Kafkas Üniversitesi
Yönetim ve Bilişim Dergisi

Year/Yıl: 2025 | Vol/Cilt: 1 | Issue/Sayı: 1
Pages: 79-98

e-ISSN: 3108-6411

KAFKAS UNIVERSITY JOURNAL OF MANAGEMENT AND INFORMATICS

Başvuru/Received: 13.12.2025 | Kabul/Accepted: 26.12.2025

Lisansüstü Öğrencilerinin Bilişim Güvenliği Farkındalığı: Nitel Bir Araştırma

(Graduate Students' Information Security Awareness: A Qualitative Research)

Ezgi Pelin Yıldız[a], Melisa Tansu Keleş[b], Selinay Sezgi[b], Elif Gül[b], Enver Faruk Özcan[b], Ahmet Yüksel[b]

[a] *Doç. Dr., Kafkas Üniversitesi, Kazım Karabekir Teknik Bilimler Meslek Yüksekokulu, yildizezgipelin@gmail.com.*

[b] *Yüksek Lisans Öğrencisi, Kafkas Üniversitesi, Sosyal Bilimler Enstitüsü, kelesmelisatansu17@gmail.com, sezgiselinay1@gmail.com, 252624007@ogr.kafkas.edu.tr, enverfaruk.ozcan@gmail.com, ahmetyksl2727@gmail.com.*

Öz

Bu araştırmanın amacı, lisansüstü öğrencilerin bilişim güvenliği farkındalık düzeylerini incelemektir. Araştırmanın katılımcı grubunu bir kamu üniversitesinin 15 lisansüstü öğrencisi oluşturmaktadır. Araştırmada nitel araştırma desenlerinden fenomenoloji çalışması kullanılmıştır. Veri toplama aracı olarak araştırmacılar tarafından geliştirilen 9 soruluk yarı yapılandırılmış görüşme formu kullanılmış olup, formun kapsam geçerliliği, dört alan uzmanının görüşleri doğrultusunda sağlanmıştır. Elde edilen veriler içerik analizi yöntemiyle çözümlenmiştir. Katılımcıların büyük çoğunluğu, güçlü ve çok aşamalı parolalar kullanma, iki aşamalı doğrulama yöntemlerinden yararlanma, verilerini düzenli olarak yedekleme ve şüpheli bağlantılardan kaçınma gibi temel güvenlik uygulamalarını alışkanlık haline getirdiklerini ifade etmiştir. Bunun yanında, kötü amaçlı yazılımlar, sosyal mühendislik teknikleri, kimlik avı saldırıları ve veri gizliliği ihlalleri hakkında farkındalık düzeylerinin oldukça gelişmiş olduğu belirlenmiştir. Elde edilen bulgular, üniversitelerde yürütülecek bilişim güvenliği politikalarının ve eğitim içeriklerinin geliştirilmesine katkı sağlayabileceği gibi uygulamaya dönük farkındalık programlarının gerekliliğini de açık biçimde ortaya koymaktadır.

Anahtar Kelimeler:
Bilişim güvenliği, Bilgi güvenliği farkındalığı, Nitel araştırma, Güvenlik tehditleri, Veri gizliliği

Makale türü:
Araştırma

Abstract

The aim of this research is to examine the information security awareness levels of graduate students. The research participants consisted of 15 postgraduate students from a public university. A phenomenological study, a qualitative research design, was used in the research. A 9-question semi-structured interview form developed by the researchers was used as the data collection tool, and the content validity of the form was ensured based on the opinions of four field experts. The obtained data were analysed using the content analysis method. The vast majority of participants stated that they have made basic security practices such as using strong and multi-factor passwords, utilizing two-factor authentication methods, regularly backing up their data, and avoiding suspicious links into habits. In addition, it was determined that their awareness levels regarding malware, social engineering techniques, phishing attacks, and data privacy breaches were quite advanced. The findings can contribute to the development of information security policies and educational content to be implemented in universities, and also clearly demonstrate the necessity of practical awareness programs.

Keywords:
Information security, Information security awareness, Qualitative research, Security threats, Data privacy

Article type:
Research

Atıf/Citation: Yıldız, E. P., Keleş, M. T., Sezgi, S., Gül E., Özcan E. F., & Yüksel, A. (2025). Lisansüstü öğrencilerinin bilişim güvenliği farkındalığı: Bir durum çalışması. *Kafkas Üniversitesi Yönetim ve Bilişim Dergisi, 1*(1), 79-98.

1. Giriş

Dijital çağ olarak adlandırılan günümüzde tüm dünyada olduğu gibi Türkiye'de de bilişim teknolojilerinin yaygınlaşmasında ve kullanımında hızlı bir artış yaşandığı görülmektedir. Eğitim, sosyalleşme, haberleşme ve ticaret gibi pek çok alanda teknolojinin günlük yaşamın ayrılmaz bir parçası hâline gelmesi hayatı büyük ölçüde kolaylaştırmış olmakla birlikte, bilgi güvenliğine yönelik tehditleri de beraberinde getirmektedir. Bu noktada kötücül yazılımlar, veri ihlalleri ve siber saldırılar hem bireyleri hem de kurumları ciddi biçimde etkileyen tehdit unsurları olarak ön plana çıkmaktadır. Bu durum, toplumun tüm kesimlerini ilgilendirdiği gibi yükseköğretim kurumları açısından da önemli bir mesele olarak değerlendirilmektedir. Nitekim lisansüstü öğrencilerin akademik çalışmaları kapsamında yoğun biçimde veri tabanlarını, veri toplama araçlarını ve bulut tabanlı depolama hizmetlerini kullandıkları dikkate alındığında, bu öğrencilerin de çeşitli güvenlik açıklarına, yani bilgi güvenliği açıklarına maruz kalabildikleri ön görülmektedir. Bilginin, gönderen ile alıcı arasında gizliliği korunarak ve bütünlüğü bozulmadan güvenli bir şekilde iletilmesi süreci bilgi güvenliği olarak tanımlanmaktadır (Vural ve Sağıroğlu, 2008). Dijital çağa geçişle birlikte internet ve akıllı telefon kullanımının küresel ölçekte hızla arttığı bilinmektedir. Uluslararası Telekomünikasyon Birliği (ITU) tarafından yayımlanan raporlarda, dünya genelinde dijital teknolojilerden ve internetten yararlanan birey sayısında kayda değer bir artış yaşandığı ortaya konulmuştur. ITU'nun 2025 yılına ilişkin öngörülerine göre yaklaşık 6 milyar kişinin, yani dünya nüfusunun %74'ünün internet kullanacağı tahmin edilmektedir. Bu oran, 2020 yılında %60 olarak kaydedilen kullanım düzeyine kıyasla önemli bir artışı temsil etmektedir. Aynı dönemde 1,3 milyar insanın internet bağımlılığı riskiyle karşı karşıya kalacağı öngörülürken, yaklaşık 2,2 milyar kişinin hâlen çevrimdışı olduğu belirtilmektedir (ITU, 2025).

Türkiye İstatistik Kurumu verilerine göre ise Türkiye'de internet kullanan bireylerin oranı 2025 yılı itibarıyla %90,9'a ulaşmıştır. TÜİK tarafından açıklanan bulgulara göre 16-74 yaş grubundaki bireylerde internet kullanım oranı 2024 yılında %88,8 iken, 2025 yılında bu oran %90,9 olarak kaydedilmiştir. Cinsiyet temelinde incelendiğinde, 2025 yılında internet kullanım oranının erkeklerde %93,6, kadınlarda ise %88,2 olduğu görülmektedir (TÜİK, 2025). Küresel ölçekte günlük ortalama internet kullanım süresinin 6 saat 38 dakika olduğu, Türkiye'de ise bu sürenin 6 saat 55 dakika ile dünya ortalamasının üzerinde seyrettiği ifade edilmektedir. İnternetin bilgi arama, aile ve arkadaşlarla iletişim kurma, haber takibi ile dizi, film ve video izleme amaçlarıyla yoğun biçimde kullanıldığı belirtilmektedir. Bu veriler doğrultusunda sosyal medya kullanıcı sayısının da artış gösterdiği gözlemlenmektedir. Dünya genelinde sosyal medya kullanıcı sayısının 5,24 milyara ulaştığı ve bu sayının dünya nüfusunun %63,9'una karşılık geldiği ifade edilmektedir. Kullanıcıların sosyal medyada günlük ortalama 2 saat 20 dakika zaman geçirdiği, Türkiye'de ise bu sürenin 2 saat 42 dakikaya ulaştığı belirtilmektedir. Instagram, TikTok, Facebook ve YouTube en yaygın kullanılan platformlar arasında yer alırken, eğlence, haber ve kısa video içerikleri en fazla tüketilen formatlar olarak öne çıkmaktadır. Ayrıca dünya nüfusunun yaklaşık %70,5'inin akıllı telefon kullandığı ve mobil cihazların internet erişiminde temel araç hâline geldiği ifade edilmektedir (Extranet, 2025).

Bilgi ve iletişim teknolojilerindeki hızlı gelişim, siber saldırılar, kişisel verilerin izinsiz kullanımı, veri hırsızlığı ve siber zorbalık gibi çeşitli güvenlik tehditlerinin ortaya çıkmasına neden olmaktadır (Seferoğlu vd., 2018). Bu bağlamda bireyler çevrimiçi ortamlarda virüsler, kimlik avı ve oltalama saldırıları gibi tehditlerle karşı karşıya kalabilmekte; kullanıcı hesapları ve kredi kartı bilgilerinin kötü niyetli kişilerin eline geçebildiği ve bu durumun çok çeşitli maddi zararlara neden olabilmektedir. Bununla birlikte internetin bilinçsiz kullanımı, bireylerin maddi zararların yanında manevi açıdan da ciddi zararlar yaşamasına yol açabilmektedir (Talan ve Aktürk, 2021).

Tüm bu bulgular birlikte değerlendirildiğinde, dijital çağa geçişle birlikte dijital teknolojilerin ve internet kullanımının gündelik yaşamda merkezi bir konuma yerleştiği anlaşılmakta, yaşamı

kolaylaştıran teknolojik gelişmelerin aynı zamanda önemli güvenlik sorunlarını da beraberinde getirdiği görülmektedir. Zaman ilerledikçe bireylerin teknolojiyle iç içe yaşadığı ve siber ortamda geçirdikleri sürenin giderek arttığını gösteren istatistiksel veriler aynı zamanda siber tehdit unsurlarına da maruz kalabilme potansiyelinin arttığına işaret etmektedir. Bu bağlamda gerçekleştirilen araştırmanın amacı, Yönetim Bilişim Sistemleri alanında lisansüstü öğrenim gören öğrencilerin bilişim güvenliği farkındalık düzeylerini incelemek ve bilgi güvenliği kapsamında sahip oldukları algı, tutum ve deneyimleri derinlemesine ortaya koymaktır. Bilişim okuryazarlığı düzeyi yüksek ve dijital sistemlerin etkin kullanımına yönelik eğitim alan bu öğrenci grubunun bilgi güvenliğine ilişkin yaklaşımlarının değerlendirilmesi, hem bireysel dijital güvenlik uygulamalarının anlaşılmasına hem de yükseköğretim kurumlarında geliştirilecek bilişim güvenliği politikalarına ve eğitim içeriklerine yönelik çıkarımlar sunulmasına katkı sağlaması açısından önemli görülmektedir.

2. Kavramsal Çerçeve

2.1. Bilgi Güvenliği Kavramı

Küresel ölçekte internetin yaygınlaşması, sosyal medyanın günlük yaşamın ayrılmaz bir parçası hâline gelmesi ve bilgiye her an erişilebilir olması, güvenlik risklerinin türünü ve kapsamını önemli ölçüde değiştirmiştir. Önceki dönemlerde ev, işyeri ve fiziksel varlıkların korunması ön plandayken, günümüzde kişisel haklar, fikri mülkiyet ve diğer kişisel verilerin yetkisiz kişilerin eline geçmesinin önlenmesi temel bir güvenlik konusu hâline gelmiştir. Bu dönüşümle birlikte bireyler, zararlı yazılımların sisteme bulaşması, sosyal medya hesaplarına izinsiz erişim sağlanması ve finansal bilgilere ulaşılması gibi risklere yönelik kaygılarla karşı karşıya kalmaktadır (Çetin, 2014; Mart, 2012). Dolayısıyla teknolojinin gündelik yaşamda sınırlı yer tuttuğu dönemlerde dijital güvenlik açıkları daha sınırlı düzeydeyken, günümüzde kullanıcıların sürekli çevrimiçi ortamlarda bulunması güvenlik tehditlerine maruz kalma olasılığını artırmaktadır.

Bilginin yalnızca güvenli biçimde saklanması ve depolanması, bilgi güvenliğinin sağlanması açısından tek başına yeterli görülmemektedir. Gereksinimler doğrultusunda bilginin farklı ortamlar arasında aktarılması kaçınılmaz hâle geldiğinden, bu süreçte de gerekli güvenlik önlemlerinin alınması önem taşımaktadır (Aslandağ, 2010). Bilgi güvenliğinin temel amacı, doğru kişinin doğru bilgiye zamanında ve doğruluğundan emin olacak şekilde erişebilmesinin güvence altına alınmasıdır. Daha kapsamlı bir ifadeyle bilgi güvenliği; bilginin kesintisiz erişilebilir olduğu bir ortamda, göndericiden alıcıya kadar gizliliği korunarak, bütünlüğü bozulmadan ve yetkisiz erişim engellenerek güvenli biçimde iletilmesini ifade etmektedir (Mart, 2012; Vural, 2007). Bu doğrultuda bireylerin bilgi güvenliği farkındalık düzeylerinin yüksek olması, güçlü kimlik doğrulama yöntemlerinin kullanılması ve eğitim kurumları ile örgütlerde güvenlik politikalarının güncel tutulması, bilgi güvenliğinin sağlanmasında belirleyici bir rol oynamaktadır.

Bilgi güvenliği, gizlilik, bütünlük ve erişilebilirlik/kullanılabilirlik olmak üzere üç temel unsurdan oluşmaktadır. Bu unsurlar, bilginin korunmasına yönelik bütüncül bir güvenlik yaklaşımının temelini oluşturmaktadır. Söz konusu unsurları genel olarak aşağıdaki şekilde tanımlamak mümkündür.

Gizlilik: Gizlilik unsuru, bilginin yalnızca yetkili kişiler tarafından erişilebilir olmasını ve yetkisiz erişimin engellenmesini ifade etmektedir. Bu ilkenin temel amacı, bilgiye erişim yetkisi bulunmayan kişiler tarafından bilginin görüntülenmesi, kopyalanması veya paylaşılmasının önüne geçilmesidir. Erişim kontrol mekanizmalarının büyük bir bölümü gizliliğin sağlanmasına yöneliktir. Kilitleme ve şifreleme gibi teknik kontroller, bilginin hangi formatta bulunduğundan bağımsız olarak gizlilik ilkesinin korunmasına yönelik uygulamalar arasında yer almaktadır (Aslandağ, 2010).

Bütünlük: Bu unsur bilginin yetkisiz kişiler tarafından değiştirilmemesi, silinmemesi veya tahrip edilmemesi anlamına gelmektedir. Bu kapsamda bilginin doğruluğunun ve güvenilirliğinin korunması

amaçlanmaktadır (Önel ve Dinçkan, 2007). Kurumsal yapılarda bilginin bütünlüğünün sağlanabilmesi için sorumlulukların açık biçimde tanımlanması, gerekli teknik ve yönetsel önlemlerin alınması ve düzenli denetimlerin gerçekleştirilmesi gerektiği vurgulanmaktadır (Ganbat, 2013).

Erişilebilirlik/Kullanılabilirlik: Bu unsur, bilginin yetkili kişi ve kurumlar tarafından ihtiyaç duyulduğu anda erişilebilir olmasını ifade etmektedir. Bu erişimin, kullanıcıların yetki düzeyleri çerçevesinde ve belirlenen zaman dilimleri içinde sağlanması gerekmektedir. Bilginin sürekliliğinin korunabilmesi amacıyla, yetkili kullanıcıların verilerin öneminin farkında olması ve sistemlerin bu gereksinimler doğrultusunda düzenli olarak yedeklenmesi büyük önem taşımaktadır (Önel ve Dinçkan, 2007).

2.2. Bilişim Sistemleri Güvenliğinin Bilgi Güvenliği İçerisindeki Yeri

Teknolojide yaşanan hızlı gelişmelerle birlikte gerçek yaşam ile dijital yaşam giderek iç içe geçmiş, bu durum bilgisayar ağlarını ve teknolojik cihazları çeşitli saldırıların hedefi hâline getirmiştir. Kritik bilgilerin büyük bir bölümünün kullanılan dijital uygulamalar aracılığıyla sanal ortamda tutulması, bilgi güvenliğini bireysel ve kurumsal düzeyde temel bir gereklilik hâline getirmiştir. Bu bağlamda, bilginin güvenliğinin sağlanması, günlük yaşamın ve kurumsal faaliyetlerin sürdürülebilirliği açısından önemli bir unsur olarak değerlendirilmekte, bu nedenle de bilgi güvenliğini tehdit eden unsurların tümünün bertaraf edilmesi hayati önem arz etmektedir (Güldüren vd., 2016; Karaarslan, 2013; Mart, 2012).

Tehdit, bir sistemin zarar görmesine yol açan istenmeyen olayların arkasındaki nedenler olarak tanımlanmaktadır (Can ve Akbaş, 2014). Bilgi güvenliği bağlamında tehditler, bilgi sistemlerindeki güvenlik açıklarından yararlanarak yetkisiz biçimde verilere erişmeyi amaçlamaktadır. Her tehdidin belirli bir kaynağı bulunmakta ve bu kaynak, sistemde mevcut olan bir zafiyetten faydalanmaktadır. Tehditlerin bilgi unsurları üzerindeki etkisi; tehlikenin gerçekleşme olasılığı, güvenlik açığının niteliği ve korunması gereken varlığın değeriyle doğrudan ilişkilidir. Uygun koşullar oluştuğunda bu tehditler, bilgi sistemlerine zarar verebilmekte ve saldırganlar tarafından kullanıldığında ciddi güvenlik sorunlarına yol açabilmektedir (Tekerek, 2008; Vural, 2007). Bilgi güvenliğine yönelik tehditler yalnızca bilişim sistemleriyle sınırlı olmayıp, sanal ortamda karşılaşılan pek çok riskin gündelik yaşam pratiklerinde de karşılık bulduğu görülmektedir. Bilgi güvenliği kapsamındaki risk alanlarının önemli bir bölümü, gerçek yaşamın içerisinde yer almakta, bu nedenle yaşanan güvenlik sorunlarını yalnızca internet kullanımına indirgemek yeterli bir yaklaşım olarak değerlendirilmemektedir. Bu tür tehditlerle mücadelede eleştirel tutumlar yerine, bireylerin ve toplulukların bilgilendirilmesi ve farkındalık düzeylerinin artırılması daha etkili bir yöntem olarak öne çıkmaktadır (Mart, 2012).

Literatürde bilgi güvenliğine ilişkin tehditlerin genel olarak insan kaynaklı, fiziksel ve yazılım kaynaklı tehditler olmak üzere üç ana başlık altında sınıflandırıldığı görülmektedir (Tekerek, 2008; Vural, 2007). Bu tehditler ile ilgili açıklamaları aşağıdaki gibi yapmak mümkün olmaktadır.

İnsan Kaynaklı Tehditler: Bilgi güvenliği kapsamında geliştirilen yazılım ve donanım temelli çözümlere rağmen, güvenlik ihlallerinin önemli bir bölümünün insan faktöründen kaynaklandığı görülmektedir. Güvenlik duvarları, kimlik doğrulama sistemleri ve veri gizleme teknikleri gibi teknolojik önlemler, insan hataları ya da kasıtlı eylemler karşısında yetersiz kalabilmektedir. Özellikle bireylerin zayıf yönlerinden yararlanmayı hedefleyen kasıtlı girişimler, insan unsurunu bilgi güvenliğinin en kırılgan bileşeni hâline getirmektedir (Güldüren vd., 2016; Vural, 2007). Bu bağlamda bilgi güvenliğinin yalnızca teknik bir mesele olarak ele alınması yeterli görülmemekte, bireylerin bilinç düzeyi ve farkındalıklarının artırılması temel bir gereklilik olarak değerlendirilmektedir. Güvenlik farkındalığına yönelik eğitimler, bireylerin hem kişisel hem de kurumsal düzeyde bilgi güvenliğine katkı sunmalarını mümkün kılmaktadır (Çetin, 2014; Aslandağ, 2010). Literatürde, bilgi güvenliği politikalarına uyumun özellikle yöneticiler ve bilişim uzmanları açısından kritik olduğu, buna karşın ihlallerin önemli bir kısmının yine bu gruplar tarafından gerçekleştirilebildiği vurgulanmaktadır (Tipton

ve Krause, 2007; Eminağaoğlu ve Gökşen, 2009). Nitekim insan kaynaklı tehditler genel olarak "farkında olmadan yapılan kullanıcı hatalarından kaynaklanan tehditler" ve "kasıtlı eylemler sonucu ortaya çıkan tehditler" olmak üzere iki grupta ele alınmaktadır (Tekerek, 2008; Vural, 2007).

Fiziksel Tehditler: Bilgi güvenliği kapsamında değerlendirilen fiziksel tehditler, çoğunlukla doğa kaynaklı olaylar ve teknik altyapıdan kaynaklanan sorunlar nedeniyle ortaya çıkmakta ve bu tehditlerin tamamen ortadan kaldırılması çoğu durumda mümkün olamamaktadır. Deprem, sel ve yangın gibi doğal afetler ile elektrik kesintileri ve donanım arızaları, bilgi sistemlerinin zarar görmesine ve hizmet sürekliliğinin kesintiye uğramasına yol açabilmektedir (Tekerek, 2008; Vural, 2007). Bu tür tehditlerin etkilerini en aza indirebilmek amacıyla, güvenlik önlemlerinin önceden planlanması ve olası acil durum senaryolarının oluşturulması gerekmektedir. Fiziksel güvenlik risklerine karşı alınacak önlemler, sistemlerin sürekliliğini sağlamaya yönelik yedekleme, felaket kurtarma ve iş sürekliliği planlarını içermelidir. Bu bağlamda fiziksel tehditlere karşı geliştirilen önleyici ve iyileştirici yaklaşımlar, bilgi güvenliğinin sürdürülebilirliği açısından kritik bir rol oynamaktadır.

Yazılım Tehditleri: Yazılım kaynaklı tehditler, yetkisiz sistem erişimi sağlanması, hizmetlerin aksatılması ve bilgilerin bütünlüğünün bozulması amacıyla gerçekleştirilen saldırıları kapsamaktadır. Saldırganlar, donanım ve yazılım bileşenlerinde bulunan güvenlik açıklarından yararlanarak bilgi sistemlerine sızmakta ve bu açıkları kendi çıkarları doğrultusunda kullanmaktadır (Ünver vd., 2009; Vural, 2007). Günümüzde bilgi sistemlerine yönelik saldırıların büyük bir bölümünün zararlı yazılımlar aracılığıyla gerçekleştirildiği ifade edilmektedir. Zararlı yazılımlar, kullanıcı farkındalığının düşük olduğu durumlarda sistemlere kolaylıkla bulaşabilmekte ve çoğu zaman tespit edilmeden uzun süre etkinliğini sürdürebilmektedir. Virüsler, truva atları, solucanlar, mantık bombaları, reklam destekli yazılımlar ve casus yazılımlar, yazılım kaynaklı tehditlerin yaygın örnekleri arasında yer almaktadır. Bu yazılımlar, sistem kaynaklarını istismar edebilmekte, kişisel ve kurumsal verilerin izinsiz biçimde ele geçirilmesine yol açabilmekte ve bilgi sistemlerinin işleyişini olumsuz yönde etkileyebilmektedir (Can ve Akbaş, 2014; Tipton ve Krause, 2007). Bu noktada yazılım kaynaklı tehditlerle mücadelede, güncel güvenlik yazılımlarının kullanılması, sistemlerin düzenli olarak güncellenmesi ve kullanıcıların zararlı yazılımlara karşı bilinçlendirilmesi büyük önem taşımaktadır. Yazılım güvenliğinin sağlanması, teknik önlemler ile kullanıcı farkındalığının birlikte ele alındığı bütüncül bir yaklaşımı gerektirmektedir.

2.3. Bilgi Güvenliği Farkındalığı Kavramı

Bilgi güvenliği farkındalığı, bireylerin bilgi kaynaklarını korumaya yönelik sahip oldukları bilgi, tutum ve davranış düzeylerini ifade etmektedir. Dijital ortamları yoğun biçimde kullanan bireyler açısından bu farkındalık, kişisel ve kurumsal bilgilerin korunmasında temel bir gereklilik olarak değerlendirilmektedir. Veri güvenliği farkındalığı, veri güvenliğini tehdit eden unsurlara karşı alınacak önlemlerin benimsenmesi, bu önlemlere ilişkin kişisel ve kurumsal politikaların geliştirilmesi ve güvenli davranışların süreklilik kazanması süreci olarak ele alınmaktadır (Siponen, 2000). Bilgi sistemi güvenliğinin çok boyutlu ve karmaşık bir yapıya sahip olması, bu sürecin etkili bir planlama ile yürütülmesini gerekli kılmaktadır. Literatürde, bilgi güvenliğinde en belirleyici unsurun insan faktörü olduğu vurgulanmakta, tüm risklerin tamamen ortadan kaldırılmasının mümkün olmadığı, ancak bilinçli ve iyi eğitilmiş bireyler aracılığıyla güvenlik açıklarının kabul edilebilir düzeye indirilebileceği ifade edilmektedir (Güldüren vd., 2016; Vural, 2007).

Bilgi güvenliği farkındalığı, yükseköğretim kurumları açısından da kritik bir öneme sahiptir. Yapılan araştırmalar, üniversitelerde kurumsal ve bireysel bilgi güvenliği düzeylerinin istenen seviyede olmadığını ortaya koymaktadır (Cox vd., 2001). Öğrencilerin akademik çalışmalar kapsamında sürekli çevrimiçi ortamda bulunmaları, kimlik, fotoğraf ve eğitim bilgileri gibi kişisel verileri sıkça paylaşmaları ve farklı cihazlar üzerinden erişim sağlamaları, onları siber tehditlere daha açık hâle

getirmektedir. Bu durum, yükseköğretim kurumlarında bilgi güvenliği farkındalığını artırmaya yönelik sistematik eğitim ve rehberlik faaliyetlerinin gerekliliğini ortaya koymaktadır.

Bilgi güvenliği farkındalığının erken yaşlarda kazanılması ise dijital risklerin yönetimi açısından ayrı bir önem taşımaktadır. Günümüz gençlerinin çevrimiçi ortamlarda fotoğraf, video ve kişisel içerikleri kontrolsüz biçimde paylaşmaları, bu bilgilerin kötüye kullanılmasına ve zamanla bir tehdit unsuruna dönüşmesine neden olabilmektedir (Güldüren vd., 2016). Küçük yaşlarda edinilen bilgi ve davranışların daha kalıcı olduğu, mahremiyet, konum paylaşımı ve dijital izler konusunda erken dönemde verilen eğitimin güvenli dijital alışkanlıkların oluşmasına katkı sağladığı belirtilmektedir. Günümüzde veri güvenliğinin iş yaşamında temel bir gereklilik hâline gelmesi, genç yaşta kazanılan bilgi güvenliği farkındalığının hem mesleki gelişimi hem de akademik çalışmalarda etik ilkelere uyumu desteklediğini göstermektedir. Bu farkındalığın artmasıyla birlikte veri kayıplarının azalabileceği, bireylerin yalnızca kendilerini değil, ailelerini ve sosyal çevrelerini de olumlu yönde etkileyebileceği değerlendirilmektedir.

2.4. Bilgi Güvenliği Farkındalığına İlişkin Önceki Araştırma Bulguları

Bilgi toplumunun gelişimiyle birlikte siber saldırılar, bilişim suçları, kişisel verilerin izinsiz kullanımı, veri hırsızlığı ve siber zorbalık gibi risklerin belirgin biçimde arttığı görülmektedir (Seferoğlu vd., 2018). Dijital teknolojilerin yaygın kullanımına karşın, kullanıcıların bu teknolojileri güvenli biçimde kullanmaya yönelik yeterli bilgi ve farkındalığa sahip olmamaları, bilgi güvenliği tehditlerinin daha da derinleşmesine neden olmaktadır (Gültekin ve Özel, 2023). Bu noktada bilgi güvenliği, bilginin gizlilik, bütünlük ve erişilebilirlik ilkeleri çerçevesinde yetkisiz erişim, değişiklik ve zarar görmeye karşı korunması süreci olarak ele alınmaktadır (Pfleeger, 1997; Puhakainen, 2006; Vural ve Sağıroğlu, 2008). Söz konusu unsurlardan herhangi birinin zedelenmesi, doğrudan güvenlik ihlallerine yol açmaktadır (Güldüren vd., 2016).

Literatürde bilgi güvenliği farkındalığı, bireylerin bilgi güvenliğine yönelik riskleri tanıma ve bu risklere karşı uygun önlemleri alma bilgi ve becerisine sahip olması şeklinde tanımlanmaktadır (Siponen, 2000; Şahinaslan vd., 2009). Yapılan çalışmalar, bilgi güvenliğinde insan faktörünün belirleyici olduğunu ve teknik önlemlerin tek başına yeterli olmadığını ortaya koymaktadır (Stanton vd., 2005; Hwang vd., 2019). Ampirik bulgular, bilgi güvenliği farkındalığının eğitim düzeyi, yaş, meslek ve dijital okuryazarlık gibi değişkenlere bağlı olarak farklılaştığını göstermektedir. Zira öğretmen adayları ve üniversite öğrencileri üzerinde yapılan araştırmalar, bu grupların önemli bir bölümünün bilgi güvenliği konusunda yeterli eğitim almadığını ve farkındalık düzeylerinin istenen seviyede olmadığını ortaya koymaktadır (Gökmen ve Akgün, 2015; Demir ve Sarı, 2023). Buna karşılık bazı çalışmalarda üniversite öğrencilerinin genel farkındalık düzeylerinin alt eğitim düzeylerinden görece yüksek olduğu, ancak farkındalığı düşük alt grupların da bulunduğu belirlenmiştir (Avcı ve Oruç, 2020).

Ortaöğretim ve daha alt yaş gruplarına yönelik araştırmalar, bilgi güvenliği farkındalığının erken yaşlarda kazandırılmasının kritik önemde olduğunu vurgulamaktadır. Bu çalışmalarda mevcut ders içeriklerinin yetersiz kaldığı ve bilgi güvenliğine yönelik eğitimlerin daha erken eğitim kademelerine yayılması gerektiği belirtilmektedir (Tekerek ve Tekerek, 2013; Derin ve Gençoğlu, 2020). Kurumsal düzeyde yapılan araştırmalar ise çalışanların genel farkındalık düzeylerinin orta seviyede olduğunu, ancak sosyal medya kullanımı ve kablosuz ağlar gibi alanlarda ciddi zafiyetler bulunduğunu ortaya koymaktadır (Parsons vd., 2014; Gün ve Çelik, 2022).

Genel bir değerlendirme yapıldığında, literatürde yer alan araştırma bulgularının bilgi güvenliği farkındalığının artırılmasında eğitim temelli, sürekli ve insan odaklı yaklaşımların temel belirleyici olduğunu ortaya koydukları görülmektedir. Bununla birlikte bilişim alanında eğitim alan ve gelecekte karar verici roller üstlenmesi beklenen gruplara yönelik çalışmaların sınırlı olduğu anlaşılmakta, bu durum, alan odaklı ve derinlemesine araştırmalara duyulan ihtiyacı açık biçimde ortaya koymaktadır.

3. Yöntem

3.1. Araştırma Modeli

Bu araştırmada, lisansüstü öğrencilerin bilişim güvenliği farkındalıklarına ve bu kapsamdaki algılarına ilişkin kavrayışların derinlemesine ortaya konulabilmesi amacıyla nitel araştırma yaklaşımı benimsenmiş ve fenomenoloji çalışması deseni kullanılmıştır. Nitel araştırmalar, bireylerin deneyimlerini kendi doğal bağlamları içerisinde ele alarak belirli bir olguyu nasıl algıladıklarını, yorumladıklarını ve anlamlandırdıklarını ortaya koymada etkili bir yaklaşım sunmaktadır (Patton, 2015). Bilişim güvenliği, kişisel tercihler, risk algısı, tehditleri tanıma ve önleyici davranışlar gibi çok boyutlu yapılar içerdiğinden, bu olgunun nitel araştırma yaklaşımıyla esnek ve ayrıntılı biçimde incelenmesi uygun görülmüştür. Fenomenoloji deseni bir başka tanımlamaya göre; birkaç kişinin bir fenomen veya belli bir kavramla ilgili yaşanmış deneyimlerinin ortak anlamını ortaya çıkaran bir desendir. Bu desen, incelenen olgunun doğal ortamında ve bütüncül bir bakış açısıyla analiz edilmesini sağlamaktadır (Stake, 1995). Bu çerçevede fenomenoloji çalışması deseni, lisansüstü öğrencilerin bilişim güvenliğine ilişkin tercih ve davranışlarının bireysel bilgi birikimi ve sosyal etkileşimlerle nasıl şekillendiğini ortaya koymak açısından uygun bir yöntem olarak değerlendirilmiştir.

3.2. Çalışma Grubu

Araştırmanın çalışma grubunu, Kafkas Üniversitesi, Yönetim Bilişim Sistemleri Anabilim Dalı'nda tezli yüksek lisans programında kayıtlı bulunan 15 öğrenci oluşturmaktadır. Yüksek lisans düzeyinde bilişim dersleri almış olmaları ve temel teknik bilgilere sahip bulunmalarından ötürü bu öğrenciler, bilişim güvenliği ve farkındalık alanlarında temel altyapıya sahiptirler. Katılımcılar gönüllülük esasına göre kararlaştırılmış ve etik ilkeler çerçevesinde veri toplama süreci yürütülmüştür.

3.3. Veri Toplama Aracı

Bu çalışmada veri toplama aracı olarak araştırmacılar tarafından geliştirilen "Lisansüstü Öğrencilerinin Bilişim Güvenliği Farkındalığı Görüşme Formu" kullanılmıştır. Görüşme formunun oluşturulma aşamasında, soruların içerik uygunluk düzeyi ve anlam bütünlüğünü sağlamak amacıyla dört alan uzmanından görüş alınmıştır. Uzmanlardan alınan geri bildirimler doğrultusunda formun dili yalın hale getirilmiş, soruların netlik düzeyi artırılmış ve kapsam bakımından gerekli düzeltmelerle form son hâline getirilmiştir. Görüşme formunda, nitel veri toplamaya elverişli açık uçlu 9 soru bulunmaktadır. Aşağıda yer alan Tablo 1'de araştırmada kullanılan ölçek ifadeleri sunulmuştur.

Tablo 1. Araştırmada kullanılan veri toplama aracı

Bilişim Güvenliği Farkındalığı Görüşme Formu Soruları
1.Günlük hayatınızda bilgi güvenliği size neyi çağrıştırıyor? Bir metafor olarak tanımlayabilir misiniz?
2.Bir lisansüstü öğrencisi olarak bilgi güvenliği farkındalığınızın zaman içinde değiştiğini gözlemlediniz mi? Cevabınız evet ise, bu değişimin sebepleri neler olabilir?
3.Bilgi güvenliği ihlali durumuna tanık olduğunuzda ya da şüphelendiğiniz herhangi ilgili bir durumda nasıl bir yol izlersiniz? Bu konuda bilgi güvenliği ile ilgili aldığınız eğitimlerin yeterli olduğunu düşünüyor musunuz?
4.Kişisel verilerinizi korumak için aldığınız önlemler nelerdir? Bu önlemlerin yeterli olduğunu düşünüyor musunuz?
5.Bir lisansüstü öğrencisi olarak karşılaştığınız en yaygın bilgi güvenliği tehditleri nelerdir? Aldığınız önlemlerin yeterli olduğunu düşünüyor musunuz ya da daha etkin önlemler almak için neler yapabilirsiniz?
6.Daha önce siber güvenliğinizi tehdit edecek bir olay yaşadınız mı? Cevabınız evet ise, bu durumla başa çıkmak için hangi yöntem ve/veya yöntemleri uyguladınız ya da uygularsınız?

7.Kişisel veya akademik verilerinizi korumak için şifreleme yöntemlerinden yararlanıyor musunuz? Eğer kullanıyorsanız, hangi yöntemleri tercih ediyorsunuz?

8.Parola güvenliği, kötü amaçlı yazılımlar, sosyal mühendislik, veri gizliliği ve güvenli internet kullanımı gibi konularda farkındalığınız ve deneyimleriniz nelerdir? Eksik gördüğünüz veya geliştirmek istediğiniz noktalar nelerdir?

9.Bir lisansüstü öğrenci olarak, bilgi güvenliği farkındalığınızı ve bilincinizi artırmak için üniversite ve/veya akademisyenlerden hangi destekleri veya uygulamaları bekliyorsunuz? Mevcut uygulamaların bu konuda yeterli olduğunu düşünüyor musunuz? Neden?

Bilgi güvenliği konusunda kaynakları ve eğitim gereksinimlerini kavramak amacıyla oluşturulmuş olan bu sorular, lisansüstü öğrencilerinin bilişim güvenliği konusundaki farkındalıklarına, tehlike algısına, risk bilinçlerine, önceki gözlemlerine göre yapılandırılmıştır. Kişisel davranış biçimi, tecrübe ve tutumlara da yoğunlaşmayı sağlamış olan bu çerçeve, bilgi güvenliğini işlevsel yönleriyle birlikte ele almıştır. Katılım tamamen gönüllülük esasına dayandırılmış olan veri toplama aşamasında, araştırmanın amacı öğrencilere açıklanmış ve etik kurallar dâhilinde bilgilendirilmiş ve onamları alınmıştır. Katılımcıların kendi görüşlerini özgür iradeyle dile getirilmesine fırsat vermiş olan veri toplama aracı, araştırmanın kavramsal çerçevesine uygun veriler elde edilmesine katkı sağlamıştır. Görüşme formu ile kazanılan veriler, araştırmanın nitel özüne elverişli olacak şekilde içerik analizi yöntemiyle değerlendirilmiştir.

3.4. Verilerin Analizi

Bu araştırmada, lisansüstü öğrencilerinin bilgi güvenliği farkındalığını tüm katmanlarını araştırmak amacıyla içerik analizi yöntemi tercih edilmiştir. Tematik içerik analizi, odaklanılan alanlardaki nitel dataların organize bir şekilde kategorize edilmesi ve anlamlı motifler ortaya çıkartılması aşamalarını içerir; böylece komplike bilgilerin belirgin biçime gelmesine olanak sağlar (Braun ve Clarke, 2019; Nowell vd., 2017). Araştırmada elde edilen görüşme verileri ilk olarak yazılı belge şeklinde düzenlenmiş olup sonrasında anlamlı ifadeler haline getirilmiştir. Benzer ifadeler arasında birliktelik sağlanarak, öğrencilerin bilgi güvenliği alanındaki kavrayışı, farkındalığının ilerleyişi, ihlaller karşısında davranışları, kişisel veri koruma yöntemleri, çok rastlanan tehditler ve riskler karşısında alınan tedbirler, şifreleme yöntemleri ve kaynak kullanımı gibi ana fikirler hazırlanmıştır. Oluşturulan temalar, öğrencilerin bilgi güvenliği alanındaki farkındalık seviyesini sergiledikleri tutum ve davranışları incelemek hedefiyle yorumlanmış, sonuçlar katılımcıların benzersiz ifadeleriyle güçlendirilmiştir (Creswell ve Poth, 2018). Böylelikle, lisansüstü öğrencilerinin bilgi güvenliği farkındalığına ilişkin algı, tutum ve uygulamalar konusunda detaylı ve bütüncül bilgilere ulaşılmıştır.

4. Bulgular

4.1. Katılımcılara Ait Tanımlayıcı Özellikler

Bu bölümde araştırmaya katılan lisansüstü öğrencilerin tanımlayıcı özelliklerine ilişkin bilgilere yer verilmiştir. Katılımcıların cinsiyet, yaş, günlük internet kullanım süreleri ve bilişim güvenliği dersi alma durumu değişkenlerine göre dağılımları tablo halinde sunularak, araştırma grubunun genel demografik yapısının anlaşılması amaçlanmıştır. Aşağıda yer alan Tablo 2'de katılımcıların tanımlayıcı özelliklerini gösterilmektedir.

Tablo 2. Katılımcıların Demografik Özellikleri

Kod	Cinsiyet	Yaş	Günlük internet kullanım süresi	Daha önce bilişim güvenliği dersi aldınız mı?
K1	Kadın	26-30 Yaş	6-10 Saat	Evet Aldım
K2	Kadın	21-25 Yaş	3-5 Saat	Evet Aldım
K3	Kadın	26-30 Yaş	1-3 Saat	Evet Aldım
K4	Kadın	26-30 Yaş	3-5 Saat	Evet Aldım
K5	Kadın	21-25 Yaş	3-5 Saat	Evet Aldım
K6	Kadın	26-30 Yaş	1-3 Saat	Hayır Almadım
K7	Kadın	26-30 Yaş	6-10 Saat	Evet Aldım
K8	Kadın	21-25 Yaş	1-3 Saat	Evet Aldım
K9	Erkek	35+ Yaş	3-5 Saat	Evet Aldım
K10	Erkek	26-30 Yaş	6-10 Saat	Hayır Almadım
K11	Erkek	21-25 Yaş	6-10 Saat	Evet Aldım
K12	Erkek	21-25 Yaş	6-10 Saat	Evet Aldım
K13	Erkek	26-30 Yaş	10+ Saat	Hayır Almadım
K14	Erkek	31-35 Yaş	6-10 Saat	Evet Aldım
K15	Erkek	31-35 Yaş	6-10 Saat	Hayır Almadım

Tablo 2'de yer alan veriler incelendiğinde, araştırmaya katılan lisansüstü öğrencilerin cinsiyet, yaş, günlük internet kullanım süresi ve bilişim güvenliği eğitimi alma durumları açısından heterojen bir yapıya sahip olduğu görülmektedir. Katılımcıların cinsiyet dağılımı kadın (8) ve erkek (7) öğrencilerden oluşmakta olup, yaş aralıklarının ağırlıklı olarak 21-30 yaş grubunda yoğunlaştığı dikkat çekmektedir. Bununla birlikte 31 yaş ve üzeri katılımcıların da araştırma grubunda yer alması, farklı yaş deneyimlerinin çalışmaya yansımasına olanak sağlamaktadır. Günlük internet kullanım süresi değişkeni açısından değerlendirildiğinde, katılımcıların büyük çoğunluğunun günde 3-10 saat aralığında internet kullandığı görülmektedir. Özellikle 6-10 saatlik kullanım süresinin yaygın olduğu, bunun yanı sıra 10 saat ve üzeri internet kullanan katılımcıların da bulunduğu dikkat çekmektedir. Bu durum, araştırma grubunun dijital ortamlarla yoğun etkileşim içerisinde olduğunu göstermektedir. Bilişim güvenliği dersi alma durumuna ilişkin bulgular incelendiğinde, katılımcıların önemli bir bölümünün daha önce bilişim güvenliği kapsamında bir ders aldığı, ancak belirli sayıda katılımcının bu yönde herhangi bir eğitim almadığı görülmektedir. Bu farklılık, katılımcıların bilişim güvenliğine ilişkin bilgi, farkındalık ve deneyim düzeylerinin değişkenlik gösterebileceğine işaret etmektedir.

4.2. Araştırma Sorularının Çözümlenmesi

4.2.1. Bilgi güvenliğine ilişkin metaforik algılar

Katılımcılara bilgi güvenliğine yönelik algılarını metaforik bağlamda değerlendirebilmek için "*Günlük hayatınızda bilgi güvenliği size neyi çağrıştırıyor? Bir metafor olarak tanımlayabilir misiniz?*" şeklinde bir soru yöneltilmiştir. Verilen yanıtlardan elde edilen bulgular, bilgi güvenliğinin katılımcılar tarafından farklı ancak ortak temalar etrafında anlamlandırıldığını göstermektedir. Buna göre katılımcılar, bilgi güvenliğini çoğunlukla koruma, sınırlandırma, denetim ve önleyici savunma işlevleri üzerinden betimlemişlerdir. Aşağıda yer alan Tablo 3'te bahse konu soru bağlamında elde edilen bulgular sunulmuştur.

Tablo 3. Bilgi güvenliğine ilişkin metaforların tematik dağılımı

Tema	Metaforlar (f)
Koruyucu/Engelleyici (f=6)	Kapı güvenliği (4), Kasa (1), Çatı (1)
Savunmacı/Teknik bariyer (f=6)	Kalkan (3), Güvenlik duvarı (2), Alarm sistemleri (1)
Denetleyici/Yönlendirici (f=3)	Trafik polisi (1), Rehber (1), Kurallar bütünü (1)

Tablo 3 incelendiğinde, bilgi güvenliğinin katılımcılar tarafından ağırlıklı olarak koruma/engelleme, savunma ve denetim-yönlendirme işlevleri üzerinden anlamlandırıldığı görülmektedir. Katılımcı ifadelerinde en sık tekrar eden metaforun "kapı güvenliği" (f=4) olduğu; bunu "kalkan" (f=3) ve "güvenlik duvarı" (f=2) metaforlarının izlediği belirlenmiştir. Bunun yanında "çatı" (f=1), "alarm sistemleri" (f=1) ve "kasa" (f=1) metaforlarıyla bilgi güvenliğinin koruyucu bir düzenek şeklinde kavramsallaştırıldığı; "trafik polisi" (f=1), "rehber" (f=1) ve "kurallar bütünü" (f=1) metaforlarıyla ise bilgi güvenliğinin yalnızca koruma değil, aynı zamanda dijital davranışları düzenleyen ve yöneten bir mekanizma olarak değerlendirildiği anlaşılmaktadır. Bu bulgular, bilgi güvenliği algısının katılımcılar tarafından hem tehditleri engelleyen hem de kullanımı düzenleyen çok boyutlu bir çerçevede ele alındığını göstermektedir.

4.2.2. Bilgi güvenliği farkındalığının zaman içerisindeki değişimine ilişkin bulgular

Katılımcılara zamana bağlı olarak bilgi güvenliği algılarının değişimini belirlemeye yönelik olarak "*Bir lisansüstü öğrencisi olarak bilgi güvenliği farkındalığınızın zaman içinde değiştiğini gözlemlediniz mi? Cevabınız evet ise, bu değişimin sebepleri neler olabilir*?" şeklinde bir soru yöneltilmiştir. Verilen yanıtlardan elde edilen bulgular, katılımcıların tamamının bilgi güvenliği farkındalıklarının zaman içerisinde arttığını göstermektedir. Bu bulgu, bilgi güvenliği farkındalığının durağan bir özellikten ziyade, süreç içerisinde gelişen bir yapı olduğunu göstermektedir. Aşağıda yer alan Tablo 4'te söz konusu soru bağlamında elde edilen bulgular sunulmuştur.

Tablo 4. Bilgi güvenliği farkındalığındaki değişime ilişkin nedenlerin tematik dağılımı

Soru	Yanıt	Tema	İfade Edilen Nedenler
Bir lisansüstü öğrencisi olarak bilgi güvenliği farkındalığınızın zaman içinde değiştiğini gözlemlediniz mi?	Tüm katılımcılar söz konusu soruya **"Evet"** yanıtı vermiştir	**Akademik Süreç Kaynaklı Nedenler (f=3)**	Lisansüstü eğitim sürecinde akademik sorumlulukların ve bilgi düzeyinin artması
		Dijital Kullanım Yoğunluğu (f=6)	Dijital ortamların her geçen gün daha yoğun ve sürekli kullanılması
		Kişisel Veri Sorumluluğu (f=5)	Kişisel ve akademik verilerin korunmasına yönelik hassasiyetin artması
		Deneyim ve Farkındalık Artışı (f=7)	Dijital riskler ve tehditler hakkında bilgi ve deneyim kazanılması

Tablo 4 incelendiğinde, katılımcıların tamamının bilgi güvenliği farkındalıklarının zaman içerisinde arttığını ifade ettikleri görülmektedir. Farkındalık düzeyindeki bu artışın, tek bir nedene bağlı olmadığı, akademik süreçler, dijital ortamlarla etkileşim sıklığı, veri güvenliğine ilişkin sorumluluk bilinci ve bireysel deneyimlerin bir araya gelmesiyle şekillendiği anlaşılmaktadır. Katılımcılar, lisansüstü eğitim sürecinde artan akademik sorumluluk ve bilgi düzeyi ile dijital veri kullanımı nedeniyle bilgi güvenliği konusuna daha fazla dikkat etmeye başladıklarını belirtmiştir. Ayrıca, kişisel ve akademik verilerin korunmasına yönelik hassasiyetin zamanla geliştiği, deneyime bağlı olarak risk unsurlarına yönelik daha fazla deneyim elde etmeleri ve zamana bağlı olarak dijital ortamlarda karşılaşılabilecek risklere ilişkin farkındalıklarının arttığını ifade edilmişlerdir. Bu bulgular, bilgi güvenliği farkındalığının lisansüstü eğitim süreciyle birlikte gelişen, deneyim temelli ve dinamik bir yapı sergilediğini ortaya koymaktadır.

4.2.3. Bilgi güvenliği ihlali durumunda izlenen yollara ve eğitim yeterliğine ilişkin bulgular

Katılımcılara herhangi bir bilgi güvenliği ihlaline tanık olmaları durumunda izleyecekleri yollara ilişkin eğilimlerini ve bu konuda alınan eğitimlerin yeterliliği noktasındaki algılarını belirlemeye yönelik olarak *"Bilgi güvenliği ihlali durumuna tanık olduğunuzda ya da şüphelendiğiniz herhangi ilgili bir durumda nasıl bir yol izlersiniz? Bu konuda bilgi güvenliği ile ilgili aldığınız eğitimlerin yeterli*

olduğunu düşünüyor musunuz?" şeklinde bir soru yöneltilmiştir. Verilen yanıtlardan elde edilen bulgular, katılımcıların bilgi güvenliği ihlallerine karşı bilinçli bir tutum sergilediklerini, ancak eğitimlerin daha uygulamalı ve senaryo temelli biçimde desteklenmesi gerektiğine yönelik bir algının bulunduğunu ortaya koymaktadır. Aşağıda yer alan Tablo 5'te söz konusu soru bağlamında elde edilen bulgular sunulmuştur.

Tablo 5. Bilgi güvenliği ihlali durumunda izlenen yollar ve eğitim yeterliğine ilişkin görüşlerin tematik dağılımı

Tema	İfade Edilen Yaklaşımlar
Önleyici ve Koruyucu Davranışlar (f=6)	Şüpheli bağlantılardan kaçınma, hesap güvenliğini kontrol etme, parolaları güncelleme
Bildirim ve Destek Arayışı (f=5)	Yetkili birimlere veya ilgili kişilere durumu bildirme
Bireysel Müdahale ve Tedbir Alma (f=9)	Hesapları kapatma, erişimleri sınırlandırma, ek güvenlik önlemleri uygulama

Tablo 5'te yer alan bulgular incelendiğinde, katılımcıların bilgi güvenliği ihlali ya da ihlal şüphesiyle karşılaştıklarında öncelikle koruyucu ve önleyici davranışlara yöneldikleri görülmektedir. Katılımcıların, şüpheli durumlarda bireysel hesap güvenliğini kontrol etme, parolaları değiştirme ve dijital ortamlardaki riskli etkileşimlerden kaçınma gibi adımlar izledikleri belirlenmiştir. Bunun yanı sıra, bazı katılımcıların olası bir ihlal durumunda yetkili kişi veya birimlere bildirimde bulunmayı tercih ettikleri, böylece sorunun bireysel müdahalenin ötesinde kurumsal düzeyde ele alınmasını gerekli gördükleri anlaşılmaktadır. İhlal şüphesinin ciddiyetine bağlı olarak bireysel tedbirlerin yanı sıra destek arayışına yönelindiği ifade edilmiştir. Bilgi güvenliği eğitimlerinin yeterliğine ilişkin değerlendirmeler incelendiğinde ise, katılımcıların büyük bölümünün aldıkları eğitimleri temel farkındalık kazandırma açısından yeterli, ancak uygulamaya dönük yönleri bakımından sınırlı buldukları görülmektedir. Bu durum, bilgi güvenliği konusunda teorik bilginin varlığına karşın, gerçek ihlal durumlarında izlenecek adımlara ilişkin deneyim ihtiyacının hissedildiğini göstermektedir.

4.2.4. Kişisel verilerin korunmasına yönelik alınan önlemlere ilişkin bulgular

Katılımcılara kişisel veri güvenliği noktasındaki algılarını belirlemeye yönelik olarak "*Kişisel verilerinizi korumak için aldığınız önlemler nelerdir? Bu önlemlerin yeterli olduğunu düşünüyor musunuz?*" şeklinde bir soru yöneltilmiştir. Verilen yanıtlardan elde edilen bulgular, katılımcıların genel olarak bu noktada bilinçli olduklarını, aldıkları önlemleri genel olarak yeterli bulduklarını ancak kişisel veri güvenliği alma noktasında birbirinden farklı yöntemler izledikleri görülmektedir. Aşağıda yer alan Tablo 6'da söz konusu soru bağlamında elde edilen bulgular sunulmuştur.

Tablo 6. Kişisel verilerin korunmasına yönelik alınan önlemlere ve yeterliliklerine ilişkin bulgular

Tema	İfade Edilen Önlemler ve Görüşler
Bireysel Güvenlik Önlemleri (f=8)	Güçlü parola kullanımı, hesap ayarlarının kontrol edilmesi, gizlilik ayarlarına dikkat edilmesi
Dijital Ortamda Temkinli Davranma (f=7)	Şüpheli bağlantılardan kaçınma, bilinmeyen kaynaklardan gelen içeriklere karşı dikkatli olma
Veri Paylaşımına Yönelik Sınırlandırma (f=4)	Kişisel bilgilerin gereksiz ortamlarda paylaşılmaması
Önlemlerin Yeterliğine İlişkin Algı (f=7)	Alınan önlemlerin genel olarak yeterli görülmesi, ancak gelişen tehditler karşısında eksiklik hissedilmesi

Tablo 6'da yer alan bulgular incelendiğinde, katılımcıların kişisel verilerini korumaya yönelik olarak öncelikle bireysel güvenlik önlemlerine başvurdukları görülmektedir. Katılımcıların, hesap güvenliğine yönelik temel uygulamaları benimsedikleri ve dijital ortamlarda gizlilik ayarlarına dikkat ettikleri belirlenmiştir. Bunun yanı sıra, katılımcıların dijital ortamlarda daha temkinli davrandıkları, özellikle

şüpheli bağlantılar ve güvenilir olmayan içeriklerden kaçınmaya özen gösterdikleri tespit edilmiştir. Ayrıca kişisel verilerin paylaşımı konusunda ise gereksiz bilgi paylaşımından kaçınıldığı ve daha seçici bir yaklaşım benimsendiği görülmektedir.

Katılımcıların verilerini korumaya yönelik aldıkları önlemler arasında güçlü şifre oluşturma, veri yedekleme, çift aşamalı kimlik doğrulama, antivirüs ve lisanslı yazılım kullanımı, şifreli depolama alanları, güvenlik duvarı ayarlarının kontrolü ve parola yöneticilerinin kullanımı gibi temel siber güvenlik uygulamalarının yer aldığı görülmektedir. Ayrıca, ortak ağlarda dikkatli hareket etme, sosyal medya gizlilik ayarlarını düzenleme ve adres çubuğundaki bağlantı doğruluğunu kontrol etme gibi davranışsal önlemler de katılımcılar tarafından belirtilmiştir. Bu bulgular, bireylerin hem teknik hem de kullanıcı alışkanlıklarına dayalı çok boyutlu koruma stratejileri geliştirdiklerini göstermektedir.

4.2.5. Karşılaşılan bilgi güvenliği tehditleri ve alınan önlemlerin yeterliğine ilişkin bulgular

Katılımcılara karşılaştıkları güvenlik tehditlerinin neler olduğunu dahası en yaygın bilgi güvenlik tehdidi olarak algıladıkları unsurun ne olduğunu belirlemeye yönelik olarak "*Bir lisansüstü öğrencisi olarak karşılaştığınız en yaygın bilgi güvenliği tehditleri nelerdir? Aldığınız önlemlerin yeterli olduğunu düşünüyor musunuz ya da daha etkin önlemler almak için neler yapabilirsiniz?*" şeklinde bir soru yöneltilmiştir. Verilen yanıtlardan elde edilen bulgular, katılımcıların karşılaştıkları bilgi güvenliği tehditleri ve bu tehditlere karşı aldıkları önlemlerin yeterliğine ilişkin değerlendirmeleri incelendiğinde, yanıtların belirli temalar etrafında yoğunlaştığı görülmektedir. İlgili temalar aşağıda yer alan Tablo 7'de sunulmuştur.

Tablo 7. Karşılaşılan bilgi güvenliği tehditleri ve önlem yeterliliğine ilişkin görüşlerin tematik dağılımı

Tema	İfade Edilen Tehditler ve Görüşler
Dijital Ortam Kaynaklı Tehditler (f=4)	Şüpheli bağlantılar, zararlı içerikler, kimlik avı girişimleri
Hesap ve Veri Güvenliğine Yönelik Tehditler (f=3)	Hesap ele geçirilme riski, kişisel verilerin izinsiz erişime açık olması
Alınan Önlemlerin Yeterliğine İlişkin Algı (f=4)	Mevcut önlemlerin temel düzeyde yeterli görülmesi
Daha Etkin Önlemlere Yönelik Farkındalık (f=4)	Ek güvenlik önlemlerine ihtiyaç duyulduğunun ifade edilmesi

Tablo 7'de sunulan bulgular incelendiğinde, katılımcıların lisansüstü eğitim sürecinde en sık karşılaştıkları bilgi güvenliği tehditlerinin dijital ortam kaynaklı riskler etrafında yoğunlaştığı görülmektedir. Katılımcılar, özellikle şüpheli bağlantılar, güvenilir olmayan içerikler ve kimlik avı girişimlerini yaygın tehditler arasında değerlendirmiştir. Bunun yanı sıra, kişisel ve akademik hesapların ele geçirilmesine yönelik risklerin de tehdit algısı içerisinde önemli bir yer tuttuğu belirlenmiştir. Aldıkları önlemlerin yeterliliğine ilişkin değerlendirmeler incelendiğinde, katılımcıların büyük bölümünün mevcut güvenlik önlemlerini temel düzeyde yeterli buldukları, ancak bu önlemlerin tüm tehditleri ortadan kaldırmak için her zaman yeterli olmayabileceğinin farkında oldukları görülmektedir. Bu durum, katılımcıların bilgi güvenliği konusunda belirli bir bilinç düzeyine sahip olduklarını göstermektedir. Daha etkin önlemler alınmasına ilişkin görüşler değerlendirildiğinde ise, katılımcıların güvenlik uygulamalarını geliştirme gereksinimi hissettikleri ve bilgi güvenliği konusunda sürekli güncel kalmanın önemine vurgu yaptıkları anlaşılmaktadır. Bu bulgular, bilgi güvenliği farkındalığının statik bir durumdan ziyade, deneyim ve karşılaşılan tehditlerle birlikte gelişen dinamik bir yapı olarak algılandığını ortaya koymaktadır.

4.2.6. Siber güvenliği tehdit eden olaylara ilişkin deneyimler ve başa çıkma yöntemleri

Katılımcılara daha önce siber güvenliklerini tehdit eden bir olay yaşayıp yaşamadıklarını ve bu tür durumlarla başa çıkmak için izledikleri yöntemlerin neler olabileceğine ilişkin görüşlerini belirleyebilmek için "*Daha önce siber güvenliğinizi tehdit edecek bir olay yaşadınız mı? Cevabınız evet ise, bu durumla başa çıkmak için hangi yöntem ve/veya yöntemleri uyguladınız ya da uygularsınız?*" sorusu yöneltilmiştir. Elde edilen yanıtlar bağlamında katılımcıların büyük bir bölümünün bilgi güvenliğiyle ilgili doğrudan bir tehdit deneyimi yaşamadığını tespit edilmiştir. Buna karşın, "Evet" yanıtı veren katılımcılar özellikle kimlik avı (phishing) girişimleriyle karşılaştıklarını ve bu durumlarda çeşitli önlemler aldıklarını ifade etmişlerdir. Bu katılımcılar genellikle şifrelerini değiştirme, şüpheli bağlantıları açmama, hesap güvenlik ayarlarını kontrol etme, iki aşamalı kimlik doğrulama kullanma ve durumu yetkili birimlere bildirme gibi etkili adımlar atmıştır. Bazı katılımcıların ayrıca antivirüs yazılımı kullanmaya başlama veya siber suçlar biriminden destek alma gibi daha kapsamlı yöntemlere yöneldikleri görülmektedir. Katılımcıların söz konusu soruya verdikleri yanıtlar incelendiğinde, yanıtların belirli temalar etrafında toplandığı görülmektedir. Bu temalar aşağıda yer alan Tablo 8'de sunulmuştur.

Tablo 8. Siber güvenliği tehdit eden olaylar ve başa çıkma yöntemlerinin tematik dağılımı

Tema	İfade Edilen Deneyimler ve Yöntemler
Bireysel Müdahale Yöntemleri (f=2)	Parola değiştirme, hesap güvenliğini kontrol etme
Koruyucu ve Önleyici Yaklaşımlar (f=1)	Şüpheli bağlantılardan kaçınma, riskli işlemleri sonlandırma
Destek ve Bildirim Süreçleri (f=1)	İlgili kişi veya birimlerden destek alma, durumu bildirme

Tablo 8'de sunulan bulgular incelendiğinde, katılımcıların büyük çoğunluğunun (n=11) daha önce siber güvenliklerini tehdit eden durumlarla karşılaşmadıklarını belirtmiş olmalarına karşın bir kısmının (n=4) bu durumlarla karşılaştıklarını ifade ettikleri görülmektedir. Bu tür durumların, bireysel dijital hesaplar ve çevrimiçi ortamlar üzerinden gerçekleştiği belirtilmiştir. Söz konusu tehditlerle başa çıkma sürecinde katılımcıların öncelikle bireysel müdahale yöntemlerine başvurdukları belirlenmiştir. Bu kapsamda, hesap güvenliğini artırmaya yönelik önlemler alınması ve mevcut erişim bilgilerinin gözden geçirilmesi öne çıkan uygulamalar arasında yer almaktadır. Bunun yanı sıra, riskli görülen dijital etkileşimlerden kaçınılması ve şüpheli işlemlerin sonlandırılması gibi koruyucu ve önleyici yaklaşımların benimsendiği ifade edilmiştir. Bazı katılımcıların ise yaşanan ya da yaşanması muhtemel siber güvenlik tehditleri karşısında destek ve bildirim süreçlerine yöneldikleri, ilgili kişi veya birimlerle iletişime geçerek süreci daha güvenli biçimde yönetmeyi tercih ettikleri anlaşılmaktadır.

4.2.7. Şifreleme yöntemlerinin kullanımına ilişkin bulgular

Katılımcılara kişisel veya akademik verilerini korumak amacıyla şifreleme yöntemlerinden yararlanma durumları ve tercih ettikleri yöntemleri belirleyebilmek için "*Kişisel veya akademik verilerinizi korumak için şifreleme yöntemlerinden yararlanıyor musunuz? Eğer kullanıyorsanız, hangi yöntemleri tercih ediyorsunuz?*" şeklinde bir soru yöneltilmiştir. Bahse konu soruya verilen yanıtlar incelendiğinde, tamamının şifreleme temelli güvenlik uygulamalarını kullandıklarını ifade ettikleri görülmektedir. Kullanılan yöntemler, işlevsel benzerlikleri dikkate alınarak temalar altında sınıflandırılmış ve söz konusu temalar aşağıda yer alan Tablo 9'da sunulmuştur.

Tablo 9. Kişisel ve akademik verilerin korunmasında kullanılan şifreleme yöntemlerinin tematik dağılımı

Tema	Kullanılan Yöntemler
Dosya ve Veri Şifreleme (f=5)	Simetrik şifreleme yöntemleri, AES tabanlı dosya şifreleme, parola korumalı arşiv oluşturma, disk şifreleme (BitLocker / FileVault), steganografi teknikleriyle veri gizleme
İletişim ve Ağ Güvenliği (f=2)	PGP/GPG ile e-posta şifreleme, VPN üzerinden güvenli bağlantı kullanma
Bulut ve Mobil Ortam Güvenliği (f=3)	Bulut servislerinde uçtan uca şifreleme, mobil cihazlarda uçtan uca yedekleme şifrelemesi
Kimlik Doğrulama ve Erişim Kontrolü (f=4)	Çift faktörlü koruma, rol tabanlı erişim kontrolü uygulama, donanım tabanlı güvenlik anahtarı (YubiKey vb.), zero-knowledge şifre yöneticisi kullanma
Çok Katmanlı Güvenlik Yaklaşımları (f=1)	Çok katmanlı koruma (şifreleme + MFA + cihaz doğrulama)

Tablo 9'da sunulan bulgular incelendiğinde, katılımcıların tamamının kişisel veya akademik verilerini korumak amacıyla farklı şifreleme yöntemlerinden yararlandıkları görülmektedir. Katılımcıların tercih ettikleri yöntemlerin, temel veri şifreleme uygulamalarından ileri düzey kimlik doğrulama ve çok katmanlı güvenlik yaklaşımlarına kadar geniş bir yelpazeye yayıldığı belirlenmiştir. Dosya ve veri şifrelemeye yönelik yöntemlerin öne çıktığı, özellikle simetrik şifreleme, AES tabanlı dosya şifreleme, disk şifreleme ve parola korumalı arşiv oluşturma gibi uygulamaların yaygın biçimde kullanıldığı görülmektedir. Bunun yanı sıra, iletişim güvenliğine yönelik olarak PGP/GPG ile e-posta şifreleme ve VPN üzerinden güvenli bağlantı kullanımı tercih edilen yöntemler arasında yer almaktadır. Bulut ve mobil ortam güvenliğine ilişkin bulgular, uçtan uca şifreleme ve mobil cihaz yedeklemelerinin şifrelenmesi gibi uygulamaların benimsendiğini göstermektedir. Ayrıca, çift faktörlü doğrulama, rol tabanlı erişim kontrolü, donanım tabanlı güvenlik anahtarları ve zero-knowledge şifre yöneticileri gibi kimlik doğrulama ve erişim kontrolüne yönelik yöntemlerin de kullanıldığı belirlenmiştir.

4.2.8. Bilgi güvenliği konularına ilişkin farkındalık, deneyim ve gelişim alanlarına yönelik bulgular

Katılımcılara, parola güvenliği, kötü amaçlı yazılımlar, sosyal mühendislik, veri gizliliği ve güvenli internet kullanımı gibi konulara ilişkin farkındalık ve deneyimleri ile geliştirmek istedikleri alanlara yönelik görüşleri belirtmeleri için "*Parola güvenliği, kötü amaçlı yazılımlar, sosyal mühendislik, veri gizliliği ve güvenli internet kullanımı gibi konularda farkındalığınız ve deneyimleriniz nelerdir? Eksik gördüğünüz veya geliştirmek istediğiniz noktalar nelerdir?*" şeklinde bir soru yöneltilmiştir. Bahse konu soruya verilen yanıtların belirli temalar etrafında toplandığı görülmektedir. Aşağıda yer alan Tablo 10'da söz konusu tamalar sunulmuştur.

Tablo 10. Bilgi güvenliği farkındalığı, deneyimler ve geliştirilmek istenen alanların tematik dağılımı

Tema	Deneyimler	Geliştirilmek İstenen Noktalar
Bilinç ve Farkındalık (f=5)	Farkındalık, bilinç, tehdit algısı	Sosyal medya hesap gizliliği, kişisel hesaplara yönelik riskler, siber güvenlik
Sorumluluk ve Tutum (f=4)	Sorumluluk, tutum, bireysel koruma	Veri gizliliği–mahremiyet, mahremiyet yönetimi, parola yönetimi
Teknik ve Uygulamalı Beceriler (f=4)	Teknik beceri, kazanımlar, keşif	Güçlü parola politikaları, kötü amaçlı yazılımları tanıma, dijital güvenlik
Güvenli İnternet Kullanımı (f=2)	Bilinç, farkındalık	Güvenli internet kullanımı, güvenli internet kullanım stratejileri

Tablo 10'da sunulan bulgular incelendiğinde, katılımcıların parola güvenliği, kötü amaçlı yazılımlar, sosyal mühendislik, veri gizliliği ve güvenli internet kullanımı gibi temel bilgi güvenliği konularında

belirli bir farkındalık ve bilinç düzeyine sahip oldukları görülmektedir. Katılımcılar, deneyimlerini çoğunlukla farkındalık, bilinç, sorumluluk, tutum ve bireysel koruma kavramları üzerinden ifade etmiştir. Bununla birlikte, katılımcıların mevcut farkındalık ve deneyimlerine rağmen bazı alanlarda kendilerini geliştirme ihtiyacı duydukları anlaşılmaktadır. Özellikle sosyal medya hesap gizliliği, parola güvenliği ve parola yönetimi, veri gizliliği ve mahremiyet yönetimi, sosyal mühendislikten korunma yöntemleri ile kötü amaçlı yazılımları tanıma konularının geliştirilmek istenen başlıca alanlar arasında yer aldığı belirlenmiştir. Teknik ve uygulamaya yönelik beceriler bağlamında, güçlü parola politikaları, dijital güvenlik uygulamaları ve siber güvenlik konularında bilgi ve becerilerin artırılmasına yönelik bir ihtiyaç hissedildiği görülmektedir. Ayrıca, güvenli internet kullanımına ilişkin stratejilerin geliştirilmesi ve bu konuda daha sistematik bir yaklaşımın benimsenmesi gerektiği ifade edilmiştir.

4.2.9. Bilgi güvenliği farkındalığını artırmaya yönelik beklenen destekler ve mevcut uygulamaların yeterliliğine ilişkin bulgular

Katılımcılara, bilgi güvenliği farkındalıklarını ve bilinçlerini artırmak amacıyla üniversite ve/veya akademisyenlerden bekledikleri destekler ile mevcut uygulamaların yeterliliğine ilişkin görüşlerini belirtmeleri için "*Bir lisansüstü öğrenci olarak, bilgi güvenliği farkındalığınızı ve bilincinizi artırmak için üniversite ve/veya akademisyenlerden hangi destekleri veya uygulamaları bekliyorsunuz? Mevcut uygulamaların bu konuda yeterli olduğunu düşünüyor musunuz?*" şeklinde bir soru yöneltilmiştir. Bahse konu soruya verilen yanıtların belli temalar etrafında toplanmış, aşağıda yer alan Tablo 11'de söz konusu tamalar sunulmuştur.

Tablo 11. Bilgi güvenliği farkındalığını artırmaya yönelik destek/beklentiler ve yeterlilik algısının tematik dağılımı

Tema	Destek/Beklenti Türleri	Yeterlilik Durumu
Eğitim ve Farkındalık Odaklı Uygulamalar (f=3)	Webinarlar ve farkındalık eğitimleri, temel farkındalıklar, siber tehdit farkındalık eğitimleri	Evet=10 Hayır:5
Uygulamalı ve Deneyim Temelli Eğitimler (f=3)	Uygulamalı siber güvenlik atölyeleri, farkındalık artırıcı simülasyonlar, uygulamalı eğitim ve gerçek örnekler	
Kurumsal Destek ve Danışmanlık (f=2)	Danışman–uzman desteği	
Teknik Altyapı ve Yazılım Desteği (f=2)	Lisanslı güvenlik yazılımları	
Politika, Erişim ve Uyarı Mekanizmaları (f=4)	Veri güvenliği politikaları, güvenli internet ve ağ erişimi, siber tehditlere uyarı mekanizmaları	
Bilgilendirme ve İletişim Araçları (f=1)	Periyodik bilgilendirme bültenleri	

Tablo 11'de sunulan bulgular incelendiğinde; öncelikle katılımcıların büyük bölümünün bilgi güvenliği farkındalığını artırmaya yönelik destek/beklentiler ve yeterlilik noktasında "yetersizlik" duyumsadıkları görülmektedir. Bunun yanı sıra yanıtlar ekseninde oluşan temalar incelendiğinde ise en fazla vurgulanan temanın Politika, Erişim ve Uyarı Mekanizmaları olduğu, katılımcıların veri güvenliği politikaları, güvenli internet ve ağ erişimi ile siber tehditlere yönelik uyarı mekanizmalarına özel bir önem atfettikleri anlaşılmaktadır. Bu durum, bilgi güvenliğinin yalnızca bireysel önlemlerle değil, kurumsal düzeyde oluşturulan yapılar ve sistemlerle desteklenmesi gerektiğine yönelik bir algının bulunduğunu göstermektedir. Eğitim ve farkındalık odaklı uygulamalar temasına ilişkin bulgular, katılımcıların webinarlar, temel farkındalık eğitimleri ve siber tehdit farkındalık etkinliklerini önemli destek unsurları olarak değerlendirdiklerini ortaya koymaktadır. Uygulamalı ve deneyim temelli eğitimler temasında, uygulamalı siber güvenlik atölyeleri, simülasyonlar ve gerçek örneklere dayalı eğitimlerin beklenti olarak öne çıktığı dikkat çekmektedir. Bu tema altında yeterlilik değerlendirmesinin

açık biçimde belirtilmemesi, katılımcıların bu tür uygulamaların sınırlı olduğu ya da geliştirilmesi gerektiği yönünde örtük bir algıya sahip olabileceklerine işaret etmektedir. Kurumsal destek ve danışmanlık ile teknik altyapı ve yazılım desteği temaları, danışman-uzman desteği ve lisanslı güvenlik yazılımlarına duyulan ihtiyacı ortaya koymaktadır. Bu temalar, bilgi güvenliği farkındalığının bireysel çabaların ötesinde, uzman desteği ve kurumsal teknik altyapı ile güçlendirilmesi gerektiğine yönelik beklentileri yansıtmaktadır. Son olarak bilgilendirme ve iletişim araçları temasında yer alan periyodik bilgilendirme bültenlerinin, daha sınırlı düzeyde ifade edilmekle birlikte, farkındalık artırıcı destek unsurları arasında değerlendirildiği görülmektedir.

5. Tartışma ve Sonuç

Bu araştırmada, Yönetim Bilişim Sistemleri alanında lisansüstü öğrenim gören öğrencilerin bilişim güvenliği farkındalık düzeyleri, bilgi güvenliğine ilişkin algıları, deneyimleri ve beklentileri nitel araştırma yaklaşımı çerçevesinde incelenmiştir. Fenomenoloji deseniyle yürütülen araştırma, bilişim güvenliği gibi teknik, davranışsal ve bilişsel boyutları bir arada barındıran çok yönlü bir olgunun, katılımcıların deneyimleri üzerinden derinlemesine anlaşılmasını amaçlamıştır. Bu bağlamda elde edilen bulgular, lisansüstü öğrencilerin bilişim güvenliği konusunda genel olarak yüksek bir farkındalık ve bilinç düzeyine sahip olduklarını ortaya koymakla birlikte, bu farkındalığın dinamik bir yapı sergilediğini ve sürekli olarak geliştirilmesi gerektiğini göstermektedir.

Araştırma bulguları, katılımcıların bilgi güvenliğini çoğunlukla koruma, engelleme, savunma ve denetim işlevleri üzerinden anlamlandırdıklarını ortaya koymuştur. Metafor analizine dayalı bulgular, bilgi güvenliğinin katılımcılar tarafından "kapı güvenliği", "kalkan" ve "güvenlik duvarı" gibi somut ve koruyucu unsurlarla ilişkilendirildiğini göstermektedir. Bu durum, bilgi güvenliğinin soyut bir bilişim kavramı olmaktan ziyade, gündelik yaşam pratikleriyle örtüşen bir güvenlik olgusu olarak algılandığını göstermektedir. Literatürde bilgi güvenliğinin bireyler tarafından fiziksel güvenlik anlayışına benzer biçimde kavramsallaştırıldığına yönelik bulgular (Vural ve Sağıroğlu; Güldüren vd., 2016), bu çalışmanın sonuçlarıyla örtüşmektedir. Ayrıca "trafik polisi" ve "rehber" metaforları, bilgi güvenliğinin yalnızca tehditleri engelleyen değil, aynı zamanda dijital davranışları yönlendiren ve düzenleyen bir mekanizma olarak algılandığını ortaya koymaktadır.

Çalışmada, katılımcıların tamamı bilgi güvenliği farkındalıklarının zaman içerisinde arttığını ifade etmiştir. Bu artışın; lisansüstü eğitim sürecinde artan akademik sorumluluklar, dijital ortamların daha yoğun kullanımı, kişisel ve akademik veri sorumluluğunun gelişmesi ve dijital tehditlere ilişkin deneyim kazanılması gibi çoklu faktörlerin bir araya gelmesiyle şekillendiği belirlenmiştir. Bu bulgu, bilgi güvenliği farkındalığının durağan bir özellik olmadığını, aksine deneyim, eğitim ve dijital etkileşimle birlikte gelişen dinamik bir yapı sergilediğini ortaya koymaktadır. Alan yazında, özellikle yükseköğretim düzeyinde bilgi güvenliği farkındalığının eğitim ve deneyimle birlikte arttığını ortaya koyan çalışmalar (Avcı ve Oruç, 2020; Özdemir ve Uluyol, 2021) bu sonucu destekler niteliktedir.

Bilgi güvenliği ihlali ya da ihlal şüphesi durumunda izlenen yollara ilişkin bulgular, katılımcıların genel olarak bilinçli, temkinli ve sorumluluk odaklı bir tutum sergilediklerini göstermektedir. Katılımcıların büyük bir bölümü, şüpheli durumlarda bireysel önleyici tedbirlere yönelmekte; parolaları güncelleme, hesap güvenliğini kontrol etme ve riskli etkileşimlerden kaçınma gibi adımlar atmaktadır. Bununla birlikte, bazı katılımcıların yetkili kişi veya birimlere bildirimde bulunmayı tercih etmeleri, bilgi güvenliğini yalnızca bireysel değil aynı zamanda kurumsal bir sorumluluk olarak gördüklerini ortaya koymaktadır. Ancak katılımcılar, aldıkları bilgi güvenliği eğitimlerini temel farkındalık kazandırma açısından yeterli bulsalar da, uygulamaya ve senaryo temelli deneyimlere dayalı eğitimlerin yetersiz kaldığını ifade etmişlerdir. Bu bulgu, literatürde bilgi güvenliği eğitimlerinin teorik düzeyde kalmasının

davranış değişikliği yaratmada sınırlı etkisi olduğunu ortaya koyan çalışmalarla (Stanton vd., 2005; Parsons vd., 2014) örtüşmektedir.

Kişisel ve akademik verilerin korunmasına yönelik bulgular, katılımcıların güçlü parolalar kullanma, iki aşamalı doğrulama, veri yedekleme, lisanslı yazılım kullanımı ve şifreleme gibi temel siber güvenlik uygulamalarını benimsediklerini göstermektedir. Bunun yanı sıra katılımcıların şüpheli bağlantılardan kaçınma ve veri paylaşımında seçici davranma gibi davranışsal önlemler geliştirdikleri belirlenmiştir. Özellikle şifreleme yöntemlerine ilişkin bulgular, lisansüstü öğrencilerin ileri düzey güvenlik uygulamalarına aşina olduklarını ortaya koymaktadır. AES tabanlı şifreleme, disk şifreleme, VPN kullanımı, PGP/GPG ile e-posta şifreleme ve donanım tabanlı güvenlik anahtarları gibi yöntemlerin ifade edilmesi, katılımcıların yalnızca farkındalık düzeyinde değil, uygulama düzeyinde de bilgi güvenliğine önem verdiklerini göstermektedir. Bu durum, bilişim okuryazarlığı yüksek bireylerin bilgi güvenliği pratiklerinde daha gelişmiş stratejiler benimsediğini ortaya koyan literatürle (Siponen, 2000; Hwang vd., 2019) uyumludur.

Katılımcıların karşılaştıkları bilgi güvenliği tehditleri incelendiğinde, en yaygın tehditlerin kimlik avı girişimleri, şüpheli bağlantılar ve zararlı içerikler olduğu görülmektedir. Katılımcılar mevcut önlemlerini temel düzeyde yeterli görmelerine rağmen, gelişen tehditler karşısında daha etkin ve güncel güvenlik uygulamalarına ihtiyaç duyduklarını ifade etmişlerdir. Bu bulgu, bilgi güvenliğinin statik değil, sürekli güncellenmesi gereken bir süreç olduğunu vurgulayan çalışmalarla (Güldüren vd., 2016; Gün ve Çelik, 2022) örtüşmektedir.

Araştırmanın dikkat çeken sonuçlarından biri de, lisansüstü öğrencilerin üniversitelerden ve akademisyenlerden bilgi güvenliği farkındalığını artırmaya yönelik beklentileridir. Katılımcılar, mevcut eğitim ve farkındalık çalışmalarını kısmen yeterli bulmakla birlikte, özellikle uygulamalı eğitimler, simülasyonlar, kurumsal politika ve uyarı mekanizmaları ile teknik altyapı desteği konularında eksiklikler bulunduğunu ifade etmişlerdir. Bu durum, bilgi güvenliğinin bireysel çabaların ötesinde, kurumsal düzeyde sürdürülebilir politikalar ve sistematik eğitimlerle desteklenmesi gerektiğini göstermektedir. Literatürde yükseköğretim kurumlarında bilgi güvenliği farkındalığının artırılmasında kurumsal yapıların belirleyici rolüne işaret eden çalışmalar (Cox vd., 2001) bu sonucu desteklemektedir.

Bu araştırma, yönetim bilişim sistemleri alanında lisansüstü öğrenim gören öğrencilerin bilişim güvenliği farkındalıklarının yüksek olduğunu, ancak bu farkındalığın sürekli desteklenmesi ve geliştirilmesi gerektiğini ortaya koymaktadır. Bilişim okuryazarlığı yüksek ve dijital sistemlerin yönetimine yönelik uzmanlık eğitimi alan bu grubun bilgi güvenliğine ilişkin tutum ve davranışları, yalnızca bireysel dijital güvenlik pratikleri açısından değil, gelecekte yer alacakları kurumsal yapılarda bilgi güvenliği kültürünün oluşumu açısından da kritik bir öneme sahiptir. Bu yönüyle çalışma, hem literatüre nitel bir katkı sunmakta hem de yükseköğretim kurumlarında bilişim güvenliği politikalarının ve eğitim içeriklerinin geliştirilmesine yönelik önemli çıkarımlar ortaya koymaktadır.

Araştırmadan elde edilen bulgular ve uluslararası literatür ışığında şu öneriler geliştirilmiştir:

1.Simülasyon Tabanlı Eğitimler: Üniversitelerin bilgi işlem birimleri tarafından, öğrencilere yönelik periyodik "oltalama (phishing) simülasyonları" düzenlenmelidir. Araştırmalar, interaktif ve simülasyon tabanlı eğitimlerin, pasif öğrenme yöntemlerine göre güvenlik davranışlarını geliştirmede çok daha etkili olduğunu göstermektedir (Aldawood ve Skinner, 2019).

2.Atölye Çalışmaları: Şifreleme, güvenli ağ kullanımı ve zararlı yazılım tespiti gibi konularda öğrencilerin bizzat uygulama yapabileceği atölye çalışmaları organize edilmelidir.

3.Müfredat Entegrasyonu: Bilişim güvenliği farkındalığının sadece ilgili bölümlerde değil, tüm lisansüstü programlarda bir "dijital yetkinlik" dersi olarak müfredata entegre edilmesi önerilmektedir.

Bunun yanı sıra yapılan bu araştırmanın birtakım kısıtlılıkları da bulunmaktadır. Öncelikle çalışma, tek bir üniversitede ve belirli bir anabilim dalında öğrenim gören sınırlı sayıda lisansüstü öğrenci ile gerçekleştirilmiştir. Bu durum, elde edilen bulguların farklı üniversitelere, disiplinlere veya öğrenci gruplarına genellenmesini sınırlandırmaktadır. Bununla birlikte araştırmada nitel fenomenoloji deseninin benimsenmesi, bulguların derinlemesine ve bağlamsal olarak incelenmesine olanak tanımış; ancak nicel ölçümlerle desteklenmemiş olması, sonuçların karşılaştırmalı olarak değerlendirilmesini sınırlamıştır. Son olarak, verilerin katılımcıların öz-bildirimlerine dayanması, sosyal beğenirlik etkisi ve bireysel algılara bağlı yanlılık olasılığını beraberinde getirebilmektedir. Bu kısıtlılıklara rağmen çalışma, lisansüstü öğrencilerin bilişim güvenliği farkındalıklarına ilişkin önemli ve bağlamsal çıkarımlar sunmaktadır.

Katkı Beyanı

Yazarlar çalışmanın tüm bölümlerine eşit katkıda bulunmuştur.

Çıkar Çatışması Beyanı

Yazarlar herhangi bir çıkar çatışması olmadığını beyan etmişlerdir.

Etik Kurul Beyanı

Çalışmada akademik ve bilimsel etik kurallarına uyulmuştur. Siirt Üniversitesi, İnsan Araştırmaları Etik Kurulu'ndan 2025/1371 tarih ve sayılı başvuru ile etik kurul izni alınmıştır. Çalışma için Kafkas Üniversitesi Sosyal ve Beşeri Bilimler Etik Kurulu'ndan 05.12.2025 tarih ve 80 sayılı kararıyla etik kurulu izni alınmıştır.

Yapay Zekâ Araçlarının Kullanımı

Yazarlar, bu çalışmanın hazırlanması sürecinde herhangi bir yapay zekâ aracı kullanmamıştır. İçerik yazarlar tarafından gözden geçirilmiştir ve nihai sorumluluk yazarlara aittir.

Kaynakça

Aldawood, H., & Skinner, G. (2019). Reviewing the effectiveness of security awareness programs: A comparison of delivery methods. *Kybernetes, 48*(5), 1666–1686.

Aslandağ, K. (2010). *Bilgi güvenliği kavramı ve bilgi güvenliği yönetim sistemleri ile şirket performansı ilişkisine dair bir uygulama* [Yüksek Lisans Tezi]. Gebze Yüksek Teknoloji Enstitüsü.

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.

Braun, V., & Clarke, V. (2019). *Thematic analysis: A practical guide.* SAGE Publications.

Can, Ö., & Akbaş, M. F. (2014). Kurumsal ağ ve sistem güvenliği politikalarının önemi ve bir durum çalışması. *TÜBAV Bilim Dergisi, 7*(2), 16-31.

Cox, A., Connolly, S., & Currall, J. (2001). Raising information security awareness in the academic setting. *Vine, 31*(2), 11-16.

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches (4th ed.).* SAGE Publications.

Çetin, H. (2014). Kişisel veri güvenliği ve kullanıcıların farkındalık düzeylerinin incelenmesi. *Akdeniz Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 14*(29), 86-105.

Demir, Ü., & Sarı, B. (2023). Okul öncesi ve çocuk gelişimi bölüm öğrencilerinin bilgi güvenliği ve dijital okuryazarlık durumlarının incelenmesi. *Kahramanmaraş Sütçü İmam Üniversitesi Sosyal Bilimler Dergisi, 20*(3), 760-769.

Derin, M. A., & Gençoğlu, M. T. (2020). Ortaokul öğrencilerinin bilgi güvenliği farkındalığı. *Savunma Bilimleri Dergisi, 38,* 159-181.

Eminağaoğlu, M., & Gökşen, Y. (2009). Bilgi güvenliği nedir, ne değildir? Türkiye'de bilgi güvenliği sorunları ve çözüm önerileri. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 11*(4), 1-15.

Extranet. (2025). *2025 yılı internet kullanım raporu.* https://www.extranet.com.tr/blog/2025-yili-internet-kullanim-raporu. Erişim tarihi: 28 Kasım 2025.

Ganbat, O. (2013). *Bilgi güvenliği yönetim sistemi ISO/IEC 27001 ve bilgi güvenliği risk yönetimi ISO/IEC 27005 standartlarının uygulanması* [Yüksek Lisans Tezi]. Ege Üniversitesi.

Gökmen, Ö. F., & Akgün, Ö. E. (2015). Bilgisayar ve öğretim teknolojileri eğitimi öğretmen adaylarının bilişim güvenliği bilgilerinin çeşitli değişkenlere göre incelenmesi. *Çukurova Üniversitesi Eğitim Fakültesi Dergisi, 44*(1), 61-84.

Güldüren, C., Çetinkaya, L., & Keser, H. (2016). Ortaöğretim öğrencilerine yönelik bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme çalışması. *İlköğretim Online, 15*(2), 682-695.

Gültekin, V., & Özel, N. (2023). Üniversite öğrencilerinin bilgi güvenliği farkındalığı: Ankara Üniversitesi örneği. *Bilgi Yönetimi, 6*(2), 310-331.

Gün, İ., & Çelik, M. (2022). Sağlık çalışanlarının bilgi güvenliği farkındalığının iş performansı üzerindeki etkisinde bilgi güvenliği stresinin aracı rolü: Covid 19 pandemi döneminde bir araştırma. *İşletme Araştırmaları Dergisi, 14*(1), 1-15.

Hwang, I., Wakefield, R., Kim, S., & Kim, T. (2019). Güvenlik farkındalığı: Bilgi güvenliği uyumluluk davranışında ilk adım. *Bilgisayar Bilgi Sistemleri Dergisi, 61*(4), 345–356.

International Telecommunication Union (ITU). (2025). *Statistics – ICT indicators and data*. https://www.itu.int/en/ITU-D/Statistics/pages/stat/default.aspx. Erişim tarihi: 28 Kasım 2025.

Karaarslan, E. (2013). Siber güvenlik deneyleri için ağ benzetici ve ağ sınama ortamlarının kullanımına dair ön inceleme. *Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, 5,* 23-32.

Mart, İ. (2012). *Bilişim kültüründe bilgi güvenliği farkındalığı* [Yüksek Lisans Tezi]. Kahramanmaraş Sütçü İmam Üniversitesi.

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods, 16*, 1-13.

Önel, D., & Dinçkan, A. (2007). Bilgi güvenliği yönetim sistemi kurulumu. *TÜBİTAK UEKAE Dergisi, 1,* 1-16.

Özdemir, A., & Uluyol, Ç. (2021). Kamu kurum ve kuruluşlarında bilgi güvenliği farkındalığı. *Türkiye Sosyal Araştırmalar Dergisi, 25*(3), 649-666.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2014). Avustralya hükümet harcamalarında bilgi birikiminin finansal üzerine bir çalışma. *Bilgi Yönetimi ve Bilgisayar Güvenliği, 22*(4), 334–345.

Patton, M. Q. (2015). *Qualitative research & evaluation methods (4th ed.).* SAGE Publications.

Pfleeger, C. P. (1997). The fundamentals of information security. *IEEE Software, 14*(1), 15-16.

Puhakainen, P. (2006). *A design theory for information security awareness* [Academic Dissertation]. University of Oulu.

Seferoğlu, S. S., Yıldız-Durak, H., Karaoğlan-Yılmaz, G., & Yılmaz, R. (2018). Bilgi güvenliği farkındalığı ve bilgi güvenliği politikalarıyla ilgili bir inceleme. B. Akkoyunlu, A. İşman ve H. F. Odabaşı (Ed.), *Eğitim teknolojileri okumaları* içinde (ss. 29-43). TOJET ve Sakarya Üniversitesi.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31-41.

Stake, R. E. (1995). *The art of case study research*. SAGE Publications.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124-133.

Şahinaslan, E., Kantürk, A., Şahinaslan, Ö., & Borandağ, E. (2009). Kurumlarda bilgi güvenliği farkındalığı, önemi ve oluşturma yöntemleri. *Akademik Bilişim, 9,* 11-13.

Talan, T., & Aktürk, C. (2021). Orta öğretim öğrencilerinin dijital okuryazarlık ve bilgi güvenliği farkındalığı seviyelerinin incelenmesi. *Kahramanmaraş Sütçü İmam Üniversitesi Sosyal Bilimler Dergisi, 18*(1), 158-180.

Tekerek, M. (2008). Bilgi güvenliği yönetimi. *Kahramanmaraş Sütçü İmam Üniversitesi Fen ve Mühendislik Dergisi, 11*(1), 132.

Tekerek, M., & Tekerek, A. (2013). A research on students' ınformation security awareness. *Online Submission, 2*(3), 61-70.

Tipton, H. F., & Krause, M. (2007). *Information security management handbook*. Auerbach Publications.

Türkiye İstatistik Kurumu (TÜİK). (2025). *Hanehalkı bilişim teknolojileri (BT) kullanım araştırması 2025.* https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2025-53925. Erişim tarihi: 28 Kasım 2025.

Ünver, M., Canbay, C., & Mirzaoğlu, A. G. (2009). *Siber güvenliğin sağlanması: Türkiye'deki mevcut durum ve alınması gereken tedbirler*. Bilgi Teknolojileri ve İletişim Kurumu (BTK).

Vural, Y. (2007). *Kurumsal bilgi güvenliği ve sızma (penetrasyon) testleri* [Yüksek Lisans Tezi]. Gazi Üniversitesi.

Vural, Y., & Sağıroğlu, Ş. (2008). Kurumsal bilgi güvenliği ve standartları üzerine bir inceleme. *Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi, 23*(2), 507-522.