Öğretim Elemanlarının Siber Bilgi Güvenliği Farkındalıkları ile Siber Zorbalık Eğilimlerinin Belirlenmesi

Aysun DÜŞMEZ, MEB, ORCID ID: 0009-0002-6792-6353
Alev ORHAN, Sivas Cumhuriyet Üniversitesi, ORCID ID:0000-0002-8999-9329
Elif ORHAN, Gazi Üniversitesi, ORCID ID:0000-0002-3949-6141

İnönü Üniversitesi
Eğitim Fakültesi Dergisi
Cilt 26, Sayı 2, 2025
ss. 603-639
DOI
10.17679/inuefd.1565813

Makale Türü
Araştırma Makalesi

Gönderim Tarihi
12.10.2024

Kabul Tarihi
27.07.2025

Öne Çıkanlar

- Eğitim fakültesi öğretim elemanlarının siber bilgi güvenliği farkındalığı.
- Öğretim elemanlarının siber zorbalık hakkındaki görüşleri.
- Üç farklı üniversitenin eğitim fakültelerinde görev yapan 27 öğretim elemanı.

Öz

Bu araştırmanın amacı, eğitim fakültesinde görev alan öğretim elemanlarının siber bilgi güvenliği farkındalığı ve siber zorbalık hakkındaki görüşlerinin belirlenmesidir. Araştırmada nitel araştırma yöntemlerinden fenomenoloji deseni kullanılmıştır. Nitel verilerin elde edilmesinde üç farklı üniversitenin eğitim fakültelerinde görev yapan 27 öğretim elemanı yer almıştır. Veriler "Siber Zorbalık ve Bilgi Güvenliğine İlişkin Görüşme Formu" kullanılarak elde edilmiştir. Nitel verilerin analizinde MAXQDA Pro2020 (20.4.0) programı kullanılmış olup veriler betimsel ve içerik analizi birlikte kullanılarak analiz edilmiştir. Elde edilen bulgulara göre öğretim elemanlarına göre siber ortam ana temasının altında siber zorbalık ve siber bilgi güvenliği olmak üzere iki tema yer almaktadır. Siber zorbalık temasının altında yer alan kodlar; siber zorbalığa maruz kalma durumu, siber zorba davranışları, mağdur olma durumu, zorba olma durumu, çözüm önerileri, korunma yöntemleri, farkındalık, algılanma durumu kodlarından oluşurken; siber bilgi güvenliği teması altında yer alan kodlar ise, korunma yöntemleri, farkındalık ve kimlik hırsızlığı kodlarından oluşmaktadır. Araştırma sonuçlarına göre öğretim elemanlarının bilgi güvenliğine yönelik görüşleri incelendiğinde, teknik donanıma ve beceriye sahip olmasalar da bilgi güvenliğinin anlamı ve önemi konusunda farkındalık sahibi oldukları bulgulanmıştır. Siber zorbalığın günümüzde çok sık karşılaşılan rahatsız edici bir durum olduğu yönündeki görüşler öne çıkmaktadır. Öğretim elemanlarıyla yapılan görüşmeler neticesinde siber zorbalık kavramını siber alanda gerçekleştirilen zorbalık olarak tanımlayan görüş hakimdir.

Anahtar Kelimeler: Bilgi güvenliği, Öğretim elemanları, Siber zorbalık, Bilgi güvenliği farkındalığı

Önerilen Atıf

Düşmez, A., Orhan, A., & Orhan, E. (2025). Öğretim elemanlarının siber bilgi güvenliği farkındalıkları ile siber zorbalık eğilimlerinin belirlenmesi. *İnönü Üniversitesi Eğitim Fakültesi Dergisi*, *26*(2), 603-639. DOI: 10.17679/inuefd.1565813

Bu makale Gazi Üniversitesi, Fen Bilimler Enstitüsü tarafından, Aralık 2023 tarihinde kabul edilen yüksek lisans tezinden üretilmiştir. 28-30 Ekim 2023 tarihlerinde Ankara'da gerçekleştirilen 10. Uluslararası Başkent Fen, Mühendislik ve Uygulamalı Bilimleri Kongresi'nde özet sözel bildiri olarak sunulmuştur.

1. Giriş

İnternet teknolojilerinde gerçekleşen yenilikler, teknolojiyi yaşamımızın vazgeçilmez bir parçası hâline getirerek, bireylerin günlük işleri kolaylaşmakta ve iletişim, online alışveriş, mobil bankacılık gibi alanlarda değişiklikler meydana getirmektedir (Çiftçi ve Sakallı, 2016). Bilgiye hızlı ve kolay erişim imkânı sayesinde, internet teknolojilerinin kullanım oranı büyük ölçüde artmış; kurumlar ve bireyler bilgilerini dijitalleştirerek elektronik ortamda koruma altına almaya başlamıştır. Büyük verilerin saklanabilmesi, veriye her zaman ve her yerden anında erişilebilmesi ile ağ üzerinden veri tabanlarına kolaylıkla ulaşılabilmesi, internet teknolojilerinin en büyük avantajları arasında yer almakta; bu durum bilgi teknolojilerinin önemini artırmakta ve bilgi güvenliği konusunu ön plana çıkarmaktadır. (Mallaboyev, Sharifjanovna, Muxammadjon ve Shukurullo, 2022).

Bilgi güvenliğini bireysel anlamda ele alırsak dijital ortamda kişisel verilerin korunması, saklanması ve erişim durumlarını içermesi anlamına gelirken, kurumsal anlamda ise bilişim cihazlarının korunması, verilerin saklanması, riskli faaliyetlere karşı tedbirler alınarak güvenliğinin sağlanması anlamına gelmektedir (Eminağaoğlu ve Gökşen, 2009). Bireyler, sosyal medya aracılığıyla gerekli donanıma sahip olmasalar bile paylaşımlarını geniş kitlelere ulaştırabilmekte; bu platformlar, bireylerin iletişim kurmasına, verilerini yaymasına ve bilgi alışverişinde bulunmasına olanak tanırken, aynı zamanda çeşitli olumsuzluklara da yol açabilmektedir. Bazı insanlar bu ortamlardan faydalanarak siber zorbalık yapabilir hâle gelmekte ve cep telefonları, e-posta, sohbet odaları, sosyal ağ siteleri gibi platformlar üzerinden insanları dolandırarak siber suç işlemektedir (Deschamps ve McNutt, 2016). Bireylerin internet kullanırken siber güvenlik ve siber suçlar hakkında bilgi sahibi olmaları siber ortamda karşılaşacakları tehlikelerden korunmaları açısından önemlidir (Aksoğan, Bayer, Gülada ve Çelik, 2018).

Bireylerin teknolojiyi amacına uygun ve bilinçli kullanmaları, verilerini korumak amacıyla teknolojik gelişmeleri yakından takip etmeleri ve bilgilerinin güvenliğini nasıl sağlayacakları konusunda bilinçli olmaları, içinde bulunduğumuz çağın gerektirdiği önemli niteliklerden olmakla birlikte yeni nesiller yetiştiren ve nesillere rol model olan değerli öğretmenlerimizin bilgi güvenliğine yönelik farkındalıkları ve donanımları da oldukça önemlidir (Canoğulları, 2021). Eğitim kurumları içerisinde ve dışında teknoloji ile sürekli etkileşim içerisinde olan gençlerimiz için oldukça ciddi bir problem olan siber zorbalık; psikolojik, sosyolojik, fizyolojik ve hatta ekonomik açıdan bireyleri olumsuz olarak etkilemekte ve suç mağduru olma konusunda onları korumasız bırakmaktadır. Bu olumsuzlukların en aza indirilebilmesi için bireylerin bilgi güvenliği konusunda bilgilendirilmesi ve bu konuda farkındalık oluşturma çalışmalarının artırılması önem arz etmektedir (Talib, 2014).

Siber zorbalık ve bilgi güvenliği için alan taraması yapıldığında Gökmen ve Akgün (2015), çalışmalarında öğretmenlik bölümünde okuyan öğrencilerin bilgi güvenliği eğitimi verebilme yeterliliklerini incelemiştir. Araştırmadan elde edilen bulgulara göre öğretmen adaylarının çoğunun bilişim güvenliğini sağlamaya yönelik bir eğitim almadıkları, birçoğunun siber bilgi güvenliği dersi vermek için yetkin olmadığı belirtilmiştir. Metin (2017), ortaokul öğretmenlerine yönelik yaptığı çalışmada, öğretmenlerin siber zorbalığa maruz kalma durumlarını ve korunma yöntemlerini belirlemeyi amaçlamıştır. Çalışma sonucunda elde edilen bulgulara göre katılımcıların %95'i siber zorbalığa maruz kaldığı raporlanmıştır. Tingiş (2022), öğretmenlerin siber zorbalık ile ilgili görüşlerini araştırmıştır. Araştırmada öğretmenlerin görüşüne göre; siber zorbalığın dijital zorbalık olduğu, karşıdaki kişiyi rahatsız etmek için yapıldığı, bilgilerin çalınması ve izinsiz paylaşım yapmanın da bir zorbalık davranışı olduğu belirtilmiştir. Yavuz (2023), öğretmenlere yönelik gerçekleştirdiği çalışmasında katılımcıların bilgi güvenliği farkındalığı ile dijital okuryazarlık düzeylerini farklı değişkenler kullanarak araştırmıştır. Araştırmaya katılan öğretmenlerin siber güvenlik farkındalığı ile dijital okuryazarlık seviyeleri arasında pozitif yönde orta düzeyde anlamlı bir ilişki olduğu belirtilmiştir. Nezgitli ve Arslan (2022), özel sektörde ve

kamu kurumlarında çalışan bireylerin bilgi güvenliği farkındalığına yönelik araştırma yapmışlardır iş yerinde bilgi güvenliğine yönelik önlem alınması, faaliyetlerde bulunulması anlamlı farklar göstermiştir. Pusey ve Sadera (2011), yaptıkları çalışmada öğretmen adaylarının siber bilgi güvenliği konusundaki bilgi seviyelerini, farkındalıklarını ve bunları öğrencilerine öğretebilme algılarını incelemiştir. Araştırma sonucuna göre öğretmen adaylarının siber bilgi güvenliği hakkında bilgi sahibi oldukları ancak bilgilerini aktarma konusunda yeterli olmadıkları belirtilmiştir. Alanda yapılan çalışmalar incelendiğinde siber güvenlik ve bilgi farkındalığı konusunda öğretmenler, öğretmen adayları ve üniversite öğrencileri üzerine çalışmaların yapıldığı fakat öğretmenlerin eğitiminden sorumlu olan eğitim fakültesi öğretim elemanları ile yürütülen çalışmaların sınırlığı olduğu fark edilmiş ve bu araştırmaya gerek duyulmuştur.

Bu araştırmanın temel amacı eğitim fakültesinde görev yapan öğretim elemanlarının siber zorbalık ile bilgi güvenliği hakkındaki görüşlerinin belirlenmesi, siber bilgi güvenliği farkındalığı ile siber zorbalık eğilim düzeylerinin ve bu süreçte yaşanan sorunların tespit edilerek, sorunlara yönelik çözüm önerilerinin ortaya konmasıdır.

Temel amacımızın dışında çalışmamızda aşağıda yer alan alt problem başlıklarına da cevap aranmıştır:

Eğitim Fakültesinde görev yapan öğretim elemanlarının;

Bilgi güvenliğine yönelik görüşleri nelerdir?

Siber zorbalığa yönelik görüşleri nelerdir?

2. Yöntem

Araştırmada, nitel araştırma yöntemlerinden fenomenoloji deseni kullanılmıştır. Fenomenolojinin veri kaynağı, araştırmanın veri kaynakları araştırılan olguyu yaşayan ve onu yansıtabilecek olan gruplardır (Yıldırım ve Şimşek, 2016). Araştırmada öğretim elemanlarının bilgi güvenliği ve siber zorbalık hakkındaki görüşleri, bu konuya dair yaşanan sorunlar ve alınması gereken önlemlere yönelik olarak "Siber Zorbalık ve Bilgi Güvenliğine İlişkin Görüşme Formu" kullanılarak elde edilmiştir.

Çalışma Grubu

Araştırmanın çalışma grubunu 2022-2023 eğitim ve öğretim yılında eğitim fakültelerinde görev yapan öğretim elemanları oluşturmaktadır. Araştırmanın çalışma grubunun belirlenmesine üniversite seçimi ile başlanmıştır. Bu aşamada üniversitelerin seçimi için URAP (University Ranking by Academic Performance) dikkate alınarak 2023-2024 İç Anadolu Bölgesi'nde yer alan eğitim fakültesinin bünyesinde barındıran devlet üniversiteleri taranmış ve toplamda 18 üniversite olduğu belirlenmiştir. Belirlenen liste aritmetik ortalama ve standart sapma baz alınarak üst, orta ve alt olmak üzere üç kısma ayrılmıştır. Aritmetik ortalamanın +1 standart sapma üstünde yer alan üniversiteler üst, +1 ile -1 standart sapma arasında yer alan üniversiteler orta grup ve -1 standart sapma altında yer alan üniversiteler ise alt grup olarak belirlenmiştir. (URAP) 2023-2024 eğitim fakültesini bünyesinde barındıran devlet üniversiteleri sıralamasında maksimum puan 1072 olarak, minimum puan ise 442 olarak tespit edilmiştir. Listenin standart sapma değeri 189,47 ve aritmetik ortalaması ise 755,76 olarak hesaplanmıştır. Yapılan hesaplamalar neticesinde 4 üniversite üst grupta, 11 üniversite orta grupta ve 3 üniversite ise alt grupta yer almaktadır. Bu gruplar tabaka olarak kabul edilmiş ve bu aşamada her gruptan bir üniversite belirlenmiştir. Tabakalı örnekleme, örnekleme hatasını azaltarak evrenin daha fazla temsil edilmesini sağlamaktadır. Tabakalı örnekleme yönteminde, örneklem hatasını minimum seviyeye indirebilmek için, geniş bir evrene ihtiyaç duyulmaktadır. Bundan dolayı evrenden alınacak örneklem sayısı fazla olduğundan daha az örneklem ile çalışabilmek için homojen evrenler kullanılmalıdır (Yıldırım ve Şimşek, 2016). Bu aşamada üç tabakadan birer üniversite belirlenmiştir. Örneklem seçiminin ikinci aşamasında ise eğitim fakültesinin farklı bölümlerinde görev yapan öğretim elemanları çalışmaya dâhil edilerek maksimum çeşitlilik

sağlanmaya çalışılmıştır. Bunun için maksimum çeşitlilik örneklem yöntemi kullanılmıştır. Bu yöntemde asıl amaç göreli olarak küçük bir örneklem oluşturmak ve bu örneklemde çalışan probleme taraf olabilecek bireylerin çeşitliliğini maksimum düzeyde yansıtmaktır (Yıldırım ve Şimşek, 2016).

Araştırmada hem üniversitelerin farklı tabakalardan seçilmesiyle hem de fakültenin farklı bölümlerinde görev alan öğretim elemanlarının seçilmesiyle maksimum çeşitlilik sağlanmaya çalışılmıştır. Araştırmanın çalışma grubuna üç üniversiteden toplamda 27 öğretim elemanı katılmıştır. Araştırmaya dahil olan üniversiteler D, E ve F olarak kodlanmıştır. D üniversitesi üst grupta yer almaktadır ve 10 öğretim elemanı çalışmaya katılmıştır. Çalışmaya katılan öğretim elemanlarından 9'u kadın, 1'i erkek olup, katılımcılar Türkçe ve Sosyal Bilimler Eğitimi, Matematik ve Fen Bilimleri Eğitimi, Eğitim Bilimleri, Temel Eğitim, Bilgisayar ve Öğretim Teknolojileri Eğitimi bölümlerinde görev yapmaktadır. F üniversitesi orta grupta yer almaktadır ve 7 öğretim elemanı çalışmaya katılmıştır. Çalışmaya katılan öğretim elemanlarından 5'i kadın, 2'si erkek olup, katılımcılar Eğitim Bilimleri, Beden Eğitimi ve Spor Eğitimi, Matematik ve Fen Bilimleri Eğitimi bölümlerinde görev yapmaktadırlar. E üniversitesi alt grupta yer almaktadır ve 10 öğretim elemanı çalışmaya katılmıştır. Çalışmaya katılan öğretim elemanlarının 2'si kadın, 8'i erkek olup, katılımcılar Türkçe ve Sosyal Bilimler Eğitimi, Eğitim Bilimleri, Beden Eğitimi ve Spor Eğitimi, Matematik ve Fen Bilimleri Eğitimi bölümlerinde görev yapmaktadırlar. Nitel araştırmada var olan olgunun veri doygunluğu sağlandığı ölçüde var olan şekliyle tanımlanması olduğu için araştırmamızda 27 kişi ile veri doygunluğuna ulaşılmış ve veri toplama sürecine son verilmiştir. Yeterli örneklem büyüklüğünün belirlenmesinde kullanılan yol gösterici ilke veri doygunluğuna ulaşılmasıdır (Baker & Edwards, 2012).

Veri Toplama Araçları

Öğretim elemanlarının siber zorbalık ve bilgi güvenliğine ilişkin görüşleri ve önerilerini almak amacıyla araştırmacı tarafından geliştirilmiş 15 adet açık uçlu sorudan oluşan yarı yapılandırılmış görüşme formu kullanılmıştır. Yarı yapılandırılmış görüşme, yapılandırılmış görüşme tekniğine göre daha esnektir. Bu görüşme yönteminde araştırmacı önceden sormak istediği soruları içeren görüşme metnini hazırlar. Ancak görüşme sürecinde araştırmacı görüşmenin akışına bağlı olarak farklı yan alt sorularla görüşmenin akışını etkileyebilir, katılımcının cevaplarını açmasını ve daha açık ifade etmesini sağlayabilir (Türnüklü, 2000). Formun hazırlanmasında güvenlik ve siber zorbalık kavramlarının ana temaları ve görüşme formunun hazırlanmasındaki temel ilkeler baz alınmıştır. Formun kapsam geçerliliğini sağlamak amacıyla üç eğitim uzmanı ve üç dil uzmanı tarafından incelenmiştir. Uzmanlardan alınan görüşler sonucunda taslak form üzerinde düzenlemeler yapılarak forma son şekli verilmiştir. "Siber Zorbalık ve Bilgi Güvenliğine İlişkin Görüşme Formu" toplam 15 sorudan oluşmaktadır. Araştırmada inandırıcılığının alt boyutu olan katılımcı ve ortam teyidi sağlanmıştır. Katılımcılarla kendilerini rahat ifade edebilecekleri ortamda görüşülmüş ve izinleri doğrultusunda görüşmeler kayıt altına alınmıştır. Katılımcılara istedikleri anda çalışmadan ayrılabilecekleri ve kayıtlarında kendilerine teslim edileceği konusunda güvence verilmiştir. Katılımcıların seçilmesinde amaçlı örnekleme yöntemlerinden maksimum çeşitlilik örneklemesi kullanılarak aktarılabilirlik sağlanmaya çalışılmıştır. Katılımcıların farklı üniversitelerden olmaları, farklı branşlardan olmaları, farklı cinsiyete sahip olmaları ile veri çeşitlemesi sağlanmıştır.

Araştırmanın inandırıcılığının alt boyutu olan doğrudan alıntıyı sağlamak amacıyla verilerin MAXQDA 2020 (20.4.0) programı ile analiz edilmesinin yanı sıra araştırmacılar birbirinden bağımsız olarak verileri kodlamışlardır. Araştırmacıların bağımsız veri toplamasının ardından araştırmacılar bir araya gelerek kodları ve temaları karşılaştırmışlar ve ortak olan kodları belirleyerek veri anahtarı oluşturmuşlardır. Araştırmacı çeşitlemesinin yanında verilerin raporlanmasında katılımcıların görüşlerine doğrudan yer verilerek alıntılama yapılmıştır. Bu aşamada ise oluşan kod haritaları ve veriler 3 eğitim bilimleri uzmanın görüşüne sunulmuş ve verilerin analizinde çeşitleme yapılmıştır.

Verilerin Çözümlenmesi ve Yorumlanması

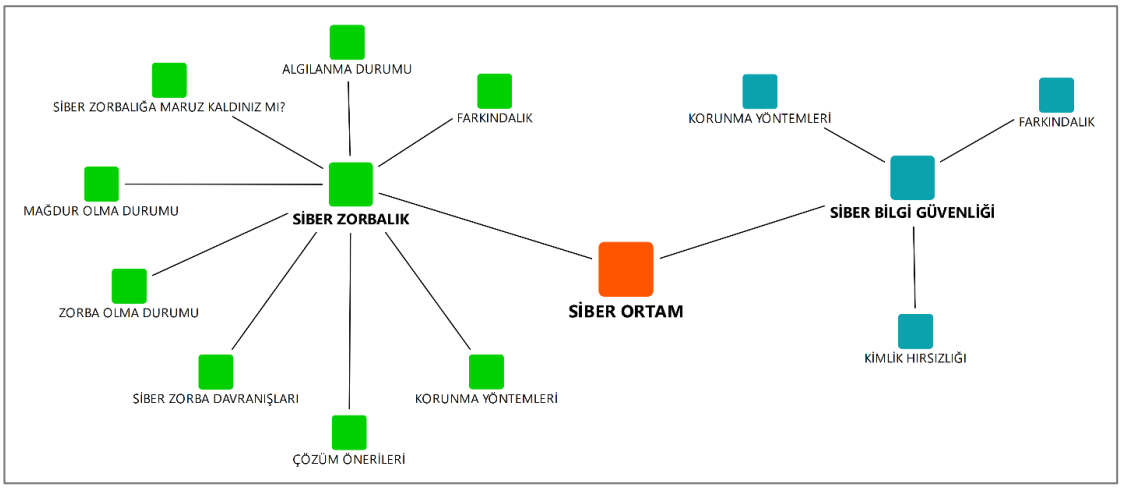
Öğretim elemanlarının siber zorbalık ve bilgi güvenliğine ilişkin görüşleri "Siber Zorbalık ve Bilgi Güvenliğine İlişkin Görüşme Formu" kullanılarak elde edilmiştir. Görüşmeler sonunda elde edilen veriler içerik analizi yöntemi ile analiz edilmiştir. Verilerin analizi MAXQDA Pro2020 (20.4.0) programında yapılmıştır. İçerik analizinde veri kaybının önlenebilmesi için katılımcılardan izin alınarak görüşmeler ses kaydına alınmıştır. Görüşmeleri ses kaydına almaktaki amaç veri kaybının önüne geçmek ve veri madenciliği yapabilmektir. Ortalama görüşme süreleri 50 dk olarak tespit edilmiştir. Ses kayıtları defalarca dinlenerek bilgisayar ortamına aktarılmış ve ham veri metinleri elde edilmiştir. Sonrasında kodlama aşamasına geçilerek analiz süreci başlamıştır. Güvenilirliği ve geçerliliği yükseltmek için çalışmamızda elde edilen veriler hiçbir yoruma yer verilmeden doğrudan alıntılar yapılarak sunulmuştur. Üç farklı üniversitenin ismi D, E ve F şeklinde kodlanmıştır. Bu üniversitelerde görev yapan öğretim elemanlarının isimleri yerine D1, E1, F1 şeklinde kodlar kullanılmıştır.

3. Bulgular

Bu bölümde araştırmanın alt problemleri olan "Öğretim elemanlarının bilgi güvenliğine yönelik görüşleri nelerdir?" ve "Öğretim elemanlarının siber zorbalığa yönelik görüşleri nelerdir?" sorularına cevap aranmıştır. Üç faklı üniversitede görev yapan öğretim elemanlarının siber zorbalık ve bilgi güvenliğine ilişkin görüşleri "Siber Zorbalık ve Bilgi Güvenliğine İlişkin Görüşme Formu" kullanılarak elde edilmiştir. Görüşmeler neticesinde içerik analiz yöntemi ile veriler analiz edilerek kodlanmıştır. Kodlardan alt temalar, alt temalardan da temalar oluşturulmuştur. Elde edilen veriler doğrultusunda kodlar, alt temalar ve temalar siber ortam ana teması altında yer almaktadır. Araştırmanın alt problemleri kapsamındaki siber ortam teması, alt temaları ve kodları Şekil 1'de verilmiştir.

Şekil 1.

Öğretim elemanlarının siber zorbalık ve bilgi güvenliğine ilişkin görüşlerinin hiyerarşik kod alt-kod modeli (kod bölüm temelli)



Şekil 1 incelendiğinde öğretim elemanlarına göre siber ortam ana temasının altında siber zorbalık ve siber bilgi güvenliği olmak üzere iki tema yer almaktadır. Siber zorbalık temasının altında; siber zorbalığa maruz kalma durumu, siber zorba davranışları, mağdur olma durumu, zorba olma durumu, çözüm önerileri, korunma yöntemleri, farkındalık, algılanma durumu kodları; siber bilgi güvenliği teması altında ise, korunma yöntemleri, farkındalık ve kimlik hırsızlığı kodları yer almaktadır. "Siber Ortam" ana temasının, "Bilgi Güvenliği" temasının altında yer alan "Farkındalık" koduna ait olan katılımcı görüşleri aşağıda yer almaktadır:

> "*Üniversitemizin düzenlediği zorunlu siber bilgi güvenliği eğitim seminerleri var 5- 6 dersten oluşan onlara katılıyorum. Sosyal medyada ya da internette bazı uyarılar*

geliyor onlara dikkat ediyorum. Aktif bir kullanıcı olduğum için dikkat ediyorum. Siber zorbalığın düşünmediğim tarafları da var ben daha çok kendi açımdan bakıyorum. Farklı farklı durumları da vardır. Bu eğitimler benim için verimli geçti. Farkındalık oluştu daha dikkatli davranıyorum. Eğitimlerin yeterli olduğunu düşünüyorum." (F7)

"*İnsanları paranoyaya yaklaştırıyor. İnsanların ne yaptığını nereye gittiğini takip eden programlar var. Hatta internete girdiğinizde hiç olmadık mailin içine sıkıştırılmış bir virüsle sizin her yaptığınız takip ediliyor. Onlara göre bilgisayarınız hayalet bilgisayar oluyor. Ne yaparsanız yapın bundan kurtulamıyorsunuz. İnternette yaptığınız her şeyi adımlarınızı takip ediyorlar*." (D2)

"Siber Ortam" ana temasının, "Bilgi Güvenliği" temasının altında yer alan "Kimlik Hırsızlığı" koduna ait olan katılımcı görüşleri aşağıda yer almaktadır:

"*Gittiğimiz alışveriş yaptığımız her yerde kimlik vb. bilgilerini veriyoruz bu riskli. Ben vatandaş olarak bir önlem alamam devletimizin bir önlem alması gerekiyor. Kurumların, özel sektörlerin bazı bilgileri istememe arşivlememe gibi bir durumu olmalı bence. Alışverişte dahi kimlik adres bilgilerimizi kullanıyoruz. Bu çok riskli bence bu konuda devletimizin bir düzenleme yapması gerekmektedir.*" (E7)

"*Kimlik hırsızlığına karşı çok önlem alınacağını düşünmüyorum. Her yerde iletişim vb. bilgilerimiz var. Web sayfam var orda adım adresim oluyor. İki yıl öncesine kadar okulun web sitesinde benim cep telefonum vardı iki yıl önce telefon numaramı sildim. Her yerde kimlik numaramızı giriyorum kişisel verilerimizi paylaşıyoruz. Ben kimlik hırsızlığına karşı bir önlem alınamayacağını düşünüyorum. Öğrencilerin not sistemine girip çocukların notlarını değiştirenler var. Sistemi hackleyip notları değiştiriyorlar. Kişi kendi çıkarları için bilgisini kullanıyor.*" (E3)

"Siber Ortam" ana temasının, "Bilgi Güvenliği" temasının altında yer alan "Korunma Yöntemleri" koduna ait olan katılımcı görüşleri aşağıda yer almaktadır:

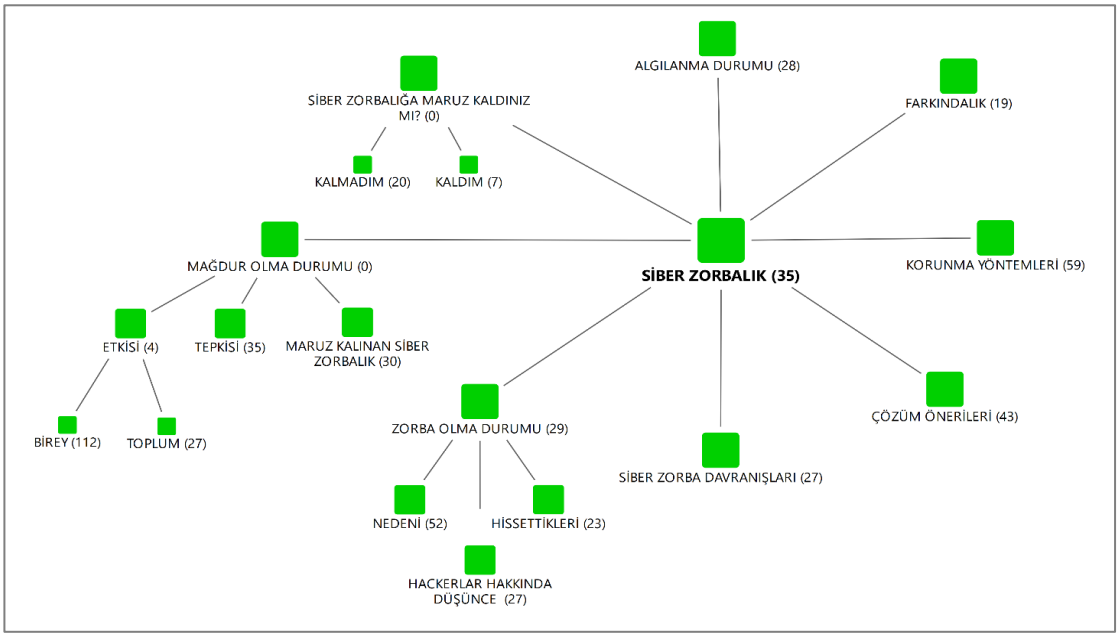
"*Hiçbir yerde kimlik numaramı vermiyorum güvenilirliğinden emin olduğum yerlerde bilgi paylaşıyorum. Kartla alışveriş yaptığımda kart bilgilerini kaydetmiyorum. Şifrelerimi kaydetmiyorum. Sanal kart kullanmak en garantisi. Telefonuma bilgi kaydetmiyorum.*" (E4)

"*Mahremiyetimin korunması için açık ağlardan internette bağlanmamayı tercih ediyorum. Belediye, kafe vb. ağlarından internete bağlanmıyorum. Evden ve okulda güvenli internetten faydalanıyorum. Kişisel verilerimi resimlerimi paylaşmıyorum. Sitelerde çerezlere dikkat ediyorum. Mikrofon özelliğini kamera özelliğini aktif etmiyorum.*" (E10)

"Siber Ortam" ana temasının "Siber Zorbalık" teması, alt temaları ve kodları Şekil 2'de verilmektedir.

Şekil 2.

Öğretim elemanlarının siber zorbalığa ilişkin görüşlerinin hiyerarşik kod alt-kod modeli (kod bölüm temelli)



Şekil 2'de Siber zorbalık temasına ilişkin alt temalar; siber zorbalığa maruz kaldınız mı, korunma yöntemleri, siber zorba davranışları, algılama durumu, mağdur olma durumu, zorba olma durumu, çözüm önerileri ve farkındalık olmak üzere sekiz kategoride incelenmiştir. Şekil 2. detaylı incelendiğinde siber zorbalığa maruz kaldınız mı alt temasının altında kaldım ve kalmadım kodlarının; Mağdur olma durumu alt temasının altında maruz kalınan siber zorbalık, tepkisi ve etkisi kodlarının; Zorba olma durumu alt temasının altında ise nedeni, hissettikleri ve hackerler hakkında düşünce kodlarının yer aldığı görülmektedir. "Siber zorbalık" temasının "algılanma durumu" koduna ait olan katılımcı görüşleri aşağıda yer almaktadır:

> "*Bana göre siber zorbalık kasıtlı veya kasıtlı olmadan karşındaki insanı psikolojik olarak arkasında kıskançlık, küçük düşürme vb. farklı sebeplerden kaynaklı olarak karşıdaki kişiyi itibarsızlaştırmaktır*." (E2)

> "*İstenmeyen davranış ya da dijital ortamda gerçekleşen insanların özel hayatları da dahil olmak üzere her şeyine yapılan istemediği müdahale*." (E7)

> "*Siber zorbalık; Bir kişinin siber ortamda iradesi dışında üzerine uygulanan tahakküm. Bir kişinin iradesi dışında medya kanalları üzerinden uğramış olduğu tahakküm.*" (F6)

"Siber Zorbalık" temasının "Zorba Olma Durumu" koduna ait olan katılımcı görüşleri aşağıda yer almaktadır:

> "*Zorba açısından, kısa süreli kişisel tatmin hissediyordur. Sonrasında bunun ona yetmeyeceğini düşünüyorum. Sürekli olarak devam edeceğini düşünüyorum. Twitter'da yorum yapan insanlara bakıyorum bazı insanların hunharca her şeyin altına yorum yapıyorlar. Bir yerde siber zorbalık gördüklerinde de buna cevap veriyorlar, zorbalığı yapan sürekli devam ediyor ancak cevap veren de sürekli yanıtlıyor. Açıklama yapıyor. Kişisel tatmin, daha fazlasını yapabilmek için yüz bulma*." (D5)

> "*Aslında aşağılık kompleksine bağlı olduğunu düşünüyorum. Ulaşılabilir kişilere ulaşabildikleri için ulaşabilme yetkisi görüyorlar kendilerinde. Konuşan biri anonim bir hesapla karşısındaki kişiye ulaşılabilir olması ona istediklerini söylüyor olması kötü bir*

durum. Kendini aşağılık gördüğünden üste çıkmaya çalışıyor ve zorbalık yapıyor. Kendilerini gizledikleri için daha rahatlar." (D6)

"*Toplumsal normlardan korktukları için internet üzerinden daha gizli, kimliği belirlemeyecek şekilde oldukları için daha rahatlıkla gerçekleştiriyorlar. Bilinçli olarak yapan insanların yine cesaretleri var ancak bunların cesareti olduğunu düşünmüyorum.*" (D8)

"*Gerçekten de psikolojik rahatsızlığı olan insanlar. Kendilerini gerçek alemde ispatlayamamış, eksikliğini başka alemlerde gerçekleştirmeye çalışanlar. Sanal alemin gerçek bir dünya olduğunu, bir parçası olduğunun farkında olmayan insanlar. Belki de bunlar yaptığının bir suç unsuru olduğunu bilmeyen, kendi vicdanını rahatlatan insanlar olduğunu düşünüyorum Bununda psikolojik bir rahatsızlığa dayalı olduğunu düşünüyorum. Sanal alemde kendilerine bir alan oluşturacaklar. Aslında bu donanımlarını bilgilerini farklı alanda kullanmak yerine yanlış alanlarda kullanıyor.*" (F3)

"Siber Zorbalık" temasının "Zorba Olma Durumu" kodunun "Nedeni" alt koduna ait olan katılımcı görüşleri aşağıda yer almaktadır:

"*Ben siber zorbaları birkaç şekilde düşünüyorum. Ekonomik maddi açıdan yapanlar olduğunu düşünüyorum, kendini tatmin etmek için yapanlar, sosyal olarak kabul görmeyen kendini bu mecrada göstermek isteyen kişiler olduğunu düşünüyorum. Ekonomik nedenler, kendini tatmin etmek, toplumdan dışlanan kişilerin kendini gösterme çabası.*" (E8)

"*Kişi siber zorbalığa maruz kalmıştır, yoksunlukları vardır, aile yaşantısındaki sorunlar, arkadaşları arasında kabul görmeyen ezilen, kendini bir şey zanneden bireylerin yaptığını bu durumların neden olduğunu düşünüyorum. Genelde toplumda ezilen insanlar, yüz yüze geldiğimizde hakkını savunamayan, kendini gösteremeyen insanların sanal alemde kendini gösterme çabası olarak ortaya çıktığını düşünüyorum. Farkında değildir karşısındaki insana nasıl zarar verdiğinin. Bilinçli olarak yaptıklarını düşünmüyorum. Bilinçsizce yapanlarda çok. Mesela okulda öğrenciler birbiriyle dalga geçiyor, fiziksel özellikleri ile dalga geçiyor. Özellikle erkek öğrencilerde daha çok yapılıyor. Bilinçli yaptıklarını düşünmüyorum. Sanal ortamda yaptığından yaptığının sonucunu bilmiyor karşısındaki insanı göremiyor tepkisini bilmiyor*" (E9)

"*Psikolojik fizyolojik kaynaklı olabilir. Yapan kişinin sadece art niyetli olduğunu düşünmüyorum. Zorbalık yapan kişinin Eksik bıraktığı bir dürtüsü olabilir. Gölge olmak bazen insanın işine yarar. Casper çizgi filminde bütün ortamlarda görünmez olarak bulunması bizim hoşumuza giderdi. Gizeme ulaşma. O kişinin zorbalığı uygularken sadece çıkar elde ederim değildir, karşısındaki kişinin özel hayatıyla ilgili elde ettiği bilgi onu yetkili kişi haline getirebilir. Ben senin hakkında bu bilgilerini biliyorum. Karşısındaki kişiye karşı bir hakimiyet, ele geçirme duygusu oluyor*." (F6)

"Siber Zorbalık" temasının "Zorba Olma Durumu" kodunun "Hissettikleri" alt koduna ait olan katılımcı görüşleri aşağıda yer almaktadır:

"*Tatmin duygusu hissediyordur. Karşımdakini sindiriyorum, dediğimi yaptırıyorum diyordur*." (D2)

"*Zorbalık yapıp yakalanmadığında amaca ulaşınca bir haz duyuyor ve bunu tekrar yaşamak için tekrar tekrar yapmak isteyecektir. Yakalanma kaygısı ile o heyecanı yaşamak için tekrar tekrar yapacaktır. Değişken aralıklı pekiştireç gibi yaptıkça haz duyacak haz duydukça yapmaya devam edecek*." (E1)

"*Heyecan duyuyordur, tatmin oluyordur. Ezikliğini, çaresizliğini, haksızlığa uğradıysa bunu hissediyordur*." (E3)

"*Sanal ortamda konuşup kendini değerli hissediyor, varlığını kanıtlamış oluyor. İyi hissediyor. Ulaşamadığı bilgilere veya mal varlığına ulaşıyor olmak onu keyiflendiriyordur. Bu ahlaki gelişim seviyesi ile ilgili. Düşük seviyede olanlar doğru ile yanlış herhangi ortamda değişiklik gösterdiğini düşündüklerinden onlar bundan rahatsızlık duymaz. Mutlu hissediyorlardır*." (D8)

"Siber Zorbalık" temasının "Zorba Olma Durumu" kodunun "Hackerler Hakkında Düşünce" alt koduna ait olan katılımcı görüşleri aşağıda yer almaktadır:

"*Hackerler aslında niyetleri ne olursa olsun yaptıkları sanal zorbalık eylemi yapıyorlar. İzin olmadan girip bilgi elde etmek, yapmış olmadığı şeyi yapıyormuş gibi göstermek doğru değil. Bizim dönemimize göre artık yazılım bilgisayar kullanımı çok arttığı için günümüzde hackerler daha fazla. Ancak yasa dışı olduğunu ve kötü niyetli olduklarından zorba olduklarını düşünüyorum*." (E1)

"*Hacker bilgilerini kötüye kullanıyorsa kötü ancak devletimizin adına istihbarat açısından kullanıyorsa iyilerdir. Hackerlerin kurduğu sadece onların girdiği siteler var ve bunlar çok tehlikeli platformlar. Hackerlerin yaptığı kolay para kazanmak bu özendirilmemeli*." (E4)

"*Hackerlerin hem iyi yanları var hem kötü yanları var. Hackerler bence çok yanlış biliniyor. Olmazsa iyi olur diye düşünüyorum. Hackerlerin bazılarının yaptıkları şeyler muazzam şeyler ancak evden çıkarken evin kapısını açık bırakırsanız o eve hırsız girer. Sosyal medyada da siz gerekli önlemleri almazsanız hackerler illaki size bulaşacaktır. Önlemini almak size bağlı*." (E8)

"*Hackerlerin çok zeki olduklarını düşünüyorum. Böyle bir yeteneğim olsun ister miydim isterdim. Bilgisayardan o kadar anlamıyorum. Keşke bu yeteneklerini yasal amaçlarla kullansalar. Aslında devletimizin, gençler çok meraklı böyle şeylere. Sırf eğlencesini çocuklar bir şeyler yapmaya çalışıyor. Devletimiz bu anlamda gençlerimize bir çağrıda bulundu. Geçtiğimiz yıl içinde çok başarılı çocuklar var. Bilişim ve hackerlik anlamında yeteneği olan çocuklar devlet bünyesinde çalışsın biz bunlara eğitim verelim diye çağrıda bulundular. Bence çok güzel düşünce*." (F5)

Siber Zorbalık" temasının "Siber Zorba Davranışları" koduna ait olan katılımcı görüşleri aşağıda yer almaktadır

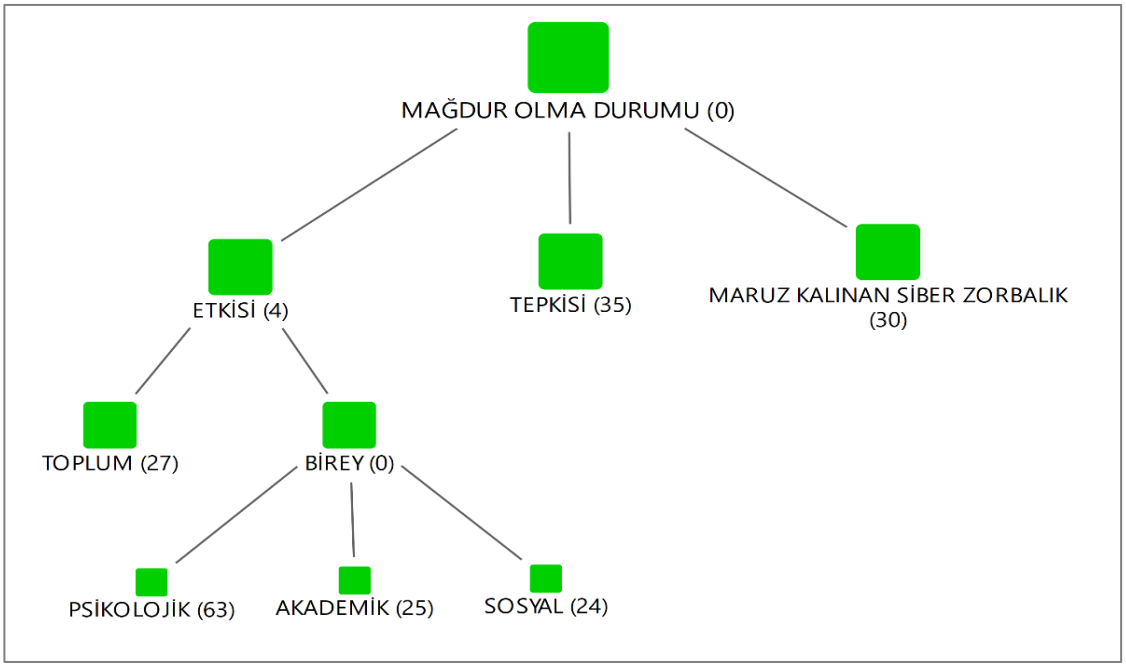
"*Siber zorbalık olarak nitelenecek davranışlar kişisel verilerin kullanılması, tanımadığımız kişiler tarafından rahatsız edici mesajlar almak, girilen siteler ve şifrelerimizin takip edilmesi örnek verilebilir. Dijital ortamlarda çocukların arasına çocuk gibi girip çocuklara ilgi duyan yetişkinlerin olması çocukları yanlış yönlendirmesi olabilir. Sanal ebeveyn olarak geçen abi ve ablalar büyük risk çünkü Çocukların cinsel eğilimlerini yönlendirme aile çatışma ortamını arttırmada da etkililer*." (E1)

Siber Zorbalık" temasının "Siber Zorbalığa Maruz Kalma Durumu" koduna ait olan katılımcı görüşlerine göre 20 katılımcının siber zorbalığa maruz kalmadığını düşündüğü ,7 katılımcının ise siber zorbalığa maruz kaldığını düşündüğünü ifade ettikleri görülmektedir. Üst grupta yer alan D üniversitesinde görev yapan öğretim elemanlarından 1 katılımcı siber zorbalığa maruz kaldığını düşündüğünü ifade ederken 9 öğretim elemanı ise siber zorbalığa maruz kalmadığını düşündüğünü ifade etmiştir. Orta grupta yer alan F üniversitesinde görev yapan öğretim elemanlarından 2 katılımcı siber zorbalığa maruz kaldığını düşündüğünü ifade ederken 5 öğretim elemanı ise siber zorbalığa maruz kalmadığını düşündüğünü ifade etmiştir. Alt grupta yer alan E üniversitesinde görev yapan öğretim elemanlarından 4 katılımcı siber zorbalığa maruz kaldığını düşündüğünü ifade ederken 6 öğretim elemanı ise siber zorbalığa maruz kalmadığını

ifade etmiştir. Şekil 3'te öğretim elemanlarının "Mağdur Olma Durumu" koduna ait olan alt kodlar yer almaktadır:

Şekil 3.

Öğretim elemanlarının siber mağdur olma durumuna ilişkin görüşlerinin hiyerarşik kod alt-kod modeli (kod bölüm temelli)



Şekil 3'te Mağdur olma durumu alt temasının kod yapısı görünmektedir. Etkisi, tepkisi ve maruz kalınan siber zorbalık başlıkları ayrıca kodlanmıştır. Katılımcılardan gelen cevaplara göre "etkisi" birey ve toplum olmak üzere ikiye ayrılmış ve bireyde psikoloji, akademik ve sosyal olmak üzere 3 yapıya ayrılmıştır. Siber Zorbalık" temasının "Mağdur Olma" kodunun "maruz kalınan Siber Zorbalık" ve "Etkisi" ve "Toplum" alt koduna ait olan katılımcı görüşleri aşağıda yer almaktadır:

> "*Siber zorbalığa maruz kaldım. Çok büyük bir olay değildi. Bilinçli olduğum için çok da etkisi altında kalmadım. Kim olduğu ne olduğu konusunda nerden geldiği niye beni bulduğu konusunda bir tedirginlik yaşadım. Ne yapacağımı bildiğim için büyük etkilemedi. Yakın zamanda telefon numaram kopyalanıp başkalarının aranması ve bunun üzerinden kanunsuz işlemlerin yapılmasını yaşadım savcılığa gidip gerekli işlemleri yaptım*." (E7)

> "*Kalsaydım eğer kişisel olarak insanlarla kavga etmekten çekinmem konuşarak anlaşmaya çalışırım. Ancak sosyal medyada kötü yorum aldığımda kalbim sıkışıyor. İstemsiz bir şekilde benim de ona cevap verme durumum olacağını düşünüyorum. Karşılık verirdim kesinlikle*." (D5)

> "*Ve bunun artarak devam edeceğini biliyorsunuz. Daha da tedirgin oluyorsunuz eliniz ayağınız dolanıyor. Her zaman başınıza gelen bir olay değil fiziki bir olay değil ki hemen reaksiyon gösteresiniz. Sebebinin neler olduğunu nasıl çözüleceği hakkında pek de bilgi sahibi değiliz. Görmediği şeyden korkar insan. Korku oluşuyor*." (F3)

> "*Toplumumuzda siber zorbalık ile ilgili bir bilinç yok. O yüzden çalışmanızı kıymetli buluyorum. Devlet nezdinde siber zorbalık ile ilgili bir birimde var. Ancak toplum nezdinde yaygınlaştırılmadığı halkımız arasında bir cehalet olduğunu düşünüyorum. Toplum olarak iyi niyetliyiz ve kandırılmaya daha çok müsaidiz. Daha çok kurbanları z kuşağı. Z kuşağı bizden daha çok teknolojiyi kullanıyorlar ancak bizden daha çok*

cahiller ve daha sonra da yaşlı kesim büyük tehlike altında. Yaşlı kesim değişime daha kapalılar, yenilikleri daha çok reddediyorlar. Siber zorbalık ile ilgili gerçekten çok büyük eğitim eksikliği var. Üniversitedeyim burada on hocadan sekizi bile bilmiyordur. Siber zorbalık ile ilgili bir eğitim almadım. Hizmet içi eğitim kapsamında vardı. Üniversite öğrencisi seviyesinde bir eğitime denk gelmedim. Bende bu konuda çok bilgisiz olduğumu düşünüyorum." (D1)

"*Toplum açısından şu an insanlarımız bu konuda çok yetersiz. Zorbalığa maruz kalma olayı çok yüksek. İnsanlarda çaresizlik bilgisizlik durumundan dolayı ne yapacaklarını bilmiyorlar. O yüzden insanlarda çaresizlik olayını çok görüyorum ne yapacaklarını bilememe durumunu. Bazen de kolluk durumlarını rahatsız etmemek içinde gitmeme eğilimi var. Belli bir yaş üstü için daha tehlikeli*." (E5)

"*Toplumsal açıdan her alanda olduğu gibi güven kaybı, huzursuzluk, tedirginlik, bir şeyleri kontrol etme kaygısı, Özellikle yaşlılarımız büyük tehlikede. Yaşlılar değil hepimiz bir şekilde maruz kalıyoruz. Emniyetten aradığını söyleyip insanları kandırmaya dolandırmaya çalışıyorlar. Birazda manevi değerleri kullanarak hepimizi bu duruma düşürmeye çalışıyorlar*." (F5)

"Siber Zorbalık" temasının "Mağdur Olma" kodunun "Birey" ve "Psikolojik", "Akademik" ve "Sosyal" alt koduna ait olan katılımcı görüşleri aşağıda yer almaktadır:

"*Siber zorbalık sosyal hayatımızı kötü etkiliyor. Mutsuz hissediyorsunuz, yaşam doyumunuzu etkiliyor, psikolojik iyi oluş düzeyi düşüyor, güvensizlik oluşuyor. Siber zorbalıkla karşılaştığınızda kaygı artıyor. Çok fazla karşılaştığınızda sürekli kaygı durumu artıyor. Psikolojik rahatsızlık meydana geliyor*." (F1)

"*Çok kötü hissettim. Kendinizi aciz hissediyorsunuz. İnsanın siber zorbalığa uğrama yaşı da çok önemli. Ben 20'li yaşların başında böyle bir zorbalığa maruz kaldım kendimi çaresiz güçsüz hissettim. Dünyadaki en kötü şey başıma gelmiş gibiydi. Şu an tabi ki böyle hissetmiyorum. İnsan kendini suçlama meyli hissediyor hiçbir suçu olmamasına rağmen. Ayrıca Fotoğrafımın başkasının elinde olma düşüncesi kötü amaçla kullanacakları düşüncesi beni çok endişelendirmişti*." (D1)

"*Korkuyorum. Zorbalığa maruz kaldığımda korku, endişe en sık hissettiğim hisler. Böyle bir şeyle karşılaştığımda ne yapmam gerektiğini aslında biliyorum. Yanlış bir mesaj ile karşılaştığımda maili açmadan silmem gerektiği cevap vermemem gerektiğini biliyorum ancak karşılaşınca korkuyorum tedirgin oluyorum*." (E4)

"*Akademik anlamda güvenliliği etkiliyor zamanı alıyor. Konsantre olmanı etkiliyor. Öğrencilerin arasında bu tarz şeyler çabuk yayılıyor. Herkes duymuş oluyor ne kadar kendini anlatmaya çalışsan da güvensizlik yaratıyor ve ders akışını etkiliyor. Normal akış bozuluyor. Aslında internet haberleşme anlamında çok güzel ancak bilginin yayılmasının kötü kullanılması hoş değil*. "(F3)

"*Öğrencilerimin bana yaptığı bir şey olursa buna maruz kalırsam dersimi seçmeyecek çok fazla öğrenci olabilir. Hocanın isminin karalanması amacıyla sosyal mecralarda onun hakkında kötü yorumlar yapılması hoca açısından sınıf yönetimini de zorlaştırır. Ön yargı oluşabilir. Diğer öğrencilerin benim hakkımdaki yorumları ile dersimi alacak öğrenciler dersimi alamayabilir. Sınıf ortamı iklimini etkileyebilir. Sınıfı toparlamak bir araya getirmek zorlaşabilir. Sınıf ortamı ne kadar huzurluysa sene sonundaki başarı da o kadar artıyor*." (D2)

"*Bir paylaşım yapacağımızda şunu da düşünüyoruz karşımızdakilerin bunu nasıl algılayacaklarını düşünüyoruz. Sosyal hayatımızı bazı durumlarda kısıtladığını düşünüyorum. Siber zorbalığa maruz kaldıktan sonraki insanlara kendini açıklama durumu, onların ne düşündüğünü düşünme durumu da kötü hissettiriyor." (D7)*

"Sosyal hayatınızı siz kendinize daha güvenli bir alan yaratmak için birçok şeyinizi kısıtlamak zorunda kalıyorsunuz. Çok kısa sürede yapılacak işleminizi güvenlik açıklarını kapatabilmek adına uzun sürüyor. Bazı işlemleri yapmaktan çekiniyorsunuz. Kimisi arama yapacakken sitenin güvenli olup olmadığını araştırıyorsunuz kimi yerlerde zorluyor bunlar. Rahatsız edici. Kısıtlayıcı bir durum oluşturuyor." (F3)

"*Sosyal hayatı etkiliyor tabi. Dijital teknolojiler her yerde. Her yaşta maruz kalabilirsiniz. Eğitimli kişilerin dahi maruz kaldığını haberlerde görüyoruz. Eğitim durumunuz, yaşınız, hayat tecrübeniz bazen çok da koruyucu olmayabiliyor. Küçük bir çocuğunda 65 yaşında bir profesörlerinde başına gelebiliyor. Her zaman her yerde karşınıza çıkabiliyor. Sosyal hayatınızda daha az fotoğraf paylaşma, dijital ortamda korunarak yaşamanıza neden oluyor. İki ucu keskin bıçak gibi aslında. Teknoloji hayatımızın vazgeçilmez alanı ancak şu an için en büyük tehditlerden biri. Dışarıda işte şuraya gitmemeliyim bu mekân da kötü insanla var başıma bir şey gelebilir, ya da gece 12'den sonra dışarı çıkmamalıyım şeklinde evde kalabilirsiniz. Gerçek yaşamda korunmak biraz daha kolay ancak siber alanda tehlikelere daha açıksınız. Bu yüzden sosyal hayatı çok etkilediğini düşünüyorum*." (F4)

"Siber Zorbalık" temasının "Korunma Yöntemleri" koduna ait olan katılımcı görüşleri aşağıda yer almaktadır:

"*Sosyal medya hesapları kullanmıyorum. Haber sitelerinde okuduğum haberlerdeki bazı kullanıcı yorumlarını okuyorum onlara katılmıyorum ancak yorum yapmıyorum. Bankacılık işlemlerimi tek bir bilgisayardan yapıyorum. Sadece okuldaki bilgisayardan banka işlemlerimi yapıyorum başka hiçbir cihazdan girmiyorum. Hiçbir mobil uygulama kullanmıyorum. Sanal kart kullanıyorum. Kişisel bilgilerimi paylaşmıyorum İsteyen siteler varsa onları tercih etmiyorum*." (E4)

"*Kişisel hesaplarımı yabancıların görmesini engelliyorum, bu tür davranışlara meyilli kişilerle her türlü iletişimden veya iletişim aracından gerçekleşebilecek etkileşimlerden kaçınıyorum*." (F1)

"*Hesaplarımı kapalı tutuyorum. Özellikle sosyal medyada bir şey paylaşmamaya çalışıyorum. Çok onur kırıcı şeyler görüyorum. Bir şey beğenmemeye bile çalışıyorum. Sosyal medyada gizli hesap kullanıyorum. Başka hesaplar kullanmıyorum. Gönderilere yorum yapmıyorum*." (E10)

"*Hayatımı çok gizemli kılmamaya çalışıyorum. Sürekli bir saklambaç oyunu oynamıyoruz, zorbalığı yapanlara cazip gelmemeye çalışıyorum. Çevremdeki insanlardan çok farklı olmadığımı, beni keşfetmek için bir gayret sarf etmemesi gerektiğini, ondan bir farkım olmadığına dair bir yaşantı sürmeye çalışıyorum. Olumsuz yorum geleceğini düşündüğüm bir paylaşım olacaksa bunun üzerinde düşünüyorum. Siber zorbalıkla ilgili bir eğitim almadım*." (F6)

"Siber Zorbalık" temasının "Çözüm Önerileri" koduna ait olan katılımcı görüşleri aşağıda yer almaktadır:

"*Siber zorbalık önlemek için kişisel anlamda bir şey yapılacağını düşünmüyorum. Zorbalığı önlemek için küçük yaşta eğitim verilmeli bilinçlendirici afişler vb. her yerde olabilir. Topluma entegrasyonları sağlanmalı ancak eğitimde ceza olduğunu da düşünüyorum. Gerçekleri düşünmemiz gerekiyor, yasal anlamda ceza verilmelidir*." (E2)

"*En başta eğitim. Eğitimi arttırmak gerekiyor. Benim de çocuğum var çocuk yaştan itibaren eğitimin verilmesi gerekiyor. Siber zorbalık nedir siber hayatta nasıl bir profil çizmesi gerektiği, nelere dikkat etmesi gerektiğine dair. Yetişkinlere de kamu spotu*

şeklinde eğitim verilebilir. Hem uygulamalı hem de görsel ve işitsel medyada verilmesi gerekir." (E5)

"*Önlenmesine ilişkin en temel görüşüm okul öncesinden başlayarak medyanın etkili, güvenli kullanımı ile ilgili eğitim verilebilir. Çocuklara yalnız olmadığına yönelik bir eğitim süreci geliştirilebilir*." (F6)

"*Tüm çocukların iyi bir çevrede iyi bir aile de büyümesi bu konuda önemli. Büyüdüklerinde suçlu bireyler olmasınlar başkalarını tehdit edecek zarar verecek bireyler olmasın. Rehabilite edilmeleri gerektiğini düşünüyorum. Özellikle bununla ilgili bakanlık kuruldu doğru bir adım olduğunu düşünüyorum. Siber zorbalığı uygulayan bireylerin mutlaka tespit edilmesi gerektiğini düşünüyorum. Önleyici rehberlik çalışmalar yapılması gerektiğini düşünüyorum. Bu konuda önce ailelerin çocuklarını dijital dünyaya ve bu dünyaya bıraktıkları ayak izleri konusunda bilgilendirmeleri gerekiyor. Denetimsiz bir şekilde çocuklarını internette dijital teknolojide bırakmamaları gerekiyor. Doğru kullanmayı öğretmeleri gerekiyor. Başkalarının haklarına nasıl saygı duyacağını haklarını nasıl koruyacağını bilmeleri gerekiyor. Okulla ilgilide ülke çapında da çalışmalar yapılmalı ve bu konuda hassasiyetle davranmaları gerekiyor. Çeşitli tedbirler almaları gerekiyor. Çünkü bu kendi halinde çözülecek bir konu olduğunu düşünmüyorum*." (F4)

"*Bence öncelikle siber zorbalığın tanıtılması ve bununla ilgili mücadeleye girişilmeli. Uygulayan insanlarda yaptıklarının siber zorbalık olduğunun farkına varsın. Bilinçli veya bilinçsiz şekilde siber zorbalık uyguluyorlar. Yaptıklarının yanlış olduğunun farkına varmaları gerekiyor bunun için ulusal bir mücadele başlatılması gerektiğini düşünüyorum*." (E7)

"Siber Zorbalık" temasının "Farkındalık" koduna ait olan katılımcı görüşleri aşağıda yer almaktadır:

"*Maalesef son yıllarda inanılmaz düzeyde siber zorbalıkta artış var ve insanlar bunları siber zorbalık olarak görmüyorlar. Yaptıklarının farkında değiller. Kişiler bu yaptıklarını kendilerinde hak olarak görmekte, yaptıklarının siber zorbalık olduğunu kabul etmemekte. İnsanlar da bu konuda bilinçsiz olduğu için farkındalık eksik*." (F2)

"*Günümüzde teknolojinin gelişmesiyle birlikte şiddetinde yönü değişmiş oluyor bunlardan biri de siber zorbalık. Bu konuda çok fazla bilgim yok ancak çevremdeki insanların maruz kalması nedeniyle biliyoruz. Şiddetin bence farklı bir boyutu. İnsanların hayatına özgürlüğüne yapılan bir tür saldırı. Normalde özellikle ilkokul ortaokullarda liselerde ergenlik döneminde daha çok zorbalık yapma birbirini ezme durumunun sosyal medya internette yapılması olarak düşünüyorum*." (E9)

"*Siber zorbalığa genellikle ortaokul ve lise çağlarındaki öğrenciler maruz kalıyor. Kendilerini nasıl korumaları gerektiğini bilmedikleri için yeterli bilinç ve dersler kapsamında çocuklara bu tip bilgilerin verilmemesi nedeniyle ne yapacaklarını bilmiyorlar. Tehdit unsurları da olabiliyor. Yaşıtları ya da kendilerinden büyük kişilerin sözlü tacizlerine de maruz kalabiliyorlar*." (D2)

4. Tartışma, Sonuç ve Öneriler

Öğretim elemanlarının bilgi güvenliği hakkındaki görüşleri, bilgi güvenliğini sağlamak için neler yaptıkları, siber zorbalık hakkındaki görüşleri, siber zorbalığa maruz kalma durumları, siber zorbalıktan korunma yöntemleri ve siber zorbalığın önlenmesine dair görüşlerini ve önerilerini almak amacıyla gerçekleştirilen görüşmeler neticesinde öğretim elemanlarının bilgi güvenliğine yönelik görüşleri incelendiğinde öğretim elemanlarının, teknik donanıma ve beceriye sahip olmasalar da bilgi güvenliğinin anlamı ve önemi konusunda bilince sahip oldukları söylenebilir. Öğretim elemanlarının verilerinin güvenliklerini sağlamak için belirttikleri önlemler arasında; güvenli parola oluşturma, cihazlarında şifre ve güvenlik yazılımı kullanma, güvenli siteleri kullanma, erişim izinlerine dikkat etme ve resmî kurumlar hariç kişisel verilerini paylaşmama görüşleri öne çıkmaktadır.

Elde edilen sonuca benzer olarak Canoğulları (2021), çalışmasında öğretmenlerin bilgi güvenliği farkındalığına yönelik görüşlerini incelemiştir. Bu çalışmasında öğretmenlerin bilgi güvenliğini net olarak ifade edemeseler de ne olduğunu bildiklerini ve orta düzeyde bilgi sahibi olduklarını belirtmiştir. Ayrıca araştırmaya katılan öğretmenlerin bilgi güvenliğine yönelik aldıkları önlemleri güvenilir internet sitelerini tercih etme, parola oluşturma, anti virüs programları kullanma ve veri paylaşmada özenli olma şeklinde belirtmiş bu önlemler de genel olarak bu tez çalışmasıyla benzerlik göstermektedir. Yine bu çalışma ile benzer olarak Kaplanoğlu (2016), farklı bölümlerde görev yapan 1355 öğretmenin katıldığı araştırmada öğretmenlerin bilgi güvenliği farkındalığını incelemiş ve öğretmenlerin bilgi güvenliği farkındalığının orta düzeyde olduğunu tespit etmiştir.

Gerçekleştirilen görüşmeler neticesinde öğretim elemanlarının bilgi güvenliğine yönelik genel bilgilerinin olduğunu ancak kendilerini koruma konusunda yeterli bilgi ve beceriye sahip olmadıkları öne çıkmaktadır. Ayrıca öğretim elemanlarının büyük bir kısmı kimlik hırsızlığına yönelik önlem alma konusunda ne yapacaklarını bilmediklerini belirtmişlerdir. Gökmen ve Akgün (2015) ve Canoğulları (2021), çalışmalarında öğretmenlerin bilgi güvenliğine yönelik kendilerini koruma konusunda yeterli bilgiye sahip olmadıklarını belirtmiştir. Bu sonuçlar elde edilen sonuçlarla benzerlik göstermektedir. Elde edilen sonuçlardan farklı olarak Yılmaz, Şahin ve Akbulut (2016), araştırmalarında öğretmenlerin veri güvenliği farkındalığının yüksek seviyede olduğunu belirtmişlerdir. Bilgi güvenliğine yönelik alınması gereken önlemler konusunda öğretim elemanları ne yapılması gerektiğini bilmedikleri ve bu konuda yetkili kurumların gerekli tedbirleri alması gerektiği yönündeki görüşler öne çıkmaktadır. Bu araştırmadaki sonuçlar alan yazında yer alan bilgilerle uyuşmaktadır (Gökmen ve Akgün, 2015; Canoğulları, 2021).

Araştırma sonucunda öğretim elemanlarının siber zorbalığa yönelik cevapları incelendiğinde siber zorbalığın günümüzde çok sık karşılaşılan rahatsız edici bir durum olduğu yönündeki görüşler öne çıkmaktadır. Öğretim elemanlarıyla yapılan görüşmeler neticesinde siber zorbalık kavramını siber alanda gerçekleştirilen zorbalık olarak tanımlayan görüş hâkimdir. Alan yazını incelendiğinde bu araştırmanın sonuçlarıyla benzer birçok çalışma mevcuttur. Tingiş (2022), çalışmasında öğretmenlerin siber zorbalık kavramını dijital zorbalık olarak belirttiklerini ifade etmiştir. Bu sonuç bu tez çalışmasıyla benzerlik göstermektedir. Cemaloğlu ve Karadağ (2019), okul müdürlerine yönelik yaptıkları çalışmada okul müdürlerinin siber zorbalık kavramını daha çok siber alanda baskı yapma şeklinde tanımladıklarını belirtmişlerdir.

Öğretim elemanlarının siber zorbalık olarak nitelendirdikleri davranışlar; sosyal medya hesabından hoşa gitmeyen mesaj ve yorumlarda bulunmak, izinsiz verileri paylaşmak, sosyal medya üzerinden dolandırıcılık yapmak, reklam amaçlı telefon çağrıları ve kısa mesajlar gönderme şeklinde öne çıkmaktadır. Araştırma bulgularıyla benzer şekilde öğretmenlerin, öğrencilerinin siber zorbalık davranışlarını tanımladığı bir araştırma da öğretmenlerin siber zorbalık olarak belirttikleri davranışlar; siber alanda izinsiz görüntü paylaşma, istenmeyen mesaj ve yorum yazma şeklinde belirtilmiştir (Tingiş, 2022).

Öğretim elemanlarına siber zorbalığa maruz kaldınız mı sorusu yöneltilmiş ve görüşme yapılan 27 öğretim elemanından 7'si siber zorbalığa maruz kaldığını belirtmiştir. Siber zorbalığa maruz kalmadığını belirten öğretim elemanlarının birçoğu çevrelerinde siber zorbalığa maruz kalan bireyler olduğunu ve bununla ilgili duydukları olayları anlatmışlardır. Araştırma sonuçları Tingiş (2022) ve Serin (2012) araştırma sonuçlarıyla benzerlik göstermektedir. Tingiş (2022), araştırmasında görüşme yaptığı öğretmenlere siber zorbalığa maruz kaldınız mı sorusunu yöneltmiş ve çoğunluğu maruz kalmadığını belirtmiştir. Araştırma sonucundan farklı olarak Metin (2017), araştırmasında öğretmenlerin çoğunluğunun siber zorbalığa maruz kaldığını belirtmiştir.

Siber zorbalığın nedenlerine yönelik öğretim elemanlarının görüşleri incelendiğinde ailevi problemlerden kaynaklı psikolojik etmenler olduğu yönünde görüşler öne çıkmaktadır. Siber zorbalığın nedenlerine yönelik çalışmalar incelendiğinde benzer sonuçlara ulaşılmıştır (Cemaloğlu ve Karadağ, 2019; Eroğlu, 2011; Çimen, 2018). Ayrıca Tingiş (2022), tarafından gerçekleştirilen araştırmada siber zorbalığın nedenlerine yönelik öğretmenlerin görüşleri alınmıştır. Görüşmeler sonucunda öğretmenler; ebeveynlerin çocukları ile yeteri kadar ilgilenmemesi, ailenin eğitim seviyesi ve ailenin ekonomik durumunun siber zorbalığa neden olduğunu belirtmiştir. Bu sonuç araştırma sonucunu desteklemektedir.

Öğretim elemanlarının siber zorbalığın etkilerine yönelik görüşleri incelendiğinde bireysel ve toplumsal olmak üzere iki tema öne çıkmaktadır. Bireysel etkileri de psikolojik, sosyal ve akademik olmak üzere üç alt temada toplanmaktadır. Öğretim elemanlarının siber zorbalığa maruz kalan bireylerin ne hissettiğine yönelik görüşleri ise genel olarak mutsuz, öfkeli ve endişe duydukları yönünde olmuştur. Ayrıca öğretim elemanlarının görüşleri incelendiğinde siber zorbalığın bireyin akademik hayatını olumsuz etkileyeceği ve sosyal ilişkilerinde de olumsuzluklara sebep olarak bireyde güvensizlik hissi oluşturacağı yönündeki görüş öne çıkmaktadır. Benzer şekilde İşçitürk ve Turan (2015), çalışmalarında öğretmen adaylarının siber zorbalığa maruz kalma durumunda en çok korktuklarını ve sinirli olduklarını belirtmişlerdir.

Öğretim elemanlarının siber zorbalığın önlenmesine yönelik görüşleri incelendiğinde genel olarak küçük yaştan itibaren siber zorbalık ile ilgili eğitim verilmesi ve okullarda bu konu hakkında çalışmalar yapılması gerektiği yönündeydi. Ayrıca atmış yaş üstü bireylere de siber zorbalık ile ilgili farkındalık eğitimleri verilmesi gerektiği birçok katılımcı tarafından ifade edilmiştir. İşçitürk ve Turan (2015), çalışmalarında öğretmen adaylarıyla siber zorbalığa yönelik görüşmeler gerçekleştirmiştir. Görüşmeler sonucunda öğretmen adaylarının siber zorbalığın önlenmesine yönelik cezalar uygulanması gerektiği, bireylerin internet kullanımlarına dikkat etmesi gerektiği ve bu konu hakkında eğitimler verilmesinin önemli olduğuna dair görüş bildirdikleri belirtilmiştir.

Araştırmadan elde edilen bulgulara göre bilgi güvenliği farkındalığı ve siber zorbalık eğilimine yönelik bu çalışma şu önerilerde bulunabilir.

Yaşanan teknolojik gelişmelerle dijitalleşmenin arttığı bu dönemde artık bütün işlemlerimizi internet ortamında gerçekleştirmekteyiz. Siber alan dediğimiz bu ortamda meydana gelecek saldırı ve tehlikelere karşı tedbirli olmak, yeterli bilgi ve beceriye sahip olarak önlem almak ancak eğitimle sağlanabilir. Bu anlamda eğitim öğretim faaliyetlerinin başında yer alan, yeni nesiller yetiştiren ve onlara rol model olan öğretmenlerimizin bilgi güvenliği ve siber zorbalığa yönelik farkındalığı önemlidir. Öğretmenlerimizin bilgi güvenliği ve siber zorbalığa yönelik bilgi sahibi olması ve bunu öğrencilerine aktarması gerekliliktir. Bu nedenle eğitim fakültesi müfredatlarına siber güvenlik ve bilgi güvenliği ile ilgili seçmeli dersler eklenmelidir. Bilgisayar ve teknik bölümlerle birlikte diğer tüm üniversite bölümlerine bilgi güvenliği ve siber zorbalığa yönelik seçmeli ders eklenebilir.

Öğretim elemanlarıyla yaptığımız görüşmelerde kendilerini kimlik hırsızlığına karşı nasıl koruyacaklarını ve siber saldırıya uğrama durumunda ne yapacaklarını bilmediklerini

belirtmişlerdir. Buradan yola çıkarak tüm kurum ve kuruluşlarda siber suçlara yönelik bir komisyon kurulabilir. Çalışanlar herhangi bir sorunla karşılaştıklarında hızlı bir şekilde ne yapacaklarına dair bilgi alabilirler. Ayrıca bu komisyonlar düzenli aralıklarla bulundukları kurumlarda zorunlu katılım sağlanmak koşuluyla siber güvenlik ve siber zorbalıkla ilgili iş ve işlemleri aksatmayacak şekilde eğitimler verebilir. Siber bilgi güvenliği ve farkındalığı hakkında kamu spotları ve sosyal sorumluluk projeleri yapılarak toplumun tüm kesimine ulaşılabilir. Bilgi güvenliği farkındalığı ve siber zorbalıkla ilgili araştırmalara kurumsal destekler verilebilir.

Öğretim elemanlarıyla yapılan görüşmeler neticesinde siber zorbalığın nedenlerine yönelik aile içi problemler ve psikolojik etmenler öne çıkmaktadır. Bu bağlamda siber zorbalık eğilimine karşı ve bilgi güvenliğinin sağlanması amacıyla aile destek birimleri oluşturulabilir. Siber zorbalığa maruz kalan bireylere yönelik ücretsiz destek hizmetleri verilebilir.

Çalışmamızda araştırma örneklemini sadece eğitim fakültesinde görev yapan öğretim elemanları oluşturmaktadır. Bu bağlamda araştırma evreni ve örneklemi değiştirilerek daha geniş kapsamlı bir çalışma ile alana katkı sunulabilir.

Etik Komite Onayı: Bu araştırma için Gazi Üniversitesi Etik Komisyonundan (10.03.2023 tarih-E.608679 sayı no) etik izin alınmıştır.

Hakem Değerlendirmesi: Dış bağımsız.

Yazar Katkıları: Yazarlar; bu makalenin araştırılması, yazarlığı ve yayımlanması için eşit düzeyde katkı sağlamışlardır.

Çıkar Çatışması: Yazarlar; bu makalenin araştırılması, yazarlığı ve yayımlanmasına ilişkin herhangi bir potansiyel çıkar çatışması beyan etmemiştir.

Finansal Destek: Yazarlar; bu makalenin araştırılması, yazarlığı ve yayımlanması için herhangi bir finansal destek almamıştır.

Yapay Zekâ Kullanımı Bildirimi: Yazarlar**;** bu makalenin araştırılması, yazarlığı ve yayımlanması için herhangi bir yapay zekâ aracından faydalanmamıştır.

Kaynakça

Aksoğan, M., Bayer, H., Gülada, M. O. ve Çelik, E. (2018). İletişim fakültesi öğrencilerinin siber güvenlik farkındalığı: İnönü Üniversitesi örneği. *Kesit Akademi Dergisi, 4*(13), 271-288. https://doi.org/10.18020/kesit.1396

Baker, S. E. ve Edwards, R. (2012). How many qualitative interviews is enough? Expert voices and early career reflections on sampling and cases in qualitative research. England:National Centre for Research Methods Review Paper.

Canoğulları, E. (2021). Öğretmenlerin bilgi güvenliği konusundaki farkındalıklarının incelenmesi. *Kalem Eğitim ve İnsan Bilimleri Dergisi*, *11*(2), 651-679. https://doi.org/10.23863/kalem.2021.219

Cemaloğlu, N. ve Karadağ, C. A. (2019). *Eğitim ve İnsani Bilimler Dergisi: Teori ve Uygulama*, *10* (20), 64-81. https://doi.org/10.58689/eibd.1385058

Çiftçi, S. ve Sakallı, H. (2016). Sınıf öğretmeni adaylarının dijital vatandaşlık düzeyleri ile siber zorbalık eğilimleri arasındaki ilişkinin incelenmesi*. Eğitim Teknolojisi Kuram ve Uygulama, 6*(2), 100-119. https://doi.org/10.17943/etku.97311

Çimen, İ. D. (2018). Ergenlerde siber zorbalık, internet aile tutumu ve aile işlevselliğinin etkisi. *Anadolu Psikiyatri Dergisi*, *19*(4), 397-404. https://doi.org/10.51982/bagimli.1020126

Deschamps, R. ve McNutt, K. (2016). Cyberbullying: What's the problem? *Canadian Public Administration, 59*(1), 45-71. https://doi.org/10.1111/capa.12159

Eminağaoğlu, M. ve 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), 01-15. https://doi.org/10.16953/deusbed.79642

Eroğlu, Y. (2011). *Koşullu öz-değer, riskli internet davranışları ve siber zorbalık/mağduriyet arasındaki ilişkinin incelenmesi.* (Yayın No. 328018) [Yüksek lisans tezi, Sakarya Üniversitesi] YÖK Ulusal Tez Merkezi. *https://doi.org/10.19126/suje.04882*

Gökmen, Ö. F. ve Akgün, Ö. E. (2015). Bilgisayar ve öğretim teknolojileri eğitimi öğretmen adaylarının bilişim güvenliği bilgilerinin çeşitli değişkenlere göre incelenmesi. *Cukurova University Faculty of Education Journal*, *44*(1), 61-84. https://doi.org/10.14812/cufej.2015.004

Gökmen, Ö. F. ve Akgün, Ö. E. (2015). Bilgisayar ve öğretim teknolojileri eğitimi öğretmen adaylarının bilişim güvenliği eğitimi verebilmeye yönelik yeterlilik algılarının incelenmesi. *İlköğretim Online*, *14*(4), 1208-1221. https://doi.org/10.17051/io.2015.04635

İşçitürk, G. B. ve Turan, E. Z. (2015). Öğretmen adaylarının siber zorba davranışlara ilişkin görüşleri. *Researcher, 3*(1), 60-68.

Kaplanoğlu, G. (2016). *Öğretmenlerin bilgi güvenliği farkındalığının incelenmesi.* (Yayın No. 450078) [Yüksek lisans tezi, Gazi Üniversitesi] YÖK Ulusal Tez Merkezi.

Mallaboyev, N. M., Sharifjanovna, Q. M., Muxammadjon, Q. ve Shukurullo, C. (2022). Informatıon securıty issues. *Conference Zone,* 241-245.

Metin, K. E. (2017). Ortaokul öğretmenlerinin siber zorbalık yaşama düzeyleri ve siber zorbalıkla başa çıkma stratejileri. *Eğitim ve Toplum Araştırmaları Dergisi, 4*(2), 33- 49. https://doi.org/10.29065/usakead.316635

Nezgitli, S. ve Gökçe Arslan, Ş. (2022). Kamu ve özel sektör için bilgi güvenliği farkındalığı üzerine bir inceleme. *Öğretim Teknolojileri ve Yaşam Boyu Öğrenme, 3*(1), 19-44. https://doi.org/10.52911/itall.1115701

Pusey, P. ve Sadera, W.A. (2011). Sibernetik, siber güvenlik ve siber güvenlik: Öğretmen adaylarının bilgisi, hazırlığı ve öğretmen eğitiminin fark yaratma ihtiyacı. *Journal of Digital Learning in Teacher Education, 28*(2), 82-88. https://doi.org/10.18074/ckuiibfd.1276923

Serin, H. (2012). *Ergenlerde siber zorbalık / siber mağduriyet yaşantıları ve bu davranışlara ilişkin öğretmen ve eğitim yöneticilerinin görüşleri*. (Yayın No. 317225) [Doktora tezi, İstanbul Üniversitesi] YÖK Ulusal Tez Merkezi. *https://doi.org/10.29065/usakead.316635*

Talib, S. (2014). *Personalising information security education.* Research Theses, University of Plymouth Faculty of Science and Technology, Malaysia, 5-14.

Tingiş, E. (2022). *Sosyal bilgiler öğretmenlerinin siber zorbalık hakkındaki görüşleri.* (Yayın No. 757893)[Yüksek lisans tezi, Akdeniz Üniversitesi] YÖK Ulusal Tez Merkezi.

Türnüklü, A. (2000). Eğitimbilim araştırmalarında etkin olarak kullanılabilecek nitel bir araştırma tekniği: Görüşme. *Kuram ve Uygulamada Eğitim Yönetimi*, *24*(24), 546-548.

Yavuz, F. (2023). Examining the relationship between teachers' digital literacy levels and personal cyber security behaviors. Fırat University Institute of Educational Sciences, Elazığ, 12-79.

Yıldırım, A. ve Şimşek, H. (2016). *Sosyal bilimlerde nitel araştırma yöntemleri.* Ankara: Seçkin Yayıncılık.

Yılmaz, E., Şahin, Y. L. ve Akbulut, Y. (2016). Öğretmenlerin dijital veri güvenliği farkındalığı. *Sakarya Üniversitesi Eğitim Fakültesi Dergisi*, *6*(2), 26-45. https://doi.org/10.19126/suje.29650

Determination of Cyber Information Security Awareness and Cyber Bullying Tendencies of Lecturers

Aysun DÜŞMEZ, MEB, ORCID ID: 0009-0002-6792-6353
Alev ORHAN, Sivas Cumhuriyet University, ORCID ID:0000-0002-8999-9329
Elif ORHAN, Gazi University, ORCID ID:0000-0002-3949-6141

Highlights

- Cyber information security awareness of education faculty lecturers.
- Instructors' views on cyberbullying.
- 27 lecturers working in the faculties of education of three different universities.

Abstract

The objective of this study is to ascertain the opinions of faculty members in the field of education regarding cyber information security awareness and the phenomenon of cyberbullying. Phenomenology design, an approach to qualitative research, was utilized in the study. A total of 27 instructors from the faculties of education at three different universities participated in the qualitative data collection process. The data were obtained through the implementation of the Interview Form on Cyberbullying and Information Security. The qualitative data was analyzed using both descriptive and content analysis with the MAXQDA Pro2020 (20.4.0) program. The following text is intended to provide a comprehensive overview of the subject matter. The findings indicate the presence of two overarching themes within the broader context of the cyber environment, namely cyberbullying and cyber information security. The following categories comprise the codes under the theme of cyberbullying: exposure to cyberbullying, cyberbully behaviors, victimization, perpetration, solution suggestions, protection methods, awareness, and perception status. The following categories comprise the codes under the theme of cyber information security: protection methods, awareness, and identity theft. The results of the research indicated that the lecturers' opinions on information security were found to be cognizant of the concept and significance of information security, despite a lack of technical equipment and skills. The prevailing perspective that cyberbullying is a pervasive phenomenon in contemporary society is given due consideration. The prevailing perspective regarding the concept of cyberbullying, as elucidated by the interviews with the lecturers, is that it constitutes bullying in cyberspace

Keywords: Information Security, Lecturers, Cyberbullying, information security awareness

İnönü University
Journal of the Faculty of Education
Vol 26, No 2, 2025
pp. 603-639
DOI
10.17679/inuefd.1565813

Article Type
Research Article

Received
12.10.2024

Accepted
27.07.2025

Suggested Citation

Düşmez, A., Orhan, A., & Orhan, E. (2025). Determining the cyber information security awareness and cyberbullying tendencies of lecturers. *İnönü University Journal of Faculty of Education*, *26*(2), 603-639. DOI: 10.17679/inuefd.1565813

This article is derived from his master's thesis accepted by Gazi University, Institute of Science and Technology, December 2023. Abstract presented as oral presentation at the 10th International Capital Science, Engineering and Applied Sciences Congress held in Ankara on October 28-30, 2023

1. Introduction

The advent of new internet technologies has rendered technology an indispensable aspect of contemporary life, facilitating individuals' daily work and precipitating transformative changes across a range of domains, including communication, online shopping, and mobile banking (Çiftçi & Sakallı, 2016). The rapid access and convenience of information afforded by the internet have led to a significant increase in the usage rate of internet technologies. This has resulted in the digitization of information and the electronic protection of data by both institutions and individuals. The capacity to store large data sets, access data instantly and from any location, and easily access databases over the network are considered among the most significant advantages of internet technologies. These developments have increased the importance of information technologies and brought the issue of information security to the forefront (Mallaboyev et al., 2022).

In the context of individual information security, the term refers to the protection, storage and access of personal data in digital environments. In the context of corporate information security, it encompasses the protection of information devices, the storage of data, and the implementation of measures to prevent the occurrence of risky activities (Eminağaoğlu & Gökşen, 2009). The use of social media allows individuals to disseminate their posts to a vast audience, even in the absence of the requisite equipment. However, the very nature of social media platforms gives rise to a multitude of negative outcomes, primarily due to their capacity to facilitate communication, data transmission to a vast audience, and information exchange. Some individuals engage in cyberbullying by exploiting these environments and perpetrate cybercrimes by defrauding others through platforms such as mobile phones, email, chat rooms, and social networking sites (Deschamps & McNutt, 2016). It is crucial for individuals to possess knowledge regarding cybersecurity and cybercrime while utilizing the Internet to safeguard themselves from the potential risks they may encounter in the digital domain (Aksoğan et al., 2018).

While it is crucial for individuals to utilize technology in a purposeful and conscious manner, closely monitoring technological advancements to safeguard their data and ensure the security of their information, it is equally important to raise awareness and equip our invaluable educators, who play a pivotal role in nurturing the next generation and serve as role models for future generations, with the knowledge and skills necessary to navigate the digital landscape securely (Canoğulları, 2021). The phenomenon of cyberbullying represents a significant challenge for young people, who are increasingly reliant on digital technologies within and beyond the educational context. This form of intimidation and harassment can have a detrimental impact on individuals across a range of domains, including psychological, sociological, physiological, and economic. Furthermore, it leaves them vulnerable to criminal victimization. In order to mitigate these negative outcomes, it is imperative to disseminate information regarding information security and to enhance awareness-raising activities on this matter (Talib, 2014).

A literature review was conducted on the subjects of cyberbullying and information security. Gökmen and Akgün (2015) examined the competencies of students in the teaching department to provide information security training. The research yielded findings indicating that the majority of pre-service teachers had not received training to ensure information security. Furthermore, the majority of these teachers lacked the competencies necessary to teach cyber information security courses. The following text is intended to provide a comprehensive overview of the subject matter. In his study on secondary school teachers, Metin (2017) sought to ascertain the extent of teachers' exposure to cyberbullying and the protective measures they employ. The study's findings indicated that a significant proportion of the sample population, specifically 95%, had experienced exposure to cyberbullying. In 2022, Tingiş conducted an investigation into the perspectives of educators concerning cyberbullying.

Teachers posit that cyberbullying constitutes a form of digital bullying, aimed at causing distress to the targeted individual. They further delineate that the unauthorized acquisition and dissemination of information constitutes a form of bullying behavior. Yavuz's (2023) study examined the participants' information security awareness and digital literacy levels. The researcher employed a multifaceted approach, utilizing a range of variables to assess these constructs among the sample group of teachers. The findings of the study indicated a positive and moderately significant relationship between the cybersecurity awareness and digital literacy levels of the teachers participating in the study. Nezgitli and Arslan's (2022) research study examined the information security awareness of individuals employed in the private sector and public institutions. The study also examined the measures and activities employed for information security in the workplace. The study's findings indicated significant differences. In their study, Pusey and Sadera (2011) examined the knowledge, awareness, and perceptions of pre-service teachers regarding their ability to teach cyber information security to their students. The findings of the research indicate that pre-service teachers possess a certain degree of knowledge in the domain of cyber information security. However, the investigation revealed a deficiency in their ability to effectively transfer this knowledge. A review of extant studies in the field revealed a paucity of research on faculty of education lecturers, despite the fact that these individuals are responsible for the education of teachers. This research was therefore deemed necessary. Studies on cybersecurity and information awareness have been carried out on teachers, prospective teachers, and university students; however, there has been a limited number of studies conducted with faculty of education lecturers.

The principal objective of this research is to ascertain the perceptions of academic staff employed at the Faculty of Education with regard to the issues of cyberbullying and information security. In addition, the research seeks to determine the extent of awareness and tendency towards cyberbullying, as well as the challenges encountered in this regard. Finally, it aims to present potential solutions to these challenges. In addition to our primary objective, we sought to address the following sub-problems, which were identified as requiring further investigation in our study.

The research is comprised of several sub-problems, which are outlined below. The lecturers working at the Faculty of Education;

What are their views on information security?

What are their perspectives on the phenomenon of cyberbullying?

2. Method

Phenomenology design, a qualitative research method, was employed in the study. The data sources for phenomenology, as outlined by Yıldırım & Şimşek (2016), are the groups that experience and can reflect upon the phenomenon under investigation. In the study, the opinions of the lecturers on information security and cyberbullying were obtained through the utilization of the 'Interview Form on Cyberbullying and Information Security', which encompassed the problems experienced on this issue and the measures to be taken.

2.1. Study Group

The study group comprises academic staff engaged in teaching and research activities within the faculties of education during the 2022-2023 academic year. The study group's research commenced with the selection of the university. At this juncture, the University Ranking by Academic Performance (URAP) 2023-2024 was consulted to ascertain the academic performance of state universities in the Central Anatolia Region that host the faculty of education. This revealed that there were 18 universities in total. The determined list was divided into three sections, designated as upper, middle, and lower, in accordance with the arithmetic mean and standard deviation. The universities that exhibited a score exceeding the arithmetic

mean by one standard deviation were identified as belonging to the upper group. Those with a score between one and minus one standard deviation were classified as belonging to the middle group, while those with a score below minus one standard deviation were designated as belonging to the lower group. (URAP) 2023-2024 ranking of state universities with a faculty of education: the maximum score was determined to be 1072, while the minimum score was determined to be 442. The standard deviation value of the list was found to be 189.47, while the arithmetic mean was calculated to be 755.76. The results of the calculations indicate that four universities are in the upper group, 11 universities are in the middle group, and three universities are in the lower group. At this juncture, the aforementioned groups were accepted as strata, thereby establishing the number of universities to be included from each group. The use of stratified sampling allows for a more representative sample of the population, thereby reducing sampling error. In order to minimize sampling error, the stratified sampling method requires a large universe to be sampled. Therefore, since the number of samples to be taken from the universe is high, homogeneous universes should be used in order to work with fewer samples (Yıldırım & Şimşek, 2016). At this juncture, one university from each of the three strata was selected. In the second stage of the sample selection process, the lecturers employed by the Faculty of Education were invited to participate in the study, ensuring maximum diversity across the sample. In order to achieve this, the maximum diversity sampling method was employed. The principal objective of this methodology is to generate a relatively modest sample size and to encapsulate the diversity of individuals who may be involved in the issue under investigation, operating at the optimal level (Yıldırım & Şimşek, 2016).

In order to ensure maximum diversity, both universities were selected from different strata, as were the lecturers working in different departments of the faculty. A total of 27 lecturers from three universities took part in the study group. The universities included in the study were assigned the codes D, E, and F. University D is situated within the upper group, and the study was conducted with the participation of ten lecturers. The lecturers who participated in the study were distributed as follows: nine were female and one was male. They were employed in the following departments: Turkish and Social Sciences Education, Mathematics and Science Education, Educational Sciences, Elementary Education, Computer Education, and Instructional Technology Education. University F is situated within the intermediate group, with seven lecturers participating in the study. The teaching staff comprised five female and two male lecturers, who were employed in the departments of Educational Sciences, Physical Education and Sports Education, Mathematics and Science Education. University E is part of the aforementioned subgroup, and 10 lecturers took part in the study. Two of the participants were female and eight were male. They were employed in the departments of Turkish and Social Sciences Education, Educational Sciences, Physical Education and Sports Education, Mathematics and Science Education.

In qualitative research, the objective is to define the existing phenomenon in such a manner that data saturation is achieved. In the present study, data saturation was reached with 27 participants, and the data collection process was consequently terminated. The fundamental principle that is employed in determining the appropriate sample size is the attainment of data saturation (Baker & Edwards, 2012).

2.2. Data Collection Instruments

A semi-structured interview form comprising 15 open-ended questions, devised by the researcher, was employed to elicit the opinions and recommendations of the lecturers on the subjects of cyberbullying and information security. A semi-structured interview allows for greater flexibility than a structured interview technique. In this interview method, the researcher prepares the interview text, including the questions they intend to pose, in advance. Nevertheless, throughout the course of the interview, the researcher is able to exert influence

over the direction of the conversation by posing additional questions, thus enabling the participant to elucidate and articulate their responses with greater precision (Türnüklü, 2000).

In the preparation of the form, the main themes of the concepts of security and cyberbullying, and the basic principles in the preparation of the interview form were taken as a basis. In order to guarantee the content validity of the form, it was subjected to an examination by three experts in the field of education and three experts in the field of language. In light of the expert feedback, the draft form was revised and finalized. The “Interview Form on Cyberbullying and Information Security” comprises a total of 15 questions.

The present study examined participant and setting confirmation, which is a sub-dimension of credibility. The participants were interviewed in a setting conducive to expressing themselves freely, and the interviews were recorded with their consent. The participants were informed that they were at liberty to disengage from the study at any time and that their records would be returned to them upon their request. In the selection of participants, maximum diversity sampling, a purposeful sampling method, was employed to ensure transferability. To ensure data diversity, a diverse sample of participants was recruited from multiple universities, various academic departments, and a range of genders.

In addition to conducting a thorough analysis of the data using the MAXQDA 2020 (20.4.0) program to ensure direct quotation, which is a sub-dimension of the credibility of the research, the researchers independently coded the data. Following the collection of independent data, the researchers convened to compare the codes and themes. They then created a data key by identifying the common codes. In addition to the triangulation of researchers, the participants' direct views were incorporated into the data reporting. At this stage, the code maps and data were presented to three educational sciences experts, and triangulation was made in the analysis of the data.

2.3. Analysing and Interpreting the Data

The opinions of the lecturers on the subjects of cyberbullying and information security were obtained through the utilization of the Interview Form on Cyberbullying and Information Security. The data obtained at the conclusion of the interviews were subjected to content analysis. The data were subjected to analysis using MAXQDA Pro 2020 (20.4.0) software. In order to prevent the loss of data resulting from content analysis, the interviews were audio recorded with the consent of the participants. The objective of audio recording the interviews was twofold: firstly, to prevent data loss and secondly, to facilitate data mining. The mean duration of the interviews was found to be 50 minutes. The audio recordings were subjected to multiple listening sessions and subsequently transferred to a digital environment, thereby enabling the retrieval of the original, unprocessed textual data. Subsequently, the coding stage was initiated, followed by the commencement of the analysis process. In order to enhance the reliability and validity of the data presented in this study, direct quotations have been provided without any interpretation. The names of three distinct universities were assigned to the codes D, E, and F, respectively. In lieu of the names of the lecturers employed at these universities, codes such as D1, E1, and F1 were utilized.

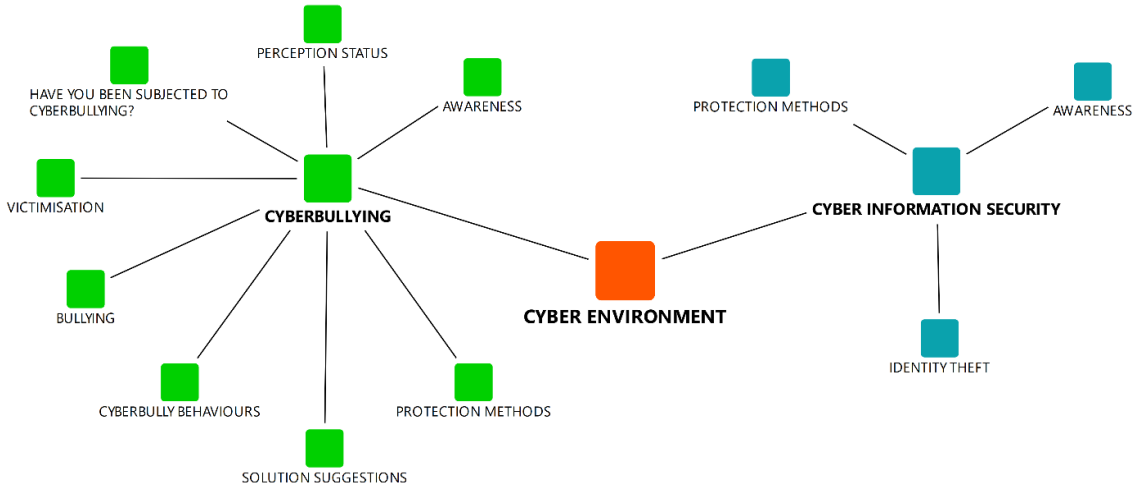
3. Findings

This section is concerned with the responses of the lecturers to the research questions “What are the views of the lecturers on information security?” and “What are the views of the lecturers on cyberbullying?”. The views of lecturers employed at three distinct universities on the subjects of cyberbullying and information security were gathered through the utilization of the Interview Form on Cyberbullying and Information Security. The data obtained from the interviews were subjected to content analysis, a method of analysis and coding that was employed to facilitate the organization and interpretation of the data. Sub-themes were derived from the identified codes, and themes were formed from the sub-themes. In alignment with the

data obtained, the following codes, sub-themes, and themes are included under the overarching theme of the cyber environment. The overarching theme of the cyber environment, along with the pertinent sub-themes and codes, is illustrated in Figure 1. These are situated within the context of the research sub-problems.

Figure 1.

A Hierarchical Model of Code Sub-Codes Based on the Views of Lecturers on Cyberbullying and Information Security



Upon examination of Figure 1, the instructors have identified two primary themes within the overarching theme of the cyber environment: cyberbullying and cyber information security. The subject of cyberbullying is addressed under the following headings: exposure to cyberbullying, cyberbully behaviors, victimization, bullying, solution suggestions, protection methods, awareness, and perception status. The theme of cyber information security is similarly explored under the following headings: protection methods, awareness, and identity theft. The participants' opinions that have been categorized as belonging to the "Awareness" code under the "Information Security" theme of the "Cyber Environment" main theme are presented below.

> *"There are compulsory cyber information security training seminars organized by our university, I attend them, consisting of 5-6 courses. I pay attention to some warnings on social media or on the internet. I pay attention to them because I am an active user. There are also aspects of cyberbullying that I do not think about, I look at it more from my own point of view. There are also different situations. These trainings were productive for me. Awareness has been raised, and I act more carefully. I think the training is sufficient." (F7)*

> *"It brings people closer to paranoia. There are programs that follow what people do and where they go. Even when you go on the internet, everything you do is tracked with a virus stuck in an unexpected email. According to them, your computer becomes a ghost computer. No matter what you do, you cannot get rid of it. They follow everything you do on the internet and your steps." (D2)*

The following section presents the participants' opinions pertaining to the "Identity Theft" code, which falls under the "Information Security" theme of the "Cyber Environment" main theme.

> *"Everywhere we go shopping, we give identity etc., information. This is risky. I cannot take a precaution as a citizen, our state needs to take a precaution. I think institutions and the private sector should have a situation such as not requesting*

some information and not archiving it. We use our identity address information even in shopping. This is very risky, I think our state should make a regulation on this issue." (E7)

"I don't think that much precaution will be taken against identity theft. We have contact etc., information everywhere. I have a web page where I have my name and address. Until two years ago, the school website had my mobile phone number, but I deleted it two years ago. I enter my ID number everywhere, we share our personal data. I don't think any measures can be taken against identity theft. There are people who hack into the grading system of students and change their grades. They hack the system and change the grades. People use their information for their own interests." (E3)

The following section presents the participant opinions belonging to the "Protection Methods" code under the "Information Security" theme of the main theme of "Cyber Environment."

"I don't give my ID number anywhere, I share information where I am sure of its reliability. When I shop with a card, I don't save card information. I don't save my passwords. Using a virtual card is the safest. I do not save information on my phone." (E4)

"I prefer not to connect to the internet from open networks to protect my privacy. I do not connect to the internet from the networks of municipalities, cafes, etc. I use the secure internet at home and at school. I do not share my personal data and pictures. I pay attention to cookies on sites. I do not activate the microphone feature and camera feature." (E10)

The overarching theme of cyberbullying, along with its constituent sub-themes and codes, is illustrated in Figure 2.

Figure 2.

A Hierarchical Model of Code-Based Sub-Codes, Which Represents the Views of Lecturers on the Phenomenon of Cyberbullying.

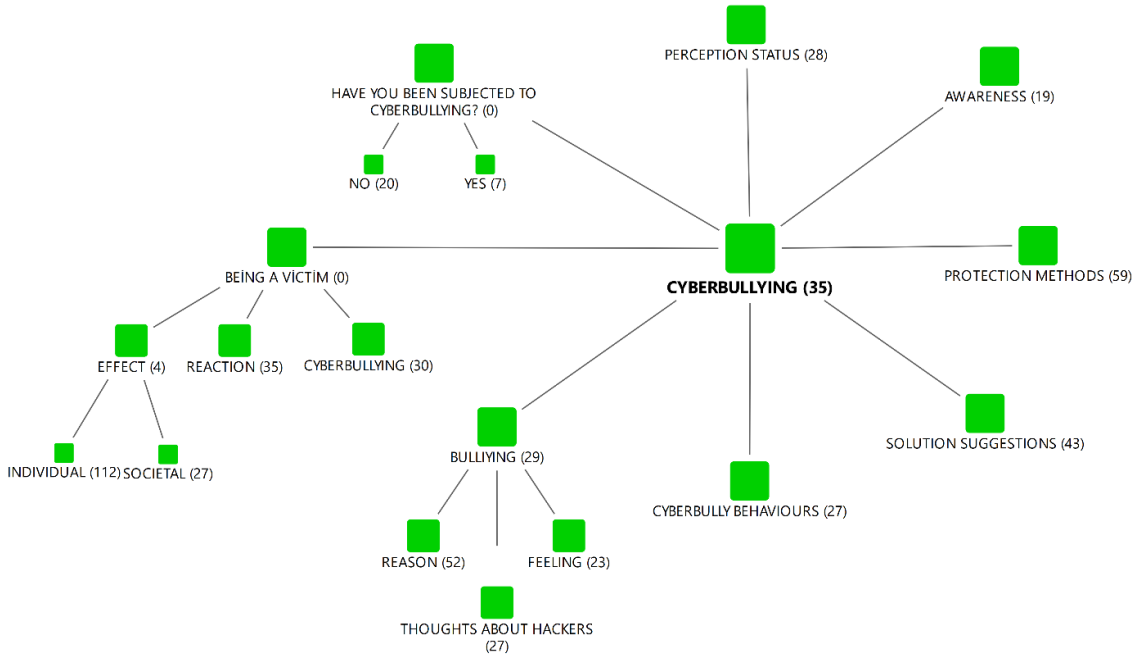


Figure 2 presents an examination of the sub-themes associated with the theme of cyberbullying, organized into eight categories: exposure to cyberbullying, protection methods, cyberbully behaviors, perception status, victim status, bully status, solution suggestions and awareness. Upon closer examination of Figure 2, it becomes evident that the sub-theme "Have you been exposed to cyberbullying?" is comprised of two distinct codes: "I have been exposed to cyberbullying" and "I have not been exposed to cyberbullying." The sub-theme of “being a victim” comprises the following codes: “cyberbullying, reaction and effect”. The sub-theme of “being a bully” comprises the following codes: “reason, feelings and thoughts about hackers”. The participant opinions pertaining to the “Perception Status” code within the “Cyberbullying” theme are presented below.

> *“In my opinion, cyberbullying is to discredit the other person psychologically, intentionally or unintentionally, due to different reasons such as jealousy, humiliation, etc.” (E2)*

> *“Unwanted behavior or unwanted intervention in everything, including the private lives of people in the digital environment.” (E7)*

> *“Cyberbullying; domination of a person against his/her will in the cyber environment. The domination of a person against his/her will through media channels.” (F6)*

The following section presents the participant opinions pertaining to the “Bully Status” code within the “Cyberbullying” theme.

> *“From the bully’s point of view: He feels a short-term personal satisfaction. I think it will not be enough for him afterwards. I think it will continue continuously. I look at the people who comment on Twitter, some people comment under everything. When they see cyberbullying somewhere, they respond to it, the bully continues to bully, but the respondent is constantly responding. They make explanations. Personal satisfaction, finding a face to do more.” (D5)*

“Actually, I think it is due to an inferiority complex. They see themselves as having the authority to reach people because they can reach people who are reachable. It is a bad situation when a speaker can reach the other person with an anonymous account and tell them what they want. Since they see themselves as inferior, they try to get on top and bully. They are more comfortable because they hide themselves.” (D6)

“Because they are afraid of social norms, they do it more easily over the internet because it is more hidden and in a way that does not identify them. People who do it consciously still have courage, but I don't think they have courage.” (D8)

“People who are really psychologically disturbed. People who have not been able to prove themselves in the real world and try to realize their deficiency in other worlds. People who do not realize that the virtual world is a real world, a part of it. Perhaps these are people who do not know that what they are doing is a criminal offence, I think they are people who relieve their own conscience. I think this is based on a psychological disorder. They will create a space for themselves in the virtual world. In fact, instead of using their knowledge in different fields, they use it in wrong fields.” (F3)

The following section presents the participant opinions pertaining to the “Reason” sub-code of the “Bully Status” code, which falls under the “Cyberbullying” theme.

“I think of cyberbullies in several ways. I think there are those who do it for economic and material reasons, those who do it for self-satisfaction, and those who want to show themselves in this medium who are not socially accepted. Economic reasons, self-satisfaction, and the effort of people who are excluded from society to show themselves.” (E8)

“The person has been subjected to cyberbullying, has deprivations, problems in family life, problems in family life, I think these situations are caused by individuals who are not accepted among their friends, who are oppressed, who think they are something. In general, I think that people who are oppressed in society, people who cannot defend their rights when we come face to face, people who cannot show themselves, emerge as an effort to show themselves in the virtual world. He is not aware of how he harms the other person. I don’t think they do it consciously. There are many who do it unconsciously. For example, at school, students make fun of each other, make fun of their physical characteristics. It is done more especially by male students. I don’t think they do it consciously. Since they do it in a virtual environment, they don’t know the consequences of what they do, they can’t see the person in front of them, they don’t know their reaction.” (E9)

“It may be psychological or physiological. I don't think the person who does it is only malicious. The person who bullies may have an impulse that they are missing. Being a shadow is sometimes useful. In the Casper cartoon, we liked the fact that he was invisible in all environments. Access to mystery. It is not only about gaining benefits while applying bullying, but the information he/she obtains about the other person's private life can make him/her an authorized person. I know this information about you. There is a sense of dominance, of taking over the other person.” (F6)

The following section presents the participant opinions belonging to the "Feelings" sub-code of the "Bully Status" code of the "Cyberbullying" theme.

The following section presents the participant opinions pertaining to the "Feelings" subcode of the "Bully Status" code within the "Cyberbullying" theme. “He feels a

sense of satisfaction. I am intimidating the other person, I am making them do what I say." (D2)

"When they bully and are not caught, they feel a sense of pleasure when they achieve the goal and they will want to do it again and again to experience the feeling of satisfaction. He will do it again and again to experience that excitement with the anxiety of getting caught. Like a variable intermittent reinforcer, he will feel pleasure as he does it and will continue to do it as he feels pleasure." (E1)

"He feels excitement, satisfaction. He feels his loser, helplessness, if he has been wronged." (E3)

"By talking online, he feels valuable, he proves his existence. He feels good. It is probably a pleasure for him to access information or assets that he cannot reach. This is related to the level of moral development. Those at a low level do not feel uncomfortable because they think that right and wrong change in any environment. They feel happy." (D8)

The following section presents the participant opinions pertaining to the sub-code "Thoughts about Hackers" of the "Bully Status" code within the "Cyberbullying" theme.

"Hackers are actually committing an act of cyberbullying, regardless of their intentions. It is not right to enter and obtain information without permission, to show what they have not done as if they have done it. There are more hackers today because the use of software and computers has increased a lot compared to our era. However, I think they are illegal and they are bullies because they are malicious." (E1)

"Hackers are bad if they misuse their information, but they are good if they use it for intelligence on behalf of our state. There are sites set up by hackers that only they can access and these are very dangerous platforms. What hackers do is to earn easy money and this should not be encouraged." (E4)

"Hackers have both good and bad sides. I think hackers are very misunderstood. I think it would be good if they weren't. Some of the things that hackers do are tremendous, but if you leave the door open when you leave the house, a thief will enter that house. If you do not take the necessary precautions on social media, hackers will infect you. It is up to you to take precautions." (E8)

"I think hackers are very smart. I wish I had such a talent. I don't know that much about computers. I wish they would use their skills for legal purposes. Actually, our state, young people are very curious about such things. Just for fun, children are trying to do something. Our state has made a call to our youth in this sense. There are very successful children in the past year. They called for children with skills in informatics and hacking to work for the state and we should give them training. I think this is a very good idea." (F5)

The following are the participant opinions belonging to the "Cyber Bully Behaviors" code of the "Cyber Bullying" theme:

"The behaviors that can be described as cyberbullying are the use of personal data, receiving disturbing messages from people we do not know, monitoring the sites we access and our passwords. In digital environments, the fact that there are adults who enter between children like children and are interested in children may mislead children. Big brothers and sisters who pass as virtual parents are a great risk because they are also effective in directing children's sexual tendencies and increasing the family conflict environment." (E1)

A total of 20 participants indicated that they had not been exposed to cyberbullying, while 7 participants stated that they had been exposed to such behavior. These findings are in line with the “Exposure to Cyberbullying” code of the “Cyberbullying” theme. Among the lecturers employed at D University in the upper group, one participant indicated that they believed they had been subjected to cyberbullying, whereas nine lecturers stated that they did not consider themselves to have been affected by such behavior. Among the lecturers employed at F University, two participants indicated that they believed they had been subjected to cyberbullying, while five stated that they did not believe they had been exposed to such behavior. Among the lecturers employed at the E University in the lower group, four participants indicated that they believed they had been subjected to cyberbullying, while six lecturers stated that they had not been exposed to such behavior. Figure 3 illustrates the sub-codes associated with the “Victimization Status” code for academic staff.

Figure 3.

This study employs a Hierarchical code-subcode model of faculty members’ views on cyber victimization (code section based)

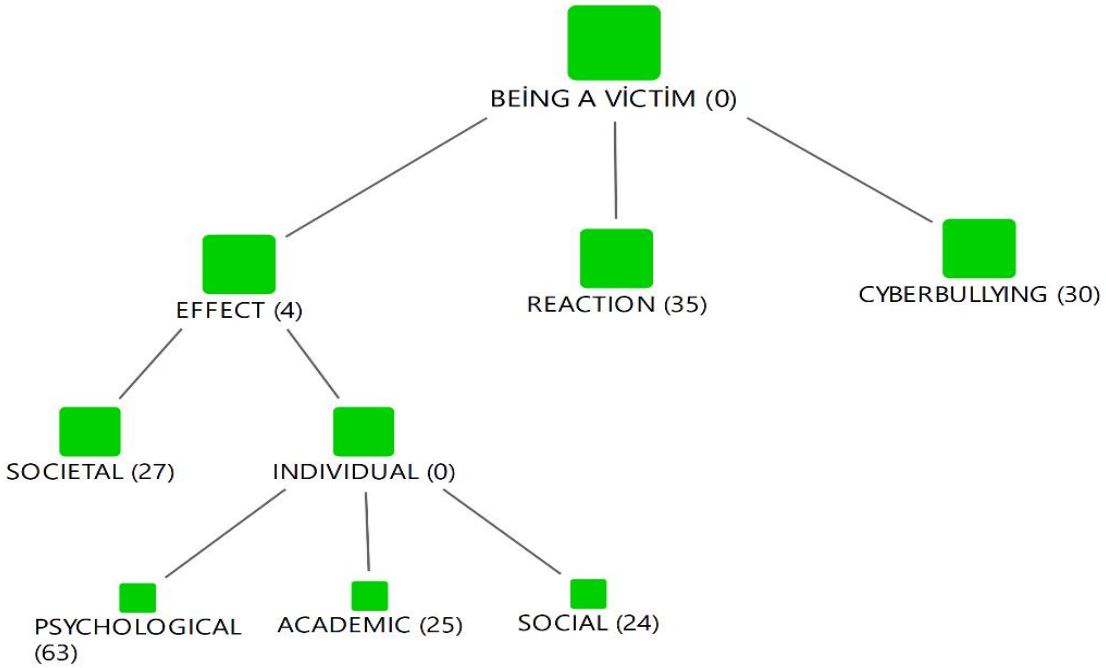


Figure 3 illustrates the code structure of the sub-theme of victimization. The titles pertaining to impact, reaction, and cyberbullying were categorized as discrete entities. The responses indicated that the "effect" could be classified into two categories: individual and societal. Additionally, the individual could be further delineated into three structural components: psychological, academic, and social.

The opinions of participants pertaining to the sub-code of “Being a Victim” within the overarching theme of “Cyberbullying” are presented below. Participants’ opinions regarding the “Cyberbullying Exposure”, “Effect”, and “Societal” subcodes of the “Becoming a Victim” code of the “Cyberbullying” theme are given below:

> *“I was exposed to cyberbullying. It was not a big event. I was not under the influence because I was conscious. I was uneasy about who and what it was, where it came from, and why it found me. It did not have a big effect because I knew what to do. I recently experienced that my phone number was copied, and others were called and illegal transactions were made through it, and I went to the prosecutor’s office and took the necessary actions.” (E7)*

"If I stayed, I personally do not hesitate to fight with people, I try to get along by talking. However, when I receive bad comments on social media, my heart gets stuck. I think I would involuntarily respond to it. I would definitely respond back." (D5)

"And you know that this will continue to increase. You are even more anxious, your hands and feet are tangled. It is not an event that happens to you all the time, it is not a physical event so that you can react immediately. We do not have much information about what the cause is and how to solve it. People are afraid of what they cannot see. Fear arises." (F3)

"There is no awareness about cyberbullying in our society. That is why I find your work valuable. There is a unit on cyberbullying in the state. However, I think there is ignorance among our people that it is not widespread in the society. As a society, we have good intentions and we are more susceptible to being deceived. Generation Z are more victims. Generation Z uses technology more than us, but they are more ignorant than us and then the elderly are in great danger. Older people are more closed to change, they reject innovations more. There is a really big lack of education about cyberbullying. I am at a university where eight out of ten professors don't even know. I did not receive any training on cyberbullying. It was part of in-service training. I did not come across a training at the university student level. I think I am very ignorant about this issue." (D1)

"In terms of society, our people are very inadequate in this regard. The incidence of bullying is very high. People do not know what to do because of helplessness and ignorance. That's why I see a lot of helplessness in people, not knowing what to do. Sometimes there is a tendency not to go in order not to disturb law enforcement. It is more dangerous for people above a certain age." (E5)

"As in all areas of society, loss of trust, restlessness, uneasiness, anxiety, anxiety to control things, especially our elderly are in great danger. Not the elderly, we are all exposed in one way or another. They say that they are calling from the police and trying to deceive and defraud people. They try to put us all in this situation by using spiritual values." (F5).

The opinions expressed by participants pertaining to the "Individual", "Psychological", "Academic", and "Social" sub-codes of the "Being a Victim" code within the "Cyberbullying" theme are presented below.

"Cyberbullying affects our social life badly. You feel unhappy, it affects your life satisfaction, the psychological well-being level decreases, insecurity occurs. Anxiety increases when you encounter cyberbullying. When you encounter too much, anxiety increases constantly. Psychological discomfort occurs." (F1)

"I felt very bad. You feel helpless. The age at which a person is cyberbullied is also very important. I was subjected to such bullying in my early 20s, and I felt helpless and powerless. It was like the worst thing in the world had happened to me. Now, of course, I don't feel like that. People feel the tendency to blame themselves, even though they have no guilt. In addition, the thought of my photo being in someone else's hands and the thought that they would use it for bad purposes worried me a lot." (D1)

"Fear and anxiety are the feelings I feel most often when I am exposed to bullying. I actually know what I should do when I encounter such a thing. When I encounter a wrong message, I know that I should delete the e-mail without opening it, but when I encounter it, I get scared and anxious." (E4)

"It affects academic safety, it takes time. It affects your concentration. Such things spread quickly among students. Everyone has heard about it and no matter how much you try to explain yourself, it creates insecurity and affects the flow of the lesson. The normal flow is disrupted. Actually, the internet is very good in terms of communication, but it is not nice to misuse the dissemination of information." (F3)

"If my students do something to me, if I am exposed to this, there may be many students who will not choose my course. Making bad comments about the instructor on social media in order to defame his/her name would also make classroom management difficult for the instructor. Prejudice may occur. Students who will take my course may not be able to take my course because of other students' comments about me. It may affect the classroom climate. It can be difficult to bring the class together. The more peaceful the classroom environment is, the higher the success at the end of the year." (D2)

"When we make a post, we also think about how others will perceive it. I think it restricts our social life in some cases. The situation of explaining yourself to people after being subjected to cyberbullying and thinking about what they think makes you feel bad." (D7)

"You have to restrict many things in your social life to create a safer space for yourself. It takes a long time to close security gaps in a very short time. You hesitate to do some transactions. Some of you are searching whether the site is safe or not when you are going to make a search, and in some places they are difficult. It is uncomfortable. It creates a restrictive situation." (F3)

"Of course it affects social life. Digital technologies are everywhere. You can be exposed at any age. We see in the news that even educated people are exposed. Your education, age, life experience may sometimes not be very protective. It can happen to a small child and a 65-year-old professor. You can always come across everywhere. Sharing fewer photos in your social life causes you to live protected in the digital environment. It's like a double-edged sword. Technology is an indispensable part of our lives, but it is one of the biggest threats for now. I should not go to this place, this place has bad people, something may happen to me, or I should not go out after 12 o'clock at night, you can stay at home. It is a little easier to be protected in real life, but you are more open to dangers in cyberspace. Therefore, I think it affects social life a lot." (F4)

The following section presents the participants' opinions pertaining to the "Protection Methods" code within the "Cyberbullying" theme.

"I don't use social media accounts. I read some user comments in the news I read on news sites. I don't agree with them, but I don't comment. I do my banking transactions from a single computer. I only do my banking transactions from the computer at school, I don't access it from any other device. I don't use any mobile applications. I use a virtual card. I don't share my personal information. If there are sites that ask for it, I don't prefer them." (E4)

"I prevent strangers from seeing my personal accounts, I avoid any kind of communication or interaction with people who are prone to such behavior." (F1)

"I keep my accounts closed. I try not to share anything especially on social media. I see very insulting things. I even try not to like anything. I use a secret account on social media. I don't use other accounts. I don't comment on posts." (E10)

"I try not to make my life too mysterious. We are not constantly playing a game of hide and seek. I try not to be attractive to bullies. I try to lead a life that I am not

very different from the people around me, that they should not make an effort to discover me, that I am no different from them. If there will be a post that I think will receive negative comments, I think about it. I have not received any training on cyberbullying." (F6)

The following section presents the participants' opinions pertaining to the "Solution Suggestions" code within the "Cyberbullying" theme.

"I don't think anything can be done personally to prevent cyberbullying. In order to prevent bullying, education should be given at a young age, awareness-raising posters, etc., can be everywhere. They should be integrated into society, but I also think that there is punishment in education. We need to think about the facts, punishment should be given in the legal sense." (E2)

"First and foremost is education. We need to increase education. I also have a child, and education should be given from a young age. What is cyberbullying, how to draw a profile in cyber life, what to pay attention to. Adults can also be trained in the form of public service announcements. It should be given both practically and in audio-visual media." (E5)

"My most basic view on prevention is that training on effective and safe use of the media can be given starting from pre-school. An education process can be developed to show children that they are not alone." (F6)

"It is important for all children to grow up in a good environment in a good family. When they grow up, they should not be criminals; they should not be individuals who will threaten others and harm others. I think that they should be rehabilitated. I think it is the right step, especially when the ministry was established. I think that individuals who practice cyberbullying must be identified. I think that preventive guidance studies should be conducted. In this regard, families should first inform their children about the digital world and the footprints they leave in this world. They should not leave their children in digital technology on the internet without supervision. They need to teach them to use it correctly. They need to know how to respect the rights of others and how to protect their rights. Studies should be conducted nationwide in relation to the school, and they should act sensitively in this regard. They need to take various measures. Because I don't think this is an issue that can be solved on its own." (F4)

"I think first of all, cyberbullying should be introduced and fought against. People who practice it should realize that what they are doing is cyberbullying. They practice cyberbullying consciously or unconsciously. They need to realize that what they are doing is wrong, and I think a national struggle should be launched for this." (E7)

The following section presents the participants' opinions that have been coded as belonging to the "Awareness" category within the "Cyberbullying" theme.

"Unfortunately, there has been an incredible increase in cyberbullying in recent years, and people don't see it as cyberbullying. They are not aware of what they are doing. People see what they do as their right and do not accept that what they do is cyberbullying. Awareness is lacking because people are also unconscious about this issue." (F2)

"Today, with the development of technology, the direction of violence has changed, and one of these is cyberbullying. I don't know much about it, but we know it because people around me are exposed to it. I think it is a different dimension of violence. It is a kind of attack on people's life and freedom. Normally, I think that

bullying and crushing each other, especially in primary, secondary and high schools during adolescence, is done on social media on the internet." (E9)

"Cyberbullying is usually experienced by middle and high school students. They don't know what to do because they don't know how to protect themselves and they don't know what to do because there is not enough awareness and such information is not given to children within the scope of lessons. There can also be threats. They may also be subjected to verbal harassment by their peers or older people." (D2)

4. Discussion, Conclusion, and Recommendations

Discuss The interviews conducted to obtain the opinions and suggestions of the lecturers about information security, the measures they take to ensure information security, their views on cyberbullying, their exposure to cyberbullying, the methods they use to protect themselves from cyberbullying and the ways in which they prevent it, indicate that the lecturers are aware of the significance and value of information security, despite lacking the requisite technical equipment and skills. In order to guarantee the security of their data, the lecturers have identified a number of measures, including the creation of secure passwords, the utilization of passwords and security software on their devices, the use of secure websites, the exercise of caution with regard to access permissions and the avoidance of the sharing of personal data with non-official institutions.

In a similar vein, Canoğulları (2021) examined teachers' perspectives on information security awareness in his study. In his study, he asserted that although teachers were unable to articulate information security in a clear manner, they possessed a fundamental understanding of the concept and demonstrated a moderate level of knowledge. Furthermore, the measures employed by the educators involved in the investigation to ensure information security were outlined as including the utilization of reliable online resources, the generation of passwords, the deployment of anti-virus software, and the exercise of caution when disseminating data. These precautions are largely analogous to those prescribed by this thesis study. Similarly, Kaplanoğlu (2016) investigated the information security awareness of teachers in a study involving 1,355 educators from diverse departments. The findings indicated that the information security awareness of teachers was at a medium level.

The interviews revealed that the lecturers possess a general understanding of information security, yet they lack the requisite knowledge and skills to safeguard their own digital security. Furthermore, the majority of the lecturers indicated that they lacked the knowledge required to implement measures to combat identity theft. In their respective studies, Gökmen and Akgün (2015) and Canoğulları (2021) have asserted that educators lack the requisite knowledge to safeguard themselves against information security threats. The results obtained are comparable to those previously documented. In contrast with the findings of the present study, Yılmaz, Şahin, and Akbulut (2016) asserted in their investigation that educators demonstrate a high level of awareness regarding data security. In regard to the measures to be taken for information security, the opinions that the lecturers are uncertain as to the appropriate course of action and that the authorized institutions should assume responsibility for implementing the necessary measures prevail. The findings of this study are consistent with the existing literature on the subject (Gökmen & Akgün, 2015; Canoğulları, 2021).

The findings of the research indicate that, when the responses of the lecturers to questions about cyberbullying are analyzed, the view that cyberbullying is a significant and prevalent issue in the present day emerges as a prominent theme. The interviews with the lecturers have led to the conclusion that the concept of cyberbullying can be defined as bullying in cyberspace. A review of the literature reveals numerous studies that yield comparable results to those of this particular study. In his study (2022), Tingiş asserted that educators equated the phenomenon of cyberbullying with the broader concept of digital bullying. The outcome of this study is

comparable to that of our previous investigation. In their study on school principals (2019), Cemaloğlu and Karadağ defined cyberbullying as "pressurizing in cyberspace."

The behaviors that the lecturers identified as cyberbullying were as follows: the posting of unkind messages and comments on social media accounts; the sharing of unauthorized data; the perpetration of fraud on social media; and the sending of phone calls and text messages for advertising purposes. The results of the present study are consistent with those of a previous investigation in which teachers were asked to define the cyberbullying behaviors of their students. The behaviors that teachers identified as cyberbullying were sharing images in cyberspace without permission, writing unwanted messages and comments (Tingiş, 2022).

The lecturers were queried as to whether they had been subjected to cyberbullying. Seven of the 27 lecturers interviewed indicated that they had been affected by such behavior. The majority of lecturers who indicated that they had not been exposed to cyberbullying reported that there were individuals in their immediate vicinity who had been affected by such incidents. These individuals had shared their experiences with the lecturers. The findings of the present study align with those of previous research conducted by Tingiş (2022) and Serin (2012). In his study, Tingiş (2022) inquired of the teachers he interviewed whether they had been exposed to cyberbullying. The majority of respondents indicated that they had not been exposed to such incidents. In contrast with the findings of the research, Metin (2017) asserted that the majority of teachers had been exposed to cyberbullying.

A review of the literature reveals that the majority of lecturers believe that psychological factors, often rooted in family problems, are the primary causes of cyberbullying. A review of the literature on the causes of cyberbullying revealed a similar set of findings (Cemaloğlu & Karadağ, 2019; Eroğlu, 2011; Çimen, 2018). Furthermore, the study conducted by Tingiş (2022) investigated the opinions of teachers regarding the causes of cyberbullying. The interviews revealed that teachers attributed the occurrence of cyberbullying to three key factors: insufficient parental interest in their children, the educational level, and economic situation of the family. This outcome is in accordance with the findings of the research project.

A thematic analysis of the opinions expressed by lecturers on the effects of cyberbullying reveals two key themes: individual and social. The individual effects are grouped into three sub-themes: psychological, social, and academic. The lecturers' opinions regarding the emotional states of individuals who have been subjected to cyberbullying were predominantly characterized by feelings of distress, anger, and anxiety. Furthermore, an analysis of the opinions expressed by the lecturers reveals a consensus that cyberbullying has a detrimental impact on an individual’s academic performance, social relationships, and sense of security. Similarly, İşçitürk and Turan (2015) asserted in their study that prospective teachers were most concerned and distressed in the event of being subjected to cyberbullying.

In examining the opinions of the lecturers on the prevention of cyberbullying, it was found that there was a consensus that education about cyberbullying should be provided from an early age and that studies should be conducted on this subject in schools. Furthermore, numerous participants asserted that individuals aged 60 and above should be provided with awareness training on cyberbullying. Furthermore, they argue that information about cyberbullying should be integrated into the curriculum of educational institutions. In their study, İşçitürk and Turan (2015) employed the use of interviews with pre-service teachers to gain insight into their perceptions of cyberbullying. The interviews revealed that prospective teachers believe that penalties should be imposed to deter cyberbullying, that individuals should exercise caution in their online activities, and that training programs on this topic are essential.

The findings of the research allow for the formulation of the following suggestions regarding information security awareness and cyberbullying tendencies.In the current era of accelerated digital transformation, driven by technological advancements, individuals and

businesses are increasingly reliant on the internet for all their transactional needs. In the context of the digital realm, known as "cyberspace," it is imperative to exercise caution and vigilance against potential threats and hazards. The acquisition of pertinent knowledge and the cultivation of essential skills are paramount in this endeavor. These objectives can be best achieved through a comprehensive educational framework. In this regard, the awareness of our teachers, who are at the forefront of educational activities, who raise new generations and serve as role models for them, regarding information security and cyberbullying is imperative. It is imperative that educators possess a firm grasp of the principles of information security and the dynamics of cyberbullying, and subsequently impart this knowledge to their students. Consequently, it is imperative that faculties of education incorporate elective courses on cyber and information security into their curricula. The integration of an elective course on information security and cyberbullying into the existing university curriculum is a potential solution. This course could be offered not only in computer and technical departments but also in other relevant fields. In the course of our interviews with lecturers, it was revealed that they lacked the necessary knowledge to protect themselves against identity theft and were uncertain of the appropriate course of action to take in the event of a cyberattack. Consequently, the establishment of a commission on cybercrime within all institutions and organizations is recommended. In the event that employees encounter any problems, they are able to access pertinent information in a timely manner. Furthermore, these commissions have the capacity to deliver training on cybersecurity and cyberbullying at regular intervals, without causing disruption to ongoing work and operations related to these issues, provided that mandatory participation is guaranteed in the institutions where they are situated.

Public service announcements and social responsibility projects on cyber information security and awareness can be organized to reach all segments of society. Institutional support is available for research on the subjects of information security awareness and cyberbullying.In light of the interviews conducted with the instructors, family problems and psychological factors emerge as primary factors contributing to instances of cyberbullying. In this context, the establishment of family support units has been proposed as a strategy to address cyberbullying tendencies and to ensure information security. Free support services are available for individuals exposed to cyberbullying.In the present study, the research sample consisted exclusively of academic staff members employed within the faculty of education. In this context, the research population and sample can be modified to facilitate the development of a more comprehensive study that contributes to the field.

Ethics Committee Approval: Ethical permission was obtained from Gazi University Ethics Commission (date 10.03.2023- number E.608679) for this study.

Peer review: Externally peer-reviewed.

Author Contributions: The authors contributed equally to the research, authorship, and publication of this article.

Conflict of Interest: The authors declare no potential conflicts of interest related to the research, authorship, and publication of this article.

Financial Disclosure: The authors have received no financial support for the research, authorship, and publication of this article.

Notice of Use of Artificial Intelligence: The author(s) did not utilize any artificial intelligence tool(s) for the research, authorship, and publication of this article.

References

Aksoğan, M., Bayer, H., Gülada, M. O., & Çelik, E. (2018). Cyber security awareness of communication faculty students: The case of İnönü University. Kesit Academy Journal, 4(13), 271-288. https://doi.org/10.18020/kesit.1396

Baker, S. E., & Edwards, R. (2012). How many qualitative interviews is enough? Expert voices and early career reflections on sampling and cases in qualitative research. England: National Centre for Research Methods Review Paper.

Canoğulları, E. (2021). Examining teachers" awareness of information security. *Kalem Journal of Education and Human Sciences*, *11*(2), 651-679. https://doi.org/10.23863/kalem.2021.219

Cemaloğlu, N., & Karadağ, C. A. (2019). School principals' views on cyberbullying. *Journal of Education and Human Sciences: Theory and Practice*, *10* (20), 64-81. https://doi.org/10.58689/eibd.1385058

Çiftçi, S., & Sakallı, H. (2016). Examining the relationship between digital citizenship levels and cyberbullying tendencies of prospective primary school teachers. *Educational Technology Theory and Practice, 6*(2), 100-119. https://doi.org/10.17943/etku.97311

Çimen, İ. D. (2018). The effect of cyberbullying, internet family attitude and family functioning in adolescents. *Anatolian Journal of Psychiatry*, *19*(4), 397-404. https://doi.org/10.5455/apd.282841

Deschamps, R., & McNutt, K. (2016). Cyberbullying: What's the problem? *Canadian Public Administration, 59*(1), 45-71. https://doi.org/10.1111/capa.12159

Eminağaoğlu, M., & Gökşen, Y. (2009). What is information security and what is not? Information security problems and solution proposals in Turkey. *Dokuz Eylül University Journal of Institute of Social Sciences, 11*(4), 01-15. https://doi.org/10.16953/deusbed.79642

Eroğlu, Y. (2011). *Examination of the relationship between conditional self-worth, risky internet behaviors and cyberbullying/ victimization.* (Publication no. 328018) [Master's Thesis, Sakarya University] YÖK National Thesis Center. *https://doi.org/10.19126/suje.04882*

Gökmen, Ö. F., & Akgün, Ö. E. (2015). Investigation of computer and instructional technology education teacher candidates' information security knowledge according to various variables. *Cukurova University Faculty of Education Journal*, *44*(1), 61-84. https://doi.org/10.14812/cufej.2015.004

Gökmen, Ö. F., & Akgün, Ö. E. (2015). Investigation of computer and instructional technology education teacher candidates' perceptions of competence to provide information security education. *Primary Education Online*, *14*(4), 1208-1221. https://doi.org/10.17051/io.2015.04635

İşçitürk, G. B., & Turan, E. Z. (2015). Pre-service teachers' views on cyberbullying behaviors. *Researcher, 3*(1), 60-68.

Kaplanoğlu, G. (2016). *Examination of teachers' awareness of information security.* (Publication no. 450078) [Master's Thesis, Gazi University] YÖK National Thesis Centre.

Mallaboyev, N. M., Sharifjanovna, Q. M., Muxammadjon, Q., & Shukurullo, C. (2022). Informatıon securıty issues. *Conference Zone,* 241-245.

Metin, K. E. (2017). Secondary school teachers' levels of cyberbullying and their coping strategies with cyberbullying. *Journal of Education and Society Research*, *4*(2), 33- 49. https://doi.org/10.29065/usakead.316635

Nezgitli, S., & Gökçe Arslan, Ş. (2022). A review on information security awareness for public and private sectors. *Instructional Technology and Lifelong Learning, 3*(1), 19-44. https://doi.org/10.52911/itall.1115701

Pusey, P., & Sadera, W.A. (2011). Cybernetics, cybersecurity and cyber safety: The need for teacher candidates' knowledge, preparation and teacher education to make a difference. *Journal of Digital Learning in Teacher Education, 28*(2), 82-88. https://doi.org/10.1080/21532974.2011.10784684

Serin, H. (2012). *Cyberbullying / cyber victimization experiences in adolescents and the views of teachers and education administrators on these behaviors.* (Publication no. 317225) [Doctoral Dissertation, Istanbul University] YÖK National Thesis Center. https://doi.org/10.29065/usakead.316635

Talib, S. (2014). *Personalizing information security education.* Research Theses, University of Plymouth Faculty of Science and Technology, Malaysia, 5-14.

Tingiş, E. (2022). *Social studies teachers' views on cyberbullying.* (Publication no. 757893)[Master's Thesis, Akdeniz University] YÖK National Thesis Centre.

Türnüklü, A. (2000). A qualitative research technique that can be used effectively in pedagogical research: Interview. *Educational Administration in Theory and Practice*, *24*(24), 546-548.

Yavuz, F. (2023). Examining the relationship between teachers' digital literacy levels and personal cyber security behaviors. Fırat University Institute of Educational Sciences, Elazığ, 12-79.

Yıldırım, A., & Şimşek, H. (2016). *Qualitative research methods in social sciences.* Ankara: Seçkin Publishing.

Yılmaz, E., Şahin, Y. L., & Akbulut, Y. (2016). Teachers' awareness of digital data security. *Sakarya University Journal of Faculty of Education*, *6*(2), 26-45. https://doi.org/10.19126/suje.29650

İletişim/Correspondence
Öğr. Gör. Dr. Alev ORHAN
alevorhan@cumhuriyet.edu.tr

Aysun DÜŞMEZ
Aysndsmz06@gmail.com

Prof. Dr. Elif ORHAN
eliforhan@gazi.edu.tr