JMTPR
Journal of Management Theory and Practices Research

Journal of **M**anagement **T**heory and **P**ractices **R**esearch
Cilt/Volume :5 | Sayı/Issue: 1 | Haziran/June 2024

AKILLI TELEFON UYGULAMALARININ KULLANICI BAZLI SİBER GÜVENLİK FARKINDALIĞI[1]

Esma ERDOĞAN[2] Mustafa COŞAR[3]

Makale İlk Gönderim Tarihi / Recieved (First): 15.02.2024 **Makale Kabul Tarihi / Accepted:** 29.04.2024

Atıf/©: Erdoğan, E., Coşar, M., (2024). Akıllı Telefon Uygulamalarının Kullanıcı Bazlı Siber Güvenlik Farkındalığı. Journal of Management Theory and Practices Research, 5(1), 15-33

Özet

Dijital ve mobil yaşam koşulları insanları hızlı ve pratik olarak erişim ve kullanım alışkanlıklarına sürüklemektedir. Akıllı telefonlar mobil uygulamalar yardımıyla iletişimden ticarete, eğitimden sağlığa pek çok günlük hayat faaliyetini yapma fırsatı sunmaktadır. Bu fırsatları değerlendirirken bilgi güvenliği unutulmaması gereken bir kavram olarak ortaya çıkmaktadır. Milyonlarca kullanıcı, cihaz ve uygulamanın etkileşimde olduğu bir ortamda kötü niyetli yaklaşımlara karşı temel bazı güvenlik önlemlerinin alınması gerekmektedir. Bu çalışmada, özellikle çocuk ve gençlere dokunma ve örnek olma niteliği olan öğretmenlerin bir mobil uygulama yüklerken nelere dikkat ettiği, uygulama hakkında ne tür bilgiler topladığı ve uygulamanın cihaz içerisinde çalışırken ne tür erişim izinleri verdiği gibi farkındalık düzeyleri belirlenmeye çalışılmıştır. Araştırma, toplam 84 katılımcı ile bir anket uygulaması sonucunda elde edilen veriler üzerinden yürütülmüştür. Araştırma bulgularına göre, katılımcıların cihazlarına uygulama indirmeden önce uygulama hakkında bilgi sahibi olmaları, çeşitli ön incelemelerde bulunmaları ve kullanıcı yorumlarını okumaları gibi parametreleri içeren bilgi toplama faktörüne göre güvenlik farkındalıklarının %74,4 olduğu görülmüştür. Ardından, uygulama indirme sırasında uygulamanın cihaz üzerindeki erişim talepleri ve katılımcıların bu talebe karşın verdikleri erişim izinleri konusundaki bilgileri ve farkındalıkları ise %78,2 olduğu bulunmuştur. Son olarak, tüm katılımcıların mobil uygulamalardaki güvenlik zafiyetlerine yönelik önlem alma farkındalık düzeylerinin ise %79,7 olduğu tespit edilmiştir.

Anaktar Kelimler: Siber Güvenlik, Bilgi Güvenliği, Mobil Uygulama, Mahremiyet, Farkındalık Düzeyi

1 Bu makale, 2022 yılında 8.Hitit Öğrenci Kongresi'nde Özet Bildiri şeklinde sunumu yapılan "Öğretmenlerin Akıllı Telefonlarda Kullanılan Mobil Uygulamaların Güvenlik Farkındalık Düzeylerinin İncelenmesi: Çorum İli Örneği" İsimli bildirinin güncellenmiş ve genişletilmiş halidir.

2 Yüksek Lisans, Hitit Üniversitesi, esmardgn19@gmail.com ,0009-0001-4595-0179

3 Dr.Öğr.Üyesi, Hitit Üniversitesi, mustafacosar@hitit.edu.tr, 0000-0001-6482-4592

USER BASED CYBER SECURITY AWARENESS OF SMARTPHONE APPLICATIONS

Citation /©: Erdoğan, E., Coşar, M., (2024). Akıllı Telefon Uygulamalarının Kullanıcı Bazlı Siber Güvenlik Farkındalığı. Journal of Management Theory and Practices Research, 5(1), 15-33

Abstract

Digital and mobile living conditions lead people to access and use habits quickly and practically. Smartphones offer the opportunity to do many daily life activities such as communication, trade, education and health with the help of mobile applications. While evaluating these opportunities, information security emerges as a concept that should not be forgotten. In an environment where millions of users, devices and applications interact, some basic security measures must be taken against malicious approaches. In this study, it has been tried to determine the level of awareness of teachers, who are an example to children and young people, what they pay attention to when installing a mobile application, what kind of information they collect about the application, and what kind of access permissions the application gives while working on the device. The research was carried out on the data obtained as a result of a questionnaire application with a total of 84 participants. According to the research findings, it was seen that the security awareness of the participants was 74.4% according to the information collection factor, which includes parameters such as having information about the application before downloading the application to their devices, making various preliminary reviews and reading user comments. Afterwards, it was found that the knowledge and awareness of the application's access requests on the device during the application download and the access permissions given by the participants in response to this request was 78.2%. Finally, it was determined that the awareness level of all participants to take precautions against security vulnerabilities in mobile applications was 79.7%.

Keywords: Cybersecurity, Information Security, Mobile Application, Privacy, Awareness Level

1. GİRİŞ

Özellikle 2000 yılında başlayan ve milenyum ismiyle anılan bilgi ve iletişim çağının insanlığa sunduğu en önemli değişim dijital ve mobil bir yaşam olmuştur. Bu yaşam penceresi aralandığında her yaştan bireyin dijitale ve mobil hayata hızlı bir şekilde uyum sağladığı görülmektedir. Bu alanda ilk akla gelen teknoloji ise mobil akıllı telefonlar gelmektedir. Mobil bir telefonun olmazsa olmazı iletişim kurma, internete bağlanma, fotoğraf ve video çekimleri yapma, konum ve güzergâh belirleme, sosyal medya ortamlarını takip ve diğer günlük aktiviteler gelmektedir.

Bilgi ve İletişim Teknolojilerinin (BİT) gelişimiyle birlikte akıllı telefonlar günlük hayatın önemli bir yerini tutmaktadır. Her geçen gün kullanıcı sayısı ve teknik özellikleri giderek artan akıllı telefonların işletim sistemi ve içerisinde çalışan uygulamaları da gelişerek arttığı görülmektedir. Akıllı telefonlar yalnızca iletişim aracı değil, aynı zamanda mobil bilgisayar özelliği taşıyan karmaşık birer teknolojik cihazlardır. İçerisinde ses ve görüntü alış-verişi sağlayan multimedya modüller, ortam değişkenlerini algılayabilen, izleyebilen ve ölçebilen sensörler ve hayatın pek çok aşamasında kullanılabilecek ek modüllerle donatılmaktadırlar. Bu tür donanımsal özellikleri çalıştırabilecek ve onları işler hale getirebilecek sayısı milyonları aşan uygulamalar geliştirilmektedir.

Her teknolojik gelişmenin faydalarının olduğu kadar zararları da olduğu bilinmektedir. Siber tehdit ve saldırılar önlem alınmadığında kullanıcının verisine, cihazına ve imajına çok çeşitli maddi ve manevi zararlar verebilmektedir. Özellikle son yıllarda dijital sistemlere yapılan siber saldırıların arttığı görülmektedir. Cybercrime Magazine (2022) yayınladığı bir raporunda; 2021'de küresel siber suç hasarı günde 16,4 milyar dolar, saatte 684,9 milyon dolar, dakikada 11 milyon dolar ve saniyede 190.000 dolar olarak gerçekleştiğini vurgulamaktadır. Bu sayıların 2025 yılına gelindiğinde 10,5 trilyon dolara ulaşacağı öngörülmektedir. Türkiye'de de durum bundan pek farklı değildir. 2020 yılında cep telefonlarına yapılan siber saldırılarının sayısının binlere ulaştığı görülmektedir.

Tekerek ve Tekerek (2013) ilköğretim ve lise düzeyinde öğrenim gören öğrencilerin bilgisayar ve internet güvenliği farkındalık seviyelerini ortaya koymaya çalışmışlardır. Araştırmada öğrencilere, internet kullanımının amacı, kaçak program indirme ve kullanımı, sohbet odaları kullanımı ve sakıncalı adreslere bağlanma gibi kullanım farkındalığını belirlemeye çalışmışlardır. Lise öğrencilerin ilkokul öğrencilerine göre farkındalık düzeylerinin daha yüksek çıktığını, kız öğrencilerin farkındalıklarının erkek öğrencilere göre daha yüksek çıktığını belirlemişlerdir.

Çocukların siber ortamlarda güvenliğinin sağlanmasında öğretmenlerin rolünün büyük olduğu bilinmektedir. Amerika Birleşik Devletlerinin ulusal bilgi güvenliği raporunda, öğrencilere çok az öğretmenin temel internet kullanım becerilerini öğrettikleri belirtilmektedir. Örneğin öğretmenlerin %23'ü güçlü şifre oluşturma, %34'ü kişisel bilgileri internette kullanma ve %33'ü özel hayata saygı gösterme ile ilgili konularda öğrencileri bilgilendirdiğini belirtilmiştir (Tekerek ve Tekerek, 2013).

Canoğulları (2021)'deki araştırmasında, 310 ilkokul ve ortaokul öğretmeninin bilgi güvenliği farkındalıklarını belirlemeye çalışmıştır. Araştırmanın sonuçlarına göre, öğretmenlerin bilgi güvenliği farkındalık düzeyleri orta düzeyin biraz üzerinde çıkmıştır. Öğretmenlerin cinsiyetlerine göre dağılımında erkek öğretmenlerin farkındalıklarının daha yüksek olduğu, yaşa göre 24-30 yaş lehine anlamlı farklılığın olduğu ve son olarak branşa göre ise, birbirlerine yakın düzeyde olduğu belirlenmiştir.

Literatürde öğrencilerin, ebeveynlerin, öğretmenlerin ve diğer kesimlerin farklı yaş, branş, bölge ve eğitim düzeyine göre bilgi güvenliği farkındalıklarını ölçen (Chen vd., 2008; Güldüren, 2013; Elçi ve Sarı, 2017; Yılmaz ve Ezin, 2017; Taner ve Kılıç, 2019; Derin ve Gençoğlu, 2020; Aljohni vd.

2021; Talan ve Aktürk, 2021; Keser ve Yayla, 2021; Uzun ve Coşar, 2022; Aksoğan ve Atıcı, 2023; Chang vd. 2023) pek çok araştırmaya rastlamak mümkündür. Ancak, mobil telefon ve uygulamaları ile ilgili bilgi güvenliği farkındalığı konusunda az sayıda çalışma ile karşılaşılmıştır. Bu yönüyle bu araştırmanın özgün olduğu ve yenilikçi yönünün var olduğu düşünülmektedir.

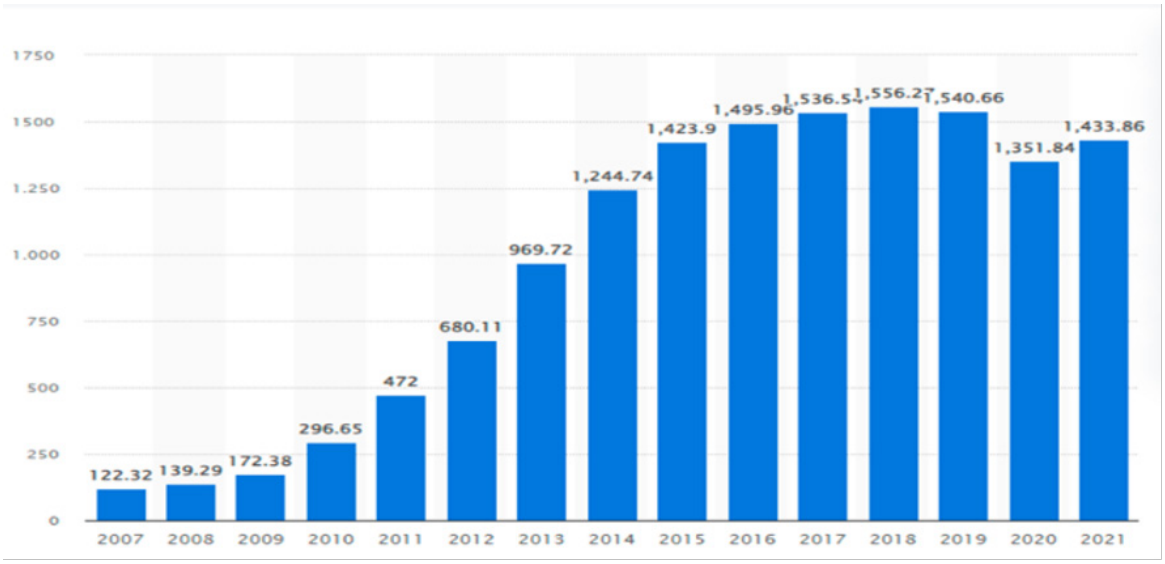
Bu çalışmada, özellikle çocuk ve gençlerin hayatına dokunma ve örnek olma niteliği olan öğretmenlerin mobil uygulamaların güvenlikleri hakkındaki düşünceleri ve bilgi güvenliği farkındalık düzeyleri ortaya konmaya çalışılmıştır. Öğretmenlerin mobil cihazlara uygulama indirirken dikkat düzeyleri, uygulama hakkındaki ön bilgileri, uygulamaların erişim taleplerine karşı hangi izinleri verdikleri ve bu izinlerin nelere yol açabileceği gibi bilgi güvenliği farkındalıklarının yanında temel bazı güvenlik önlemlerini alıp almadıkları belirlenmeye çalışılmıştır.

2. KAVRAMSAL ÇERÇEVE

Mobil telefon, cep telefonu, akıllı telefon gibi çeşitli isimlerde anılmaktadır. Bu telefonlar, donanım olarak kasa, ekran, anakart, devre elemanları, bağlantı modülleri, sensörler, hafıza ve güç üniteleri gibi temel parçalardan oluşmaktadır. Yazılım olarak ise, işletim sistemi ve farklı amaçlar için geliştirilmiş farklı özelliklere sahip uygulamalardan oluşmaktadır.

Şekil 1'de verilen grafiğe bakıldığında, 2007-2009 yılları arasında 100 milyonlar civarında olan akıllı telefon satış rakamlarının 2021 yılına gelindiğinde 1.4 milyarı aştığı raporlanmaktadır. Bu artışın 12 kata yakın bir oranda artmış olması dikkatleri üzerine çekmektedir.

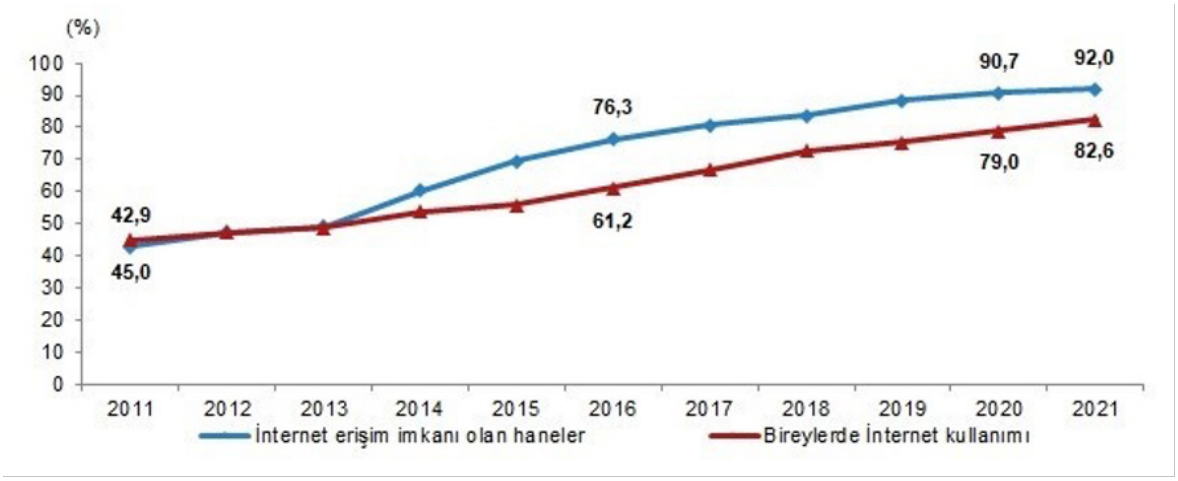
Şekil 1. 2007-2021 Yılları Arasında Dünya Çapında Son Kullanıcılara Satılan Akıllı Telefon Sayısı



Kaynak: (Statista, 2022)

TUİK'in "Hane Halkı Bilişim Teknolojileri (BT) Kullanım Araştırması" raporuna göre, Türkiye'de 2021 yılı itibariyle 16-74 yaş aralığında ki bireylerin %94,9'unun akıllı telefon kullanıcısı olduğu belirtilmektedir. Aynı raporda, 2021 yılında hanelerin %92,0'ının evden internete erişim olanağına sahip olduğu, tüm bireylerinde %82,6'sının bireysel internet kullanıcısı olduğu belirlenmiştir. Şekil 2'de görüldüğü gibi, internet kullanımının 2011-2021 yılları arasındaki on yıllık değişimi özetlenmeye çalışılmıştır (TUİK, 2021).

Şekil 2. 2011-2021 Yılları Arasında İnternet Erişim Olanağı Olan Haneler ve Bireylerde İnternet Kullanımı Oranları



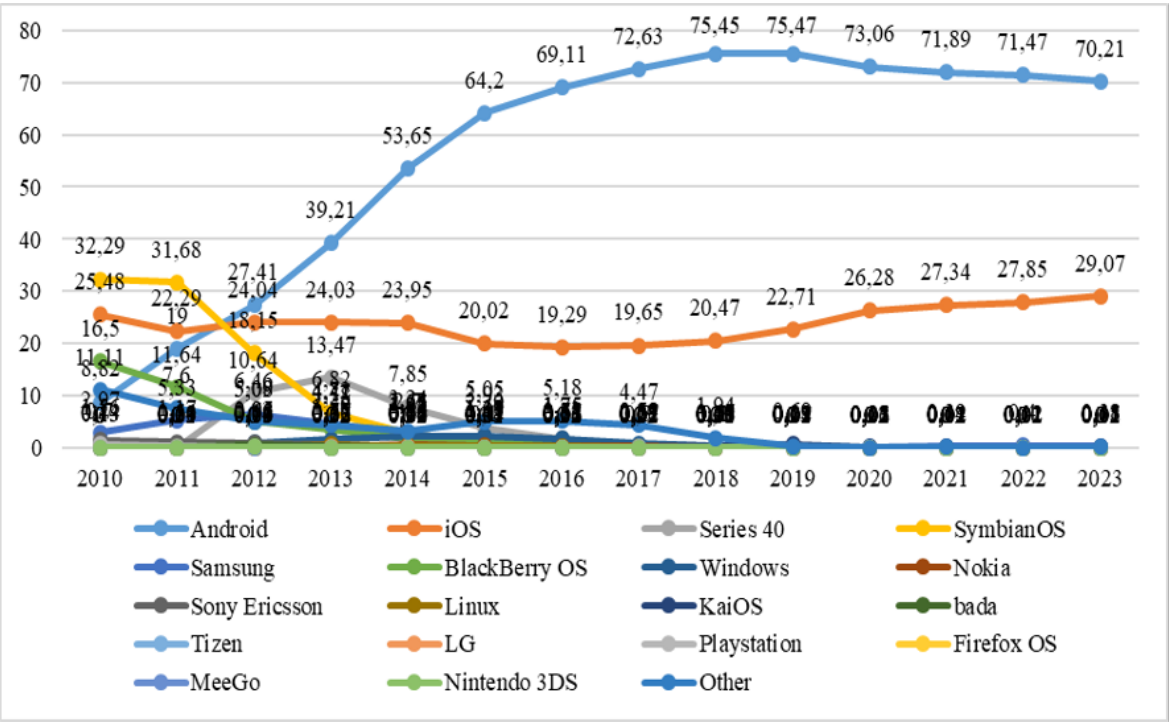
Kaynak: (TUİK, 2021)

Akıllı telefon ve internet kullanımının bu kadar hızla artmasındaki etkenlerin başında, kullanım kolaylığı ve içerisinde hayatı kolaylaştıran birçok uygulama ve programın çalıştırılabilmesi olduğu söylenebilir. Akıllı telefonlar kullanıcılarına telefon görüşmeleri yapmalarını sağlamak yanında, çoğu bilgisayarlarda bulunan e-posta alışverişi, ofis belgelerini düzenlemek, kişisel notlarını tutmak, takvim ile hatırlatma ve planlamalar yapmak gibi çok çeşitli işlemi gerçekleştirmelerine olanak tanımaktadır (Kim ve Hovav, 2011).

Akıllı telefonların içerisine kurulan mobil işletim sistemi cihazın donanım birimlerinin görevlerini yapmasını ve kullanıcı ile arasındaki iletişimi kurmasını sağlayan temel yazılımdır. Asıl görevi cihazın çalışmasını sağlamaktır. En yaygın kullanılan mobil işletim sistemlerine örnek olarak; Android, IoS, Windows Mobile, HarmonyOS, MIUI, PalmOs ve BlackBerry verilebilir.

StatCounter kuruluşunun 2023 yılında paylaştığı bir araştırma raporuna göre 2010-2023 yılları arası mobil işletim sistemlerinin dünya geneli pazar paylarına göre 2023 yılında ilk sırayı %70'lik bir oran ile Android işletim sistemi, %29'luk bir oranla ikinci sırayı İOS işletim sistemi, %0,1'ler civarında diğer işletim sistemlerinin aldığı belirtilmiştir. Bu işletim sistemlerinin isimleri ve yıllara göre kullanım oranlarındaki değişimi Şekil 3'te gösterilmiştir.

Şekil 3. Dünya Geneli Akıllı Telefon İşletim Sistemi Pazarı

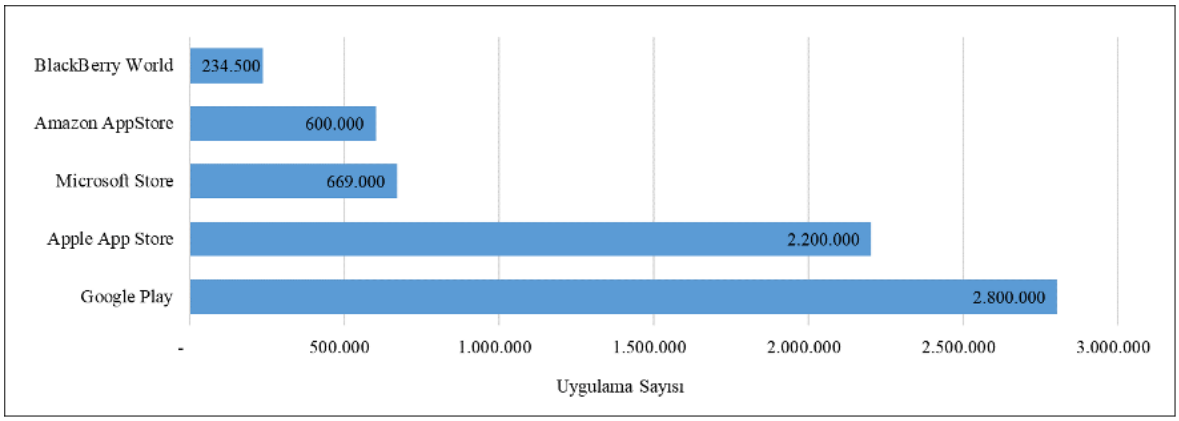


Kaynak: (StatCounter, 2023)

Akıllı telefonda kullanılan işletim sistemine göre kullanıcıya sunulan uygulamalarda çeşitlilik göstermektedir. Bu uygulamaları işletim sisteminin yapısına ve sürümüne göre çeşitli isimlerde ve özelliklerde bu marketlerde yer aldığı görülmektedir. En çok kullanılan işletim sistemlerinin uygulama marketleri, Google Android işletim sistemi için Google Play, İOS işletim sitemi için, Apple App Store uygulama marketi ve Windows işletim sistemi için Microsoft Store mağazası kullanılmaktadır.

Mobil uygulamalar üzerine yapılan bazı araştırmalara göre Google Play, 2 milyon 800 bin adet farklı uygulamaya ev sahipliği yapmaktadır. Şekil 4'te verilen grafiğe bakıldığında, ikinci sırada Apple'ın App Store uygulama marketinin 2 milyon 200 bin adet uygulamaya yer verdiği görülebilir. Ayrıca, Microsoft Store, Amazon Appstore ve BlackBerry Word gibi farklı uygulama marketlerinin de uygulama sayılarının yüzbinlere ulaşmış olduğu görülmektedir.

Şekil 4. Uygulama Marketlerindeki Toplam Uygulama Sayıları



Kaynak: (Teknolojituru, 2017)

Uygulama marketlerinde yer alan bu uygulamaların bir kısmı ücretli, bir kısmı da ücretsiz olarak kullanıcıya sunulmaktadır. Google Play uygulama marketine bakıldığında mevcut uygulamaların %96,3'ünün ücretsiz, %3,7'sinin de ücretli olarak kullanıcıya sunulduğu görülmektedir (Teknolojituru, 2017). Bu oran ilk bakışta doğru gibi görünse de, bazı uygulamaların ücretsiz olarak sunulduktan sonra tam olarak çalıştırılabilmesi için uygulama içi satın almalar ile ücrete tabi olduğu unutulmamalıdır.

Apple firmasının 2022 yılı Uygulama Mağazası Şeffaflık Raporuna (2022 App Store Transparency Report) göre, mağazasında 1.783.232 adet uygulamanın olduğunu, bu uygulamaların bazılarının ön inceleme sırasında bazılarının da son değerlendirmelerden sonra mağaza listesinden kaldırıldığı belirtilmektedir. Mağazadan kaldırılan uygulamaların sayıları ve kaldırılma nedenleri Tablo 1'de özetlenmeye çalışılmıştır (Apple, 2023).

Tablo 1. Uygulamanın Apple Uygulama Mağazasından Kaldırılma Nedenleri

Kaldırılma Nedeni	**Uygulama Sayısı**
Performans Değerleri	1.018.415
Yasal Düzenlemeler	441.972
Tasarım Özellikleri	212.464
Ticari Kaygı	152.391
Güvenlik Açıkları	92.598
Diğer	79.736

Kaynak: (Apple, 2023).

Kullanıcılar internet bankacılığı, sosyal medya uygulamaları, e-devlet, eğitim ve iş hayatlarıyla ilgili kişisel verilerinin olduğu farklı uygulamalar kullanmaktadırlar. Bu uygulamalar akıllı telefona indirildiğinde, uygulamaları tam kapasitede kullanabilmek için mobil cihaz üzerinde bazı ayarlara erişim izinlerinin verilmesi gerekmektedir.

Karlı, Doğru ve Doğru (2018)'deki çalışmalarında kullanıcıların uygulamalara verdikleri izinleri listelemişlerdir. Günümüzde yeni uygulama mağazalarının ve uygulama geliştirme yöntemlerinin eklenmesi ve kullanıcı davranışlarının da değişmesi nedeniyle farklı iziler de ortaya çıkmaktadır. Bu izinlerin güncel listesi aşağıdaki şekilde oluşturulmuştur.

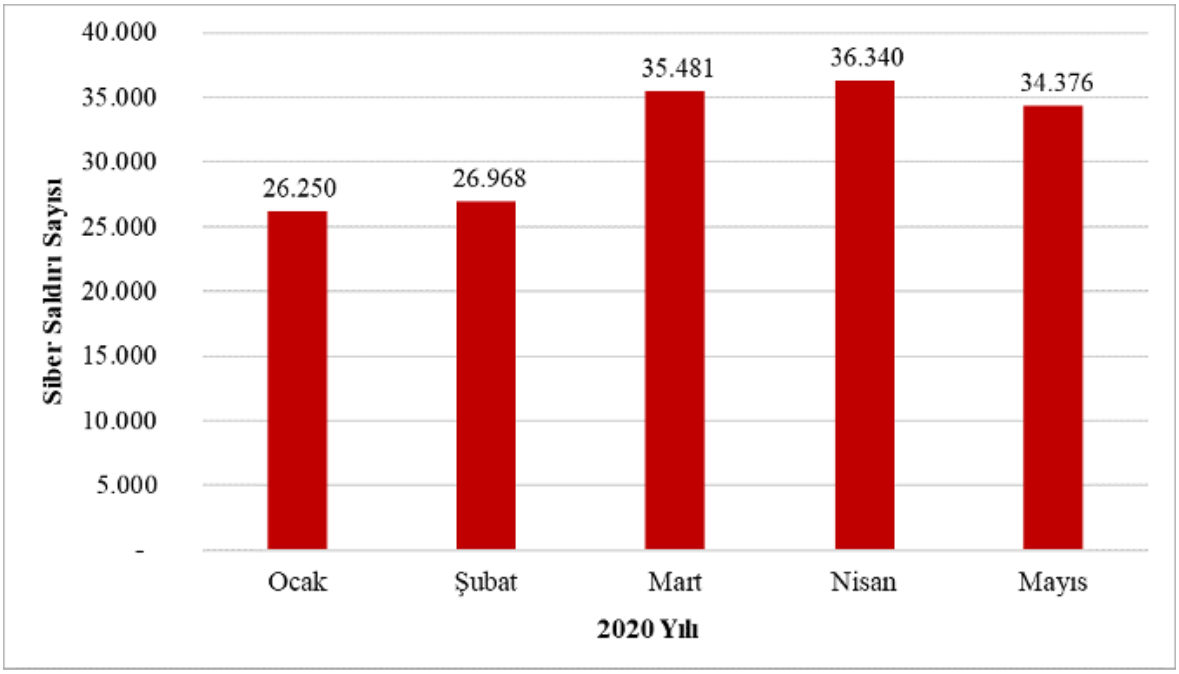
- **Telefon ayarları izni:** Telefonun cihaz ayarları, uygulama özellikleri ve kullanıcı tercihlerinin yapıldığı ayarlar bölümüne erişim iznidir. Bu izin telefonun donanım ve yazılım ayarlarını yetkisiz ve izinsiz bir şekilde başkalarının yönetime açabilir.
- **Bağlantı izni:** Telefondan bulunan ve diğer cihazlarla bağlantı yapmayı sağlayan Bluetooth, Wi-Fi ve Kızılötesi gibi ağ modüllerine erişim iznidir. Bu izin ile bağlantı kontrolü ve veri iletim kontrolü yetkisiz ve izinsiz takip edilebilir.
- **Depolama birimleri izni:** Telefonda bulunan bellek (RAM, Disk, Manyetik Kart… vb.) depolama birimlerine erişim iznidir. Telefonda depolanan kayıtlı bilgi ve belgelerin yetkisiz ve izinsiz erişimine izin verilmiş olur.
- **Rehber izni:** Telefon içerisinde kayıtlı kişi listesi olan rehbere erişim iznidir. Bu izin ile rehberde katılı olan isim, telefon numarası, e-posta adresi ve diğer tanıtıcı bilgilerin erişimi sağlanmış olur. Bu bilgilere arama listelerinde yer alan son gelen ve giden aramalar da dâhil olabilir.
- **Mesaj izni:** Telefon kartı üzerinden yapılan ve SMS (Short Message Service) adı verilen tüm mesajların erişim iznidir. Bu izin sonucunda mesaj göndereni, içeriği ve diğer eklentileri erişime açılmış olur.
- **Takvim izni:** Özel ve iş amaçlı etkinliklerin yer ve zamanının kaydedildiği telefon takvimine erişim iznidir. Uygulama bu erişim izni ile takvim verilerinin gizliliği ve güvenliğini ihlal ederek kayıtları okuyabilir, alıp paylaşabilir.
- **Kamera izni:** Cihazda bulunan ön ve arka kameraların erişim iznidir. Uygulama bu erişim izniyle kullanıcıdan habersiz fotoğraf ve video çekebilir.
- **Mikrofon izni:** Telefonun ses alma ve kaydetme özelliğine erişim iznidir. Bu erişim izni ile iletişim sırasındaki ve ortamdaki diğer konuşma seslerinin tümünün dinlenmesi ihlali söz konusu olabilir.
- **Konum bilgisi izni:** Telefonun donanımında yer alan GPS (Global Positioning System) modülü yardımıyla kullanıcının anlık konum bilgisinin erişim iznidir. Bu izin sayesinde kişinin nerede olduğu yetkisiz bir şekilde elde edilmiş olur.
- **Galeri izni:** Telefonda bulunan fotoğraf ve videoların bulunduğu galeriye erişim iznidir. Bu izin ile telefon kamerası ile çekilmiş veya daha farklı ortamlardan alınarak kaydedilmiş görüntü dosyalarının erişimi yapılabilir.
- **Diğer çevre birim izinleri:** Telefonda yer alan sensörler tarafından toplanan bilgilere erişim iznidir. Bu izin sayesinde sağlık bilgileri, ortam ısısı, nemi, mekânsal özellikler vb. bilgilere erişim yapılabilir.
- **Diğer uygulama izinleri:** Telefonda yer alan web tarayıcı, sosyal medya uygulamaları ve diğer amaçlar için kullanılan uygulamalara ve bunların verilerine erişim iznidir.

Yukarıda sıralanan izinler yetkisiz ve izinsiz erişime izin vererek bilgi çalınmasına, değiştirilmesine ve paylaşılmasına neden olmaktadır. Uygulama indirme ve telefona yükleme sırasında istenen bu izinler akıllı telefonlarda gizlilik ve güvenlik açığı oluşturmaktadır. Bu açığı kullanan yetkisiz ve kötü niyetli kişiler kullanıcının mahrem bilgilerine erişerek özel hayatın gizliliğini ve mahremiyetini tehlikeye atmaktadırlar. Bu güvenlik açığı kötü amaçlı yazılım üreten yazılım korsanlarının da (hacker) harekete geçmesine sebep olmaktadır. Bundan dolayı akıllı telefonlara yapılan siber saldırı sayıları da giderek

artmakta ve kullanıcılar için tehlike arz etmektedir.

CyberMag Siber Güvenlik Dergisinde paylaşılan bir yazıda, Türkiye'de Ocak-Haziran 2020 döneminde ilk beş aylık mobil telefon kullanıcılarına yönelik siber saldırıların sayısının 159.415'e ulaştığı belirtilmektedir (CyberMag, 2022). Şekil 5'teki verilere bakıldığında toplam 159.415 olan bu saldırıların aylık bazda, 2020 yılının ilk iki ayında 26 binler sınırından son üç ayda 35 binler sınırına ulaştığı görülmektedir. Bu sayıların sadece raporlanan verileri içerdiği unutulmamalıdır. Raporlanmayan verilerde dikkate alındığında bu sayıların daha da artabileceği düşünülmektedir.

Şekil 5. 2020 yılında Türkiye'de Akıllı Telefonlara Yapılan Siber Saldırı Sayıları



Kaynak: (CyberMag, 2022)

Qamar, Karim ve Chang (2019) yılındaki çalışmalarında mobil cihazlara yönelik zararlı yazılımların bir incelemesini yapmışlardır. Araştırmaya göre, incelenen Android uygulamalarının 53'ünde kişilerin, resimlerin, Wi-Fi bilgilerinin, cihaz ve SIM verilerinin kesilmesine ve ses kaydına erişilmesine neden olan yeni RedDrop adında kötü niyetli bir programa rastlanmıştır. Buna karşın, Aljedaani vd. (2023)'e göre son zamanlarda yapılan bazı araştırmalara göre, son kullanıcıların mobil cihazlar ve uygulamaları hakkındaki güvenlik özelliklerine ilişkin bilgi veya anlayış eksikliğinin hala bir tehdit olarak göz ardı edildiğini vurgulamaktadırlar.

Yukarıda verilen araştırma raporlarındaki sayılar ve oranlar kişisel verilerin korunması ve mahremiyetinin sağlanması açısından mobil telefonların daha dikkatli kullanılması, bilgi güvenliği farkındalıklarının artırılması ve bazı temel önlemlerin alınması gerektiğini ortaya koymaktadır.

4. ARAŞTIRMA

Bu başlık altında, araştırmanın konusu ve amacı, evreni ve örneklemi, varsayımları ve yöntemi verilmiştir.

4.1. Araştırmanın Amacı ve Önemi

Bu çalışma, özellikle çocuk ve gençlerle etkileşimde bulunan ve onlara örnek teşkil edebilecek öğretmenlerin mobil uygulamaların güvenliği konusundaki bilinç düzeyleri ve düşüncelerini incelemeyi amaçlamaktadır. Araştırma, öğretmenlerin mobil cihazlarına uygulama yüklerken gösterdikleri dikkat seviyesini, uygulamalar hakkında sahip oldukları ön bilgileri, uygulamaların erişim isteklerine hangi izinleri verdiklerini ve bu izinlerin potansiyel sonuçlarını değerlendirmektedir. Ayrıca, öğretmenlerin bilgi güvenliği konusunda farkındalıklarının yanı sıra temel güvenlik önlemlerini alma durumları da belirlenmeye çalışılmaktadır.

4.2. Araştırmanın Evreni ve Örneklemi

Araştırmaya Çorum ilinde Milli Eğitim Bakanlığına bağlı ilkokul, ortaokul ve liselerde görev yapan farklı branşlardan öğretmenler katılmıştır. Katılımcılar öğretmenlerin dahil olduğu sosyal medya iletişim gruplarına (Whatsapp, Bib vb.) iletilen katılım davetine olumlu dönüş yapanlardan oluşmaktadır. Katılan ve anket sorularını eksiksiz cevaplayan öğretmen sayısı 84 olmuştur. Öğretmenlerden 48'i kadın, 36'sı ise erkektir. Katılımcıların demografik özelliklerine bakıldığında 25-35 yaş arası 28, 35-50 yaş arası 47, 50 ve üzeri yaşta ise 9 kişiden oluşmaktadır. Mesleki çalışma yılı yönünden katılımcı dağılımı ise 1-10 yıl arası 13, 10-25 arası 59, 25 yıl ve üzeri tecrübe sahibi olanlar ise 4 kişidir. Araştırma grubunun demografik özellikleri Tablo 2'de özetlenmeye çalışılmıştır.

Tablo 2. Araştırma Katılımcılarının Demografik Özellikleri ve Sayıları

Demografik Özellikler		**Katılımcı Sayısı**
Cinsiyet	Kadın	48
	Erkek	36
Yaş Aralığı	25-35 yaş arası	28
	35-50 yaş arası	47
	50 yaş ve üzeri	9
Mesleki Tecrübe	1-10 yıl arası	13
	10-25 yıl arası	59
	25 yıl ve üstü	4
Mesleki Alan	Bilişim Teknolojileri	28
	Sosyal Bilimler	28
	Fen Bilimleri	

Araştırmanın katılımcıları, branş bazında Bilişim Teknolojileri, Sosyal Bilimler ve Fen Bilimleri alanlarına ayrılarak 3 grup üzerinde yapılmıştır. Araştırmanın eşit ölçüm değerlerine sahip olması için her grup 28 kişi olacak şekilde eşit katılımcıya ulaştırılmıştır. Katılımcıların tümü akıllı telefon kullandığını ve uygulama mağazalarından uygulama yüklediklerini beyan etmişlerdir.

4.3. Araştırmanın Yöntemi

Yapılan araştırma da veri toplamak için "Akıllı Telefonlarda Kullanılan Mobil Uygulamaların Güvenlik Farkındalık Ölçeği" hazırlanmıştır. Kullanılan veri toplama ölçeği 3 alt faktör ve 25 sorudan oluşmaktadır. Tablo 3'te verilen ölçme aracı 25 maddeden ve 5'li likert cevap seçeneğinden oluşmaktadır. Cevap seçenekleri ve puan değerleri; Her zaman 5, Sık sık 4, Ara sıra 3, Nadiren 2 ve Hiçbir zaman 1 olarak hazırlanmıştır

Araştırmanın ölçme aracı olan anket araştırmacılar tarafından geliştirilmiştir. Anketin ilk bölümü yaş, cinsiyet, ve mesleki branş gibi demografik bilgilerin toplandığı sorulardan oluşmaktadır. İkinci kısımda ise, araştırmanın amacı olan mobil uygulamaların kullanıcı bazlı siber güvenlik farkındalığını belirlemeye dönük soruları içermektedir. Araştırmanın kapsamına yönelik anket soruları kullanıcıların mobil cihaz kullanımı sırasında uygulama mağazalarından uygulama indirme alışkanlıklarını, indirme öncesinde ki uygulamanın güvenilirliğine yönelik yaklaşımlarını ve son olarak; indirme sırasında ve sonrasında uygulama tarafından kullanıcıdan talep edilen erişim izinlerine yönelik ortaya çıkan tutumlarını belirlemek üzere tasarlanmıştır.

Veri toplama ölçeğinin ikinci bölümü üç farklı alt faktörü kapsayacak şekilde oluşturulmuştur. Bu alt faktörler; 13 madde içeren Bilgi Toplama, 7 madde içeren Erişim Denetimi ve 5 madde içeren Önlem Alma faktörü olarak isimlendirilmiştir. Faktörler ve içerdiği sorularla (maddeler) ilgili bilgiler Tablo 3' te verilmiştir.

Tablo 3. Veri Toplama Ölçeği Faktörleri ve İçerdiği Maddeler

Faktör	Madde Sayısı	Faktör Adı	İçerdiği Maddeler
1	13	Bilgi Toplama	M1,M2,M3,M4,M5,M6,M7,M8,M9,M10,M11,M12,M13
2	7	Erişim Denetimi	M14,M15,M16,M17,M18,M19,M20
3	5	Önlem Alma	M21,M22,M23,M24,M25

İlk Faktör olan Bilgi Toplama Faktörü kullanıcıların uygulama mağazalarından uygulama indirmeden önce uygulama hakkında bilgi toplanmasını içermektedir. Bu bilgiler, uygulamanın ücretli olup olmaması, uygulamanın üreticisi, daha önce kullananların bıraktığı yorumlar, indirme sayısı ve güncel tutulup tutulmadığı gibi bilgilerdir. Erişim Denetimi faktöründe, uygulamanın cihaza kurulumu sırasında kullanıcıdan talep ettiği erişim izinlerini içeren maddeler yer almaktadır. Bu maddeler, kamera, ses ve depolama alanları gibi temel erişimleri soran bilgilerdir. Son olarak, Önlem Alma Faktöründe ise, uygulamanın talep ettiği izinler karşısında kullanıcının bilgisini ve tutumunu ölçen maddelerin yanı sıra, uygulamanın kullanıcından habersiz çalışmasını fark edip etmediğini öğrenmeye çalışan temel güvenlik farkındalık düzeyini ölçmeye yönelik maddeler yer almaktadır.

Anket uygulaması, Covid-19 önlemleri kapsamında yüz yüze teması en aza indirmek için dijital olarak Google Form ortamında hazırlanmış ve katılımcılara sunulmuştur. Bu anketin linki katılımcılara eposta ve diğer sosyal medya ağları aracılığı ile ulaştırılmıştır. Daha sonra elde edilen veriler bilgisayar ortamına taşınmıştır. Katılımcıların cevaplarından hatalı, esik veya boş bırakılanlar hesaplama dışına çıkarılmıştır. Tam eksiksiz olarak işaretlenen veriler matematiksel ve istatistiksel analizlere tabi tutulmuştur. Bu analizler bilgisayar ortamında Microsoft Excel ve SPSS v21 paket programında yapılmıştır.

4.4. Bulgular ve Tartışma

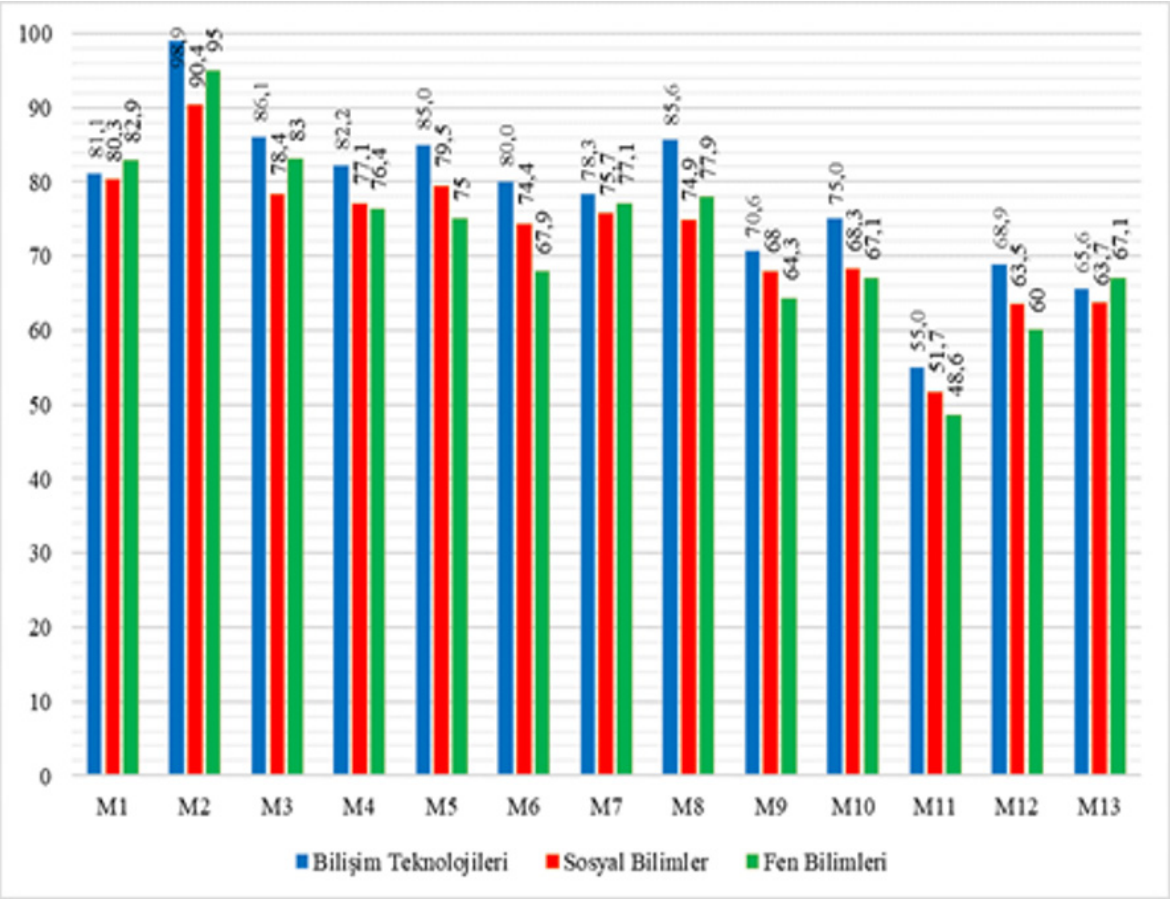
Araştırmanın katılımcılarından elde edilen verileri çeşitli hesaplamalar ve analizler sonucunda bulguları elde edilerek bu bölüm altında verilmiştir. Araştırmanın ölçme aracı olan anket ilk olarak ön denemeye tabi tutularak geçerlik ve güvenilirlik analizi yapılmıştır. Bu deneme sonucunda anketin geçerlik ve güvenilirlik testi Cronbach Alpha değeri 0.81 hesaplanmış ve uygulanabilir düzeyde olduğu tespit edilmiştir. Bu aşamadan sonra ölçme değerleri üç alt faktör altında değerlendirilmeye çalışılmıştır.

Bilgi Toplama Faktörü

Öğretmenlerin mobil uygulama indirme alışkanlıklarını ve uygulamayı indirmeden ve yüklemeden

önce uygulama hakkındaki davranışları Bilgi Toplama Faktörü altında toplanmıştır. Bu faktör uygulama indirme sırasında temel bazı ön bilgi toplama ve analiz etme tutumlarını ortaya çıkarmak üzere 13 maddeden oluşmaktadır. Öğretmenler 3 farklı branşa ayrıldıktan sonra onlardan alınan cevaplara göre bilgi toplama faktörü sonuçları Şekil 6'da sunulmuştur.

Şekil 6. Üç Farklı Branş Kategorisinde Bilgi Toplama Faktörü



Bilgi Toplama faktöründe yer alan M1 ve M13 maddelerinin cevaplarında branş bazında farkındalık düzeyinin Fen Bilimleri branşında diğer branşlara oranla daha yüksek olduğu görülmektedir. Bu maddeler mobil cihazlara uygulama yükleme oranını ve uygulamaların reklam içerip içermediğine dikkat etmeyi ölçen maddelerdir.

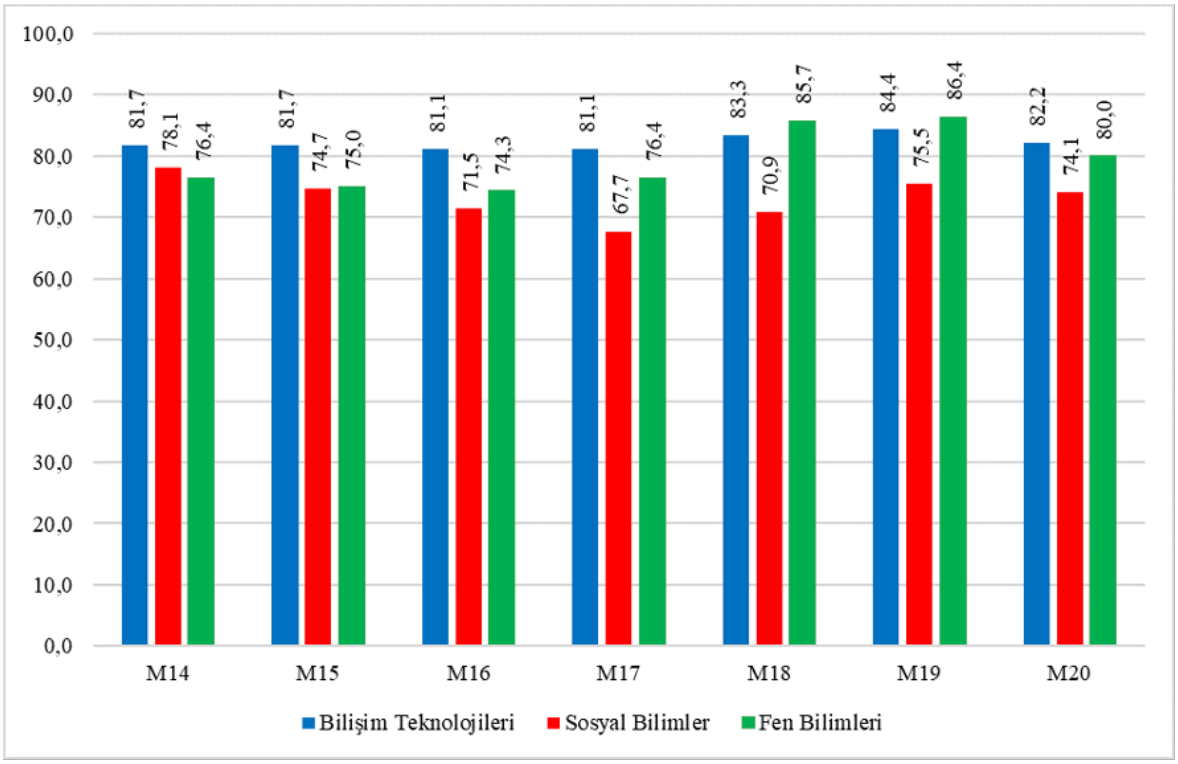
Bu faktörün M1 ve M3 maddeleri dışında geriye kalan 11 maddesinde ise Bilişim Teknolojileri grubunun cevapları doğrultusunda farkındalık düzeyleri daha yüksek çıkmıştır. Bu maddeler uygulamanın özelliklerini, kullanıcı yorumlarını ve üreticisi hakkındaki bilgileri içermektedir. Sosyal Bilimler gurubuna bakıldığında ise M1, M2, M3, M8 ve M13 numaralı maddelerde farkındalık düzeyinde 3. sırada yer aldığı görülmektedir. Buna karşın, geri kalan diğer 8 maddede ise Sosyal Bilimler grubunun Bilgi Toplama farkındalık düzeyinin 2. sıraya yükseldiği anlaşılmaktadır.

Erişim Denetimi Faktörü

Ölçeğin alt faktörlerden bir diğeri olan Erişim Denetimi faktörü uygulama indirme sırasında uygulamanın kullanıcıdan ne tür erişim izinleri istediği ve kullanıcının bu izinlerine yönelik nasıl bir tutum izlediği ölçülmeye çalışılmıştır. Katılımcılardan alınan cevaplar karşısında oluşturulan grafik

Şekil 7'de görülmektedir.

Şekil 7. Üç Farklı Branş Kategorisinde Erişim Denetimi Faktörü



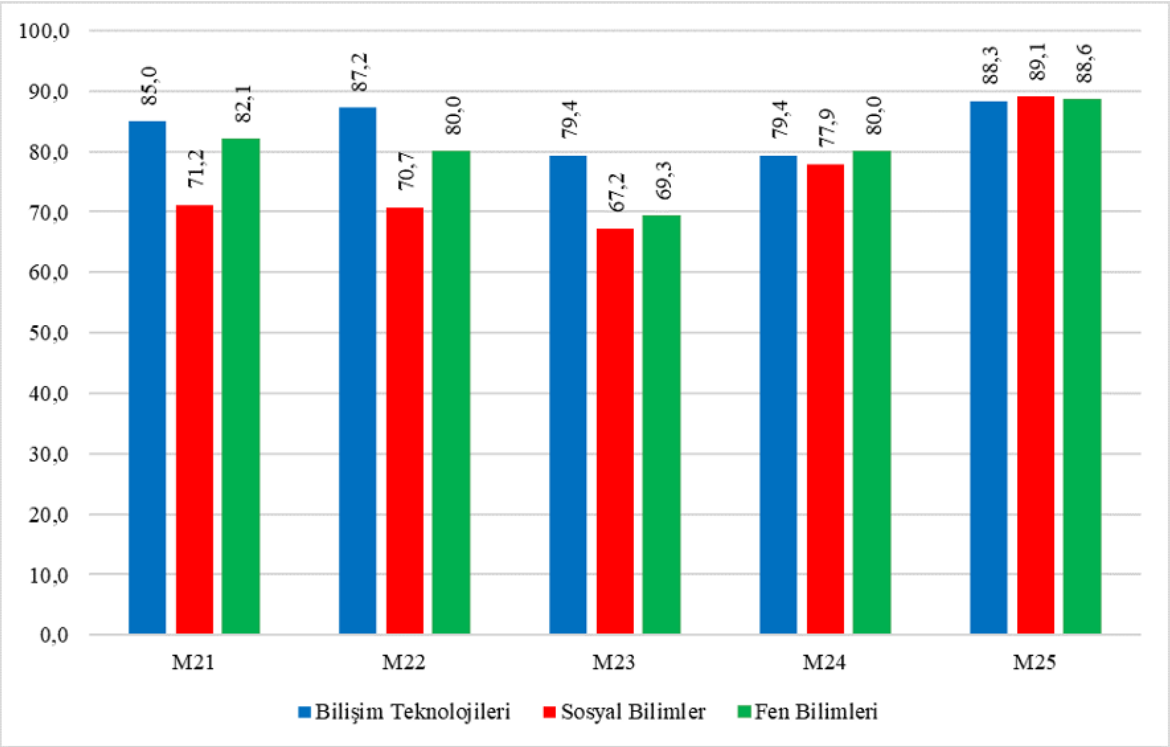
Üç farklı branşa sahip öğretmenlerin Erişim Denetimi faktörü cevapları incelendiğinde Bilişim Teknolojileri grubunun, faktörün M14, M15, M16, M17 ve M20 numaraları maddelerinde farkındalık düzeylerinin diğer branşlara göre daha yüksek olduğu görülmüştür. Ölçeğin M18 ve M19 maddelerinde ise Fen Bilimleri grubunun farkındalık düzeyi diğerlerine göre daha yüksek çıkmıştır. Bu maddeler, uygulamanın kullanıcının cihazındaki konum bilgisine ve mesajlarına erişim izin talebine yönelik aldığı tutumu ölçen bilgileri içermektedir.

Sosyal Bilimler grubu ise faktörün yalnızca M14 numaralı maddesinde farkındalık düzeyi olarak 2. sırada yer almıştır. Bu madde, uygulamanın kullanıcının cihazının kamerasına erişim iznini kontrol etmeyi ölçen bir bilgi içermektedir. Faktörün diğer maddelerinde ise Sosyal Bilimler grubu erişim denetimi farkındalık düzeyi yönünden 3. sırada yer almaktadır.

Önlem Alma Faktörü

Alt faktörlerden bir diğeri olan uygulamaların çalıştırılması sırasında ve sonrasında bilgi güvenliğini sağlama yönünde alınan temel önlemler bazında genel bir Önlem Alma durumu incelenmiştir. Önlem Alma faktöründe M21-M25 arası 5 madde bulunmaktadır. Katılımcılardan alınan veriler analiz edildiğinde üç farklı branş bazında Şekil 8'deki grafik elde edilmiştir. Grafiğe genel olarak bakıldığında değerlerin 67 ile 89 arasında ortalamanın üzerinde değerleri içerdiği görülmektedir.

Şekil 8. Üç Farklı Branş Kategorisinde Önlem Alma Faktörü



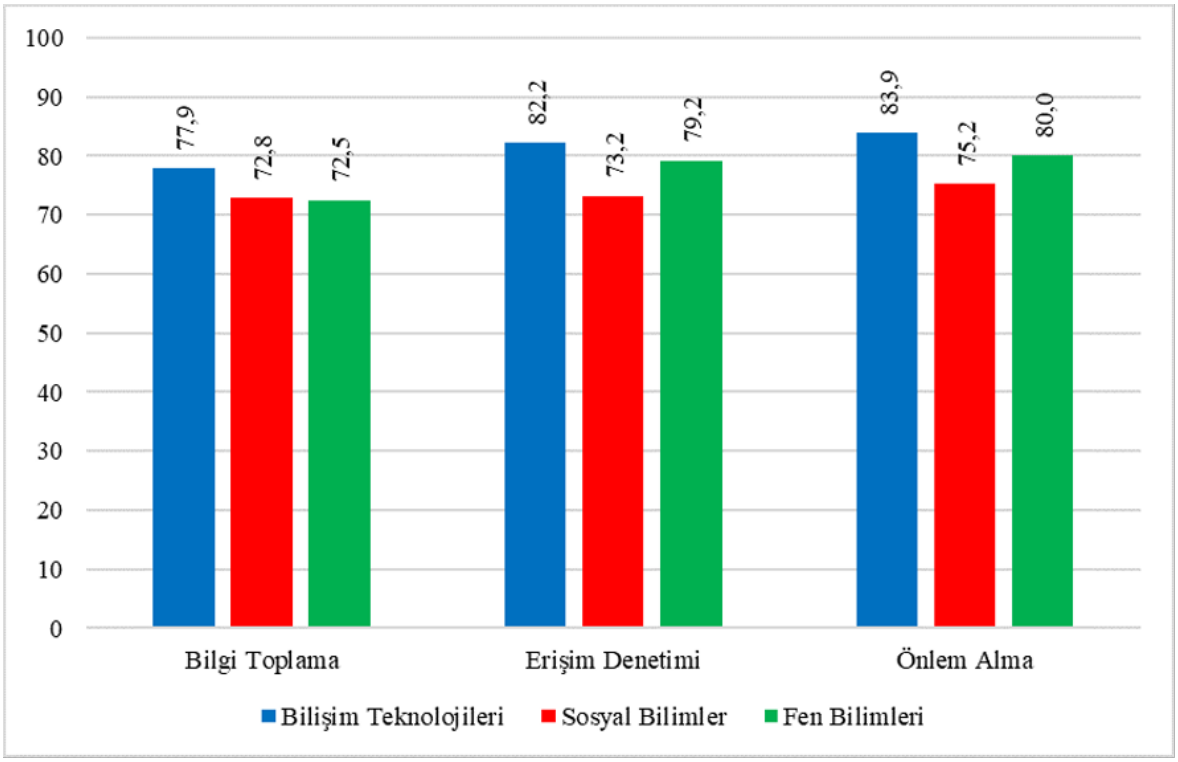
Şekil 8'e ayrıntılı bir şekilde bakıldığında, faktörün M21, M22 ve M23 maddelerinde Bilişim Teknolojileri grubunun önlem alma düzeyi diğer branşlara göre daha yüksek çıkarak 1. sırada olduğu görülmektedir. Ayrıca, bu faktörün M23 numaralı maddesi olan "Uygulamaların telefonumda benden habersiz çalışıp çalışmadığını kontrol ederim" önermesi diğer önermelere göre daha düşük bir oranda çıktığı görülmektedir. Bu durumun, bir uygulamanın çalışıp çalışmadığını anlamak için biraz daha fazla teknik bilgi ve beceri gerektirmesinden dolayı olabileceği düşünülmektedir.

Faktörün "Uzun süre kullanmadığım uygulamaları telefonumdan kaldırırım" şeklindeki M24 numaralı maddesinde bütün branşların değerleri birbirine yakın olsa da, Fen Bilimleri grubu 80,0 değeri ile ilk sırayı almıştır. Diğer yandan, faktörün "Telefonuma gereksiz uygulama yüklemem" şeklindeki M25 numaralı maddesinde ise yine üç branşın değerleri birbirlerine çok yakın olsa da, Sosyal Bilimler grubu farkındalık düzeyinin 89,1 ile diğerlerine göre daha yüksek çıktığı görülmektedir. Bu faktörün M25 maddesi dışında ki önermelerde Sosyal Bilimler grubunun Önlem Alma farkındalık düzeyi diğer iki gruba göre daha düşük çıkarak 3. sırada yer almasına neden olmuştur.

Faktörlere Göre Güvenli Kullanım Farkındalığı

Katılımcıların, veri toplama aracındaki bilgi toplama, erişim denetimi ve önlem alma durumuna göre faktörlere ayrılan tüm maddelerinin geneline verdikleri cevapları üç farklı branş bazında yüzdelik olarak hesaplanmıştır. Bu hesaplanan değerler ışığında Şekil 9'daki grafik elde edilmiştir. Grafiğe genel olarak bakıldığında, değerlerin 72,5 ile 83,9 arasında ortalamanın üstünde yer aldığı ancak, her üç branşında bu değerlere göre farkındalıklarının ideal düzeyde olmadığı düşünülmektedir.

Şekil 9. Faktörlere Göre Güvenli Kullanım Farkındalığı

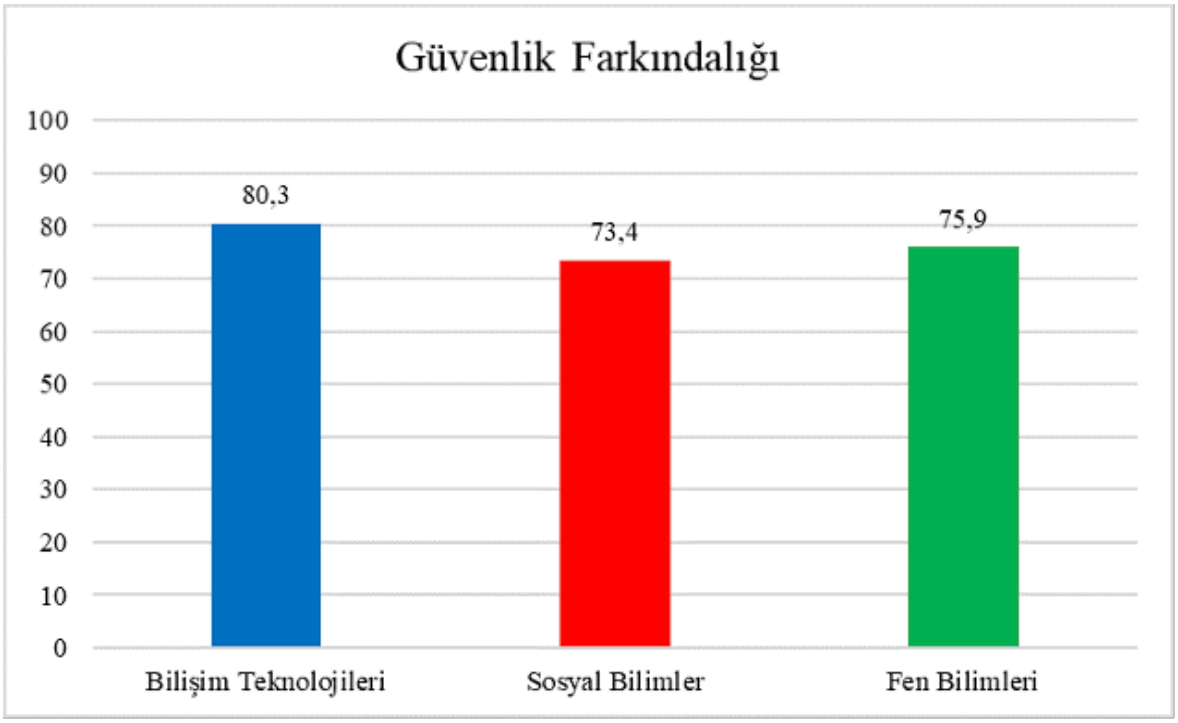


Faktörler ve branş grupları tek tek ele alındığında Bilgi Toplama faktöründe Şekil 9'da görüldüğü gibi sırasıyla, Bilişim Teknolojileri grubu %77.9, Sosyal Bilimler grubu %72.8 ve Fen Bilimleri ise %72.5'lik bir farkındalık düzeyine sahip olduğu belirlenmiştir. Erişim Denetimi faktöründe farkındalık düzeyleri; Bilişim Teknolojileri grubu %82.2 ile ilk sırayı alırken, Fen Bilimleri grubu ise %79,2 ile ikinci sırada yer almıştır. Buna karşın, Sosyal Bilimler grubu %73.2 ile son sırada yer almışlardır. Son faktör olan Önlem Alma faktörüne göre ise sıralama Bilişim Teknolojileri grubu %83,9 ile ilk sırada, Fen Bilimleri %80 ile ikinci ve Sosyal Bilimler grubu ise %75,2 ile üçüncü sırada yer almıştır.

Branş Dağılımına Göre Güvenlik Farkındalıkları

Araştırmanın katılımcıları olarak üç farklı branşta yer alan öğretmenlerin anket uygulamasına verdikleri tüm cevaplar bir araya getirilerek genel bir gruplar arası Güvenlik Farkındalığı değerleri hesaplanmıştır. Bu gruplandırma sonucunda elde edilen bulgular Şekil 10'daki grafikte sunulmuştur. Bu grafiğe genel olarak bakıldığında, bilişim teknolojilerine meslekleri bakımından yakınlığı olan, bilgi ve becerileri yüksek olan Bilişim Teknolojileri grubunun doğal olarak yüksek değerlere sahip olduğu görülmektedir. Ancak, genel farkındalık kapsamında durum bu doğrultuda çıkmış olsa da maddeler bazında böyle çıkmayacağı önceki bulgularda ortaya konmuştur. Ayrıca, farkındalık düzeyinin kapsamı ne olursa olsun mesleki bilgi ve beceriler ile her zaman doğru orantılı olarak yüksek düzeyde olamayacağı da gözlerden kaçırılmamalıdır. Bunun nedenleri arasında, insani farklılıklar, demografik özellikler, çevre şartları, eğitim düzeyi ve sosyo-ekonomik düzeyler gibi faktörler belirleyici olmaktadır.

Şekil 10. Üç Farklı Branş Kategorisinde Güvenlik Farkındalığı



Bu grafiğe bakıldığında, Bilişim Teknoloji grubunun farkındalık düzeyi %80.3 çıkarak genel güvenlik farkındalık düzeyinin ilk sırasında yer almıştır. Fen Bilimleri grubu %75.9 ile ikinci sırada yer alırken, Sosyal Bilimler grubunun ise %73.4 oranı ile üçüncü sırada yer aldığı görülmektedir.

SONUÇ ve TARTIŞMA

Araştırma, üç farklı branş grubuna ayrılan öğretmenlerin mobil uygulamalar hakkındaki düşünceleri, bilgi birikimleri ve bilgi güvenliği farkındalık düzeylerini belirlemeye yönelik olarak 84 katılımcı ile yürütülmüştür. Anket uygulaması sonucunda toplanan veriler ışığında, BIT konusunda deneyimli, eğitimli ve hem kullanıcı hem de geliştirici olarak değerlendirilebilecek olan Bilişim Teknolojileri grubunun farkındalıklarının diğer iki gruba göre daha yüksek çıktığı görülmüştür. Ardından, Fen Bilimleri grubu ve son olarak ta Sosyal Bilimler grubunun geldiği görülmüştür.

Grupların cihazlarına uygulama indirmeden önce uygulama hakkında bilgi sahibi olmaları, çeşitli ön incelemelerde bulunmaları ve kullanıcı yorumlarını okumaları gibi parametreleri içeren bilgi toplama faktörüne göre ortalama olarak güvenlik farkındalıklarının %74,4 olduğu görülmüştür. Grupların, uygulama indirme sırasında erişim talepleri ve verdikleri erişim izinleri konusundaki bilgileri ve farkındalıkları ise %78,2 olduğu belirlenmiştir. Son olarak, tüm katılımcıların uygulamaların çalışması öncesi-sırası-sonrası dönemlerde önlem alma farkındalık düzeylerinin ise %79,7 olduğu tespit edilmiştir.

Mobil yaşamın en önemli bileşeni olan akıllı telefonlarda kullanılan uygulamaların bilgi ve siber güvenlik farkındalığı doğru ve güvenli bir kullanım için çok büyük önem taşımaktadır. Akıllı telefon kullanıcılarının marka ve model bazlı en az bir uygulama kullanmakta ve yenilerini uygulama mağazalarından cihazlarına yükledikleri bilinmektedir. Bu cihaz ve uygulama bileşeni ile günlük hayatın merkezinde olan pek çok iş ve işlem rahat ve kolay bir şekilde yapılabilmektedir. Özellikle devletin kurumsal iş süreçleri, ticari faaliyetler, ödeme işlemleri, iletişim ortamları ve diğer pek çok faaliyet bu uygulamalar sayesinde yapılabilmektedir. Bu tür faaliyetleri gerçekleştirebilmek için internet

üzerinden cihaz, sunucu ve veri tabanlarına bağlanarak karşılıklı bilgi alışverişi, kimlik doğrulama mekanizmaları ve onay işlemleri yapılmaktadır. Bu durumu fırsat bilen kötü niyetli kullanıcılar ve kötü amaçlı yazılım üreticileri bazı uygulamalar aracılığıyla kullanıcılardan izinsiz ve yetkisiz bir şekilde cihazlarına erişebilmektedirler. Ardından, yine izinsiz ve yetkisiz bir şekilde mahrem bilgilere erişilebilmektedirler. Coşar'ın (2022) belirttiği gibi, siber güvenlik zafiyetlerinin yaşanmaması için siber dünyanın içerisinde öncelikli olarak temel siber güvenlik önlemlerinin alınması ve kullanıcıların uygulama bazlı bilgi ve siber güvenlik farkındalık düzeyinin artırılması gerekmektedir.

Özellikle mobil cihazlarda bilgi ve siber güvenliği sağlamak için kullanım sırasında özenli ve dikkati olunması gerekmektedir. Uygulama mağazalarından programların indirilme sayıları, kullanıcı yorumları, erişim istekleri, geliştirici tanımlaması gibi bilgilerin incelenmesi, ardından ön güvenlik taramalarının yapılarak indirilmesi gerektiği unutulmamalıdır. Ardından, uygulamaların kullanıcıdan habersiz çalışıp çalışmadığı, izinsiz bağlantı yapıp yapmadığı gibi siber güvenlik unsurlarının da bilinmesi gerekmektedir. Ayrıca, araştırma bulguları ve sonuçlarına göre genel farkındalık düzeyleri orta ve üst sayılabilecek bir düzeyde çıkmış olsa da, kullanıcıların yaş, cinsiyet ve meslek farkı gözetmeksizin kurs, seminer ve hizmet içi eğitimlerle bilgi güvenliği farkındalık düzeylerinin artırılması gerektiği ortaya çıkmıştır.

Akıllı telefon kullanımı sırasında mutlaka bir güvenlik yazılımı çalıştırılarak kullanıcıdan habersiz ve izinsiz erişim durumları denetlenmelidir. Periyodik olarak anti virüs yazılımları ile cihaz taramaları yapılarak açıklar ve saldırılar denetim altına alınmalıdır. Uygulama denetimi yanında, güvenliğinden endişe duyulabilecek herkese açık bağlantı ortamlarında cihazın bağlantı modülleri kontrol edilerek izinsiz ve yetkisiz erişimlere kapatılmalıdır. Bu ve bunun gibi temel bazı güvenlik önlemleri ile gizlilik ve güvenlik temel düzeyde sağlanmaya çalışılmalıdır.

Son olarak, sosyal mühendislik saldırıları olarak sınıflandırılan ve kişinin manipüle edilmesine neden olan saldırılara karşı paylaşılan bilgilerin doğrulama ve onaylama mekanizmalarından geçirilerek harekete geçme bilinci kazanılmaya çalışılmalıdır. Dijital bir dünyada hayatta kalabilmek için, teknoloji okuryazarlığının kazanılması, bilinçli kullanım ilkelerinin benimsenmesi ve güvenlik farkındalığının artırılması faaliyetlerine gelecek zamanlarda daha fazla ihtiyaç duyulacağı unutulmamalıdır.

KAYNAKÇA

Aksoğan, M. & Atıcı, B. (2023). Akademisyenlerin Dijital Veri Güvenliği Farkındalıkları Üzerine Bir Araştırma: Malatya Örneği. Gümüşhane Üniversitesi Sosyal Bilimler Dergisi, Cilt:14, Sayı:2, ss.429-439.

Aljedaani B., Ahmad, A., Zahedi, M. & Babar, M.A. (2023). End-users' knowledge and perception about security of clinical mobile health apps: A case study with two Saudi Arabian mHealth providers, Journal of Systems and Software, Volume: 195, https://doi.org/10.1016/j.jss.2022.111519

Aljohni, W., Elfadil, N., Jarajreh, M. & Gasmelsied, M. (2021). Cybersecurity awareness level: The case of Saudi Arabia University students. International Journal of Advanced Computer Science and Applications, Vol:12, Issue:3, pp.276-281. https://doi.org/10.14569/IJACSA.2021.0120334

Apple. (2023). 2022 App Store Transparency Report. Erişim tarihi: 5 Mayıs 2023, Erişim adresi: https://www.apple.com/legal/more-resources/docs/2022-App-Store-Transparency-Report.pdf

Canoğulları, E. (2021). Öğretmenlerin Bilgi Güvenliği Konusundaki Farkındalıklarının İncelenmesi, Kalem Uluslararası Eğitim ve İnsan Bilimleri Dergisi, Cilt:11, Sayı:2, ss.651-679, https://doi.org/10.23863/kalem.2021.219

Chang, V., Golightly, L., Xu, Q.A., Boonmee, T. & Liu, B.S. (2023). Cybersecurity for children: An investigation into the application of social media. Enterprise Information Systems, https://doi.org/10.1080/17517575.2023.2188122

Chen, C. C, Medlin, D.B. & Shaw, R. S. (2008). A Cross□Cultural Investigation of Situational Information Security Awareness Programs. Information Management & Computer Security, Vol:16, Issue:4, pp.360-376, https://doi.org/10.1108/09685220810908787

Coşar, M. (2022). Siber Dünyanın Karanlık Yüzü: Deepweb ve Darknet. Journal of Management Theory and Practices Research, Cilt:3, Sayı:1, ss:58-71.

CyberMag. (2020). 2020'de Türkiye'de Akıllı Telefonlara Yönelik Saldırıların Sayısı Karantina Döneminde Yaşanan Artışla Yaklaşık 160.000'e Ulaştı. Erişim tarihi: 2 Mayıs 2023, Erişim adresi: https://www.cybermagonline.com/2020de-turkiyede-akilli-telefonlara-yonelik-saldirilarin-sayisi-karantina-doneminde-yasanan-artisla-yaklasik-160000e-ulasti

Cybersecurity Magazine. (2022). 2022 Official Cybercrime Report by Cybersecurity Ventures, Erişim tarihi: 2 Mayıs 2023, Erişim adresi: https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

Derin, M. A. & Gençoğlu, M. T. (2020). Ortaokul Öğrencilerinin Bilgi Güvenliği Farkındalığı. Savunma Bilimleri Dergisi, Cilt:38, ss.159-181, https://doi.org/10.17134.khosbd.813459

Elçi, A. C. & Sarı, M. (2016). Bilişim teknolojileri ve yazılım dersi öğretim programına yönelik öğrenci görüşlerinin dijital vatandaşlık bağlamında incelenmesi. Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, Cilt:25, Sayı:3, ss.87-102.

Güldüren, C. (2015). Yükseköğretim Kurumlarındaki Öğretim Elemanlarının Bilgi Güvenliği Farkındalık Düzeylerinin Değerlendirilmesi, Yayımlanmamış Doktora Tezi, Ankara Üniversitesi BÖTE, Ankara, 2015.

Karlı, İ., Doğru, S. & Doğru, Y. B. (2018). Akıllı Telefonların Uygulama İzinleri Üzerine Bir Farkındalık Çalışması. AJIT-e: Academic Journal of Information Technology, Cilt:9, Sayı:31, ss.153-167, https://doi.org/10.5824/1309-1581.2018.1.010.x

Keser, H. & Yayla, H. G. (2021). Fatih Projesi Uygulanan Okullardaki Öğretmenlerin Bilgi Güvenliği Farkındalık Düzeylerinin İncelenmesi. Milli Eğitim Dergisi, Cilt:50, Sayı:229, ss.9-40.

Kim, S. & Hovav, A. Z. (2011). The Impact of Smart Phone Usability on Group Task Performance in A University Environment: Media Synchronicity Perspective. International Conference on Information Resources Management (CONF-IRM), 2011, Seul.

Qamar, A., Karim, A. & Chang, V. (2019). Mobile malware attacks: Review taxonomy & future directions. Future Generation Computer Systems, Volume 97, pp.887-909, https://doi.org/10.1016/j.future.2019.03.007

Statista. (2022). Smartphone Sales Worldwide 2007-2021 | Statista. Erişim tarihi: 2 Mayıs 2023, Erişim adresi: https://www.statista.com/statistics/263437/global-smartphone-sales-to-end-users-since-2007/

StatCounter. (2023). Mobile Operating System Market Share Worldwide 2010 – 2023. Erişim Tarihi: 2 Mayıs 2023, Erişim adresi: https://gs.statcounter.com/os-market-share/mobile/worldwide/#yearly-2010-2023

Talan, T. & Aktürk, C. (2021). Orta Öğretim Öğrencilerinin Dijital Okuryazarlık ve Bilgi Güvenliği Farkındalığı Seviyelerinin İncelenmesi. Kahramanmaraş Sütçü İmam Üniversitesi Sosyal Bilimler Dergisi, Cilt:18, Sayı:1, ss.158-180, https://doi.org/10.33437/ksusbd.668255

Taner, E. & Kılıç, İ. (2019). Güvenlik Güçlerinin Bilgi Güvenliği Farkındalığını Belirlemeye Yönelik Bir Araştırma. Güvenlik Bilimleri Dergisi, Cilt:8, Sayı:2, ss.253-269, https://doi.org/10.28956/gbd.646321

Tekerek, M. & Tekerek, A. (2013). Öğrencilerin Bilgi Güvenliği Farkındalığı Üzerine Bir Araştırma. Turkish Journal of Education, Cilt:2, Sayı:3, ss.61-70, https://doi.org/10.19128/turje.181065

Teknolojituru. (2017). Uygulama Mağazalarında Kaç Milyon Uygulama Var? Erişim tarihi: 2 Mayıs 2023, Erişim adresi: https://teknolojituru.com/2017/07/05/uygulama-magazalarinda-kac-milyon-uygulama-var/

TUİK. (2021). Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması, 2021. Erişim tarihi: 15 Mayıs 2023, Erişim adresi: https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2021-37437,

Uzun, E. & Coşar, M. (2022). Lise Çağındaki Öğrencilerin Sosyal Medya Ortamları Hakkında Bilgi Güvenliği Farkındalık Düzeyleri, Hitit Ekonomi ve Politika Dergisi, Cilt:2, Sayı:1, ss.50-61.

Yılmaz, F. G. & Çavuş Ezin, Ç. (2017). Ebeveynlerin Bilgi Güvenliği Farkındalıklarının İncelenmesi. Eğitim Teknolojisi Kuram ve Uygulama, Cilt:7, Sayı:2, ss.41-57, https://doi.org/10.17943/etku.288874