

Research Article/Araştırma Makalesi

## University Employees' Awareness of Digital Data and Personal Cyber Security (A Case Study of IT Departments)

Cengiz GÜNDÜZALP \*1 

<sup>1</sup> Kafkas University Kazım Karabekir Vocational School, Kars, Turkey, [cengizgunduzalp@kafkas.edu.tr](mailto:cengizgunduzalp@kafkas.edu.tr)


\* Corresponding Author: [cengizgunduzalp@kafkas.edu.tr](mailto:cengizgunduzalp@kafkas.edu.tr)

### Article Info

Received: 31 March 2021

Accepted: 2 July 2021

**Keywords:** Digital data security, personal cyber security, awareness, cross-sectional survey

 10.18009/jcer.907022

**Publication Language:** Turkish

### Abstract

This study was carried out to determine the digital data security and cyber security awareness of the employees in the information technology departments of universities in Turkey. The study was conducted by cross-sectional survey model. The findings obtained from the study showed that there is a weak positive relationship between the awareness of providing digital data security and the awareness of providing personal cyber security. In addition, it was observed that employees' awareness of providing digital data security and personal cyber security differed significantly by variables of age, professional experience, educational background and position. Consequently, it has been understood that the awareness of providing digital data security and personal cyber security owned by employees at information technology departments of universities is high and these awareness's are influenced by gender, age, professional experience, educational background and the task undertaken.



**To cite this article:** Gündüzalp, C. (2021). Üniversite çalışanlarının dijital veri ve kişisel siber güvenlik farkındalıkları (bilgi işlem daire başkanlıkları örneği). *Journal of Computer and Education Research*, 9 (18), 598-625. DOI: 10.18009/jcer.907022


## Üniversite Çalışanlarının Dijital Veri ve Kişisel Siber Güvenlik Farkındalıkları (Bilgi İşlem Daire Başkanlıkları Örneği)

### Makale Bilgisi

Geliş: 31 Mart 2021

Kabul: 2 Temmuz 2021

**Anahtar kelimeler:** Dijital veri güvenliği, kişisel siber güvenlik, farkındalık, kesitsel tarama

 10.18009/jcer.907022

**Yayın Dili:** Türkçe

### Öz

Bu çalışma, Türkiye'deki üniversitelerin bilgi işlem daire başkanlıklarında çalışanların dijital veri güvenliği ve siber güvenliği sağlama farkındalıklarını belirlemek amacıyla gerçekleştirilmiştir. Çalışma kesitsel tarama modeli ile yürütülmüştür. Çalışmadan elde edilen bulgular, dijital veri güvenliği ve kişisel siber güvenliği sağlama farkındalıkları arasında pozitif yönlü zayıf bir ilişki olduğunu göstermiştir. Ayrıca çalışanların dijital veri güvenliğini sağlama ve kişisel siber güvenlik farkındalığının yaş, mesleki deneyim, eğitim durumu ve görev değişkenlerine göre anlamlı düzeyde farklılaştığı gözlemlenmiştir. Sonuç olarak üniversitelerin bilgi işlem daire başkanlıklarındaki çalışanların dijital veri güvenliği ve kişisel siber güvenliği sağlama farkındalıklarının yüksek ve bu farkındalıklar üzerinde cinsiyet, yaş, mesleki deneyim, öğrenim durumu ve üstlenilen görevinde etkili olduğu anlaşılmıştır.

## Summary

# University Employees' Awareness of Digital Data and Personal Cyber Security (A Case Study of Information Technology Departments)

Cengiz GÜNDÜZALP \*<sup>1</sup> 

<sup>1</sup> Kafkas University Kazım Karabekir Vocational School, Kars, Turkey, [cengizgunduzalp@kafkas.edu.tr](mailto:cengizgunduzalp@kafkas.edu.tr)

\* Corresponding Author: [cengizgunduzalp@kafkas.edu.tr](mailto:cengizgunduzalp@kafkas.edu.tr)

## Introduction

With regards to awareness of providing digital data security and personal cyber security, it can be considered that especially large-scale organizations have more responsibilities in this aspect. Universities come first among these institutions. They are institutions that have a lot of personnel within themselves and give service to large masses. It can be thought that this situation causes an increase in the number of the digital data that universities need to keep under control and threats and dangers against these data. This can bring awareness of providing digital data security and personal cyber security a particular importance. In this aspect, people working in information technologies departments in universities can take responsibility. Starting from this point of view, this study was carried out. The aim of this study is to determine awareness of providing digital data security and cyber security owned by employees who assume various positions in different units of information technologies departments of the universities in Turkey by different variables.

## Method

The research was carried out by cross-sectional survey model. The population of the study was determined as employees assuming different positions in various units of information technologies departments of the universities in Turkey. Out of 1440 people to whom the form and scales were sent, 417 people answered the personal information form and scales, the data collected from 410 people was evaluated since the responses of 7 people to the form and scales were incomplete. The data collection tools of the study are The Scale of Digital Data Security Awareness, The Scale of Providing Personal Cyber Security and The Personal Information Form. In the data analysis process, firstly, the frequency and percentage values of the employees participating in the study regarding their gender, age, professional experience, educational background and positions were identified. Later, the

mean and standard deviation values for the items of the Scales of Digital Data Security Awareness and Providing Personal Cyber Security were determined and whether the scores obtained from the scales had normal distribution was examined. Pearson correlation analysis was used to reveal the relationship between Scales of Digital Data Security Awareness and Providing Personal Cyber Security. Independent sample t-test was used to reveal the difference in terms of gender in the groups, and ANOVA test was used to determine the difference between groups in terms of age, professional experience, educational background and position. The Games-Howell test, one of the Post-Hoc tests, was used to determine which group or groups caused the difference between groups.

### **Results**

The findings obtained from the study show that the majority of the participants are male in terms of gender, the number of participants between the ages of 31-40 and 41-50 in terms of age, the number of those with 6-10 and 16-20 years of experience in terms of professional experience, and the number of those with graduate and undergraduate degrees in terms of educational background are higher. Regarding the position of the participants, it was determined that the number of instructors was higher than that of other participants. On the other hand, the findings of the study showed that the average scores of the participants regarding the answers given to the items in Scale of Digital Data Security Awareness was 4.60, and the average scores of the answers they gave to the items in Scale of Awareness of Providing Personal Cyber Security was 3.33. In other findings obtained from the study, it was observed that there was a weak positive relationship between Digital Data Security Awareness and Awareness of Providing Personal Cyber Security, gender did not make a significant difference in terms of Digital Data Security Awareness, but it made a significant difference in terms of Awareness of Providing Personal Cyber Security. On the other hand, the variables of age, professional experience, educational background and position made a significant difference in Digital Data Security Awareness and Awareness of Providing Personal Cyber Security in all groups.

## Discussion and Conclusion

The results obtained at the end of the study showed that the employees' awareness of providing digital data security and personal cyber security is high. This result can be described as a desired situation for information technologies employees. Another result of the study showed that there is a weak positive correlation between awareness of providing digital data security and personal cyber security. In this aspect, it can be seen as a natural result that there is a relationship between two concepts that can be described as interrelated, but it is meaningful that this relation is weak. Another different result obtained from the study is that there is no significant difference between the groups in terms of awareness of digital data security. This may indicate that the gender of the employees does not have a significant impact on awareness of digital data security. On the other hand, it was concluded that the employees' awareness of providing personal cyber security differs according to gender. It can be stated that male employees are more conscious in terms of awareness of providing cyber security. On the other hand, the results of the study showed that there were significant differences between the groups in terms of age, professional experience, educational background and position in the context of awareness of providing digital data security and personal cyber security. It can be stated that employees in the age group of 51-60 are more successful in terms of awareness of digital data security, and those in the age group of 21-30 are more successful in terms of awareness of providing cyber security. On the other hand, it can be thought that employees with 16-20 years of professional experience are more experienced in terms of awareness of providing digital data security and cyber security. In terms of educational background, it can be stated that PhD graduate employees are the most successful group in terms of both awareness of providing digital data security and awareness of providing cyber security. In terms of the positions of employees, it can be thought that network administrators and computer operators have more experience in terms of awareness of providing digital data security and engineers in terms of awareness of providing cyber security. As a result, the results obtained from this study showed that the awareness of providing digital data security and cyber security owned by employees at information technologies departments of universities is high. On the other hand, it was concluded in this study that there is a relationship between the employees' awareness of providing digital data security and cyber security and different variables have an effect on these awareness.

## Giriş

Teknolojik gelişmelerin oldukça hızlı gerçekleştiği günümüzde çeşitli alan ve kavramlara yönelik dijitalleşme faaliyetlerinin de aynı hızda değişim gösterdiği görülmektedir. Farklı kavram ve alanlarda gerçekleşen dijitalleşmenin, özellikle dijital ortamların kullanımı ve yaygınlaşmasına önemli katkılar sunduğu ifade edilebilir. Bu dijital ortamların en dikkat çekici olanının internet olduğu söylenebilir. İnternetin çok hızlı bir şekilde gelişmesiyle birlikte, veri ve bilgi alışverişlerine ilişkin süreçlerde dijital iletişim ortamlarının kullanımı giderek artmıştır (Solichin & Ramadhan, 2017). Öyle ki dijital iletişim ortamları bugün birçok kurum veya kişi tarafından çeşitli amaçlar için farklı şekillerde kullanılabilen ortamlar olarak görülmektedir. Bu durumun doğal bir sonucu olarak dijital iletişim ortamlarda yer alan kurum ve kişilere ilişkin dijital veriler hızlı bir şekilde çoğalmaktadır. Dijital ortamlarda bilgilerin çoğalması, kişilere ait verilerin gizli tutulmasına yönelik ihtiyacı ve buna ilişkin hizmet sağlayıcılara duyulan güvenin arttırılmasını gerektiren veri güvenliği ile alakalı sorun ve problemleri ortaya çıkarabilmektedir (Praveena & Smys, 2017). Ayrıca bilgi ve iletişim dünyasının hızlı bir değişim içinde olması da dijital verilerle ilgili yeni güvenlik sorunlarının ortaya çıkmasına katkı sunmaktadır (Aldridge, Medina & Ralphs, 2010). Öyle ki dijital ortamda her gün yedi milyondan fazla veri kaydı ele geçirilmektedir ve sadece 2020'nin ilk çeyreğinde siber dolandırıcılık ve suistimal olayları %20 artmıştır (Simplilearn, 2021). Bu bakımdan dijital ortamlarda gerçekleşen dijital iletişimdeki en temel ve önemli sorunlardan birisi, internet ağı üzerinden iletimi yapılan dijital verilerin güvenliğidir (Solichin & Ramadhan, 2017). Canbek ve Sağıroğlu (2006) dijital veri güvenliğini, “elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması sırasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için güvenli bir bilgi işleme platformu oluşturma çabalarının tümü (s. 168)” olarak ifade etmişlerdir. Bu anlamda veri güvenliği, dijital bilgileri yetkisiz erişim, bozulma veya hırsızlığa karşı koruma uygulaması (IBM, 2020) olarak görülebilir. Belirtilen ifadeler dikkate alındığında dijital ortamdaki verilen saklanması, taşınma ve bütünlüğünün bozulmaması adına kişi ve kurumların farklı teknolojileri işe koşmalarının bir gereklilik olduğu ifade edilebilir. Bu bakımdan Vural ve Sağıroğlu (2008) kişilerin ve kurumların farklı teknolojilerden yararlanırken onlara yönelik tehdit ve tehlikeleri önceden düşünerek gerekli önlemleri aldıklarında dijital veri güvenliğini sağlamış olacaklarını ifade ederek buna vurgu yapmışlardır.

Dijital veri güvenliğini sağlama adına yapılan süreçler, işlemler ve faaliyetler belirlenirken “siber” kavramını gözden kaçırmamak gerekir. Yaşar (2014) siberin bilgisayarlar ve bilgisayarların birbiri ile iletişim kurmasına imkan sunan ve ağlarla ilgisi olan kavramların tamamı olduğuna dikkat çeker. Bu anlamda bilişim sistemleri ve bu sistemleri birbirine bağlayan ağları içeren ortamlarda siber ortam olarak ifade edilebilir (AFAD Sözlüğü, 2019). Siber ortamlar günlük hayatta oldukça sık bulunduğumuz, farklı işlemlerimizi yürüttüğümüz, dijital verilerin aktığı ve siber güvenliğin ön planda tutulması gereken ortamlar olarak düşünülebilir. Siber güvenlik kavramı “Siber alemi oluşturan bilişim sistemlerinin saldırılardan korunmasını, verilerin gizlilik, bütünlük ve erişilebilirliğinin boyutlarının ele alınmasını, saldırıların ortaya çıkarılmasını, bunun sonucunda da önlem alma ve zarar görmemesi için yapılan çalışmalar” olarak tanımlanmıştır (T.C Ulaştırma Bakanlığı, 2016). Ayrıca siber güvenlik, siber tehditlere karşı kurum, kuruluş ve kişisel kullanıcıların verilerini korumak amacıyla kullanılan araç gereç, yönetmelik, rehber, faaliyetler ve teknolojilerin tamamı olarak görülmektedir (Özbek, 2019). Siber güvenlik, ağların tamamını, bilgisayar ve bilgisayar sistemlerini ve diğer dijital bileşenleri ve içinde depolanan verileri yetkisiz erişime karşı korumayı kapsar (Simplilearn, 2021) ve siber tehditleri önlemek adına gerekli olan işlemleri etkili bir şekilde uygulamayı gerekli kılar. Nitekim günümüzde dijital ortamlarda kurumlara ve kişilere yönelik siber tehditler oldukça artmıştır ve artmaya da devam etmektedir. Öyle ki küresel anlamda siber tehditler, her geçen yıl sayısını arttırarak veri ihlalleriyle birlikte hızlı bir şekilde gelişimini sürdürmektedir (Kaspersky, 2021). Risk Based Security’nin (2019) raporuna göre sadece 2019’un ilk dokuz ayında 5,183 ihlalin rapor edildiği ve 7,9 milyar kaydın açığa çıktığı görülmüştür. Bu değerler 2018 yılının ortalarındaki değerler ile karşılaştırıldığında, toplamdaki ihlal sayısı %33,3, açığa çıkan toplam kayıt sayısı %112 artmıştır. Bu değerlerin kurumlar ve kişiler için maddi ve manevi bakımından oldukça büyük bir değere karşılık geldiği ifade edilebilir. Örneğin büyük bir şirkete yapılan başarılı bir siber saldırının ortalama maliyetinin 2,6 milyon dolar olduğu ve şirketin uğradığı bir veri ihlalinin yaklaşık maliyetinin 3,9 milyon dolar olduğu değerlendirilmiştir (STM ThinkTech, 2021). International Data Corporation’ın dünya genelinde siber güvenlik çözümlerine yönelik olarak yapılan harcamaların 2022’ye kadar 133,7 milyar dolara ulaşacağını öngörmesi de (Kaspersky, 2021) bu bakımdan dikkate değerdir. STM ThinkTech’in (2021) raporuna göre ise 2020 yılının sonunda, kamu kurumları ve özel şirketlerin güvenlik hizmetlerine ilişkin

bütçelerinin %50'si siber güvenlik bütçelerine ayrılacaktır. Belirtilen durumlar dikkate alındığında siber ortamlardaki dijital verilerin güvenliği oldukça önem arz eden bir kavram olarak görülebilir.

İnsanlar, süreçler ve teknolojinin neden olduğu veri kayıplarını en aza indirmek için veri güvenliği farkındalığına ihtiyaç duyulur (Mediapharm, 2019). Küresel Bilgi Güvenliği Araştırması'ndan elde edilen sonuçlarda 2018 yılında dış tehditlerin sebep olduğu siber güvenlik tehditlerinin sayısal olarak azaldığı fakat kurum, kuruluş veya organizasyon içinde bulunan veya bunlarla bağlantılı kişiler ve benzeri kurum içi sebeplerden kaynaklı güvenlik ihlallerin göz ardı edilmeyecek kadar arttığı belirtilmiştir (PWC, 2018). Bu anlamda bireyler kurumların ve kendilerinin bilgi güvenliklerini tehdit edebilecek eylemlerini bilinçli bir şekilde gerçekleştirmemektedirler (Gökçearslan, Günbatar & Sarıtepeci, 2021). Bilgi güvenliğine yönelik tehdit ve ihlallerin birçoğu bireylerin bilgi güvenliği farkındalıklarındaki eksikliklerden kaynaklanmaktadır (Taha & Dahabiyeh, 2020). Bilgi güvenliği farkındalığı bu bakımdan, kurum ve kuruluşlardaki kullanıcıların güvenlik misyonlarının farkında olmasını ifade eder (Siponen, 2000). Bu açıdan özellikle büyük kitlelere hitap eden, bünyesinde oldukça fazla kişi çalışan ve sunduğu imkânlarından oldukça fazla kişinin yararlandığı kurum veya kuruluşlar dikkate değerdir. Üniversiteler bu kurumlar arasında yer almaktadır. Öyle ki yüzlerce hatta binlerce öğrenci ve çalışana sahip bu kurumlarda dijital veri güvenliği ve siber güvenlik ile ilgili sorunların yaşanması oldukça doğal bir durum olarak görülebilir. Bu anlamda üniversitelerde dijital veri güvenliğinin ve siber güvenliğin sağlanması adına görev yapan bilgi işlem daire başkanlıkları oldukça öneme sahip birimler olarak görülmektedir. Bu birimler dijital veri güvenliği ve siber güvenliğin sağlanması adına yönetim merkezi olarak kabul edilmektedir. Bu anlamda bu birimlerdeki çalışanların ve özellikle yönetim seviyesindeki kişilerin farkındalık ve anlayışı, bilgi güvenliği kültürünün oluşturulması açısından önemlidir (Kocamustafaoğulları, 2013). Bilgi güvenliği ihlallerine ilişkin riskleri ortadan kaldırmak ve en aza indirmek için en önemli faktörün güvenlik farkındalığı olduğu ifade edilebilir (Safa, Von Solms & Futch, 2016). Bu açıdan üniversitelerin bilgi işlem daire başkanlıklarında değişik görevlerde çalışanların dijital veri güvenliği ve siber güvenlik farkındalığı dikkate değer bir durum olarak görülmüştür ve çalışma buradan hareketle gerçekleştirilmiştir.

### *Araştırmanın Amacı*

Bu çalışmanın amacı, Türkiye’deki üniversitelerin bilgi işlem daire başkanlıklarında farklı birimlerde çeşitli görevler üstlenen çalışanların farklı değişkenlere (cinsiyet, yaş, eğitim düzeyi, mesleki deneyim ve görev) göre dijital veri güvenliği ve siber güvenliği sağlama farkındalıklarını belirlemektir. Bu amaçtan hareketle aşağıdaki sorulara cevaplar aranmıştır:

- 1) Bilgi işlem daire başkanlıklarında farklı görevler üstlenen çalışanların dijital veri güvenliği farkındalıkları (DVGF) ve kişisel siber güvenliği sağlama farkındalıkları (KSGSF) arasında anlamlı bir ilişki var mıdır?
- 2) Bilgi işlem daire başkanlıklarında farklı görevler üstlenen çalışanların dijital veri güvenlik farkındalıklarında cinsiyet, yaş, mesleki deneyim, öğrenim durumu ve görev değişkenleri açısından anlamlı bir farklılık var mıdır?
- 3) Bilgi işlem daire başkanlıklarında farklı görevler üstlenen çalışanların kişisel siber güvenlik farkındalıklarında cinsiyet, yaş, mesleki deneyim, öğrenim durumu ve görev değişkenleri açısından anlamlı bir farklılık var mıdır?

## **Yöntem**

### *Araştırma Modeli*

Araştırma, tarama modellerinden kesitsel tarama modeli ile gerçekleştirilmiştir. Kesitsel tarama veri toplama sürecinin bir seferde yapıldığı bir tarama türüdür (Frankel ve Wallen, 2000) ve amacı olgunun zaman içindeki değişimini değil herhangi bir zamandaki durumunu tanımlamaktır (Özdemir, 2015, s. 81). Tarama modelleri nesnelere, toplumların, kurumların yapısını ve olayların işleyişini tanımlamak amacıyla kullanılabilir (Özdemir, 2015) araştırma yöntemleridir. Belirtilen durumlar dikkate alındığında çalışmada üniversite çalışanlarının DVGF ve KSGSF’leri arasında anlamlı bir ilişki olup olmadığı ve DVGF ve KSGSF’lerinin cinsiyet, yaş, mesleki deneyim, öğrenim durumu ve görev değişkenleri açısından anlamlı bir farklılık gösterip göstermediği incelenip oldukça geniş bir kitlenin mevcut durumdaki durumu tanımlanmak istenildiğinden kesitsel tarama modeli kullanılmıştır.

### *Evren ve Örneklem*

Araştırmanın evrenini, Türkiye’deki üniversitelerin bilgi işlem daire başkanlıklarının çeşitli birimlerinde farklı görevler üstlenen (daire başkanı, şube müdürü, mühendis,



çözümleyici, programcı bilgisayar işletmeni, memur vb.) çalışanlar oluşturmaktadır. Üniversitelerin resmi web sitelerinden bilgi işlem daire başkanlıklarında görevli çalışanların kurumsal e-mail adreslerine ulaşılarak bu adreslere dijital ortamda kişisel bilgi formu, veri güvenliği farkındalık ölçeği ve kişisel siber güvenliği sağlama ölçeği gönderilmiş ve çalışanlardan formu ve ölçekleri gönüllük esasına göre cevaplamaları talep edilmiştir. Türkiye'deki toplam 206 üniversitenin 174'ündeki 1440 çalışana kişisel bilgi formu ve ölçekler gönderilmiştir. 32 üniversitenin çalışanlarına ulaşamamıştır. Form ve ölçeklerin gönderildiği 1440 kişiden, 417 kişi kişisel bilgi formunu ve ölçekleri cevaplamış, 7 kişinin forma ve ölçeklere verdikleri cevaplar eksik olduğundan, 410 kişiden toplanan veriler değerlendirilmiştir. Çalışma katılımcılarının cinsiyet, yaş, mesleki deneyim, öğrenim durumu ve görevlerine ilişkin bilgiler Tablo 1'de sunulmuştur.

**Tablo 1.** Katılımcıların özelliklerine ilişkin bilgiler

		f	%
Cinsiyet	Erkek	348	84.87
	Kadın	62	15.12
Yaş	20-30	86	20.97
	31-40	168	40.97
	41-50	126	30.73
	51-60	24	5.85
	60 üstü	6	1.46
Mesleki Deneyim	1-5	56	13.65
	6-10	132	32.19
	11-15	60	14.63
	16-20	102	24.87
	20 yıl üstü	60	14.63
Öğrenim Durumu	Lise	12	2.92
	Ön Lisans	42	10.24
	Doktora	48	11.70
	Yüksek Lisans	126	30.73
	Lisans	182	44.39
Görev	Memur	6	1.46
	Network	6	1.46
	Ağ Yönetimi	12	2.93
	Tekniker	12	2.92
	Yazılım	17	4.15
	Bilgisayar İşletmeni	18	4.39
	Teknisyen	19	4.63
	Sistem/Sistem Yönetim	19	4.63
	Daire Başkanı	24	5.85
	Donanım	31	7.56
	Programcı	36	8.78
	Mühendis	54	13.17
	Şube Müdürü / Şube Müdür V. / Müdür /Müdür Yrd.	60	14.63
Öğretim Görevlisi	96	23.41	

Katılımcıların yaş, mesleki deneyim, öğrenim durumu ve görevlerine ilişkin tanımlayıcı istatistikler Tablo 2’de yer almaktadır.

**Tablo 2.** Katılımcıların yaş, mesleki deneyim, öğrenim durumu ve görevlerine ilişkin tanımlayıcı istatistikler

	Yaş	N	$\bar{X}$	SS
DVGF	21-30	86	147.49	11.775
	31-40	168	146.99	12.322
	41-50	126	152.90	7.796
	51-60	24	153.54	4.423
	60 üstü	6	150.00	7.589
KSGSF	21-30	86	87.51	8.540
	31-40	168	84.08	7.280
	41-50	126	82.88	4.707
	51-60	24	77.92	5.838
	60 üstü	6	68.00	5.215
	Mesleki Deneyim	N	$\bar{X}$	SS
DVGF	1-5	56	143.96	13.257
	6-10	132	146.98	11.978
	11-15	60	149.73	9.008
	16-20	102	156.23	3.037
	20 yıl üstü	60	151.15	8.671
KSGSF	1-5	56	80.20	7.126
	6-10	132	78.86	6.127
	11-15	60	78.60	10.567
	16-20	102	83.19	5.406
	20 yıl üstü	60	80.72	7.351
	Öğrenim Durumu	N	$\bar{X}$	SS
DVGF	Lise	12	140.25	21.709
	Ön Lisans	42	145.38	15.771
	Lisans	182	143.04	16.499
	Yüksel Lisans	126	149.29	10.655
	Doktora	48	151.15	7.979
KSGSF	Lise	12	82.33	6.985
	Ön Lisans	42	81.83	8.430
	Lisans	182	77.15	9.693
	Yüksel Lisans	126	82.40	5.270
	Doktora	48	85.21	5.044
	Görev	N	$\bar{X}$	SS
DVGF	Ağ Yönetimi	12	157.75	2.137
	Bilgisayar İşletmeni	18	157.33	2.114
	Daire Başkanı	24	155.50	5.316
	Donanım	31	150.74	8.583
	Memur	6	151.67	4.633
	Mühendis	55	152.25	5.793
	Network	6	155.33	3.559
	Öğretim Görevlisi	96	148.44	8.622
	Programcı	36	139.64	15.290
	Sistem/Sistem Yönetimi	19	144.58	14.385
	Şube Müdürü	60	145.38	16.833
	Tekniker	11	153.36	5.904

	Teknisyen	19	153.16	4.451
	Yazılım	17	149.88	7.664
	Ağ Yönetimi	12	80.92	2.109
	Bilgisayar İşletmeni	18	82.94	2.127
	Daire Başkanı	24	82.33	2.014
	Donanım	31	83.94	8.587
	Memur	6	82.33	11.237
	Mühendis	55	89.65	6.507
KSGSF	Network	6	83.50	9.772
	Öğretim Görevlisi	96	85.82	7.986
	Programcı	36	79.81	9.606
	Sistem/Sistem Yönetimi	19	81.74	9.261
	Şube Müdürü	60	82.78	8.994
	Tekniker	11	79.82	5.250
	Teknisyen	19	82.68	5.034
	Yazılım	17	83.29	5.253

### Veri Toplama Araçları

#### Dijital Veri Güvenliği Farkındalığı Ölçeği (DVGFÖ)

Dijital veri güvenliği farkındalığı ölçeği Yılmaz, Şahin ve Akbulut (2015) tarafından geliştirilmiştir. Ölçek tek boyutludur ve ölçeğin tamamı olumlu ifadelerden oluşmaktadır. Ölçek toplam 32 maddeden oluşmaktadır ve ölçekteki ifadeler beşli likert şeklindedir. Ölçekteki beşli likert ifadeleri “Kesinlikle Katılıyorum (5)”, “Katılıyorum (4)”, “Kararsızım (3)”, “Katılmıyorum (2)”, “Kesinlikle Katılmıyorum (1)” biçiminde derecelendirilmiştir. Ölçeğin Cronbach alfa ( $\alpha$ ) iç tutarlılık katsayısı .945’tir (Yılmaz, Şahin & Akbulut, 2015).

Katılımcıların DVGFÖ’nde yer alan maddelere verdikleri cevaplara ilişkin ortalama ve standart sapma değerleri Tablo 3’te sunulmuştur.

**Tablo 3.** DVGFÖ maddelerine ilişkin ortalama ve standart sapma değerleri

		$\bar{X}$	SS
2	“Parola oluştururken harf, sayı ve özel karakter kullanmanın önemini bilirim”	4.86	.33
8	“E-posta ile gelen kimlik bilgilerini doğrulama mesajlarına (parola, kredi kartı vb.) itibar edilmemesi gerektiğini bilirim.”	4.85	.42
28	“Cep telefonuna gelen tek kullanımlık parola ile yapılan giriş işlemlerinin güvenliği arttırdığını bilirim.”	4.82	.41
13	“Parola hatırlatmak için kullanılan güvenlik sorularına başkalarının tahmin edemeyeceği cevaplar verilmesi gerektiğini bilirim.”	4.76	.59
12	“Antivirüs yazılımı kullanmanın önemini bilirim.”	4.75	.52
17	“Üzerinde çalışma yapılan dosyaların birden fazla ortamda yedeklenmesi gerektiğini bilirim.”	4.75	.69
3	“Farklı işlemler için farklı parola kullanmanın önemini bilirim.”	4.74	.47
14	“Parola oluştururken karakter sayısının fazla olmasının önemini bilirim.”	4.74	.57
15	“Parolaların herhangi bir ortamda saklanmasının güvenlik riski oluşturacağını farkındayım.”	4.74	.52
11	“Programların, üreticinin kendi sitesinden indirilmesinin önemini bilirim.”	4.72	.56

32	"Lisanslı olmayan yazılımların güvenlik açıkları oluşturabileceğinin farkındayım."	4.72	.53
18	"Başkalarının tahmin edemeyeceği parolalar oluşturmaya dikkat ederim."	4.70	.76
30	"İnternet sitelerinde kullanıcı oturumunu kapatırken "güvenli çıkış" bağlantısını kullanmanın önemini bilirim."	4.70	.54
7	"İşletim sisteminin (Windows, Android vb.) güncel olmasına dikkat ederim."	4.69	.57
10	"Güvenli olmadığını düşündüğüm e-postaları açmadan silmeye dikkat ederim."	4.69	.73
9	"Taşınabilir depolama birimlerini (Flash bellek, taşınabilir sabit disk) kullanmadan önce virüs taraması yapılması gerektiğini bilirim."	4.67	.60
27	"Elektrik kesintisine karşı dizüstü bilgisayarları bataryası ile kullanmanın önemini bilirim."	4.67	.56
19	"İnternet adres çubuğunda yanlış yönlendirme olup olmadığına dikkat ederim."	4.66	.66
24	"İzinsiz kullanılmaması için cihazlara (akıllı telefon, tablet, bilgisayar vb.) parola konulabileceğinin farkındayım."	4.64	.78
26	"İşletim sisteminin (Windows, Android vb.) güvenlikle ilgili uyarılarını dikkate alırım."	4.63	.53
16	"Verilerin, çeşitli uygulamalar (dropbox, google drive vb.) kullanılarak İnternet ortamında saklanabileceğini bilirim."	4.60	.80
22	"Parolaların belirli aralıklarla değiştirilmesi gerektiğinin farkındayım."	4.60	.74
25	"Kendime ait olmayan cihazlarda, parola gerektiren işlemler yapmamaya dikkat ederim."	4.60	.70
6	"Flash bellekleri, veri saklamak yerine sadece veri taşımak için kullanmanın farkını bilirim."	4.57	.69
4	"İzinsiz kullanılmaması için dosyalara parola konulabileceğinin farkındayım."	4.55	.79
1	"Zararlı yazılımlar (virüs, solucan, Truva atı vb.) konusunda bilgi sahibiyim."	4.45	.82
23	"Almak istemediğim çöp e-postaları "spam/gereksiz/önemsiz" olarak işaretlemeye dikkat ederim."	4.40	.89
29	"Sanal klavye kullanmanın önemini bilirim."	4.33	1.02
31	"İnternet sitelerinde kullanılan güvenlik sertifikaları hakkında bilgi sahibiyim."	4.31	.92
21	"Karmaşık yapıdaki parolaların kırılabilceğini bilirim."	4.17	1.11
20	"Taşınabilir depolama birimlerini (Flash bellek, taşınabilir sabit disk) "Donanımı Güvenle Kaldır" seçeneğini kullanarak çıkartmaya dikkat ederim."	4.14	1.06
5	"Güvenlik duvarı yazılımları konusunda bilgi sahibiyim."	4.10	1.03
		4.60	

Tablo 3'e göre katılımcıların DVGFÖ'ndeki maddelere verdikleri cevaplara ilişkin ortalama puanın 4.60 olduğu görülmüştür. Bu durum çalışmaya katılanların dijital veri güvenliğine ilişkin farkındalıklarının en üst seviyeye (Kesinlikle katılıyorum) oldukça yakın olduğunu göstermektedir.

#### *Kişisel Siber Güvenliği Sağlama Ölçeği (KSGSÖ)*

Kişisel siber güvenliği sağlama ölçeği, Erol, Şahin, Yılmaz ve Haseski (2015) tarafından geliştirilmiştir. Ölçek toplam 25 maddeden oluşmaktadır ve 5 alt boyuta sahiptir. Bunlar: Kişisel gizliliği koruma, güvenilmeyenden kaçınma, önlem alma, ödeme bilgilerini koruma ve iz bırakmamadır. Ölçekteki ifadeler beşli likert şeklindedir. Likert ifadeler "Her zaman (5)", "Sık sık (4)", "Ara sıra (3)", "Nadiren (2)" ve "Hiçbir zaman (1)" biçiminde

derecelendirilmiştir. Ölçekteki 10 madde ters maddedir. Ölçeğin Cronbach alpha katsayısı ( $\alpha$ ) 0.735'tir (Erol vd., 2015).

Katılımcıların KSGSÖ'nde yer alan maddelere verdikleri cevaplara ilişkin ortalama ve standart sapma değerleri Tablo 4'te sunulmuştur.

**Tablo 4.** KSGSÖ maddelerine ilişkin ortalama ve standart sapma değerleri

		$\bar{X}$	SS
8	"Şahsi bilgisayarım dışında kullandığım bilgisayarlarda bilgilerimin kalmamasına dikkat ederim."	4.69	.64
9	"İnternet üzerinden yapılan para ve kontör isteklerini dikkate almam."	4.69	.80
4	"Şifrelerimi belirlerken basit dizilimler kullanmaktan kaçınırım."	4.67	.62
10	"Tanımadığım kişilerden gelen sosyal ağ arkadaşlık isteklerini kabul etmem."	4.60	.85
11	"Güvenmediğim sitelere üye olmam."	4.57	.80
3	"Bilgisayarımda anti-virüs yazılımı bulundururum."	4.51	.94
2	"Kullandığım yazılımları güncellerim."	4.32	.84
15	"İnternet bankacılığı işlemlerimi şahsi bilgisayarımdan yaparım."	4.32	1.00
21	"Sosyal ağ. e-posta gibi hesaplarda işlem bittiğinde oturumu kapatırım."	4.22	1.20
1	"Web sayfalarında güvenlik bağlantılarını (https://) ve sertifikalarını kontrol ederim."	4.18	.78
16	"Online alışveriş işlemlerini şahsi bilgisayarımdan yaparım."	4.16	1.00
22	"Güvenmediğim sitelerden dosya indirmem."	4.13	1.37
14	"Web geçmişini temizlerim."	4.11	1.02
23	"İnternette kullandığım hesapların (e-posta. sosyal ağ vb.) şifrelerini değiştiririm."	4.04	1.02
6	"Web tarayıcımın güvenlik ayarlarını düzenlerim."	3.85	1.04
5	"İnternet şifrelerimin tümünün aynı olmasına dikkat ederim."	2.21	1.3
12	"Tanımadığım kişilerle web kamerası kullanarak sesli ve görüntülü iletişim kurarım."	2.02	1.45
18	"Sosyal paylaşım sitelerinde kişisel bilgileriime yer veririm."	1.92	1.17
7	"E-posta ile gelen kimlik doğrulama mesajlarını (kullanıcı adı. şifre vb. istekler) cevaplarım."	1.91	1.44
13	"İnternet ortamında gerektiği zaman kişisel bilgilerimi (TC No. Doğum Tarihi. GSM No vb. ) paylaşıyorum."	1.9	1.28
24	"Unutmamak için akılda kalan kolay bir şifre belirlerim."	1.83	1.13
20	"Sosyal ağlarda yer alan reklamlar üzerinden alışveriş yaparım."	1.80	1.18
19	"İnternet üzerinden yer bildirim yaparım."	1.73	1.13
17	"Tanımadığım kişilerden gelen e-posta eklerini açarım."	1.54	1.02
25	"Banka. online alışveriş siteleri gibi sitelerden gelen e-postalara (kart no. şifre vb. istekler) itibar ederim ve yanıtlarım."	1.51	1.00
		3.33	

Tablo 4 incelendiğinde katılımcıların KSGSÖ'nden elde ettikleri toplam ortalama puanın 3.33 olduğu görülmüştür. Bu durum katılımcıların kişisel siber güvenlik sağlama farkındalıklarının "Ara sıra" düzeyine yakın olduğunu göstermektedir.

#### Veri Toplama Süreci

Araştırmaya ilişkin veriler toplamadan önce Kafkas Üniversitesi Sosyal ve Beşeri Bilimler Etik Kurulu Başkanlığı'ndan (07.10.2020 tarih ve 14 sayılı oturumun 5.kararı)

çalışma için gerekli izinler alınmıştır. Daha sonra üniversitelerin web sayfalarından bilgi işlem daire başkanlığı çalışanlarına ait kurumsal e-mail adresleri toplanmıştır. Bu e-mail adresleri üzerinden dijital olarak katılımcılara bilgilendirici metinler içeren kişisel bilgi formu, dijital veri güvenliği farkındalık ölçeği formu ve kişisel siber güvenliği sağlama ölçeği formu gönderilerek gönüllülük esasına uygun olarak çalışmaya katkı sunmaları istenmiştir. Dijital ortamda toplanan veriler çalışmanın amacı ve araştırma soruları göz önünde bulundurulurken analizler için uygun hale getirilmiştir.

### *Verilerin Analizi*

Bilgi işlem daire başkanlıklarının çeşitli birimlerde farklı görevler üstlenen çalışanların DVGF ve KSGSF arasındaki ilişki ve DVGF ve KSGSF bakımından, cinsiyet, yaş, eğitim düzeyi, mesleki deneyim ve görev değişkenlerinin anlamlı bir farklılık oluşturup oluşturmadığı incelenmiştir. Bu amaç doğrultusunda ilk olarak çalışmaya katılan çalışanların cinsiyet, yaş, mesleki deneyim, öğrenim durumu ve görevlerine ilişkin frekans ve yüzde değerleri tespit edilmiştir. Daha sonra DVGF ve KSGSF ölçeklerinin maddelerine ilişkin ortalama ve standart sapma değerleri belirlenmiş ve ölçeklerden elde edilen puanların normal dağılım gösterip göstermediği incelenmiştir. Bunun için çarpıklık ve basıklık değerleri dikkate alınmıştır. Çarpıklık ve basıklık ( $C_{DVGFÖ} = -1.284$ ,  $B_{DVGFÖ} = 1.104$  ve  $C_{KSGSFÖ} = .778$ ,  $B_{KSGSFÖ} = 1.238$ ) değerlerinden puanların normal dağılım gösterdiğine ilişkin sonuçlara ulaşılmıştır. Çarpıklık ve basıklık değerlerinin  $-1.5 / +1.5$  değerleri arasında olması verilerin normal dağılım gösterdiği ifade etmektedir (Tabachnick & Fidell, 2007). Çalışmanın birinci araştırma sorusunu cevaplamak için DVGF ve KSGSF arasındaki ilişkiyi ortaya koymak adına Pearson korelasyon analizi yapılmıştır. Çalışmanın ikinci ve üçüncü araştırma sorularını cevaplamak için cinsiyetler açısından farkın ortaya konulması adına bağımsız örneklem t-testi, yaş, mesleki deneyim, öğrenim durumu ve görev açısından gruplar arası farkın belirlenmesi için ise ANOVA testi kullanılmıştır. Diğer taraftan varyansların ve örneklem boyutlarının eşit olmaması dikkate alınarak gruplar arasındaki farkın hangi grup yada gruplardan kaynaklandığını belirlemek için Post-Hoc testlerinden Games-Howell testi kullanılmıştır.

### *Sınırlılıklar*

Çalışmada evrenin tamamına ulaşmak mümkün olmadığından form ve ölçeklerin gönderildiği 1440 kişiden, 417 kişi kişisel bilgi formunu ve ölçekleri cevaplamış, 7 kişinin

forma ve ölçeklere verdikleri cevaplar eksik olduğundan, 410 kişiden toplanan veriler değerlendirilmeye alınmıştır. Çalışma verileri web ortamında üniversitelerin bilgi işlem daire başkanlıklarında görevli çalışanların kurumsal e-mail adreslerine dijital ortamda kişisel bilgi formu, DVGFÖ ve KSGSFÖ gönderilerek gönüllük esasına göre cevaplamaları talep edilerek toplanmıştır. Çalışmanın veri toplama sürecinde, gönderilen toplu e-maillerin üniversitelerin güvenlik duvarları tarafından engellenmesi ve çalışanların önemli bir çoğunluğunun kurumsal e-maillerini aktif olarak kullanmamasından kaynaklı olarak önemli bir sayıda çalışana ulaşmak mümkün olmamıştır.

## Bulgular

Çalışma katılımcılarının dijital veri güvenliği farkındalıkları (DVGF) ve kişisel siber güvenliği sağlama farkındalıkları (KSGSF) arasındaki ilişkiyi gösteren Pearson korelasyon analiz sonuçları Tablo 5'te yer almaktadır.

**Tablo 5.** DVGF ve KSGSF arasındaki ilişki

	N	r	p
DVGF - KSGSF	410	.143**	.004

\*\* Korelasyon .001 düzeyinde anlamlıdır.

Tablo 5'e göre katılımcıların dijital veri güvenliği farkındalıkları (DVGF) ve kişisel siber güvenliği sağlama farkındalıkları (KSGSF) arasında pozitif yönlü zayıf bir ilişki olduğu görülmüştür.

### İkinci Araştırma Sorusuna İlişkin Bulgular

Katılımcıların dijital veri güvenliği ve kişisel siber güvenliği sağlama farkındalıklarının cinsiyete göre anlamlı bir fark gösterip göstermediğini belirlemek adına yapılan bağımsız gruplar t-testi sonuçları Tablo 6'da sunulmuştur.

**Tablo 6.** DVGF'nin cinsiyete göre karşılaştırılması

	Cinsiyet	N	$\bar{X}$	SS	Sd	t	p
DVGF	Erkek	348	147.70	14.317	111.571	1.685	.095
	Kadın	62	150.19	9.955			

Tablo 6 incelendiğinde DVGF açısından cinsiyetin anlamlı bir fark oluşturmadığı görülmüştür ( $p = .095 > .05$ ). Kadınların ( $\bar{X} = 150.19$ ) DVGF'lerinin erkeklere ( $\bar{X} = 147.70$ ) göre daha yüksek olduğu ifade edilebilir.

Çalışmaya katılan çalışanların dijital veri güvenliği farkındalıklarının yaşa, mesleki deneyime, öğrenim durumuna ve görevine göre anlamlı bir fark gösterip göstermediğini belirlemek adına yapılan ANOVA testi sonuçları Tablo 7’de yer almaktadır.

**Tablo 7.** DVGF’nin yaşa, mesleki deneyime, öğrenim durumuna ve göreve göre karşılaştırılması

			Kareler Top.	sd	Kareler Ort.	F	p
Yaş	DVGF	Gruplar arası	3251.59	4	812.89	7.240	.000
		Grup içi	45474.28	405	112.28		
		Toplam	48725.87	409			
Mesleki Deneyim	DVGF	Gruplar arası	7271.28	4	1817.82	19.065	.000
		Grup içi	38617.09	405	95.35		
		Toplam	45888.38	409			
Öğrenim Durumu	DVGF	Gruplar arası	4645.088	4	1161.27	5.747	.000
		Grup içi	81833.00	405	202.05		
		Toplam	86478.08	409			
Görev	DVGF	Gruplar arası	8981.70	13	690.90	6.468	.000
		Grup içi	42300.87	396	106.82		
		Toplam	51282.57	409			

Tablo 7’ye göre grupların tamamında yaş, mesleki deneyim, öğrenim durumu ve görev değişkenleri DVGF’de anlamlı bir fark oluşturmuştur (< .05).

Yaş, mesleki deneyim, öğrenim durumu ve görev değişkenlerinin DVGF’de oluşturduğu farkın hangi grup ya da gruplardan kaynaklandığını belirlemek için yapılan Games-Howell testi sonuçları Tablo 8’de yer almaktadır.

**Tablo 8.** DVGF’nin yaş, mesleki deneyim, öğrenim durumu ve göreve ilişkin games-howell test sonuçları

Bağ. Değ.	Bağmz. Değ. (Yaş)	P	Bağ. Değ.	Bağmz. Değ. (Görev)	P		
DVGF	Games-Howell	21-30	.002	Daire Bşk.	Öğr. Gör.	.000	
		51-60			Programcı	.000	
		31-40			Şub. Müd.	.006	
	Games-Howell	51-60	.000	Donanım	Ağ Yön.	.009	
		41-50			Bilg. İşl.	.015	
		31-40			Programcı	.027	
Games-Howell	51-60	.002	Memur	Programcı	.038		
	31-40			Mühendis	Ağ Yön.	.000	
DVGF	Games-Howell	.000	DVGF	Games-Howell	Bilg. İşl.	.000	
					1-5	Programcı	.002
					16-20	Programcı	.000
					20 yıl üstü	Programcı	.008
					6-10	Şub. Müd.	.029
					11-15	Öğr. Gör.	.000
	Games-Howell	16-20	.000	Programcı	Ağ Yön.	.000	
		6-10			Bilg. İşl.	.000	
		11-15			Daire Baş.	.000	
		20 yıl üstü			Ağ Yön.	.000	
		1-5			Bilg. İşl.	.000	
		20 yıl üstü			Daire Bşk	.000	



		16-20	.000			Donanım	.027
Bağ. Değ.	Bağmz. Değ. (Öğrenim Durumu)		p			Memur	.038
	Lisans	Yük.Lis.	.001			Mühendis	.002
		Doktora	.000			Network	.000
	Yük. Lis.	Lisans	.001			Tekniker	.005
	Doktora	Lisans	.000			Teknisyen	.001
Bağ. Değ.	Bağmz. Değ. (Görev)		p			Sist/Sist.Yön.	Ağ Yön.
	Ağ Yön.	Donanım	.009			Bilg. İşl.	Bilg. İşl.
		Mühendis	.000			Şube Müd.	Ağ Yön.
		Öğr. Gör.	.000				Bilg. İşl.
		Programcı	.000				Daire Bşk
		Sist. Yön.	.040			Tekniker	Programcı
		Şub. Müd.	.000				Network
		Teknisyen	.033				
	Bilg. İşl.	Donanım	.015				
		Mühendis	.000				
		Öğr. Gör.	.000				
		Programcı	.000				
		Sist. Yön.	.040				
		Şub. Müd.	.000				
		Yazılım	.046				

Tablo 8 incelendiğinde DVGF açısından 60 yaş üstü hariç diğer yaş grupları arasında, anlamlı bir farklılığın olduğu görülmüştür. DVGF’de 16-20 arası mesleki deneyime sahip olan grup, diğer gruplardan belirgin olarak farklılık göstermiştir. Lisans, yüksek lisans ve doktora derecesine sahip gruplar arasında DVGF’de anlamlı farklılığın olduğu belirlenmiştir. Diğer taraftan DVGF’de farklı görevler üstlenen çalışanlar arasından anlamlı farklılıkların olduğu görülmüştür.

### Üçüncü Araştırma Sorusuna İlişkin Bulgular

Çalışanların kişisel siber güvenliği sağlama farkındalıklarının cinsiyete göre anlamlı bir fark gösterip göstermediğini belirlemek için yapılan bağımsız gruplar t-testi sonuçları Tablo 9’da yer almaktadır.

**Tablo 9 . KSGSF’nin cinsiyete göre karşılaştırılması**

	Cinsiyet	N	$\bar{X}$	SS	Sd	t	p
KSGSF	Erkek	348	84.00	7.131	408	2.732	.007
	Kadın	62	81.85	5.401			

Tablo 9 incelendiğinde KSGSF açısından cinsiyetin anlamlı bir fark oluşturduğu görülmüştür ( $p = .007 < .05$ ). Erkeklerin ( $\bar{X} = 84.00$ ) KSGSF’lerinin kadınlara ( $\bar{X} = 81.85$ ) göre daha yüksek olduğu ifade edilebilir.

Katılımcıların kişisel siber güvenliği sağlama farkındalıklarının yaşa, mesleki deneyime, öğrenim durumuna ve görevine göre anlamlı bir fark gösterip göstermediğini belirlemek için yapılan ANOVA testi sonuçları Tablo 10'da yer almaktadır.

**Tablo 10.** KSGSF'nin yaşa, mesleki deneyime, öğrenim durumuna ve göreve göre karşılaştırılması

		Kareler Top.	sd	Kareler Ort.	F	p
KSGSF	Gruplar arası	3632.68	4	908.17	19.628	.000
	Grup içi	18739.36	405	46.27		
	Toplam	22372.05	409			
KSGSF	Gruplar arası	1308.27	4	327.06	6.481	.000
	Grup içi	20439.14	405	50.46		
	Toplam	21747.42	409			
KSGSF	Gruplar arası	3659.60	4	914.90	14.748	.000
	Grup içi	25124.26	405	62.03		
	Toplam	28783.87	409			
KSGSF	Gruplar arası	3348.37	13	257.56	4.513	.000
	Grup içi	22603.10	396	57.079		
	Toplam	25951.47	409			

Tablo 10'a göre grupların tamamında yaş, mesleki deneyim, öğrenim durumu ve görev değişkenleri KSGSF'de anlamlı bir fark oluşturmuştur ( $< .05$ ).

Yaş, mesleki deneyim, öğrenim durumu ve görev değişkenlerinin KSGSF'de oluşturduğu farkın hangi grup ya da gruplardan kaynaklandığını belirlemek için yapılan Games-Howell testi sonuçları Tablo 11'de sunulmuştur.

**Tablo 11.** KSGSF'nin yaş, mesleki deneyim, öğrenim durumu ve göreve ilişkin games-howell test sonuçları

Bağ. Değ.	Bağmz. Değ. (Yaş)	P	Bağ. Değ.	Bağmz. Değ. (Görev)	P	
KSGSF Games-Howell	21-30	31-40	KSGSF Games-Howell	Ağ Yön.	Mühendis	.000
		41-50		Öğr. Gör.	.001	
		51-60		Bilg. İşl.	Mühendis	.000
		60 üstü		Daire Bşk.	Mühendis	.000
	31-40	21-30		Öğr. Gör.	.015	
		51-60		Mühendis	Ağ Yön.	.000
		60 üstü		Bilg. İşl.	.000	
	41-50	21-30		Daire Bşk.	.000	
		51-60		Programcı	.000	
		60 üstü		Şub.Müd.	.001	
		60 üstü		Tekniker	.003	
	51-60	21-30		Teknisyen	.002	
		31-40		Yazılım	.015	
		41-50		Öğr. Gör.	Ağ Yön.	.001
		60 üstü		Daire Bşk.	.015	
	60 üstü	21-30		Programcı	Mühendis	.000
		31-40		Şub. Müd.	Mühendis	.001
		41-50		Tekniker	Mühendis	.003
		51-60		Teknisyen	Mühendis	.002

Değ.		(Mesleki Deneyim)					
KSGSF	Games-Howell	6-10	16-20	.000	Yazılım	Mühendis	.015
		11-15	16-20	.020			
		16-20	6-10	.000			
			1-15	.020			
Bağ. Değ.	Bağmz. Değ. (Öğrenim Durumu)		P				
KSGSF	Games-Howell	Ön Lisans	Lisans	.020			
		Lisans	Ön Lisans	.020			
			Yük. Lis.	.000			
			Doktora	.000			
		Yük. Lis.	Lisans	.000			
			Doktora	.014			
		Doktora	Lisans	.000			
			Yük. Lis.	.014			

Tablo 11 incelendiğinde KSGSF açısından bütün yaş grupları arasında anlamlı bir farklılığın olduğu görülmüştür. KSGSF’de 1-5 ve 20 yıl üstü mesleki deneyime sahip gruplar ile diğer gruplar arasında anlamlı bir farklılık oluşmadığı fakat diğer gruplar arasında anlamlı bir farkın olduğu görülmüştür. Doktora, yüksek lisans, lisans ve ön lisans derecesine sahip gruplar arasında KSGSF’de anlamlı farklılığın olduğu belirlenmiştir. Diğer taraftan KSGSF’de farklı görevler üstlenen çalışanlar arasından anlamlı farklılıkların olduğu görülmüştür.

### Tartışma ve Sonuç

Bu çalışmada Türkiye’deki üniversitelerin bilgi işlem daire başkanlıklarında görev yapan çalışanların dijital veri güvenliği ve siber güvenliği sağlama farkındalıklarının farklı değişkenler açısından belirlenmesine çalışılmıştır. Üniversitelerin bilgi işlem daire başkanlıklarındaki çalışanların, kurumun ve kurumda görev yapan diğer çalışanların dijital ortamlardaki verilerinin güvenliğini sağlamada ve siber ortamlardaki tehdit ve tehlikelerin önlenmesinde, önemli görevler üstlendiği düşünüldüğünde çalışanların farkındalıklarının ortaya konulmasının gelecekteki çalışmalara yön vereceği öngörülmektedir.

#### *Dijital Veri Güvenliği ve Kişisel Siber Güvenliği Sağlama Farkındalıkları Arasındaki İlişki*

Çalışma sonucunda çalışanların dijital veri güvenliği ve kişisel siber güvenliği sağlama farkındalıklarının yüksek olduğu belirlenmiştir. Ayrıca bu iki farkındalığa ilişkin değerler arasında pozitif yönlü zayıf bir ilişki bulunmuştur. Kurum ve kuruluşların hitap ettiği kitlelere daha iyi deneyim sağlamak ve bu kitlelere sunduğu hizmetleri daha iyi hale getirmek için dijitalleşme çabaları sergilemesinin ve zaman içinde buna bağlı öğelere daha bağımlı hale gelmesinin (Abawajy, 2014) bu duruma etkisi olmuş olabilir. Dijital ortamlarda

üretilen bilgi miktarının çok hızlı bir şekilde artmasına bağlı olarak çok farklı bilgi güvenliği tehditlerinin ortaya çıkmasının da (Ki-Aries & Faily, 2017; Kruger & Kearney, 2006) çalışanların daha yüksek bir farkındalığa sahip olmasına etkisi olduğu düşünülebilir. Elde edilen sonuçlar Şahinaslan, Kantürk, Şahinaslan ve Borandağ'ın (2009) araştırma bulguları ile benzerlik göstermektedir. Araştırmacıların yaptıkları çalışmalarından elde ettikleri sonuçlara dayanarak, kurumlardaki bilgi güvenliğini sağlama adına sadece teknik açıdan alınan önlemlerin yeterli olmayacağı, önemli olan faktörün insan olduğu ve bilgi güvenliğine yönelik farkındalık düzeyinin artırılmasının gerektiğini ifade etmeleri bu çalışmanın sonuçlarına paralellik göstermektedir. Aynı şekilde Avcı ve Oruç'un (2020) üniversite öğrencilerinin kişisel siber güvenlik davranışları ve bilgi güvenliği farkındalıklarını inceledikleri benzer bir çalışmadan elde ettikleri bilgi güvenliği farkındalığı ile kişisel siber güvenlik sağlama farkındalığı alt boyutları arasında yüksek düzeyde ilişki bulunmaması da bu çalışmanın sonuçları ile benzerlik göstermektedir. Dijital veri güvenliği ve kişisel siber güvenliği sağlama farkındalıkları kavramlarının birbirlerini tamamlayıcı niteliklere sahip oldukları ve birbirlerini önemli ölçüde etkileme potansiyelinde oldukları düşünüldüğünde aralarındaki ilişkinin zayıf olması dikkate değer bir durum olarak görülebilir. Nitekim siber güvenlik farklı birçok teknolojiyi kullanarak savunması zayıf olan dijital sistemleri, bilgileri, verileri korumayla ilgili bir kavramdır (Von Solms & Von Solms, 2018) ve dijital veri güvenliği de bu kavramlar arasında oldukça önemli bir yer tutmaktadır. Canbek ve Sağıroğlu'nun (2006), dijital veri güvenliği için dijital ortamlarda veri bütünlüğünün bozulmadan ve izinsiz erişimleri engelleyerek verilerin saklanması ve taşınması için bilgi akışının gerçekleştiği platformların güvenli hale getirilmesine dikkat çekmeleri dijital veri güvenliği ile siber güvenlik arasındaki ilişkiye bu yönde bir vurgu yapmaktadır. Bu anlamda dijital veri güvenliği ve kişisel siber güvenliği sağlama farkındalıkları arasındaki yakın ilişki göz önünde bulundurularak bu ilişkinin güçlendirilmesi adına farklı çalışmaların yapılmasının önemli katkılar sunacağı düşünülmektedir.

*Dijital Veri Güvenliği Farkındalıklarının Cinsiyet, Yaş, Mesleki Deneyim, Öğrenim Durumu ve Göreve Göre Farklılıkları*

Çalışma sonuçları kadın çalışanların dijital veri güvenlik farkındalıklarının erkek çalışanlara göre daha yüksek olduğunu ve gruplar arasında cinsiyete göre anlamlı bir farklılığın olmadığını göstermiştir. Oluşan durum kadınların erkeklere göre dijital ortamda

karşılaşabilecekleri tehlikelerden daha haberdar olmalarından (Mart, 2012) kaynaklanmış olabilir. Ayrıca bu durum kadınların bilgi güvenliği tutumlarının erkeklere göre daha yüksek olmasından da (Arıtürk, 2015) kaynaklanabilir. Çalışmadan elde edilen sonuçlar Mart'ın (2012), Yılmaz ve diğerlerinin (2015), Arıtürk'ün (2015) ve Bıkmaz'ın (2017) araştırma bulguları ile paralellik göstermektedir. Öte yandan çalışma sonuçlarından dijital veri güvenliği farkındalıkları bağlamında yaş, mesleki deneyim, öğrenim durumu ve görev bakımından gruplar arasında anlamlı farklılıklar olduğu anlaşılmıştır. Oluşan durum herkesin bilgi sistemlerini koruma konusunda farklı özelliklere sahip olduğunun (Cokro, Tofani & Wang, 2020) ve dijital veri güvenliği farkındalıklarının farklı değişkenlerden etkilendiğinin bir göstergesi olarak görülebilir. Bu bakımdan üniversitelerin bilgi işlem bölümlerinde çalışanların bilgi güvenliği farkındalıklarının artırılması gerekliliğini (Kocamustafaoğulları, 2013) yerine getirmelerinin sonuçlar üzerinde etkisi olmuş olabilir. Ayrıca bu durum çalışanların kurumun bilgi güvenliğini sağlamakla birlikte kurumun bütün paydaşlarına ilişkin bilgi güvenliğinden de sorumlu olduğunun (Karabatak & Karabatak, 2019) bilincinde olmalarından kaynaklanabilir. Elde edilen sonuçlar Taner ve Kılıç'ın (2019) araştırma bulguları ile benzer niteliktedir. Çalışmada dijital veri güvenliği farkındalığı bakımından 60 yaş üstü yaş grubu hariç diğer yaş grupları arasında anlamlı farklar bulunmuştur. 51-60 yaş grubunun dijital veri güvenliği farkındalığı diğer yaş gruplarından daha yüksektir. Bu durum 51-60 yaş grubundaki çalışanların dijital veri güvenliği farkındalığı bakımından daha deneyimli ve bilinçli olmasından kaynaklanmış olabilir. Ayrıca yaş ile bilgi güvenliği farkındalığı arasında, yaşla birlikte gelişen doğrusal bir ilişkinin (McCormac, Zwaans, Parsons, Calic, Butavicius & Pattinson, 2017) olması da bu duruma etki etmiş olabilir. Karadağ ve Abuhanoğlu (2015) tarafından yapılan çalışmadan elde edilen yaşlı katılımcıların bilgi güvenliği farkındalığının daha yüksek olduğuna yönelik bulgularda bu paraleldedir. Diğer taraftan çalışmadan çalışanların dijital veri güvenliği farkındalıklarının mesleki deneyime göre farklılaştığı anlaşılmıştır. 16-20 yıllık mesleki deneyimi olan grup diğer gruplardan anlamlı şekilde ayrılmıştır. Öyle ki bu grubun dijital veri güvenliği farkındalıkları diğer gruplara göre daha yüksek olmuştur. Bu grupta yer alan çalışanların dijital veri güvenliği farkındalıkları bakımından daha bilinçli ve deneyim sahibi olduğu düşünülebilir. Bu anlamda mesleki deneyimin dijital veri güvenliği farkındalığını etkilediği düşünülebilir. Fakat çalışmadan elde edilen sonuçlar Yılmaz'ın (2015) çalışma sonuçları ile çelişmektedir. Bu durumun ortaya çıkmasına belirtilen çalışmaya sadece

öğretmenlerin dâhil edilmesi sebep olmuş olabilir. Öte yandan çalışmadan elde edilen sonuçlar dijital veri güvenliği farkındalıklarının farklı öğrenim durumlarına göre gruplarda farklılaştığını göstermiştir. Doktora mezunu çalışanların dijital veri güvenliği farkındalıkları diğerlerinden daha yüksektir. Bu durum doktora mezunu çalışanların dijital veri güvenliği konusunda daha fazla bilgi ve deneyime sahip olduğunun bir göstergesi olarak görülebilir. Nitekim dijital veri güvenliğine ilişkin tehdit ve tehlikelerde insan faktörünün sahip olduğu bilgi ve deneyim önemli bir yere sahiptir. Dijital veri güvenliğine yönelik tehdit ve tehlikelerin kaynağı, bilinçsiz ve bilgisizce, gerekli ve yeterli alt yapı olmadan farklı teknolojilerin işe koşulmasına bağlı olarak ve sistemlere zarar vermeye yönelik davranışların sonucu olarak görülebilir (Tekerek, 2008). Doktora mezunu çalışanların bu açıdan daha bilinçli olduğu düşünülebilir. Oluşan durum farklı eğitim kademelerinde edilen bilgi ve deneyimlerin çalışanların dijital veri güvenliği farkındalıkları üzerinde etkili olmasından kaynaklanabilir. Çalışmadan elde edilen sonuçlar Yılmaz'ın (2015) çalışma sonuçları ile farklılık göstermektedir. Oluşan durum çalışma örnekleminin önemli bir çoğunluğunun lisans mezunu öğretmenlerden oluşmasından kaynaklanmış olabilir. Diğer taraftan bu çalışmanın diğer bir sonucu dijital veri güvenliği farkındalıkları bağlamında çalışanların kurumlarında üstlendikleri görevler bakımından gruplar arasında anlamlı farklılıkların olduğunu göstermiştir. Taner ve Kılıç'ın (2019) çalışma sonuçları bu sonuçlara benzer niteliktedir. Dijital veri güvenliği farkındalığı bakımından ağ yöneticileri ve bilgisayar işletmenleri diğer gruplardan anlamlı bir şekilde ayrılmış ve farkındalıkları daha yüksek olmuştur. Kurumlarda web tabanlı sistemlerin yoğun olarak kullanılmaya başlanması, bu kurumlarda bu sistemlerle ilgilenen ve bu sistemleri yoğun olarak kullanan çalışanlarda dijital veri farkındalıklarının oluşmasına ve artmasına sebep olmuş olabilir. Bunun da üstlenilen görev ile bağlantılı olduğu düşünülebilir. Belirtilen durumlar dikkate alındığında dijital veri güvenliği farkındalıklarını konu edinen çalışma sayısının oldukça sınırlı olduğu görülmektedir. Bu durum göz önünde bulundurulduğunda gelecekteki çalışmalarda dijital veri güvenliği farkındalıklarına yönelik çalışma sayısının artırılmasının ve dijital veri güvenliği farkındalıklarının farklı değişkenlere göre incelenmesinin alana önemli katkıları olacağı düşünülmektedir.

*Kişisel Siber Güvenliği Sağlama Farkındalıklarının Cinsiyet, Yaş, Mesleki Deneyim, Öğrenim Durumu ve Göreve Göre Farklılıkları*

Çalışma sonuçlarına göre erkek çalışanların siber güvenliği sağlama farkındalıkları kadın çalışanlara göre daha yüksektir ve erkek ve kadın çalışanlar arasında siber güvenliği sağlama farkındalıkları bakımından anlamlı bir farklılık vardır. Bu durum erkek ve kadın çalışanlar arasında siber güvenlikle ilişkili bilgi, tutum ve davranışsal farklılıklardan kaynaklanmış olabilir (Maennel, Mases & Maennel, 2018). Kadın çalışanların sağlıklı siber davranışları oluşturma ve sürdürme süreçlerini iyi yapamamasının da bu sonuca etkisi olmuş olabilir (Vishwanath, Neo, Goh, Lee, Khader, Ong & Chin, 2020). Çalışma sonuçları ile Anwar, He, Ash, Yuan, Li ve Xu'nun (2017), Karacı, Akyüz ve Bilgici'nin (2017), Özbek'in (2019), Karakaya ve Yetgin'in (2020) araştırma bulguları benzerlik göstermektedir. Ancak çalışmanın sonuçları Harrington, Anderson ve Agarwal'ın (2006), Karacı, Akyüz ve Bilgici'nin (2017), Ünal ve Ergen'in (2018) siber güvenliği sağlama farkındalıkları bakımından cinsiyetin anlamlı bir fark oluşturmadığı çalışma sonuçları ile çelişmektedir. Bu duruma belirtilen çalışmaya sadece lisans öğrencilerinin dâhil edilmesinin sebep olduğu düşünülebilir. Diğer taraftan çalışma sonuçlarından kişisel siber güvenliği sağlama farkındalıkları bağlamında yaş, mesleki deneyim, öğrenim durumu ve görev bakımından gruplar arasında anlamlı farklılıklar olduğu anlaşılmıştır. İnsan davranışlarını etkileyen çok sayıda faktörün var olduğu (Coventry, Briggs, Blythe & Tran, 2014) düşünüldüğünde bu duruma kişisel siber güvenliği sağlama farkındalıklarının farklı değişkenlerden etkilenmesinin sebep olduğu düşünülebilir. Çalışma sonuçlarından kişisel siber güvenliği sağlama farkındalıkları bakımından bütün yaş grupları arasında anlamlı farklılıklar olduğu anlaşılmıştır. Karakaya ve Yetgin'de (2020) yaptıkları çalışmada siber güvenliği sağlama adına yaşın belli konularda farklılık oluşturduğuna vurgu yapmaları bu yöndedir. Çalışma grupları arasında oluşan farkın kaynağı olarak 21-30 ve 60 yaş üstü gruplar olduğunu düşünülebilir. Nitekim bu gruplar diğer gruplardan anlamlı şekilde farklılaşmıştır. Kişisel siber güvenliği sağlama farkındalığı bakımından 21-30 yaş grubu farkındalığı en yüksek, 60 yaş üstü grubu ise farkındalığı en düşük grup olarak ifade edilebilir. Daha küçük yaş grubunda yer alan çalışanların güncel teknolojilere daha iyi ayak uydurması, yaş ilerledikçe bunun daha zor gerçekleşmesi bu duruma etki etmiş olabilir. Nitekim bilgi ve iletişim teknolojilerine dayalı sistem ve işlemlerin günceliğini takip ederek bunları etkili ve verimli bir şekilde kullanabilmek adına gerekli uyum sürecinin belli bir yaşın üstündeki çalışanlarda

daha zor gerçekleştirebileceği de göz önünde bulundurulabilir. Öte yandan kişisel siber güvenliği sağlama farkındalıkları açısından mesleki deneyim grupları arasında anlamlı bir farklılık oluşturmuştur. Oluşan durumun siber güvenlik konusuna yönelik ana etkenler olarak görülen bilgi, beceri ve anlayışın (Hogan, 2005) mesleki deneyim ile artmasından kaynaklandığı düşünülebilir. Gruplar arası farkın kaynağı 16-20 yıllık mesleki deneyime sahip çalışanların bulunduğu grup olarak belirlenmiştir. Diğer grupların kişisel siber güvenliği sağlama farkındalıkları açısından benzer özelliklere sahip olduğu ifade edilebilir. Bu anlamda mesleki deneyimin kişisel siber güvenliği sağlama farkındalıkları üzerinde çok etkili olmadığı da düşünülebilir. Diğer taraftan kişisel siber güvenliği sağlama farkındalıkları bakımından öğrenim durumu gruplarında anlamlı bir farklılık oluşmuştur. Lisans mezunu çalışanlar ön lisans, yüksek lisans ve doktora mezunu çalışanlardan anlamlı şekilde ayrılmıştır. Siber güvenliği sağlama farkındalıkları bakımından lisans mezunu çalışanların yer aldığı grup farkındalığı en düşük olan grup, doktora mezunu çalışanların yer aldığı grup ise farkındalığı en yüksek grup olmuştur. Bu açıdan öğrenim durumlarındaki farklılıkların siber güvenliği sağlama farkındalıkları üzerinde etkili olduğu düşünülebilir. Nitekim doktora mezunu çalışanların hem dijital veri güvenliği hem de siber güvenliği sağlama farkındalıklarının yüksek bulunması bu yönde bulunmuş bir sonuç olarak görülebilir. Bu grupta yer alan çalışanların siber güvenliği sağlama farkındalıkları diğer gruplardan daha yüksek olmuştur. Buda bu grupta yer alan çalışanların siber güvenliği sağlama açısından daha çok bilgi ve deneyime sahip olmalarından kaynaklanmış olabilir. Bununla beraber çalışanların siber güvenliği sağlama farkındalıklarının kurumlarındaki görevlerine göre anlamlı farklılıklar gösterdiği anlaşılmıştır. Oluşan bu durum düzenlemelere ve yönergelere bağlı kalınarak, güvenlik politikaları oluşturmayı vurgulayarak, personeller arasında siber güvenlik bilincini geliştirmeye (Hadlington, 2018; Pendley, 2018) odaklanılmasından kaynaklanmış olabilir. Elde edilen sonuçlar Taner ve Kılıç'ın (2019) araştırma bulguları ile benzerdir. Kişisel siber güvenliği sağlama farkındalığı açısından mühendisler diğer gruplardan anlamlı bir şekilde ayrılarak farkındalıkları daha yüksek olmuştur. Bu durumun bilgisayar bilgisi daha fazla olan çalışanların siber güvenlik farkındalıklarının daha yüksek olabileceğinden (Zwilling, Klien, Lesjak, Wiechetek, Cetin, & Basim, 2020). kaynaklanabileceği düşünülebilir. Asher ve Gonzalez'in (2015) siber güvenlik konusunda bilgi sahibi olan kişilerin farklı siber saldırı türlerini ayırt edebildiklerini, bilgi sahibi olmayan kişilerin saldırı türlerine duyarlı olmadıklarına dikkat çekmesi de bu yöndedir. Bu



anlamda çalışanların siber güvenliği sağlama farkındalıklarına kurumda üstlenilen görevin etkileri olduğu düşünülebilir. Yapılan çalışmalar dikkate alındığında literatürde siber güvenliği sağlama farkındalıkları bakımından çalışma sayısının oldukça az ve incelenen değişken sayısının sınırlı olduğu görülmüştür. Bu bakımdan gelecekte bu alana yönelik çalışma sayılarının artırılmasının ve bu çalışmalarda farklı değişkenlerin incelenmesinin alana faydalı olacağı ifade edilebilir.

Sonuç olarak dijital verilerin oldukça hızlı bir şekilde arttığı siber ortamlarda özellikle büyük kitlelere hizmet veren kurumların dijital veri güvenliği ve siber güvenliği sağlama konularına önem vermesi gerekliliği bulunmaktadır. Nitekim bu kurumların kendilerinin, çalışanlarının ve hizmet verdiği kişilerin siber ortamdaki dijital verilerinin güvenliği ve bu ortamların güvenliği direk veya dolaylı olarak kurumun sorumluluğundadır. Bu anlamda çalışan ve hizmet verdiği kişi sayısı oldukça fazla olan kurumlarda bu işler bilgi işlem görevlileri tarafından yürütülmektedir. Bu durum da burada çalışan kişilerin dijital veri güvenliği ve siber güvenliği sağlama adına daha yüksek bir farkındalığa sahip olmalarını gerektirmektedir. Dijital veri güvenliği ve siber güvenliği sağlama adına yüksek farkındalığa sahip bilgi işlem birimi çalışanları ile kurumun, kurum çalışanlarının ve hizmet verilen kişilerin dijital verileri korunacak, siber tehdit ve tehlikelere karşı önlemler alınarak etkili bir şekilde müdahalelerde bulunulacaktır.

*Etik Kurul Belgesi*

*Etik Kurul Komisyon Adı: Kafkas Üniversitesi Sosyal ve Beşeri Bilimler Etik Kurul*

*Başkanlığı*

*Etik Kurul Belge Tarihi: 07/10/2020*

*Etik Kurul Belgesi Sayı ve Numara: 28644117-840.99/43*

*Yazar Katkı Beyanı*

**Cengiz GÜNDÜZALP:** Kavramsallaştırma, metodoloji, verilerin toplanması, işlenmesi, analizi, yorumlanması, denetim, inceleme-yazma ve düzenleme.

## Kaynaklar

- Afet ve Acil Durum Yönetimi Başkanlığı. (2019). Siber ortam nedir? Retrieved form <https://www.afad.gov.tr/tr/23792/Aciklamali-Afet-Yonetimi-TerimleriSozlugu>.
- Aldridge, J., Medina, J., & Ralphs, R. (2010). The problem of proliferation: guidelines for improving the security of qualitative data in a digital age. *Research Ethics*, 6(1), 3-9.
- Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69, 437-443

- Arıttürk, M. (2015, Şubat). Bilgi farkındalığı ve bilgi güvenliğinin karşılaştırılması. XVII. Akademik Bilişim Konferansı, Anadolu Üniversitesi, Eskişehir. Retrieved from <https://ab.org.tr/ab15/kabul.html>.
- Avcı, Ü. & Oruç, O. (2020). Üniversite öğrencilerinin kişisel siber güvenlik davranışları ve bilgi güvenliği farkındalıklarının incelenmesi. *İnönü Üniversitesi Eğitim Fakültesi Dergisi*, 21(1), 284-303. doi: [10.17679/inuefd.526390](https://doi.org/10.17679/inuefd.526390)
- Ben-Asher, & N., Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, 48, 51-61.
- Bıkmaz, Z (2017). Sağlık yönetimi bölümü öğrencilerinin mobil güvenlik farkındalığı ve dijital veri güvenliği farkındalıklarının belirlenmesi. *Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi*, 1(1), 22-30.
- Canbek, G. ve & Sağıroğlu, Ş. (2006). Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. *Politeknik Dergisi*, 9(3), 165-174.
- Cokro, R. S., Tofani, R., & Wang, G. (2020). Designing integrated data security system. *International Journal*, 9(6), 27-30.
- Coventry, L., Briggs, P., Blythe, J., & Tran, M. (2014). Using behavioural insights to improve the public's use of cyber security best practices improve the public's use of cyber. *Project Report. Government Office for Science*, 1-20.
- Erol, O., Şahin, Y. L., Yılmaz, E., & Haseski, H. İ. (2015). Personal cyber security provision scale development study. *International Journal of Human Sciences*, 12(2), 75-91.
- Frankel, J. R., & Wallen, N. E. (2000). *How to evaluate and design research in education*. NewYork: McGraw-Hill.
- Gökçearslan, Ş., Günbatar, M. S., & Sarıtepeci, M. (2021). Ortaöğretim Öğrencilerinin Bilgi Güvenliği Farkındalıklarının İncelenmesi. *Yüzyüncü Yıl Üniversitesi Eğitim Fakültesi Dergisi*, 18(1), 354-373.
- Hadlington, L. (2018). Employees attitudes towards cyber security and risky online behaviours: an empirical assessment in the United Kingdom. *International Journal of Cyber Criminology*, 12(1), 269-281.
- Harrington, S., Anderson, C., & Agarwal, R. (2006, Aralık). Practicing safe computing: Message framing, self-view, and home computer user security behavior intentions. *27th ICIS 2006*. Milwaukee, Wisconsin. Retrieved from <http://aisel.aisnet.org/icis2006/93>.
- Hogan, J. (2005) Motivation. In J.J. Bolhuis (Ed.), *The behaviour of animals: Mechanisms, function and evolution* (pp. 41-70. Malden, MA: Blackwell Publishing.
- IBM (2020). Why is data security important? Retrieved from <https://www.ibm.com/topics/data-security>.
- Karabatak, S. & Karabatak, M. (2019, Haziran). Information security awareness of school administrators," *7th International Symposium on Digital Forensics and Security (ISDFS)*. Fırat Üniversitesi, Barcelos. Retrieved from <https://ieeexplore.ieee.org/abstract/document/8757525>.
- Karacı, A., Akyüz, H. İ., & Bilgici, G. (2017). Üniversite öğrencilerinin siber güvenlik davranışlarının incelenmesi. *Kastamonu Eğitim Dergisi*, 25(6), 2079-2094.
- Karadağ, M. & Abuhanoğlu, H. (2015). Sosyo-kültürel özelliklerin bilgi güvenliği farkındalığı üzerine etkisi: Gülhane Askeri Tıp Fakültesi Eğitim Hastanesi'nde bir çalışma. *The Journal of Academic Social Science Studies*, 36, 379-386.

- Karakaya, A., & Yetgin, M. A. (2020). Karabük üniversitesi çalışanlarına yönelik kişisel siber güvenlik üzerine araştırma. *Kahramanmaraş Sütçü İmam Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 10(2), 157-172.
- Kaspersky (2021). Siber güvenlik nedir? Retrieved from <https://www.kaspersky.com.tr/resource-center/definitions/what-is-cyber-security>.
- Ki-Aries, D., & Faily, S. (2017). Persona-centred information security awareness. *Computers & Security*, 70, 663–674.
- Kocamustafaoğulları, M. (2013). *Bilgi güvenliği farkındalığı ve uygulama seviyesi değerlendirmek için bilgi güvenliği prototip uygulaması*. (Yayımlanmamış yüksek lisans tezi). YÖK Ulusal Tez Merkezi veri tabanından elde edildi. (Tez no: 335475)
- Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, 25(4), 289–296.
- Maennel, K., Mases, S., & Maennel, O. (2018). Cyber hygiene: The big picture. *Lecture Notes in Computer Science (Including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics)*, 11252 LNCS, 291–305. [https://doi.org/10.1007/978-3-030-03638-6\\_18](https://doi.org/10.1007/978-3-030-03638-6_18)
- Mart, İ. (2012). *Bilişim kültüründe bilgi güvenliği farkındalığı*. (Yayımlanmamış yüksek lisans tezi). YÖK Ulusal Tez Merkezi veri tabanından elde edildi. (Tez no: 318088)
- McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, 69, 151-156.
- Mediapharm (2019). The data security awareness programme. Retrieved from <https://www.mediapharm.co.uk/blog/data-security-awareness>.
- Özbek, Y. (2019). *Öğretmen adaylarının siber güvenlik farkındalıklarının incelenmesi*. (Yayımlanmamış yüksek lisans tezi). YÖK Ulusal Tez Merkezi veri tabanından elde edildi. (Tez no:569578)
- Özdemir, E. (2014). *Tarama yöntemi*. In M. Metin (Ed.), *Kuramdan uygulamaya eğitimde bilimsel araştırma yöntemleri içinde* (2.baskı, s. 78-97). Ankara: Pegem Akademi.
- Özdemir, E. (2015). *Tarama yöntemi*. M. Metin (Ed.), *Kuramdan uygulamaya eğitimde bilimsel araştırma yöntemleri içinde* (ss. 99-114) Ankara: Pegem Akademi.
- Pendley, J. A. (2018). Finance and accounting professionals and cybersecurity awareness. *Journal of Corporate Accounting & Finance*, 29(1), 53-58.
- Praveena, A., & Smys, S. (2017, Nisan). Ensuring data security in cloud based social networks. *2017 International Conference of Electronics, Communication and Aerospace Technology (ICECA)*, RVS Technical Campus, Coimbatore. Retrieved from [https://www.aconf.org/conf\\_89022.html](https://www.aconf.org/conf_89022.html).
- PWC (2018). Küresel bilgi güvenliği araştırması 2018. Retrieved from <https://www.pwc.com.tr/tr/hizmetlerimiz/dijital-hizmetler/siber-guvenlik-ve-verikoruma-hizmetleri/yayinlar/kuresel-bilgi-guvenligi-arastirmasi-2018.html>
- Risk Based Security (2019). Data breach quickview report. Retrieved from <https://www.riskbasedsecurity.com/2019/11/12/number-of-records-exposed-up-112>.
- Safa, N. S., Von Solms, R., & Fatcher, L. (2016). Human aspects of information security in organisations. *Computer Fraud & Security*, 2016(2), 15-18.
- Simplilearn (2021). What is digital security: Overview, types, and applications explained. Retrieved from <https://www.simplilearn.com/what-is-digital-security-article>.
- Siponen MT. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8(1), 31–41.

- Solichin, A., & Ramadhan, E. W. (2017, Ekim). Enhancing data security using DES-based cryptography and DCT-based steganography. *3rd International Conference on Science in Information Technology (ICSITech)*, Universitas Pendidikan Indonesia, Bandung. Retrieved from <https://ieeexplore.ieee.org/xpl/conhome/8241142/proceeding>.
- STM ThinkTech (2021). Siber tehdit durum raporu. Retrieved from [https://thinktech.stm.com.tr/uploads/raporlar/pdf/271202116230558\\_stm\\_siber\\_tehdit\\_durum\\_raporu\\_ekim\\_aralik\\_2020.pdf](https://thinktech.stm.com.tr/uploads/raporlar/pdf/271202116230558_stm_siber_tehdit_durum_raporu_ekim_aralik_2020.pdf).
- Şahinaslan, E., Kantürk, A., Şahinaslan, Ö., & Borandağ, E. (2009). Kurumlarda bilgi güvenliği farkındalığı, önemi ve oluşturma yöntemleri. *Akademik Bilişim*, 9, 11-13.
- T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı (2016). 2016-2019 Ulusal siber güvenlik stratejisi. Retrieved from [http://www.udhb.gov.tr/doc/siberg/2016-2019\\_guvenlik.pdf](http://www.udhb.gov.tr/doc/siberg/2016-2019_guvenlik.pdf).
- Tabachnick, B. G., Fidell, L. S., & Ullman, J. B. (2007). *Using multivariate statistics*. Boston, MA: Pearson.
- Taha, N., & Dahabiyeh, L. (2021). College students information security awareness: a comparison between smartphones and computers. *Education and Information Technologies*, 26(2), 1721-1736.
- Taner, E., & Kılıç, İ. (2019). Güvenlik güçlerinin bilgi güvenliği farkındalığını belirlemeye yönelik bir araştırma. *Güvenlik Bilimleri Dergisi*, 8(2), 253-269.
- Tekerek, M. (2008). Bilgi güvenliği yönetimi. *KSÜ Fen ve Mühendislik Dergisi*, 11(1), 132.
- Ünal, A.N., & Ergen, A. (2018). Siber uzayda yeterince güvenli davranıyor muyuz? İstanbul ilinde yürütülen nicel bir araştırma. *MCBÜ Sosyal Bilimler Dergisi*, 16(2), 191-216. doi: 10.18026/cbayarsos.439489
- Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*, 128. <https://doi.org/10.1016/j.dss.2019.113160>
- Von Solms, B. & Von Solms, R. (2018). Cybersecurity and information security—what goes where? *Information & Computer Security*. 26(1), 2–9.
- Vural, Y. ve & Sağiroğlu, Ş. (2008). Kurumsal bilgi güvenliği ve standartları üzerine bir inceleme. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, 23(2), 507-522.
- Yaşar, H. (2014). *Kurumsal siber güvenliğe yönelik tehditler ve mücadele yöntemleri: Eylem planı örneği*. (Yayımlanmamış yüksek lisans tezi). YÖK Ulusal Tez Merkezi veri tabanından elde edildi. (Tez no: 362468)
- Yılmaz, E. (2015). *Öğretmenlerin dijital veri güvenliği farkındalığı*. (Yayımlanmamış doktora tezi). YÖK Ulusal Tez Merkezi veri tabanından elde edildi. (Tez no: 395184)
- Yılmaz, E., Şahin, Y. L., & Akbulut, Y. (2015). Dijital veri güvenliği farkındalığı ölçeğinin geliştirilmesi. *Online Academic Journal of Information Technology (AJIT-e)*, 6(21), 23-40.
- Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber security awareness, knowledge and behavior: a comparative study. *Journal of Computer Information Systems*, 1-16.