdik ancak daha sonra hem satıcı Ö. C.'nin hem de nakliyeciyi M. A.'nın telefonlarına ulaşamadık."

Genel ağı haber, 9 Mart 2023

? Çiftçi ve oğlunun bu alışverişte yaptıkları yanlışlar nelerdir? Haklarını aramak için neler yapabilirler?

Yukarıdaki haberde yaşanan soruna benzer bir durumda karşılaşmamak için ne yapmalıyız?

İnternet/ sanal dolandırıcılıktan korunmak için;

- Güvenliğinden emin olunmayan internet sitelerinden alışveriş yapmayınız.
- Telefon aramalarında bankanızdan aradığını söyleyen kişilere kişisel bilgilerinizi vermeyiniz.
- Cep telefonunuza gelen mesajların hepsinin doğruluğuna inanmayınız.
- Telefon üzerinden ürün satmak isteyen kişilere güvenmeyiniz.
- ATM'lerde işlem yaparken kamera, kart giriş mekanizması gibi alanları kontrol ediniz. Buradan kopyalanan bilgilerle internet üzerinden kartınızdan para çekilebilir, alışveriş yapılabilir.
- Sosyal medya sitelerine üye olurken kişisel bilgilerinizle giriş yapmayınız.

İnternet dolandırıcılığı sonrasında;

- En yakın karakola veya Cumhuriyet Başsavcılığına bir dilekçe ile şikâyetle bulununuz.
- Bilgi Teknolojileri Kurumu, Bilgi ve İhbar Merkezi'ne 120 numaralı telefona ihbar ediniz.

Yaşadığımız çevrede bazen çeşitli sebeplerden dolayı hizmet aksaklıkları yaşarız. Örneğin temiz bir çevrede yaşamak hepimizin hakkıdır. Temelde temiz çevre hakkı birçok hak ile bağlantılıdır. Bunlar yaşam, sağlıklı ve temiz bir havayı soluma, temiz suya sahip olma, sağlıklı ve yeterli yiyeceğe sahip olma haklarıdır. Hiçbir kişi, kurum ya da kuruluş temiz çevrede yaşama hakkımızı elimizden alamaz. Devlet, vatandaşlarının temiz bir çevrede yaşaması için gerekli tedbirleri almakla sorumludur. Bu hakkı kullanma konusunda sorun çıktığında hakkımızı ilgili kurumlara başvurarak aramalıyız.



Kaynak: MEB. (2025). 6.Sınıf. s.30

Resim 4.59'da bilgi güvenliği farkındalığı oluşturma açısından oldukça etkili bir içerik bulunmaktadır. Gerçek bir dolandırıcılık örneği üzerinden internet alışverişinde meydana gelebilecek olumsuzluklar somut bir şekilde anlatılmış. Bu tip dolandırıcılık yöntemlerinden korunmak için farkındalık sağlayıcı bilgilere yer verilmiş; güvenilmeyen sitelerden alışveriş yapılmaması, telefon dolandırıcılığı için arayan kötü niyetli kişilere kişisel banka bilgilerinin verilmemesi gerektiği, cep telefonlarına gelen mesajların hepsinin doğruluğuna inanılmaması gerektiği gibi tespitler yapılmıştır. Ayrıca örnekteki gibi olumsuz durumlarla karşılaşınca tüketici haklarının nasıl aranacağı ve resmi başvuru yolları da belirtilmiştir. Resim 4.59 ile gerçek yaşamdan alınan bir örnek daha açıklayıcı olmuş bireysel olarak farkındalık oluşturarak uygulanabilir bilgiler sunmuştur.

Resim 4.60: Bilgi Kutucuğu

Sorunumuzun çözümü için ilgili kurumlara dilekçe ile başvuru yapabiliriz. Bunun için karşılaştığımız sorunu ve çözüm talebimizi içeren bir dilekçe yazıp ilgili kuruma ulaştırmamız gerekir. Sorunların çözümü için yetkili makamlara dilekçe vermek anayasamızın 74. maddesine göre sahip olduğumuz bir haktır.



74. Madde: Vatandaşlar ve karşılıklılık esası gözetilmek kaydıyla Türkiye’de ikamet eden yabancılar kendileriyle veya kamu ile ilgili dilek ve şikâyetleri hakkında, yetkili makamlara ve Türkiye Büyük Millet Meclisine yazı ile başvurma hakkına sahiptir.

Karşılaştığımız sorunların çözümü için yetkili makamlara dilekçe verebileceğimiz gibi bu kurumların ihbar hatlarını da arayabilir ya da bu kurumlara e-posta gönderebiliriz.

Sorunlar Karşısında Hakkımızı Aramak İçin Başvurabileceğimiz Kurumlar

- Tüketici Hakları Mahkemesi
- Belediye
- Valilik
- Tüketici Hakları İl/İlçe Hakem Heyeti
- Reklam Kurulu
- Tüketici Hakları Merkezi
- Muhtarlık
- Kaymakamlık
- Tüketici Hakları Derneği



Kaynak: MEB. (2025). 6.Sınıf. s.31

Resim 4.61: Bilgi Kutucuğu



Çocukların ve gençlerin haklarını, hak arama yollarını öğrenmelerini amaçlayan Kamu Denetçiliği Kurumuna www.kdkcocuk.gov.tr genel ağ adresinden ulaşabilirsiniz.

Kaynak: MEB. (2025). 6.Sınıf. s.31

Resim 4.62: Bilgi Kutucuğu



Türkiye Selçuklu Devleti ve Anadolu beyliklerine ait eserleri İstanbul’da bulunan Türk ve İslam Eserleri Müzesinin www.sanalmuze.gov.tr genel ağ adresini ziyaret ederek inceleyebilirsiniz.



Kaynak: MEB. (2025). 6.Sınıf. s.82

Resim 4.63: Bilgi Kutucuğu



Ülkemiz ormanları hakkında daha fazla bilgi sahibi olmak için
www.ogm.gov.tr gencl ağ adresini ziyaret edebilirsiniz.



Kaynak: MEB. (2025). 6.Sınıf. s.113

Resim 4.60, 4.61, 4.62 ve 4.63'te resmi kurum ve kuruluşların web bağlantı adresleri farklı etkinlikler yoluyla sunulmuş ve dijital erişim farkındalığı sağlanmıştır. Bu noktada kurum ve kuruluşların web adresi farkındalığı sağlanmış ancak doğrudan bilgi güvenliği farkındalığına yönelik bilgi verilmemiştir.

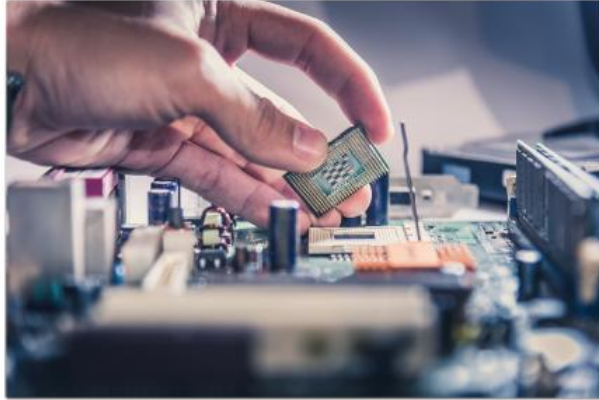
Resim 4.64: Bilgi Kutucuğu

- Milli işletim sistemi PARDUS'un yeni sürümleri geliştirilerek başta kamu kurumları olmak üzere kullanımı yaygınlaştırılacaktır (Görsel 4.16).
- KOVİD-19 ve grip aşısı geliştirilmiş olup kanser ilacı geliştirilme çalışmaları devam etmektedir. Bu aşı ve ilaç projeleri ile aşıda, ilaçta dışa bağımlılığımız azaltılacaktır.
- TÜBİTAK öncülüğünde savunma sanayi şirketlerinin de ortak olduğu Türkiye'nin ilk büyük ölçekli çip fabrikası 2016'da açıldı (Görsel 4.17). Üniversite-sanayi iş birliği açısından örnek bir proje olan çip fabrikası ile üniversitede geliştirilen teknolojinin ticarileşmesi sağlanmaktadır.



Görsel 4.16

Ülkemizde son yıllarda savunma sanayisinde alanında önemli gelişmeler kaydedilmektedir. TUSAŞ (Türk Havacılık Uzay Sanayii) tarafından geliştirilen helikopter, uçak ve İHA'lar (insansız hava aracı) hem ülkemiz ihtiyacının karşılanmasında hem de ülkemizin ihracatında önemli paya sahiptir. Savunma sanayisindeki çalışmalar sonucu Atak helikopteri, TCG (Türkiye Cumhuriyeti Gemisi) Anadolu gemisi kullanılmaya bağlanmış, milli muharip savaş uçağı Kaan ilk deneme uçuşunu gerçekleştirmiştir. Teknokentlerin ve teknoloji üniversitelerinin sayısı gün geçtikçe artmaktadır. Türkiye Uzay Ajansı kurulmuş, ülkemiz uzay araştırmalarına katılmıştır.



Görsel 4.17: Bilgisayar çipi

- ❓ T. C. Sanayi ve Teknoloji Bakanlığının çalışmaları, hangi alanlarda bilim ve teknolojinin gelişmesini sağlamaktadır?
- ❓ Bu çalışmaların ülkemiz ekonomisine katkıları nelerdir?

Kaynak: MEB. (2025). 6.Sınıf. s.140

Resim 4.64'te bilgi güvenliği açısından değerlendirildiğinde doğrudan bir bilgi yer almamış olsa da dolaylı olarak önemli bir farkındalık oluşturmuştur.

Yerli işletim sistemi (PARDUS) ve yerli çip üretimi, dışa bağımlılığı azaltarak siber güvenlik risklerini en aza indirmede önemli bir rol oynar.

Resim 4.65: Düşünelim Kutucuğu

İnsanlar, tarih öncesi çağlardan itibaren yaşamlarını kolaylaştırmak, içinde yaşadığımız dünya hakkında daha fazla bilgi sahibi olmak gibi nedenlerle çok sayıda keşif ve buluş yapmışlardır. Bu çalışmalar sayesinde bilim ve teknolojinin gelişmesini sağlamışlardır. Günümüzde bilim ve teknoloji alanındaki çalışmalar baş döndürücü bir hızla devam etmektedir. Daha yirmi yıl önce ismini dahi duymadığımız akıllı telefonlar, üç boyutlu yazıcılar, elektrikli otomobiller, hızlı trenler, güneş enerjisi santralleri, insansı robotlar, lazerle yapılan ameliyatlar, genel ağdan alışveriş gibi yenilikler yaşamımızda yer almaya başlamıştır (*Görsel 4.23 ve 4.24*).

? Yukarıdaki metinde yer alan gelişmelerden hangisi sizce daha önemlidir? Neden?



Görsel 4.23



Görsel 4.24

Kaynak: MEB. (2025). 6.Sınıf. s.142

Resim 4.65'te doğrudan bilgi güvenliği ile ilgili içerik yer almamış fakat teknolojik gelişmenin insan yaşamına etkisi üzerinde durulmuş, teknolojiye gelişmelerin oldukça hızlı olduğu belirtilmiştir.

Resim 4.66: İnceleyelim Kutucuğu

Bilimsel ve teknolojik gelişmelerin gelecekte nerelere varacağına, insanları nasıl etkileyeceğine dair fikirleri inceleyelim.

Gelecekte hangi buluş ve teknolojik gelişmeler olacak? Yapay zekâ sıraladı...

Gelişen teknoloji ve bilim dünyası, geleceğe yönelik büyüleyici bir keşifler ve buluşlar vadisiyle bizi karşılıyor. İnsanlık, her geçen gün sınırlarını zorlayarak hayal bile edemeyeceğimiz yeniliklerle karşımıza çıkıyor. Gelecekteki buluşlar, yaşamımızı kökten değiştirecek ve dünyamızı daha da ileri taşıyacak potansiyele sahip olacak.

İşte yapay zekânın sıraladığı gelecekte karşılaşılabileceğimiz bazı teknolojik buluş ve gelişmeler:

Kendi Kendine Sürüş: Otonom araç teknolojisinin gelişmesi, ulaşımı daha verimli, güvenli ve erişilebilir hâle getirebilir. Kendi kendine giden otomobiller ve kamyonlar, trafik kazalarını azaltabilir ve yolculuk sürelerini optimize edebilir.

Beyin-Bilgisayar Arayüzleri: Beyin-bilgisayar arayüzleri, insanların düşünceleriyle bilgisayarları veya diğer cihazları kontrol etmelerini sağlayabilir. Bu, nörolojik bozuklukları olan kişilere yardımcı olabilir ve beyin sağlığına genel bir yaklaşım sağlayabilir.

Kuantum Bilgisayarlar: Kuantum bilgisayarlar, klasik bilgisayarların sınırlarını aşabilir ve karmaşık problemleri çok daha hızlı çözebilir. Bu teknoloji finans, tıp ve bilim alanlarında karmaşık hesaplamaların yapılmasını sağlayabilir.

Uzay Teknolojisi: Uzay yolculuğunda ve keşifte büyük ilerlemeler olması bekleniyor. Uzay turizmi daha yaygın hâle gelebilir ve Mars'a insan gönderme hedefleri gerçeğe dönüşebilir.

Küresel İnternet Erişimi: Dünya üzerinde hâlâ internet erişimi olmayan milyonlarca insan var. Bu, uydu teknolojisinin yardımıyla değişebilir ve dünyanın her yerindeki insanların bilgiye ve eğitime erişimini artırabilir.



Görsel 4.27



Görsel 4.28



Görsel 4.29



Görsel 4.30

Kaynak: MEB. (2025). 6.Sınıf. s.144

Resim 4.66'da doğrudan bilgi güvenliği ile ilgili içerik yer almamış ancak, otonom araçlar, beyin-bilgisayar arayüzleri, kuantum bilgisayarlar, uzay teknolojisi ve küresel internet erişimi başlıkları altında bilgiler anlatılmış. Bu sistem ve teknolojiler bilgi güvenliği açısından oldukça önemli riskler barındırıyor.

Bu teknolojiler veri güvenliği açısından oldukça önemli olmakla birlikte hem bireysel hem de toplumsal olarak ciddi derecede güvenlik tehditleri oluşturabilir. Bu içerikte yeni teknolojilerin getirdiği bilgi güvenliği risklerine de değinilmesi farkındalığı artırıcı niteliktedir.

Resim 4.67: Bilgi Kutucuğu

Biyoteknoloji: Gen düzenleme ve özelleştirilmiş ilaçlar gibi devrim niteliğindeki tıbbi tedavileri mümkün kılabilir. Ayrıca, daha verimli ve sürdürülebilir tarım yöntemleri geliştirebilir.

Yapay Genel Zeka (AGI): AGI, insan beyninin tüm kapasitelerini taklit etme yeteneğine sahip bir yapay zeka türüdür. Bu, problem çözme, soyut düşünme ve hatta duygusal zeka gibi becerileri içerir. AGI, insanların ve makinelerin birlikte çalışma şeklini tamamen değiştirebilir ve tüm endüstrilerde devrim yaratabilir.

Çevresel Teknolojiler: Sürdürülebilir enerji kaynakları ve karbon yakalama teknolojileri, iklim değişikliğiyle mücadelede önemli rol oynayabilir. Daha verimli güneş panelleri, daha güçlü rüzgâr türbinleri 2050 yılına kadar hayatımızın bir parçası olabilir.

İleri Sağlık Teknolojileri: Sağlık hizmetlerinde, yapay zeka ve büyük verinin kullanılması, hastalıkları daha erken ve daha doğru bir şekilde teşhis etmeyi mümkün kılabilir. Ayrıca, nanoteknoloji ve kişiselleştirilmiş ilaçlar, daha etkili tedaviler ve daha sağlıklı bir yaşlanma süreci için kapılar açabilir.

Füzyon Enerjisi: Nükleer füzyon, güneş enerjisinin aynısını kullanır ve son derece verimli bir enerji kaynağıdır. Ancak, bunu kontrol etmek ve enerjiye dönüştürmek büyük bir zorluktur. Bu teknolojiyi geliştirmek ve ticari kullanıma sunmak, 2050'ye kadar iklim değişikliğiyle mücadelede büyük bir adım olabilir.

Genel ağ haberi, 21 Mayıs 2023



Görsel 4.31



Görsel 4.32



Görsel 4.33



Görsel 4.34

Kaynak: MEB. (2025). 6.Sınıf. s.145

Resim 4.67’de yaşamımızı etkileyen teknolojilerden bahsedilmiş ancak doğrudan bilgi güvenliği farkındalığı oluşturan içeriğe rastlanmamıştır. Bu türden içeriklerin ileri teknoloji geliştirmeleri içerdiğinden bilgi güvenliği süreçlerine de değinilmesi farkındalık oluşturur.

Resim 4.68: Bilgi Kutucuğu

Yapay zekâ, bir bilgisayarın veya bilgisayar kontrollü robotun genellikle akıllı varlıklarla ilişkili görevleri yerine getirme yeteneğidir. Yapay zekâ, bir insanın yapabileceği bazı görevleri daha fazla veriyle daha hızlı bir şekilde yapılmasına imkân tanıyarak hayatımızı kolaylaştırmaktadır. Bu sebeple, yapay zekâ; sesli asistanlar, dil çevirileri, öneri sistemleri, yolbul (navigasyon), sosyal güvenlik, sağlık hizmetleri, e-ticaret ve yardımcı robot uygulamalarıyla günlük hayatımızda yer almaktadır.



Görsel 4.37

Kaynak: MEB. (2025). 6.Sınıf. s.146

Resim 4.68’de yapay zekâ tanımı ve günlük yaşamdaki uygulama alanları anlatılıyor. İçerik doğrudan bilgi güvenliği farkındalığını geliştirici bir bilgi içermiyor. Halbuki yapay zekâ uygulamaları kişisel verileri işleme, otomatik karar verme, e-ticaret, sağlık hizmetleri, akıllı güvenlik gibi kritik altyapıların yönetiminde rol aldığı için bilgi güvenliği açısından oldukça önemli riskler barındırmakta. Bu açıdan yapay zeka uygulamalarında içerik oluştururken bilgi güvenliği açısından taşıdığı risklere değinilmesi farkındalık için oldukça önemlidir.

Resim 4.69: Örnek Olay Kutucuğu



Görsel 4.43

Kitaplardan gerekli bilgileri not aldıktan sonra araştırmama genel ağda devam ettim. Daha güvenilir bilgiler içerdiğini bildiğim “gov” ve “edu” uzantılı adreslerden ihtiyaç duyduğum bilgileri not aldım. Bu genel ağ adreslerini ve o günün tarihini araştırmamın kaynağında göstermek üzere yazmayı unutmadım.

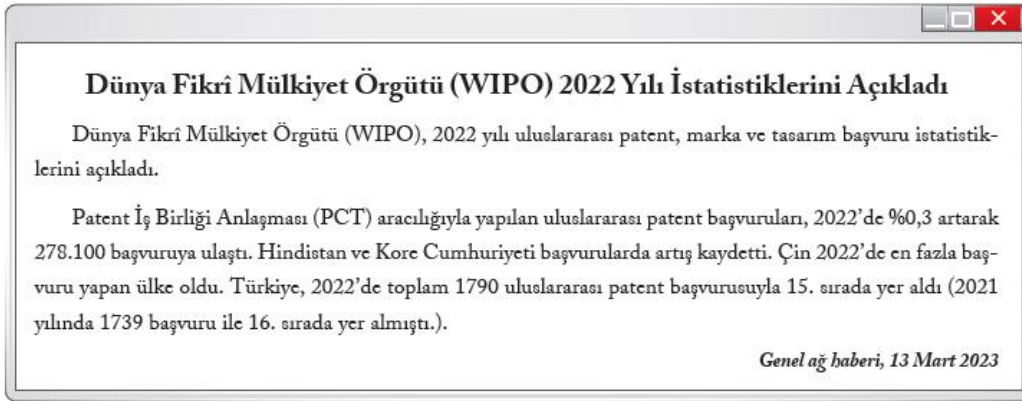
Kaynak: MEB. (2025). 6.Sınıf. s.150

Resim 4.69’da bilgi güvenliği ve dijital okuryazarlık açısından oldukça etkili ve bilinçlendirici bir örnek. Burada internetten yapılan araştırmaların

güvenilir kaynaklardan (.gov, .edu) yapılması yanlış bilgiye ulaşmayı engellemesi açısından önemli bir farkındalık oluşturuyor. Ayrıca bilgiye ulaşırken eleştirel düşünme ve doğrulama alışkanlığı da kazandırıyor. Resim 4.69'a bu açıdan bakıldığında bilgi güvenliği farkındalığı kazandırması açısından oldukça etkilidir.

Resim 4.70: Bilgi Kutucuğu

Yazılı, sesli ya da görüntülü bir eser nasıl telif hakları ile koruma altına alınıyorsa buluşlar da patent hakkı alınarak korunur. **Patent** kısaca, bilimsel ve teknik bir buluşun ya da böyle bir buluşu uygulama alanında kullanma hakkının kimine ait olduğunu gösteren resmi belgedir. Patent, buluş sahibinin buluşunu kendisinden izin almaksızın diğer kişilerin belirli bir süre üretmesini, kullanmasını, satmasını engellemektedir. Patent yasalarının amacı, buluş yapmayı ve yeni fikirleri teşvik etmektir. Bir ülkede ne kadar yeni patent alınıyorsa o ülke teknik, ekonomik ve sosyal açıdan o ölçüde gelişmiştir. Ülkemizde bilimsel ve teknolojik gelişmelerin artmasıyla alınan patent sayısında da önemli artış sağlanmıştır. Aşağıdaki haber patent başvurusu ve bilimsel çalışmalar konusunda ülkemizde gerçekleşen ilerlemeyi göstermektedir.



Kaynak: MEB. (2025). 6.Sınıf. s.154

Resim 4.71: Bilgi Kutucuğu



Telif haklarıyla ilgili daha ayrıntılı bilgi almak için T. C. Kültür ve Turizm Bakanlığı Telif Hakları Genel Müdürlüğü'nün www.telifhaklari.gov.tr genel ağ adresini, patent ile ilgili ise T. C. Sanayi ve Teknoloji Bakanlığı Türk Patent ve Marka Kurumunun www.turkpatent.gov.tr genel ağ adresini ziyaret edebilirsiniz.



**Telif Hakları
Genel
Müdürlüğü**



**Türk Patent
ve Marka
Kurumu**

Kaynak: MEB. (2025). 6.Sınıf. s.155

Resim 4.70 ve 4.71'de patent tanımı yapılmış ve öneminden bahsedilmiştir. Doğrudan bilgi güvenliği ilişkili bilgiler içermese de fikri mülkiyet ve patentler, bilgi güvenliği ile önemli ilişkiye sahiptir. Patent başvuruları ve fikri mülkiyet hakları önemli teknik ve ticari veriler içermektedir. Bu bilgilerin yetkisiz erişime ve veri sızıntısına karşı korunması gerekmektedir. Bu tip içeriklerde bilgi güvenliği açısından bilgiler verilerek örneğin; patent başvurularının dijital

ortamda yapılırken şifrelenmesi, siber saldırılara karşı güvenli sunucularda saklanması gibi farkındalık oluşturuıcı içerikler yer alabilir.

Resim 4.72: Etkinlik Zamanı Kutucuğu



Etkinlik Zamanı

Cumhurbaşkanının sayfada verilen görevleri dışında diğer görevlerini https://tecb.gov.tr/cumhurbaskanligi/gorev_yetki/ genel ağ adresinden araştırarak defterinize yazınız ve sınıfta paylaşınız.



Görsel 6.10: Cumhurbaşkanlığı Külliyesi

Kaynak: MEB. (2025). 6.Sınıf. s.212

Resim 4.73: Bilgi Kutucuğu

Halkın istek, şikâyet ve düşüncelerini almak da Cumhurbaşkanlığının sorumluluklarından biridir. Bunun için Cumhurbaşkanlığına bağlı kısa adı “CİMER” olan Cumhurbaşkanlığı İletişim Merkezi kurulmuştur (Görsel 6.11).

Yargı Gücü: Vatandaşlarla devlet arasında ve vatandaşların kendi aralarında çıkan uyuşmazlıkların millet adına bağımsız mahkemelerde çözülmesi yetkisine yargı gücü denir. Anayasamıza göre ülkemiz bir hukuk devletidir ve yargı yetkisi bağımsız mahkemelerce kullanılır.

Görsel 6.11

Kaynak: MEB. (2025). 6.Sınıf. s.213

Resim 4.74: Bilgi Kutucuğu



15 Temmuz 2016’da gerçekleşen darbe teşebbüsüyle ilgili daha ayrıntılı bilgi için Cumhurbaşkanlığımızın www.tecb.gov.tr genel ağ adresini ziyaret edebilirsiniz.



T. C.
Cumhurbaşkanlığı

Kaynak: MEB. (2025). 6.Sınıf. s.225

Resim 4.72, 4.73 ve 4.74’te resmi kurum ve kuruluşlara ait web site uzantıları (URL) bağlantı linki verilmiş, devlet kurumlarına ait site uzantılarının nasıl olması gerektiği konularında farkındalık kazandırıcı niteliktedir. Dolaylı olarak kazandırılan bu bilgi web site uzantılarının sonundaki ...gov.tr alan adının

sadece devlet kurumlarının kullandığının belirtilmesi ile sahte web site dolandırıcılığı farkındalığı kazandırılabilir.

Resim 4.75: Bilgi Kutucuğu

Sanayi devrimiyle birlikte üretimin fabrikalarda yapılmaya başlanması, ulaşımdaki gelişmeler, ülkeler ve bölgeler arasında ürün ve hizmet alışverişini artırmıştır. Bunun yanı sıra bilgi teknolojilerinin sürekli gelişmesi ülkeler arası ekonomik ilişkileri geliştirmiş ve hatta zorunlu hâle getirmiştir. E-ticaret, internet aracılığıyla yapılan alışveriş işlemleridir. Sanal ortamda mağazalardan alışveriş çok tercih edilmektedir. Türkiye'nin coğrafi konumunun sağladığı avantajdan da yararlanarak e-ticaret yoluyla hem Avrupa'ya hem Türk cumhuriyetlerine hem de Orta Doğu'daki ülkelere ihracat günden güne artmaktadır (Görsel 7.16).



Görsel 7.16

Kaynak: MEB. (2025). 6.Sınıf. s.255

Resim 4.75 incelendiğinde e-ticaretin gelişimi ve dijital gelişmelerin ticari alana etkisinden bahsedilmiş; ancak bilgi güvenliği ile ilgili doğrudan bir bilgi içermiyor. Fakat e-ticaret bilgi güvenliği açısından oldukça önemli riskler barındırıyor. Kişisel ve finansal bilgilerin gizliliği, e-ticaret sitelerinin güvenli olup olmadığı, kimlik avı (Phishing) ve dolandırıcılık gibi istenmeyen durumlara karşı farkındalık kazandırıcı bilgiler içerikte yer alabilir.

Resim 4.76: Bilgi Kutucuğu

BTK'den "Sosyal Medyaya Selam Olsun!" Kampanyası

Bilgi Teknolojileri ve İletişim Kurumunca (BTK), Türkçenin doğru kullanımı için sosyal medyada kampanya başlatıldı. "Sosyal Medyaya Selam Olsun!" etiketiyle başlatılan kampanya için hazırlanan görsellerde "npyen, tm, nbr, aco, kib" gibi kısaltılan kelime ve cümlelerin üstü çizilerek bunların asıl kullanımları yazıldı.

Genel ağ haberi, 21 Ağustos 2017

Görsel 7.37

Kaynak: MEB. (2025). 6.Sınıf. s.271

Resim 4.76'da Türkçenin doğru kullanımı ile ilgili teşvik edici bir içerik yer alıyor. Doğrudan bilgi güvenliği ile ilişkili olmayan bu içerik dolaylı olarak

önemlidir. Dijital ortamlarda doğru ve açık iletişimin desteklenmesi bilgi karmaşasının önüne geçmenin ve doğru bilgiye ulaşmanın koşullarındandır.

4.2.6. 2024 Sosyal Bilgiler 7.Sınıf Ders Kitabında Bilgi Güvenliği Bağlamında Kazanım (Öğrenme Çıktısı) ile İlgili Bulgular

Sosyal Bilgiler 7.sınıf ders kitabında doğrudan bilgi güvenliği farkındalığını arttırıcı ünite 4.Ünite olan “Geçmişten Günümüze Bilim” ünitesi olmuştur.

Yazının ve bilginin yolculuğu konusuna yer verilmiş,

Kavram, Değer ve Beceriler;

1- Teknoloji kavramı

Bu ünite kapsamında;

1- Bilginin korunması, yaygınlaştırılması ve aktarılmasında değişim ve sürekliliği incelemeyi,
Becerisinin öğrenilmesi amaç edinilmiştir.

5.Ünite “Üretim ve Sosyal Hayat” boyutuna ilişkin kategorilerin sınıflandırılması;

1- Dijital teknolojiler ve ticaret

2- Teknolojinin sosyal ve ekonomik hayat üzerindeki etkileri

Kavram, değer ve beceriler,

1- E-ticaret

Bu ünite kapsamında;

1- “Üretim teknolojisindeki gelişmelerin sosyal ve ekonomik hayata etkilerini değerlendirmeyi”
2- “Dijital teknolojilerin üretim, dağıtım ve tüketim ağında meydana getirdiği değişimleri” öğrenme çıktısı olarak verilmiştir.

Tablo 4.5: Sosyal Bilgiler 7.Sınıf Ders Kitabı Bilgi Güvenliği Açısından Değerlendirilmesi

İnceleme Kriteri	Alt Boyutlar
Sınıf Düzeyi	7.Sınıf
Öğrenme Alanı	Tüm Öğrenme Alanları
Kazanım	1-“Bilginin korunması, yaygınlaştırılması ve aktarılmasında değişim ve sürekliliği incelemeyi” 2- “Üretim teknolojisindeki gelişmelerin sosyal ve ekonomik hayata etkilerini değerlendirmeyi” 3-“Dijital teknolojilerin üretim, dağıtım ve tüketim ağında meydana getirdiği değişimleri öğrenme”
Bilgi Güvenliği Boyutu Etkiliği	Gizlilik, Bütünlük ve Erişilebilirlik
Okuryazarlık Becerisi	Dijital okuryazarlık, Medya Okuryazarlığı, Eleştirel Sorgulama
Etkinlik Türü	Yazılı Metin, Görsel, İnternet Bağlantı linki, Karekod,
Teknik Kavram Kullanımı	Ortalama, bilgi çarpıtma (dezenformasyon), e-ticaret, kimlik avı, CD, DVD, blu-ray, harici disk, flash bellek
Günlük Yaşamla İlişkilendirme Durumu	Var “Genel ağ haberi örneği”, Sosyal Medya ve İnternet Kullanımı
Açıklık ve Anlaşılabilirlik Düzeyi	Açık
Bilgi Güvenliği Bilinci Geliştirme Potansiyeli	Yüksek

Kaynak: Yazar tarafından oluşturulmuştur.

Tablo 4.5’te belirtilen bulgular doğrultusunda bilgi güvenliği ve süreçleri ile ilgili kazanım, beceri, kavram ve diğer alt kategorilere ait destekleyici bulgular, doğrudan ve dolaylı olarak önleyici bilgi güvenliği farkındalığı kazandırma süreçlerinde etkili olabilmektedir. Bu kapsamda elde edilen bilgiler bilgi güvenliği kategorisinde sosyal mühendislik ve kimlik avı süreçlerinde öğrencilere farkındalık kazandırıcı niteliktedir ve bulgular görseller ile desteklenmiştir.

Resim 4.77: Etkinlik Kutucuğu



Genel ađ, XX. yüzyılda kullanılmaya başlanmıřtır. Bu teknolojinin kullanılmaya başlanma-sı insanların hayatını nasıl etkilemiş olabilir?

Televizyon, cep telefonu, genel ađ gibi teknolojiler insan ve toplum hayatını hem kolaylařtırmıř hem de toplumda birtakım deđiřikliklere neden olmuřtur. Bu teknolojiler, bazı alanlarda ihtiyaçları karřılarken bazı alanlarda bireyin ve toplumun alışkanlıklarında, kùltüründe farklılıklar meydana gel-mesine yol açmıřtır. řimdi bu gelişmeleri ve deđiřimleri Türkân Hanım'dan dinleyelim.



Televizyon hayatımıza girmeden önce açık hava sinemaları (Görsel 1.8) vardı. Her hafta sonu aileler sinemaya giderdi. Açık hava sinemaları komřuların, tanıdıkların buluřma yeri gibiydi. İnsanlar salona film başlamadan önce gelir, sohbet ederdi. Sinemaya evde yaptıkları börek, pasta gibi yiyecekleri getirir, birbirlerine ikram ederlerdi. Film bittikten sonra eve dö-nerken yol boyu film hakkında konuřurlardı.

O dönemde komřular, tanıdıklar, akrabalar sık sık birbirleri-ne misafirlieđe giderlerdi. İnsanlar uzun kiř akřamlarında soh-bet eder, dama oynar, radyo dinler, masal ve öykü anlatır, mısır patlatır, soba üstünde kestane piřirirdi. Çocuklar bütün yıl parklarda, yeřil alanlarda oyun oynardı.

Kaynak: MEB. (2025). 7.Sınıf. s.26

Resim 4.77'de teknolojinin toplumsal yařama etkisi ve günlük alışkanlıklarımızı nasıl etkilediđine dair bilgiler yer almakta. Ancak doğrudan bilgi güvenliđine dair bilgi yer almamakta.

Resim 4.78: Etkinlik Kutucuğu

Televizyonun ardından bir başka önemli gelişme genel ağın kullanılmaya başlanması oldu. Genel ağ aracılığıyla sosyal medya kullananlar, arkadaşlarıyla istediği zaman sesli veya görüntülü görüşebiliyor (Görsel 1.10). Üstelik genel ağdaki çeviri programları sayesinde birbirinin dilinden anlamayan iki kişi rahatlıkla iletişim sağlayabiliyor. Genel ağın eğitime de çok büyük katkıları var. Torunum ödevlerini yaparken, merak ettiği bir konuyu araştırırken genel ağdan yararlanıyor. Bilmediğim konuları torunuma soruyorum. Genel ağa bakıp beni bilgilendiriyor. Ancak sosyal medyanın dolayısıyla genel ağın iletişimde sağladığı kolaylıkların yanında bazı olumsuz etkileri de bulunuyor. İnsanların büyük bir kısmı sosyal medyada gereğinden fazla zaman geçiriyor. Bazı insanlar sosyal medya, bazıları ise oyun bağımlısı hâline geliyor. Bu durum kişinin hem sosyal hayatını hem de sağlığını tehdit ediyor.



Görsel 1.10: Genel ağ aracılığıyla sosyal medya üzerinden görüntülü iletişim



Genel ağda oluşturulan sosyal ağlar üzerinden görsel ve işitsel materyal paylaşımını, bilgi aktarımını ve haberleşmeyi sağlayan iletişim ortamına sosyal medya denir. Sosyal medya kullanımının olumlu ve olumsuz yönleri neler olabilir? Tartışınız.

Kaynak: MEB. (2025). 7.Sınıf. s.28

Resim 4.78’de genel ağ(internet) ve sosyal medya üzerinden iletişim, eğitim ve bilgiye erişim açısından sağlanan kolaylıklar gösterilmiş aynı zamanda sosyal medyanın olumsuzluklarından bahsedilmiş. Ancak bilgi güvenliğini sağlayıcı doğrudan bir uyarı veya bilgilendirme içermiyor.

Resim 4.79: Bilgi Kutucuğu

Genel ağ teknolojisinin gelişmesi alışveriş anlayışında değişikliklerin ortaya çıkmasına yol açtı. İnsanlar mağazalara gitmeden genel ağ üzerinden alışveriş yapabilir hâle geldi (Görsel 1.11). Bu gelişme günlük yaşamda insanlara büyük kolaylık sağladı. Ancak bu gelişmenin olumsuz etkileri de bulunmaktadır. Örneğin televizyonda, radyoda ve diğer medya araçlarında sürekli ve yoğun reklama maruz kalan bazı insanlarda alışveriş bağımlılığı ortaya çıktı. İnsanlar ihtiyaçları olmayan ürünleri düşünmeden almaya başladı. Bu durum aile ekonomisine zarar verdi.



Görsel 1.11: Genel ağ üzerinden alışveriş

Televizyon, genel ağ, cep telefonu gibi teknolojik ürünler kitle iletişiminde yeni boyutlar kazandı. İnsanlar, toplumlar, kültürler arasındaki etkileşim arttı. Günümüzde insanlar aradıkları bilgiye, görüntüye istedikleri zaman ve yerde rahatlıkla ulaşabiliyor. Sosyal medya aracılığıyla istediği herhangi bir bilgiyi insanlarla paylaşabiliyor ve tepkilerini farklı şekillerde anında dile getirebiliyor.

Genel ağ, akıllı cep telefonu gibi iletişimde yaşanan gelişmeler kamu hizmetlerinin niteliğini arttırdı. Resmi kurumlarla ilgili birçok iş, e-devlet üzerinden yapılmaktadır. Vergi ödeme, sınav başvurusu yapma, bilgi edinme gibi birçok hizmete e-devlet ortamında ulaşılabilir.

Günümüzde televizyon, genel ağ ve akıllı cep telefonları kamuoyu oluşturmada son derece etkilidir. Haber ve bilgiler, bu teknolojiler sayesinde hızla yayılmakta; gruplar, sivil toplum kuruluşları bir araya gelip kamuoyu oluşturabilmektedir. Oluşturulan kamuoyu sayesinde imza ve yardım kampanyaları düzenlenebilmekte (Görsel 1.12), dayanışma faaliyetleri yürütülmektedir.



Görsel 1.12: Kahramanmaraş depremi sonrası düzenlenen bir yardım kampanyasında toplanan yardım malzemeleri

Toplumda sözlü veya yazılı haber alma imkânı sağlayan teknik araçlara medya denir. Günümüzde dünya, medya aracılığıyla âdeta küçük bir köy hâline geldi. Ancak bu teknolojiler, zararlı fikir ve unsurların yayılmasına da sebep oldu. Bu nedenle medyanın gerekli güvenlik önlemleri alınarak kullanılması gerekir.

Kaynak: MEB. (2025). 7.Sınıf. s.29

Resim 4.79’da genel ağ(internet) alışveriş ve iletişim gibi alanlarda ortaya çıkardığı değişim, e-ticaret kullanımının artması, sosyal medya kullanımı ile bilgiye hızlı erişim, kamu hizmetlerinin dijitalleşmesi ve teknolojinin toplumsal hayatı anlatılıyor. Bu kapsamda görsel 3’te dijitalleşmenin hayatın her alanına girmesi üzerine yapılan vurguda bilgi güvenliğinin önemi dolaylı olarak belirtiliyor.

Resim 4.80: Örnek Olay Kutucuğu

Günümüzde bilgi çarpıtma (dezenformasyon), insanların yanlış bilgilendirilmesi bakımından ciddi bir sorundur. Kişi, kurum ve kuruluşları herhangi bir konuda bilinçli olarak yanlış bilgilendirmeye karşı mücadele edilmesi, halkın doğru haber alma hakkı açısından oldukça önemlidir (Görsel 1.14).



Görsel 1.14: Türkiye Cumhuriyeti Cumhurbaşkanlığı İletişim Başkanlığı tarafından yanlış haberler ile ilgili hazırlanan bülten

Kaynak: MEB. (2025). 7.Sınıf. s.33

Resim 4.80’de bilgi güvenliği farkındalığını sağlamada oldukça önemli olan “Oltalama” hakkında bilgi verilmiş ve bilgi çarpıtma (dezenformasyon) ve yanlış bilgilendirme konularına dikkat çekilmiştir. Özellikle sosyal medya ve internet sitelerinde, devlet kurumlarının isim ve logoları kullanılarak yapılan dolandırıcılık girişimlerine karşı uyarılar yer alıyor. Resmi olarak Cumhurbaşkanlığı İletişim Başkanlığı tarafından hazırlanan bülten örnekleriyle, kişilerin yanlış bilgilendirmeye karşı bilinçli olması gerektiği vurgulanıyor. Burada özellikle bilgi güvenliği açısından bilgi ve farkındalık kazanmak için gerekli bilgilerin edinilebileceği kurum belirtilmiş bunun yanında bizlere internet ve sosyal medya uygulamalarından ulaşan kişi ve kişilerin teyit edilmesi ve sorgulayıcı nitelikte yaklaşılması gerektiği belirtilmiştir. Bu görsel bilgi güvenliği açısından oldukça etkili ve bilgilendirici içerik sunuyor. Bu tür içerikler, özellikle sosyal mühendislik saldırılarına, kimlik avı (phishing) girişimlerine ve sahte

haberlerle yapılan dolandırıcılıklara karşı kişisel farkındalığı artırır. Bilgi güvenliğinin sadece teknik önlemlerle değil, aynı zamanda bireylerin bilinçli ve eleştirel yaklaşımıyla da sağlanabileceğini gösterir.

Resim 4.81: Bilgi Kutucuğu

Medya okuryazarlığı; bireylerin gazete, dergi, radyo, televizyon, genel ağ vb. kaynaklarda yer alan bilgileri eleştirel bir şekilde okumaları, dinlemeleri veya izlemelerini kapsar. Zaman zaman kamuoyunun yanlış yönlendirilmesi için bilinçli şekilde yanlış haber yayımlandığı ya da olayların olduğundan farklı yansıtıldığı görülmektedir. Bu durumda sorgulayıcı olmak; yazılı, görsel, sözlü mesajların doğruluğu konusunda kuşkucu davranmak gerekir. Bağımsız ve güvenilir kaynakları takip etmek, eleştirel düşünmek doğru bilgi almak bakımından önemlidir.

Doğru bilgi alma hakkını kullanmada yaşanan sorunlarda bireylere önemli görevler düşmektedir. Günümüzde bireyler medya okuryazarlığının gereği olarak yazılı, görsel ve işitsel iletişim araçlarına erişebilmekte ve bu organlardan yararlanabilmektedir. Bireyler; her gün çeşitli iletişim araçlarından birçok video, resim, haber, bilgi, mesaj vb. almaktadır (Görsel 1.16). Bireylerin medyadan yararlanırken seçici olması, haber ve mesajların doğruluğunu güvenilir kaynaklardan sorgulaması gerekir. Bu nedenle iletişim organlarından bilgi edinirken eleştirel bir gözle değerlendirme yapılmalıdır. Herhangi bir konuda yorum yapılırken öncelikle haberin ve olayın doğruluğu sorgulanmalıdır.



Görsel 1.16: Bireyler, her gün medya araçlarından birçok mesaj almaktadır.

Kaynak: MEB. (2025). 7.Sınıf. s.34

Resim 4.81’de Medya okuryazarlığı ile ilgili bilgi verilerek bilgi güvenliği farkındalığı için önemli bir temel oluşturulmuştur. Belirtilen görsel de ayrıca eleştirel bilgi edinme ve sorgulama da yer alıyor. Bireylerin gazete, dergi, radyo, televizyon ve genel ağ gibi kaynaklardan edindikleri bilgileri eleştirel bir bakış açısıyla değerlendirmeleri bu bilgi ve haberlerin doğruluğunu güvenilir kaynaklardan sorgulamalarının gerektiği belirtiliyor. Bahse konu görselle oluşturulan bilgi güvenliği farkındalığı için önemli bir temel oluşturuyor çünkü bilgi güvenliği sadece teknik önlemlerle değil, aynı zamanda bireylerin dijital ortamlarda karşılaştıkları bilgiye ulaşma durumlarında bilgi ve mesajları sorgulama, doğrulama ve eleştirel düşünme becerileriyle de sağlanır. Özellikle sosyal medya, e-mail, haber siteleri ve genel ağ üzerinden yayılan yanlış bilgiler, dolandırıcılık girişimleri ve sosyal mühendislik saldırıları, bireylerin medya okuryazarlığı sayesinde daha kolay tespit edilebilir.

Resim 4.82: Bilgi Kutucuğu

XX. yüzyılda teknolojinin gelişmesiyle bilgiler CD, DVD, blu-ray (bulurey) disk, harici disk, flash (fılaş) bellek, hafıza kartı gibi birçok aygıta yüklenebilmekte, bu aygıtlarda saklanabilmekte ve istenildiğinde kullanılabilir. Gelişen teknolojilerle aygıtların kapasiteleri arttırılmakta ve kısa zamanda yeni aygıtlar üretilmektedir. Bunun yanı sıra bilgiler, fiziksel bir aygıta gerek duyulmadan doğrudan genel ağ üzerindeki bazı uygulamalarda da arşivlenebilmektedir. Bulut teknolojisi adı verilen uygulamalarla arşivlenen bilgilere yenileri eklenebilmekte, gerektiğinde bunların üzerinde bilgisayar, akıllı televizyon, cep telefonu ve tabletlerle türlü değişiklikler yapılabilmektedir (Görsel 4.8).



Görsel 4.8: Bulut teknolojisinde genel ağ üzerinden bilgiler depolanabilmektedir.

Kaynak: MEB. (2025). 7.Sınıf. s.155

Resim 4.82’de teknolojinin ilerlemesiyle birlikte bilgilerin CD, DVD, blu-ray, harici disk, flash bellek gibi fiziksel ortamlarda saklanabildiği; ayrıca bulut teknolojisi sayesinde bilgilerin genel ağ (internet) üzerinden de depolanabildiği anlatılıyor. Görselde bulut teknolojisiyle farklı cihazların (bilgisayar, tablet, akıllı telefon, sunucu vb.) internete bağlı olarak veri alışverişi yaptığı gösterilmiş. Burada bilgi güvenliği açısından risklere ve alınması gereken önlemlere değinilmemiş, oysaki bulut depolama gibi hizmetler yetkisiz erişim ve veri sızıntısı, verilerin şifrelenmeden saklanması, veri bütünlüğünün korunamaması gibi durumlarda gizlilik ihlali ile istenmeyen zararlı süreçlerin ortaya çıkmasına sebep olabilir. Bilgi güvenliği farkındalığı ve etkililiği açısından güçlü şifre ve iki faktörlü kimlik doğrulama, verilerin şifrelenmesi, güvenilir ve kurumsal olarak yüksek standartlara sahip hizmet sağlayıcıların tercih edilmesi gibi önemli noktalarda vurgulanması önemlidir.

Resim 4.83: Bilgi Kutucuğu

Geçmişte hayal bile edilemeyecek bilimsel ve teknolojik gelişmeler günümüzde hızla insanlığın hizmetine sunulmaktadır. Ay'a ve Dünya'nın yörüngesine insanlı; Mars, Venüs gezegenleriyle bazı uydulara hatta Güneş sistemi dışına insansız uzay yolculukları yapılmaktadır. Ay'a, Mars'a ve bir asteroide uzay aracı indirilebilmiştir (Görsel 4.10). Dünya yörüngesindeki iletişim uydularıyla genel ağ, haberleşme, konum bulma olanaklarından anında yararlanılabilmektedir. Tıp, ulaşım, gen teknolojisi, yenilenebilir enerji alanlarındaki çalışmalar insanlığa büyük katkıda bulunmaktadır.



Görsel 4.10: Curiosity (Küryosıdt), Mars'ta araştırma yapan araç

Günümüzde bilim ve teknolojiye yaşanan yenilikler, büyük oranda Avrupa'da XV. yüzyılla birlikte başlayan gelişmelere dayandırılmaktadır. Bu gelişmelerden bazıları şunlardır: Avrupa'da XV. yüzyılda modern matbaa icat edildi; Dünya merkezli evren modeli, yerini Güneş merkezli evren modeline bıraktı; Dünya'nın yuvarlak olduğu ispat edildi, kütle çekim kanunu bulundu, buhar makinesi icat edildi. Bu gelişmeler Avrupa'nın bilimin merkezi olmasına katkı sağladı.

Kaynak: MEB. (2025). 7.Sınıf. s.165

Resim 4.83'te bilimsel teknolojilerin gelişimi ve insanlık üzerinden etkilerinden bahsediliyor. Görsel bilgi güvenliği açısından doğrudan bilgi içermiyor, bu kapsamda anlatılan teknolojik gelişmelerin ve özellikle uzay araştırmalarının bilgi güvenliğiyle yakından ilişkili olduğu belirtilmeli ve bu hususla ilgili bilgi güvenliği farkındalığı kazandırılabilir.

Resim 4.84: Bilgi Kutucuğu

Bilişim teknolojilerindeki gelişmeler sadece sanayide değil; ulaşım, iletişim, tarım, eğitim (Görsel 5.14), sağlık gibi alanlarda büyük kolaylıklar sağladı. Sanayide bazı alanlarda işçilerin yaptığı işlerde robotlar kullanılmaya başlandı. Modern ulaşım araçları, yük ve yolcu taşımacılığının hızını ve miktarını artırarak yolcu taşımacılığını konforlu hâle getirdi. İletişim araçları ile genel ağ sayesinde haberleşme, sesli ve görüntülü yapılmaya başlandı.



Görsel 5.14: Günümüzde eğitimde bilişim teknolojilerinden yararlanılmaktadır.

Kaynak: MEB. (2025). 7.Sınıf. s.192

Resim 4.85: Bilgi Kutucuğu

Günümüzde bilişim, genetik, nanoteknoloji, tıp, astronomi alanlarında önemli gelişmeler yaşanmaktadır. Bu gelişmelerin yaşandığı ülkelerin ekonomisi büyümekte, refah seviyeleri günden güne yükselmektedir. Bu durum toplumların bilişim toplumlarına dönüşmesini sağlamaktadır.

Günümüzde dünyanın büyük şirketleri sosyal medya, e-ticaret ve bilişim sektörlerinde hizmet vermektedir. Bundan dolayı bilgiye ve onu üretecek insana verilen değer ile eğitime verilen önem ülkelerin gelişmesinde başlıca faktörler olmuştur.

Kaynak: MEB. (2025). 7.Sınıf. s.193

Resim 4.84 ve 4.85'te bilişim teknolojileri alanındaki gelişmelerden ve hayatımıza etkilerinden bahsedilmiş, bu gelişmelerin insanların hayatında refah seviyesini yükselttiği, ekonomi ve eğitim gibi birçok alanda etkili olduğu vurgulanmıştır. Bu kapsamda bilgi güvenliği ve süreçleri ile ilgili doğrudan bir uyarı veya bilgilendirme içermiyor.

Resim 4.86: Bilgi Kutucuğu

Bilişim teknolojisi, yapay zekâ, genetik, nanoteknoloji gibi alanlardaki gelişmeler farklı meslekleri ortaya çıkarmaktadır. Robot koordinatörlüğü, yapay zekâ mühendisliği, e-spor oyunculuğu, siber teknoloji uzmanlığı, giyilebilir teknoloji uzmanlığı, veri bilimciliği, mesleki tedavi uzmanlığı, sanal gerçeklik eğitimciliği (Görsel 5.23), bilgi programcılığı (Görsel 5.24), insansız hava aracı pilotluğu (Görsel 5.25) ve 3D yazıcı mühendisliği (Görsel 5.26) günümüzde ortaya çıkan mesleklerdendir. Bu meslekler, bilimsel ve teknolojik gelişmeler sonucu ortaya çıkan alanlara yöneliktir.



Görsel 5.23: Sanal gerçeklik eğitimcisi



Görsel 5.24: Bilgi programcısı



Görsel 5.25: İnsansız hava aracı pilotu



Görsel 5.26: 3D yazıcı mühendisi

Kaynak: MEB. (2025). 7.Sınıf. s.202

Resim 4.86’da bahsedilen tüm meslekler bahsedilen tüm meslekler ve teknolojik alanlar bilgi güvenliğiyle yakından ilişkilidir ve ciddi riskler içerir. Bu tür içeriklerde yeni mesleklerin ve teknolojilerin bilgi güvenliği süreç ve gereksinimlerine de değinilmesi hem öğrenciler hem de genel kullanıcılar için oldukça önemli farkındalık oluşturur. Kişisel verilerin korunması, siber tehdit ve süreçleri, güvenli yazılım geliştirme ve cihaz kullanımı, dijital ortamlarda veri bütünlüğü ve gizliliği gibi son derece önemli süreçlerde bilişsel farkındalık kazandırılabilir.

Resim 4.87: Bilgi Kutucuğu

Önümüzdeki yıllarda özellikle genetik, yapay zekâ ve uzay alanlarındaki gelişmeler günümüzde mevcut olmayan birçok mesleği ortaya çıkaracaktır. İnsan organları üretilebilecek, deri altına takılabilen küçük bir cihazla hastalıklar belirlenebilecek, insandan bağımsız ulaşım araçlarıyla yük ve yolcu taşımacılığı yapılabilecektir. Bunun yanında gezegenler arası insanlı yolculuklara çıkılabilecek, Mars'ta yaşam alanları oluşturulabilecek ve buralarda insanlar yaşayabilecektir. Araç programcılığı, gezegenler arası uzay aracı kaptanlığı (Görsel 5.27), yaşam alanı uzmanlığı, sanal hekimlik (Görsel 5.28) gelecekte ortaya çıkabilecek mesleklerden bazılarıdır.



Görsel 5.27: Uzay aracı kaptanı



Görsel 5.28: Sanal hekim

Kaynak: MEB. (2025). 7.Sınıf. s.203

Resim 4.87’de gelecekte dijital teknolojiler alanında birçok önemli mesleğin ortaya çıkacağı belirtilmiş ancak doğrudan bilgi güvenliğiyle ilgili bir mesleğe ve bilgilendirmeye yer verilmemiş. Bu doğrultuda anlatılan teknolojik gelişmeler ve yeni meslekler, bilgi güvenliği açısından çok önemli riskler ve gereklilikler barındırıyor.

Resim 4.88: Örnek Olay Kutucuğu

Şimdi Fatma'nın mesleki tercihlerine göre nasıl bir planlama yaptığını inceleyiniz.

Ben Fatma Aktan. İlkokul 2. sınıftan beri evimizdeki bilgisayarı kullanıyorum. Bilgisayarda genellikle araştırma yapıyorum, ilgi duyduğum konularla ilgili bilgileri öğreniyorum, yeni gelişmeleri takip ediyorum.

Bilgisayar yazılımlarına ilgi duyuyorum. Belediyenin sağladığı imkânlarla üç yıldır kodlama dersi görüyorum. Bu derste bilgisayar, akıllı telefon ve tablet için yazılımların nasıl yapıldığını öğreniyorum. Geçen yıl ilk bilgisayar yazılımımı yaptım. Bu yıl arkadaşlarımla sosyal bilgiler dersi için bir yazılım üzerinde çalışıyoruz. Ders yılı sonuna kadar bu yazılımı tamamlayacağız. Hazırladığımız yazılımlar şimdilik oldukça basit düzeyde ama zamanla daha gelişmiş yazılımlar yapacağıma eminim.

İnsanlara yardımcı olmaktan keyif alıyorum. Matematik dersinde oldukça başarılıyım. Ders çalışma grubumuzda matematikle ilgili konularda arkadaşlarıma yardımcı oluyorum.

İlgi, yetenek ve kişisel özelliklerimi dikkate aldığımda hem bilgisayar yazılımcısı hem de sanal hekim olabileceğimi düşünüyorum. Böylece hastalıkları akıllı aletlerle belirleyebileceğim yazılımlar yapmayı planlıyorum. Bunun için ortaokuldan sonra fen lisesine gitmeyi istiyorum. Üniversitede ise tıp ve bilgisayar yazılımları alanlarında eğitim görmeyi planlıyorum. Üniversiteden sonra bir taraftan mesleğimi yaparken diğer taraftan alanımda uzmanlaşıp bu alanda öğrenciler yetiştirmek istiyorum.

Fatma'nın mesleki tercihlerine yönelik planlaması nasıl yorumlanabilir?



Kaynak: MEB. (2025). 7.Sınıf. s.204

Resim 4.88’de bir öğrencinin belli bir zamandan beri bilgisayar kullanmakta olduğundan bahsedilmiş. Bu ifade genellenebilir nitelikte çünkü bilgisayar ve yazılım teknolojisi her geçen gün daha da gelişmekte ve ulaşılabilir nitelikte olmakta. Belirtilen görsel de yazılım geliştirme çalışmaları ve bunun üzerine çeşitli araştırmaların yapıldığı ifade ediliyor. Ancak burada doğrudan bilgi güvenliği ile ilgili bilgi yer almamakla birlikte bu farkındalık için önemli bir fırsat sunuyor.

Resim 4.89: Etkinlik Kutucuğu

6. DİJİTAL TEKNOLOJİLER VE TİCARET



Sizce insanlar ihtiyaçlarının bir kısmını doğrudan mağazaya giderek karşılamak yerine neden e-ticaretle karşılamaktadır?

Dijital teknolojiler kullanılmaya başlanmadan önce tüketiciler; ihtiyaçlarının tamamını mağaza, market, pazar gibi yerlerden karşılamaktaydı. Üreticiler ürünlerini tarla, bahçe, fabrika, atölye vb. yerlerde üretmekte; dağıtım aşamasında bu ürünler satışın yapılacağı yerlere ulaştırılmakta ve tüketiciler de bu yerlere giderek ürünleri satın almaktaydı (Görsel 5.31).



Görsel 5.31: Üretim, dağıtım ve tüketim ağı



Görsel 5.31'i inceleyerek üretim, dağıtım ve tüketim aşamalarında hangi faaliyetlerin yapıldığını açıklayınız.

Kaynak: MEB. (2025). 7.Sınıf. s.206

Resim 4.89’da dijital teknolojiler ve ticaret başlığı ile günümüzde daha ulaşılabilir olan teknolojinin artık hayatımızın her alanında yer alması ve en çok kullandığımız alanlardan olan e-ticaretin üzerindeki etkisi belirtilmeye çalışılıyor. Ancak burada dijitalleşme ve kullandığımız genel ağ uygulamalarındaki bilgi güvenliği süreçlerine yer verilmediği görülüyor.

Resim 4.90: Bilgi Kutucuğu

Genel ağ teknolojisi ile bilgisayar, tablet bilgisayar, akıllı cep telefonu, TV gibi teknolojilerdeki gelişim ticarete önemli değişikliklere yol açmıştır. Günümüzde firmalar, ürettikleri ürünlerin ticaretini gerçek ortamların yanı sıra sanal ortamlarda da yapabilmektedir. Müşteriler, ihtiyaç duydukları ürünleri genel ağ yoluyla e-ticaret şirketlerinden satın alabilmekte ve bu ürünler, kuryeler aracılığıyla müşterilere güvenli bir şekilde ulaştırılabilmektedir. Günümüzde ürün teslimatı, insansız hava araçları kullanılarak da yapılmaya başlanmıştır; gelecekte e-ticaret alanında bu araçlardan daha fazla yararlanılacağı öngörülmektedir.

Genel ağ üzerinden yapılan alışveriş hem tüketiciler hem de e-ticaret şirketleri açısından kolay ve daha az maliyetlidir. Satış yapılan mekânın kirası, personel gideri, enerji sarfiyatı vb. masraflar ortadan kalktığından e-ticaret, daha kârlı olabilmektedir. Günümüzde gıda maddelerinden teknoloji ürünlerine, tekstilden ev eşyalarına hatta yurt dışından satın alınan prefabrik evlere kadar binlerce ürünün e-ticareti yapılmaktadır. Tüketiciler, e-ticareti kullanarak dağıtımçı şirketlerin aracılığı olmadan ürünlerini doğrudan üreticilerden satın alabilmektedir.

Genel ağ üzerinden bilgisayar oyunları, programları, yazılımları; bilgisayar ve cep telefonu uygulamaları gibi sanal / dijital ürünlerin ticareti yapılabilmektedir. Bu ürünler ücretli veya ücretsiz olabilmektedir. Müşterilerin film izleme, müzik dinleme vb. ihtiyaçlarını genel ağ üzerinden karşılaması, mağazalarda satılan CD, DVD vs.nin satışını düşürmektedir. Bu da müzik ve film sektörü ile ilgili satışların daha çok genel ağ üzerinden yapılması durumunu ortaya çıkarmıştır.

Kaynak: MEB. (2025). 7.Sınıf. s.206

Resim 4.91: Bilgi Kutucuğu

Genel ağ üzerinden alışveriş yapmak her geçen gün kolaylaşmaktadır. Özellikle Covid-19 salgını sürecinde genel ağ üzerinden alışveriş daha da yaygınlaşmış, daha çok firma e-ticarete başlamıştır. E-ticaretle tüketicinin mağazaya gitmesine, fiyat ve kalite karşılaştırması için farklı mağazaları dolaşmasına gerek kalmaz; bütün bu işlemler, genel ağ bağlantısı olan cihazlarla yapılabilir. Kredi kartı, alışveriş kartı vb. kullanılarak ya da kapıda ödeme seçeneği tercih edilerek verilen siparişler, tüketicinin istediği adrese ulaştırılmaktadır (Görsel 5.32). Ancak genel ağ üzerinden yapılan alışverişlerde satın alınan ürünlerin ödemesi yapılırken çok dikkatli olunmalı, hesap bilgileri paylaşılmadan önce sitenin güvenilirliği mutlaka kontrol edilmelidir.



Görsel 5.32: E-ticaretle satın alınan ürünler, kişinin istediği adrese teslim edilir.

E-ticaret, girişimcilere büyük fırsatlar sunmaktadır. Bu sayede az sermayeyle e-ticaret şirketleri kurulabilmekte ve aşağıdaki haber yazısında olduğu gibi başarı hikâyeleri ortaya çıkabilmektedir.



Manisa'da Genel Ağdan Satış Yaparak Başladı! Şimdi Milyonluk Şirketin Sahibi Oldu

Manisa'da kendi işini kurma hayalinin peşinden koşan kadın girişimci D. E. A, bebek ürünlerini genel ağ üzerinden satarak başladığı işinde milyonluk şirketin sahibi oldu. Tek başına başladığı işinde sürekli büyüyerek 25 kişiye istihdam sağlayan kadın girişimci, kadınlara tavsiyelerde bulundu.

Kadınlara asla vazgeçmemeleri noktasında çağrıda bulunan kadın girişimci "Çünkü çok fazla denedim ama en sonunda başardım. Kadınlar vazgeçmesinler, mutlaka çabalarının karşılığını alacaklar. Şu an Türkiye'nin her köşesine mutlaka kargom gitmiştir." dedi.

Genel ağ haberi, 28.11.2019.
(Kısaltılmıştır.)

Kaynak: MEB. (2025). 7.Sınıf. s.207

Resim 4.91’de bilgi güvenliğinin sağlanması konusunda önemli bilgiler yer almaktadır. Genel ağ ve genel ağ üzerinden yapılan ticaretin hayatımızdaki gelişmelerden etkilenmesi ve hayatımıza getirdiği kolaylıklardan bahsedilmiştir. Burada önemli olarak belirtilen husus; genel ağ üzerinden yapılan alışverişlerde satın alınan ürünlerin ödemesinin yapılırken dikkatli olunmalı, hesap bilgileri paylaşılmadan önce sitenin güvenilirliği kontrol edilmelidir şeklindedir.

Resim 4.92: Etkinlik Kutucuğu



Etkinlik Zamanı

Ticaretin geçmişte ve günümüzde nasıl yapıldığını, gelecekte nasıl yapılacağını ilgili kutucuklara yazınız.



Etkileşimli İçerik

Geçmişte ticaret	Günümüzde ticaret	Gelecekte ticaret
.....		
.....		
.....		
.....		

 Dijital teknolojiler üretim, dağıtım ve tüketim ağını nasıl etkilemiştir?

Kaynak: MEB. (2025). 7.Sınıf. s.207

Resim 4.92’de yer alan etkinlikte ticaretin zaman içerisindeki gelişimine değinilmiş teknolojinin ticaret üzerindeki etkisi sorulmuştur. Doğrudan bilgi güvenliğı farkındalığını geliştirici bir bilgi verilmemiştir.

SONUÇ

Bu çalışmada 2024 Sosyal Bilgiler öğretim programı ve ders kitaplarının bilgi güvenli konusunda verimliliği araştırılmış ve bilgi güvenliği boyutunda ne kadar önleyici güvenlik farkındalığı sağladığı incelenmeye çalışılmıştır. Genel olarak bilgi güvenliği konusu özellikle “Teknoloji ve Sosyal Bilimler” öğrenme alanında içerisinde sistematik bir şekilde ele alınmıştır. Ders kitaplarında ise özellikle 4. sınıftan itibaren bilgi güvenliği farkındalığı oluşturulmaya çalışıldığı; üst sınıflarda (5., 6. ve 7.) dijital vatandaşlık, dijital okuryazarlık, telif hakkı, e-ticaret, genel ağ, dijital depolama teknolojileri, çevrimiçi teknolojiler, sosyal mühendislik, dijital ayak izi gibi konular üzerinden daha karmaşık ve bütüncül kavramlara geçiş yapıldığı görülmektedir. Ancak kitaplarda bilgi güvenliğiyle ilgili kavramların teknik yönlerinin zaman zaman yeterince açıklanmadığı ve bazı terimlerin öğrenci düzeyinde somutlaştırılmadığı gözlemlenmiştir. Bu durum, Talan ve Aktürk (2021)’ün çalışmalarındaki ortaokul öğrencilerinde dijital güvenlik konularına ilişkin kavramsal karmaşa bulunduğu dair bulgularıyla paralellik göstermektedir. Buradan hareketle internet adresinin doğruluğunu ve güvenilirliğini nasıl teyit ederiz veya doğrularız şeklinde bilgi güvenliğini sağlayan sorulara ve bunun yanında sosyal mühendislik süreçlerinde sıkça kullanılan sahte internet erişim adresi aldatmacasını nasıl engel olabiliriz sorusuna cevap verebilmek önleyici güvenlik açısından oldukça önemlidir. Örnek verecek olursak e-devlet erişim adresi <https://www.turkiye.gov.tr/> şeklindedir. Burada belirtilmesi gereken gerçek ve güvenilir internet erişim adresinin gov.tr şeklinde bitmesi gerektiğidir. Tek bir farkındalık ile gerçek ve sahte web site ayrımı yapılarak birçok olumsuz sonucun önüne geçilebilir. Bu doğrultuda ders kitaplarında gerek etkinliklerde gerekse diğer görsel ve bilgilendirme kutucuklarında bu bilgiler işlenebilir. Bununla birlikte, ders kitaplarında teknik terimlerin tanımsız sunulması, Çelik ve Kılıçoğlu (2022) müfredat içeriklerinin öğrencinin bilişsel gelişim düzeyine göre yeniden düzenlenmesi gerektiği yönündeki önerileriyle de örtüşmektedir. Ayrıca, bilgi güvenliği boyutundaki temel bilgilerin ve kavramların özellikle görsel ve etkinlik temelli anlatımlarla desteklenmesinin etkili olacağı yönündeki Ünal Peker (2015) çalışması da bu araştırmada elde edilen kitap inceleme verileriyle uyumlu bir eğilimi işaret etmektedir. Sonuç olarak, bu çalışma Türkiye'deki Sosyal Bilgiler öğretim programı ve ders kitaplarının bilgi

güvenliğine ilişkin içeriği sunduğunu, ancak kavramsal netlik, açıklık ve uygulama bütünlüğü açısından bazı geliştirme alanlarının varlığını da işaret etmektedir. Ancak, özellikle teknik kavramların öğrenci düzeyine uygun şekilde sadeleştirilmesi, içeriklerin günlük yaşamla daha somut bağlantılar kuracak biçimde sunulması gibi geliştirme alanları bulunmaktadır.

Öneriler;

- Bilgi güvenliğiyle ilgili teknik kavramlar (örneğin dijital ayak izi, URL, veri işleme) öğrenci düzeyine uygun biçimde sadeleştirilmeli ve örneklendirilmelidir.
- Sınıf içerisi etkinliklerde bilgi güvenliği ile ilgili olumsuz durumlarda karşılaşıldığında ne yapılması gerektiğine dair bilgilendirici hikaye ve drama örneklerine yer verilmelidir.
- Önemli kurum ve kuruluşların web bağlantı adresleri örneklendirilerek bu adreslerin bir tane olduğu ve sahte web bağlantı adreslerinden ayrıştırılmasını sağlayacak bilgiler (.com, .edu, .gov gibi uzantıların açıklamaları yapılmalı) belirtilmelidir.
- Kişisel e-mail adreslerimize gönderilen e-postalar açılmadan önce gönderen kontrolünün yapılması ve gönderildiği web bağlantı uzantı adresi kontrol edilmesi farkındalığını oluşturu bilgileri ve görseller yer almalıdır.
- Ders kitaplarında bilgi güvenliğine dair içerikler yalnızca bir üniteye toplanmamalı, farklı öğrenme alanları ile ilişkilendirilerek disiplinlerarası bir yaklaşım benimsenmelidir.
- Öğretmenlere yönelik bilgi güvenliği eğitimi artırılmalı; etkinlik, içerik ve örnek uygulamalarla desteklenmelidir.
- Öğrencilerin aktif katılım sağlayacağı, bilgi güvenliğini deneyimleyecekleri proje tabanlı etkinliklere ders kitaplarında daha fazla yer verilmelidir.
- MEB tarafından geliştirilen dijital içeriklerde (EBA, interaktif etkinlikler) bilgi güvenliği temalı öğrenme materyalleri çoğaltılmalıdır.
- Dijital paylaşım sitelerinden edinilen bilgilerin kaynak doğrulamasının yapılması ve eleştirel analiz süreçlerini geliştirici bilgiler yer almalıdır.

KAYNAKÇA

- Abraham, S., & Chengalur-Smith, I. (2010). An Overview of Social Engineering Malware: Trends, Tactics, And Implications. *Technology in Society*, 32(3), 183–196.
- Akay, İ. G. (2014). *Bilgi Güvenliği Yönetim Sistemleri: Bilgi Güvenliği Uygulama Mülakatları*. Yayınlanmamış Yüksek Lisans Tezi. Bilecik: Bilecik Şeyh Edebali Üniversitesi, Sosyal Bilimler Enstitüsü.
- Akgün, Ö., & Topal, M. (2015). Eğitim Fakültesi Son Sınıf Öğrencilerinin Bilişim Güvenliği Farkındalıkları: Sakarya Üniversitesi Eğitim Fakültesi Örneği. *Sakarya University Journal of Education*, 5(2), 98–121.
- Akkoyunlu, B., & Kurbanoglu, S. (2003). Öğretmen Adaylarının Bilgi Okuryazarlığı ve Bilgisayar Öz-Yeterlik Algıları Üzerine Bir Çalışma. *Hacettepe Üniversitesi Eğitim Fakültesi Dergisi*, 24(24).
- Alataş, Ş., & Atan, M. (2007). Phishing: İnternet Denizinin Popüler Avlanma Yöntemi, XII. Türkiye’de İnternet Konferansı, Bilkent Üniversitesi, Ankara, 8-10, 226-236.
- Alhassan, M. M., & Adjei-Quaye, A. (2017). Information security in an organization. *International Journal of Computer (IJC)*, 24(1), 100–116.
- Alkalbani, A., Deng, H., & Kam, B. (2015). Organisational Security Culture and Information Security Compliance For e-Government Development: The Moderating Effect Of Social Pressure.
- Altun, N., & Alpan, G. B. (2021). Temel Eğitim Programlarında Dijital Okuryazarlık. *Eğitim ve Toplum Araştırmaları Dergisi*, 8(2), 280–294.
- APWG, Anti-Phishing Çalışma Grubu, Phishing Etkinlik Trendleri Raporu, 2024, <https://apwg.org/trendsreports/> adresinden Ocak 2025 tarihinde erişildi.
- Ateş, S., & Küçük, S. (2023). Öğretmenlerin Bilgi Güvenliği Farkındalık ve Dijital Okuryazarlık Durumlarının İncelenmesi. *Necmettin Erbakan Üniversitesi Ereğli Eğitim Fakültesi Dergisi*, 5(2), 491-534.
- Avcı, Ü., & Oruç, O. (2020). Üniversite Öğrencilerinin Kişisel Siber Güvenlik Davranışları ve Bilgi Güvenliği Farkındalıklarının İncelenmesi. *İnönü Üniversitesi Eğitim Fakültesi Dergisi*, 21(1), 284–303.
- Bağcı, H. (2009). Sosyal Mühendislik ve Denetim. *Denetişim*, (1), 42–51.
- Barcus, F. E. (1959). *Communications Content: Analysis of The Research, 1900–1958*. Yayınlanmamış Doktora Tezi. University of Illinois.
- Baykara, M., Daş, R., & Karadoğan, İ. (2013, Mayıs). Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi. *In 1st International Symposium on Digital Forensics and Security (ISDFS’13)* (Vol. 20, s. 21).

- Can, N. (2002). Eğitim Örgütlerinde İnsan Kaynakları Yönetiminin Bütünleştirme İşleviyle İlgili Görevler. *Gaziantep Üniversitesi Sosyal Bilimler Dergisi*, 5(1), 228–231.
- Canbek, G. (2005). *Klavve Dinleme ve Önleme Sistemleri: Analiz, Tasarım ve Geliştirme*. Yayınlanmamış Yüksek Lisans Tezi. Ankara: Gazi Üniversitesi, Fen Bilimleri Enstitüsü.
- Canbek, G., & Sağiroğlu, Ş. (2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme. *Politeknik Dergisi*, 9(3), 165–174.
- Canbek, G., & Sağiroğlu, Ş. (2007a). Çocukların ve Gençlerin Bilgisayar ve İnternet Güvenliği. *Politeknik Dergisi*, 10(1), 33–39.
- Canbek, G., & Sağiroğlu, Ş. (2007b). Kötücü ve Casus Yazılımlar: Kapsamlı Bir Araştırma. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, 22(1), 121-136.
- Ceyhun, Y., & Çağlayan, M. U. (1997). *Bilgi Teknolojileri Türkiye için Nasıl Bir Gelecek Hazırlamakta*. Türkiye İş Bankası Kültür Yayınları.
- Chandarman, R., & Van Niekerk, B. (2017). Students' Cybersecurity Awareness At a Private Tertiary Educational Institution. *The African Journal of Information and Communication*, 20, 133–155.
- Chandy, J. (2022, Aralık). Review on Malware, Types, and Its Analysis. *International Journal for Research in Applied Science and Engineering Technology*, 10(12), 386–390. <https://doi.org/10.22214/ijraset.2022.47887>
- Christensen, L.B, Johnson, B.R, ve Turner, L.A. (2014). *Araştırma Yöntemleri Desen ve Analiz* (A. Aypay, Çev.). Ankara: Anı Yayıncılık. (2015).
- Cohen, L., Manion, L., & Morrison, K. (2007). *Research Methods in Education* (6.th ed.). New York, NY: Routledge.
- Crowe, A. R. (2006). Technology, Citizenship, and The Social Studies Classroom: Education For Democracy In a Technological Age. *International Journal of Social Education*, 21(1), 111–121.
- Çelik, H., & Kılıçoğlu, G. (2022). Ortaokul Öğrencilerinin Dijital Okuryazarlık Düzeylerinin Belirlenmesi (Determining the digital literacy levels of secondary school students). *Journal of Anatolian Cultural Research (JANCR)*, 6(2), 115–134.
- Çubukcu, A., & Bayzan, Ş. (2013). Türkiye’de Dijital Vatandaşlık Algısı ve Bu Algıyı İnternetin Bilinçli, Güvenli ve Etkin Kullanımı ile Artırma Yöntemleri. *Middle Eastern & African Journal of Educational Research*, 5(1), 148-174.
- Değirmenci, N., & Demiral, D. G. (2023). Bilgi Güvenliği Farkındalığı Üzerine Üniversite Öğrencilerine Yönelik Araştırma. *Karadeniz Sosyal Bilimler Dergisi*, 15(29), 613–635.

- Derin, M. A., & Gençoğlu, M. T. (2020). Ortaokul Öğrencilerinin Bilgi Güvenliği Farkındalığı. *Savunma Bilimleri Dergisi*, (38)r, 159–181.
- Durna, U., & Demirel, Y. (2008). Bilgi Yönetiminde Bilgiyi Anlamak. *Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, (30), 129–156.
- Eminağaoğlu, M., & Gökşen, Y. (2009). Bilgi Güvenliği Nedir, Ne Değildir? Türkiye'de Bilgi Güvenliği Sorunları ve Çözüm Önerileri. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, C11/S4.
- Eravcı, D. B. (2020). Kurumların Dijital Dönüşümü: Büyük Veri. *Çalışma İlişkileri Dergisi*, 11(1), 90–112.
- Ersöz, B., & Özmen, M. (2020). Dijitalleşme ve Bilişim Teknolojilerinin Çalışanlar Üzerindeki Etkileri. *AJIT-e: Academic Journal of Information Technology*, 11(42), 170–179.
- Farmer, L. (2010). 21. Century standarts for information literacy. *Leadership*, 39(4), 20-22.
- Fortinet. (2025). Spyware Definition. *Fortinet Cyberglossary*. Şubat 26, 2025 tarihinde <https://www.fortinet.com/resources/cyberglossary/spyware> adresinden alındı.
- Fortinet. (2025, 26 Şubat). Truva Atı Virüsü Nedir? Fortinet Cyberglossary.Şubat 26, 2025 tarihinde <https://www.fortinet.com/uk/resources/cyberglossary/trojan-horse-virus> adresinden alındı.
- Gökçearslan, Ş., Günbatar, M. S., & Sarıtepeci, M. (2021). Ortaöğretim Öğrencilerinin Bilgi Güvenliği Farkındalıklarının İncelenmesi. *Van Yüzüncü Yıl Üniversitesi Eğitim Fakültesi Dergisi*, 18(1), 354–373.
- Gündüz, M. Z., & Daş, R. (2016). Sosyal mühendislik: Yaygın ataklar ve güvenlik önlemleri. In P. D. M. Sağiroğlu, P. D. M. Alkan, P. D. E. Akyıldız, & D. D. S. Akleyek, Ed, 9.
- Gündüz, M. Z., & Daş, R. (2021). Akıllı Şebekeler: Siber Güvenlik Unsurları ile Veri İletimi. *Bingöl Üniversitesi Teknik Bilimler Dergisi*, 2(2), 47–61.
- Hanus, B., & Wu, Y. A. (2016). Impact Of Users' Security Awareness On Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management*, 33(1), 2–16.
- IBM. (2025). What Is Cybersecurity. *Ibm Think*. Ocak 5, 2025 tarihinde <https://www.ibm.com/think/topics/cybersecurity> adresinden alındı.
- Jones, C., & Mitchell, K. J. (2016). Defining and Measuring Youth Digital Citizenship. *American Behavioral Scientist*, 60(8), 835–855.
- Kağnıcıoğlu, C. H., & Özdemir, E. (2017). Endüstri 4.0 Bağlamında Eskişehir İlindeki KOBİ'lerin Değerlendirilmesi. *PressAcademia Procedia*, 3, 900–908.

- Kamber, E., & Bolatan, G. İ. S. (2019). Endüstri 4.0 Türkiye Farkındalığı. *Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 11(30), 836–847.
- Karaduman, H., & Öztürk, C. (2014). Sosyal Bilgiler Dersinde Dijital Vatandaşlığa Dayalı Etkinliklerin Öğrencilerin Dijital Vatandaşlık Tutumlarına Etkisi ve Dijital Vatandaşlık Anlayışlarına Yansımaları-The Effects of Activities For Digital Citizenship On Students' Attitudes Toward Digital. *Journal of Social Studies Education Research*, 5(1), 38–78.
- Kaspersky. (2025). Botnet Nedir? *Kaspersky*. Şubat 23, 2025 tarihinde <https://www.kaspersky.com.tr/resource-center/threats/botnet-attacks> adresinden alındı.
- Kaspersky. (2025). Adware Nedir? *Kaspersky Resource Center*. Şubat 26, 2025 tarihinde <https://www.kaspersky.com/resource-center/threats/adware> adresinden alındı.
- Kaspersky. (2025). Truva Atı Virüsü Nedir: Türleri ve Temizleme Yöntemleri. *Kaspersky Resource Center*. Şubat 26, 2025 tarihinde <https://www.kaspersky.com.tr/resource-center/threats/trojans> adresinden alındı.
- Kavak, A., & Odabaş, H. (2023). Üniversite Kütüphanelerinde Teknolojik ve Kurumsal Bilgi Güvenliği Önlemlerinin Uygulanma Yeterliliği. *Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 14(2), 293–332.
- Kaya, M. N. Ö. V. A. (2013). Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler. *Güvenlik Stratejileri Dergisi*, 9(18), 145–181.
- Khidzir, N. Z., Mat Daud, K. A., Ismail, A. R., Abd. Ghani, M. S. A., & Ibrahim, M. A. H. (2018). Information security requirement: The relationship between cybersecurity risk confidentiality, integrity and availability in digital social media. In *Regional Conference on Science, Technology and Social Sciences (RCSTSS 2016): Theoretical and Applied Sciences* (s. 229–237). Springer Singapore.
- Korucu, O. (2021). Yeni Normal Dünya Düzeninin Siber Güvenlik ve Bilgi Güvenliğine Etkileri. *Yönetim Bilişim Sistemleri Dergisi*, 7(1), 44–60.
- Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced Social Engineering Attacks. *Journal of Information Security and Applications*, 22, 113–122.
- Lee, J. K., & Doolittle, P. E. (2006). Social Studies and History Teachers' Uses Of Non- Digital and Digital Historical Resources. *Social Studies Research and Practice*, 1(3), 291–311.
- Livingstone, S. (2004). Media Literacy and the Challenge Of New Information and Communication Technologies. *Communication Review*, 7(1), 3–14.
- Lohani, S. (2019). Social Engineering: Hacking Into Humans. *International Journal of Advanced Studies of Scientific Research*, 4(1).

- Martin, A. (2005). DigEuLit–a European Framework for Digital Literacy: A Progress Report. *Journal of eLiteracy*, 2(2), 130–136.
- Mbanaso, U. M., & Dandaura, E. S. (2015). The Cyberspace: Redefining a New World. *IOSR Journal of Computer Engineering (IOSR-JCE)*, 17(3), 17–24.
- Milli Eğitim Bakanlığı. (2024). 4. Sınıf Sosyal Bilgiler Ders Kitabı [PDF]. Şubat 12, 2025 tarihinde https://mufredat.meb.gov.tr/Dosyalar/TTKB/%C4%B0lkokul/4/Sosyal%20Bilgiler/c1_sosyal_bilgiler_4.pdf adresinden alındı.
- Milli Eğitim Bakanlığı. (2024). 5. Sınıf Sosyal Bilgiler Ders Kitabı [PDF]. Şubat 18, 2025 tarihinde https://mufredat.meb.gov.tr/Dosyalar/TTKB/Ortaokul/5/Sosyal%20Bilgiler/c1_sosyal_bilgiler_5.pdf adresinden alındı.
- Milli Eğitim Bakanlığı. (2024). 6. Sınıf Sosyal Bilgiler Ders Kitabı [PDF]. Şubat 25, 2025 tarihinde https://mufredat.meb.gov.tr/Dosyalar/TTKB/Ortaokul/6/Sosyal%20Bilgiler/c1_sosyal_bilgiler_6.pdf adresinden alındı.
- Milli Eğitim Bakanlığı. (2024). 7. Sınıf Sosyal Bilgiler Ders Kitabı [PDF]. Mart 15, 2025 tarihinde https://mufredat.meb.gov.tr/Dosyalar/TTKB/Ortaokul/7/Sosyal%20Bilgiler/c1_sosyal_bilgiler_7.pdf adresinden alındı.
- Milli Eğitim Bakanlığı. (2024). Sosyal Bilgiler Dersi Öğretim Programı (4.–7. sınıflar) [PDF]. Şubat 12, 2025 tarihinde <https://tymm.meb.gov.tr/upload/program/2024programsos4567Onayli.pdf> adresinden alındı.
- Mouton, F., Malan, M. M., Leenen, L., & Venter, H. S. (2014, Ağustos). Social Engineering Attack Framework. In *2014 Information Security for South Africa* (s. 1–9). IEEE.
- NCSS. (2025). What is Social Studies? *National Council for the Social Studies*. Mart 12, 2025 tarihinde <https://www.socialstudies.org/about/definition-social-studies> adresinden alındı.
- NIST Computer Security Resource Center. (2024). Information security [Glossary]. Aralık 22, 2024 tarihinde <https://csrc.nist.gov/glossary/term/infosec> adresinden alındı.
- Önal, İ. (2010). Tarihsel Değişim Sürecinde Yaşam Boyu Öğrenme ve Okuryazarlık: Türkiye Deneyimi. *Bilgi Dünyası*, 11(1), 101–121.
- Özcan, A. B. (2011). Uluslararası Güvenlik Sorunları ve Abd'nin Güvenlik Stratejileri. *Sosyal Ekonomik Araştırmalar Dergisi*, 11(22), 445–466.
- Özdemir, A., & Uluyol, Ç. (2021). Kamu Kurum ve Kuruluşlarında Bilgi Güvenliği Farkındalığı. *Türkiye Sosyal Araştırmalar Dergisi*, 25(3), 649–666.

- Özden, M., & Saban, A. (2019). *Nitel Çalıştırma Paradigma ve Teorik Temeller*. Anı Yayıncılık.
- Peltier, T. R. (2005). Implementing an Information Security Awareness Program. *Information Security Journal: A Global Perspective*, 14(2), 37–49. <https://doi.org/10.1080/19393550500322732>
- Puhakainen, P. (2006). *A Design Theory for Information Security Awareness*. University of Oulu.
- Ribble, M. (2015). *Digital Citizenship in Schools: Nine Elements All Students Should Know*. International Society for Technology in Education.
- Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, 11(4), 89. <https://doi.org/10.3390/fi11040089>
- Samonas, S., & Coss, D. (2014). The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security. *Journal of Information System Security*, 10(3).
- Sancak, K. (2013). Güvenlik Kavramı Etrafındaki Tartışmalar ve Uluslararası Güvenliğin Dönüşümü. *Karadeniz Teknik Üniversitesi Sosyal Bilimler Dergisi*, 6, 123-134
- Savaş, S., Topaloğlu, N., & Yılmaz, M. (2012). Veri Madenciliği ve Türkiye’deki Uygulama Örnekleri. *İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi*, 11(21), 1–23.
- Schlienger, T., & Teufel, S. (2002). Information Security Culture: The Socio- Cultural Dimension in Information Security Management. In *Security in the Information Society: Visions and Perspectives* (s. 191–201).
- Singh, A., Vaish, A., & Keserwani, P. K. (2014). Information Security: Components and Techniques. *International Journal of Advanced Research in Computer Science and Software Engineering*, 4(1).
- Siponen, M. T. (2001). Five Dimensions of Information Security Awareness. *SIGCAS Computers and Society*, 31(2), 24–29.
- Solichin, A., & Ramadhan, E. W. (2017, Ekim). Enhancing Data Security Using DES-Based Cryptography and DCT-Based Steganography. In *2017 3rd International Conference on Science in Information Technology (ICSITech)* (s. 618–621). IEEE. <https://ieeexplore.ieee.org/document/8257187>
- Solomon, M. G., & Chapple, M. (2004). *Information Security Illuminated*. Jones & Bartlett Learning.
- Stanton, J., Caldera, C., Isaac, A., Stam, K., & Marcinkowski, S. (2003). Behavioral Information Security: Defining the Criterion Space. *Proceedings of the 2nd Workshop on Economics and Information Security (WEIS)*.

- Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end-user security behaviors. *Computers & Security*, 24(2), 124–133.
- Syamsuddin, I. (2009). The Application of AHP to Evaluate Information Security Policy Decision Making. *International Journal of Simulation: Systems, Science and Technology*, 10(5).
- Şahinaslan, E., Kantürk, A., Şahinaslan, Ö., & Borandağ, E. (2009). Kurumlarda Bilgi Güvenliği Farkındalığı, Önemi ve Oluşturma Yöntemleri. *Akademik Bilişim*, 9, 11–13.
- Şeker, Ş. (2013). *İş Zekası ve Veri Madenciliği*. Cinius Yayıncılık.
- Şeşen, Y., & Kuzucuoğlu, A. H. (2021). Veri ve Bilgi Güvenliği Bağlamında İstihbarat Faaliyetleri. *Library Archive and Museum Research Journal*, 2(2), 93–110.
- Şişkin, D. Ş. (2020). *Üniversite Kütüphanelerinde Bilgi Güvenliği ve Kişisel Verilerin Korunması: Ankaradaki Üniversite Kütüphanelerinin Değerlendirilmesi*. Yayımlanmamış Yüksek Lisans Tezi. Ankara: Sosyal Bilimler Enstitüsü.
- Taha, N., & Dahabiyeh, L. (2021). College Students' Information Security Awareness: A Comparison Between Smartphones and Computers. *Education and Information Technologies*, 26(2), 1721–1736.
- Tahir, R. (2018). A Study on Malware and Malware Detection Techniques. *International Journal of Education and Management Engineering*, 8(2), 20.
- Talan, T., & Aktürk, C. (2021). Ortaöğretim Öğrencilerinin Dijital Okuryazarlık ve Bilgi Güvenliği Farkındalığı Seviyelerinin İncelenmesi. *Kahramanmaraş Sütçü İmam Üniversitesi Sosyal Bilimler Dergisi*, 18(1), 158–180.
- Teknolojileri, B., Araştırma, İ. K. S., & Başkanlığı, S. G. D. (2022). *Dijitalleşen Dünyada Bilişim Suçları ve Mücadele Yöntemleri*. Sektörel Araştırma ve Strateji Geliştirme Dairesi Başkanlığı.
- Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the Introduction of Information Security Awareness Programmes in Organisations. *European Journal of Information Systems*, 24(1), 38–58.
- Turan, S., & Avcı, E. K. (2018). 2018 Sosyal Bilgiler Öğretim Programı'nın Dijital Vatandaşlık Bağlamında İncelenmesi. *Journal of Education and New Approaches*, 1(1), 28-38.
- Ulaşanoğlu, M. E., Yılmaz, R., & Tekin, M. A. (2010). Bilgi Güvenliği: Riskler ve Öneriler. *Bilgi Teknolojileri ve İletişim Kurumu*, Ankara.
- Ünal Peker, D. (2015). Bir eğitim programındaki dijital vatandaşlık öğeleri ve ortaöğretim öğrencilerinin dijital vatandaşlık düzeylerinin belirlenmesi. 24. *Ulusal Eğitim Bilimleri Kongresi*, Niğde, Türkiye.

- Vardal, N. (2009). *Yükseköğretimde Bilgi Güvenliği: Bilgi Güvenlik Yönetim Sistemi için Bir Model Önerisi ve Uygulaması*. Yayınlanmamış Doktora Tezi. Ankara: Gazi Üniversitesi, Eğitim Bilimleri Enstitüsü.
- Vasani, V., Bairwa, A. K., Joshi, S., Pljonkin, A., Kaur, M., & Amoon, M. (2023). Comprehensive Analysis of Advanced Techniques and Vital Tools for Detecting Malware Intrusion. *Electronics*, 12(20), 4299. <https://doi.org/10.3390/electronics12204299>
- Voogt, J., Fisser, P., Pareja Roblin, N., Tondeur, J., & Van Braak, J. (2013). Technological Pedagogical Content Knowledge: A Review of the Literature. *Journal of Computer Assisted Learning*, 29(2), 109–121.
- Vural, Y. (2007). *Kurumsal Bilgi Güvenliği ve Sızma (Penetrasyon) Testleri*. Yayınlanmamış Yüksek Lisans Tezi. Ankara: Gazi Üniversitesi, Fen Bilimleri Enstitüsü.
- Yalçın, A. (2022). Sosyal Bilgiler, Dijital Okuryazarlık ve Artırılmış Gerçeklik Uygulamaları. In *Sosyal Beşerî ve İdari Bilimler Temel Alanında Akademik Çalışmalar VI* (s. 19–30).
- Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., & Sprissler, E. (2018). Finding the Weakest Links in the Weakest Link: How Well Do Undergraduate Students Make Cybersecurity Judgment? *Computers in Human Behavior*, 84, 375–382.
- Yee, C. K., & Zolkipli, M. F. (2021). Review on Confidentiality, Integrity and Availability in Information Security. *Journal of ICT in Education*, 8(2), 34–42.
- Yıldırım, A., & Şimşek, H. (2008). *Sosyal Bilimlerde Nitel Araştırma Yöntemleri*. Ankara: Seçkin Yayıncılık.
- Yıldırım, Ö.F. (2013). *The Role of Extra-Curricular Activities on Students' Knowledge, Skills, and Attitudes Toward Climate Change, Climate Change Adaption and Mitigation (M.S. thesis)*. Middle East Technical University. Ankara, Türkiye.
- Yılmaz, H. (2014). Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması ve Bilgi Güvenliği Risk Analizi. *Denetim*, (15), 45–59.
- Wagner, A., & Brooke, C. (2007). Wasting Time: The Mission Impossible With Respect to Technology-Oriented Security Approaches. *Electronic Journal of Business Research Methods*, 5(2), 117–124.
- WASD. (2025). Dijital 2025: Dijitalin Küresel Durumuna İlişkin Temel Rehber. We Are Social. Haziran 15, 2025 tarihinde <https://wearesocial.com/uk/blog/2025/02/digital-2025-the-essential-guide-to-the-global-state-of-digital/> adresinden alındı.

WASD. (2025). We Are Social 2025: Global ve Türkiye Verileriyle Dijital Dünya. Clicksus. Mayıs 14, 2025 tarihinde <https://www.clicksus.com/we-are-social-2025-global-ve-turkiye-verileriyle-dijital-dunya> adresinden alındı.

Whitman, M. E., & Mattord, H. J. (2012). *Principles of Information Security*. Cengage Learning.

Wiersma, W. (2000) Research Methods in Education: An Introduction. 7th Edition, Boston, MA



ÖZ GEÇMİŞ

Adı ve Soyadı : Talha Hakan KAYGISIZ

Bildiği Yabancı Diller :

Aldığı Sertifikalar :

Uzmanlık Alanı :

Derece	Bölüm/Program	Üniversite	Yıl
Lisans	Sosyal Bilgiler Öğretmenliği	Atatürk Üniversitesi	2015
Y. Lisans			

Görevler :

Görev Unvanı	Görev Yeri	Yıl

Eserler:

A. Uluslararası hakemli dergilerde yayımlanan makaleler:

A1.

B. Uluslararası bilimsel toplantılarda sunulan ve bildiri kitaplarında (proceedings) basılan bildiriler:

B1. Kaygısız, T. H. (2025). Sosyal Bilgiler Öğretim Programı ve Ders Kitaplarında Bilgi Güvenliği. 13. Uluslararası New York Sosyal, Beşeri, İdari ve Eğitim Bilimlerinde Akademik Çalışmalar Kongresi.

C. Yazılan ulusal/uluslararası kitaplar veya kitaplardaki bölümler:

C1. Yazılan ulusal/uluslararası kitaplar:

C1.1.

C2. Yazılan ulusal/uluslararası kitaplardaki bölümler:

C2.1.....

D. Ulusal hakemli dergilerde yayımlanan makaleler:

D1.....

E. Ulusal bilimsel toplantılarda sunulan ve bildiri kitaplarında basılan bildiriler:

E1.....

F. Sanat ve tasarım etkinlikleri:

F1.....

G. Diğer yayınlar: (Yukarıdaki maddelerde yer alan başlıklardaki kategorilere girmeyen ve belirtilmek istenen tüm eserler bu maddenin altında belirtilecektir.)

G1.....

