
GAZİ ÜNİVERSİTESİ
Gazi
1926

# ÖĞRETMENLERİN BİLGİ GÜVENLİĞİ FARKINDALIĞININ İNCELENMESİ

**GÜLSÜM KAPANOĞLU**

**YÜKSEK LİSANS TEZİ**

**BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ**

**ANABİLİM DALI**

**GAZİ ÜNİVERSİTESİ**

**EĞİTİM BİLİMLERİ ENSTİTÜSÜ**

**Eylül, 2016**

# TELİF HAKKI ve TEZ FOTOKOPİ İZİN FORMU

Bu tezin tüm hakları saklıdır. Kaynak göstermek koşuluyla tezin teslim tarihinden itibaren 24 ay sonra tezden fotokopi çekilebilir.

**YAZARIN**

Adı : Gülsüm

Soyadı : KAPANOĞLU

Bölümü : Bilgisayar ve Öğretim Teknolojileri Eğitimi

İmza :

Teslim tarihi :

**TEZİN**

Türkçe Adı: Öğretmenlerin Bilgi Güvenliği Farkındalığının İncelenmesi

İngilizce Adı: Examining The Information Security Awareness Of Teachers

# ETİK İLKELERE UYGUNLUK BEYANI

Tez yazma sürecinde bilimsel ve etik ilkelere uyduğumu, yararlandığım tüm kaynakları kaynak gösterme ilkelerine uygun olarak kaynakçada belirttiğimi ve bu bölümler dışındaki tüm ifadelerin şahsıma ait olduğunu beyan ederim.

Yazarın Adı Soyadı: Gülsüm KAPANOĞLU

İmza: ……..……

## JÜRİ ONAY SAYFASI

Gülsüm Kapanoğlu tarafından hazırlanan "Öğretmenlerin Bilgi Güvenliği Farkındalığının İncelenmesi " adlı tez çalışması aşağıdaki jüri tarafından oy birliği / oy çokluğu ile Gazi Üniversitesi Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı'nda Yüksek Lisans tezi olarak kabul edilmiştir.

**Danışman:** Prof. Dr. Halil İbrahim BÜLBÜL

(BÖTE, Gazi Üniversitesi) .....

**Üye:** Doç. Dr. Tolga GÜYER

(BÖTE, Gazi Üniversitesi ) .....

**Üye:** Yrd. Doç. Dr.Yasemin DEMİRASLAN ÇEVİK

(BÖTE, Hacettepe Üniversitesi) .. .....

Tez Savunma Tarihi:

Bu tezin Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı'nda Yüksek Lisans tezi olması için şartları yerine getirdiğini onaylıyorum.

Prof. Dr. Ülkü ESER ÜNALDI .....

Eğitim Bilimleri Enstitüsü Müdürü

# TEŞEKKÜR

Çalışmam süresince bana her konuda yardımcı olan ve desteğini esirgemeyen değerli danışmanım Prof. Dr. Halil İbrahim Bülbül'e,

Tez yazımı süresince tecrübe ve bilgisiyle yol gösteren, desteğini ve zamanını esirgemeyen ve yüksek lisans eğitimim boyunca ufkumu genişletmemi ve farklı bakış açıları kazanmamı sağlayan değerli hocalarıma,

Çalışmama gönüllü olarak katılan değerli öğretmenlerimize,

Yoğun çalışmam süresince bana hem görüşleriyle hem de varlıklarıyla destek olup katkı sağlayan tüm çalışma arkadaşlarıma,

Yüksek Lisans süresi boyunca çalışmalarıma maddi destek sağlayan TÜBİTAK'a,

Hayatımın her evresinde yanımda olan, başarılarıma yardımcı olan sevgili aileme teşekkürü borç bilirim.

# ÖĞRETMENLERİN BİLGİ GÜVENLİĞİ FARKINDALIĞININ İNCELENMESİ

**(Yüksek Lisans Tezi)**

**Gülsüm KAPANOĞLU**

**GAZİ ÜNİVERSİTESİ**
**EĞİTİM BİLİMLERİ ENSTİTÜSÜ**
**Eylül 2016**

## ÖZ

Bu çalışmanın amacı öğretmenlerin interneti güvenli kullanım durumlarını ve bilgi güvenliği farkındalık düzeylerini belirlemektir. Çalışma, Devlet Planlama Teşkilatının Türkiye'yi ayırdığı 12 bölgeden (NUT12) 6 farklı branşta 1355 öğretmenin katılımı ile gerçekleştirilmiştir. Araştırmada ilişkisel tarama yöntemi kullanılmıştır. Veri toplama aracı olarak, araştırmacı tarafından geliştirilen "*Öğretmenlerin Bilgi Güvenliği Farkındalığı Anketi* " kullanılmıştır. Elde edilen veriler ışığında öğretmenlerin bilgi güvenliği farkındalık düzeylerinin "orta düzeyde" olduğu sonucuna varılmıştır. Bilgi güvenliği farkındalıklarının branşlara, alınan bilgi güvenliği eğitimine, öğrenim durumuna, yaşanılan bölgeye, internet kullanım süresine ve yaşa göre anlamlı farklılıklar gösterdiği görülmüştür.

Bilim Kodu :

Anahtar Kelimeler : Bilgi güvenliği, Bilgi Güvenliği Farkındalığı, Farklı branşlardaki öğretmenler, Güvenli kullanım

Sayfa Adedi : ..

Danışman : Prof. Dr. Halil İbrahim BÜLBÜL

# EXAMINING THE INFORMATION SECURITY AWARENESS OF TEACHERS

**(M.S. THESIS)**

**Gülsüm KAPANOĞLU**

**GAZI UNIVERSITY**
**GRADUATE SCHOOL OF EDUCATIONAL SCIENCES**
**September, 2016**

## ABSTRACT

The aim of this research is to examine the security awareness of the teachers from different branches. The study was carried out in 12 regions (NUT12) of Turkey which were determined by the State Planning Organization. 1355 teachers from 6 different branches participated in this study. Descriptive analysis method was used to evaluate the data. "The Teachers' Information Security Awareness Survey" was developed and employed by the researcher as a data collection tool. The data analysis revealed that the information security awareness of the teachers was medium. A statistically significant difference was found between different branches of teachers. In addition, a statistically significant difference was found in terms of age, information security training accomplished, level of education, place of residence, and internet usage time.

Science Code :

Key Words : Information Security, Information Security Awareness, Teachers ın Dıfferent Branches, Safely use

Page Number :

Supervisor : Prof. Dr. Halil İbrahim BÜLBÜL

# İÇİNDEKİLER

TELİF HAKKI ve TEZ FOTOKOPİ İZİN FORMU ..... i
ETİK İLKELERE UYGUNLUK BEYANI ..... ii
TEŞEKKÜR ..... iv
ÖZ ..... v
ABSTRACT ..... vi
İÇİNDEKİLER ..... vii
TABLOLAR LİSTESİ ..... xiii
SİMGELER VE KISALTMALAR ..... xviii
BÖLÜM I ..... 1
GİRİŞ ..... 1
Problem Durumu ..... 1
Araştırmanın Amacı ..... 4
Araştırmanın Önemi ..... 5
Sayıltılar ..... 7
Sınırlılıklar ..... 7
Tanımlar ..... 7
BÖLÜM II ..... 9
KAVRAMSAL ÇERÇEVE ..... 9
Bilgi Nedir? ..... 9
Bilgi ve Bilgisayar Güvenliği ..... 10
Bilgi Güvenliği İlkeleri ..... 13

Kullanılabilirlik ..... 13
Gizlilik ..... 14
Bütünlük ..... 15
Kimlik Tespiti ..... 17
İnkâr Edememe ..... 17
Sorumluluk ..... 17
Süreklilik ..... 17
Kayıt Tutma ..... 17
Güvenirlik ..... 18
Bilgi Güvenliğini Sağlama Süreçleri ..... 18
Sistemlere Yapılan Saldırılar ve Türleri ..... 19
Bilgi Güvenliğini Tehdit Eden Unsurlar ..... 21
Virüsler (Viruses) ..... 22
Truva Atları (Trojons) ..... 23
Solucanlar (Worm) ..... 24
Reklam Destekli Yazılım (Adware) ..... 24
Tuş Kaydedici Yazılımlar (Keylogger) ..... 25
Casus Yazılım Ve İz Sürme Çerezleri (Spyware Cookie and Tracking Cookie) ..... 25
Damlatıcılar ..... 25
Şifre ve Gizli Soru Tahmini ..... 25
Omuz Sörfü ..... 26
Çöpe Dalma (Dumpster Diving) ..... 26
Mantık Bombaları ..... 26
Sql İnjeksiyon (Sql Injection Attack) ..... 26
Rootkitler ..... 27

Exploit ..... 27
Tarayıcı Soyma ..... 27
Telefon Çeviriciler ..... 28
Hırsız Yazılım (Thiefware) ..... 28
Web Böcekleri (Web Bugs) ..... 28
Uzaktan Yönetim Aracı, RAT (Remote Administration Tool) ..... 28
Zombi Bilgisayar ..... 28
Bot Ağı (botnet) ..... 29
Ağ taşkını (flooder) ..... 29
Şifre kırıcılar (password cracker) ..... 29
Sondaj Aracı (Probe Tool) ..... 30
Arama Motoru Soyguncusu (Search Hijacker) ..... 30
Koklayıcı (Sniffer) ..... 30
Kandırıcı (Spoofer) ..... 30
Pharming ..... 30
Zamanlı Saldırı (Timing Attack) ..... 31
Web Sayfası Hızsızlığı ..... 31
Spam Mail ..... 32
Sosyal Mühendislik ..... 32
İnsan Tabanlı Yapılan Saldırı Yöntemleri, Bu saldırı yöntemini gerçekleştirmek, insanlarla etkileşime geçmeye bağlıdır ve kişi-kişi iletişim kurulması gerekmektedir. ..... 33
Bilgisayar Tabanlı Yapılan Saldırı Yöntemleri ise, istenilen bilgileri ele geçirmek için yazılım kullanarak yapılan saldırı yöntemleridir. ..... 34
Sosyal Mühendislikten Korunmak ..... 37
İlgili Araştırmalar ..... 38

BÖLÜM III ..... 46
YÖNTEM ..... 47
Araştırmanın Modeli ..... 47
Araştırmanın Evreni ..... 47
Araştırmanın Örneklemi ..... 48
Veri Toplama Aracı ..... 49
Uzman Görüşü Alma ..... 50
Pilot Uygulama Ve Ölçeğe Son Şeklini Verme ..... 51
Açımlayıcı faktör analizi ..... 51
Geçerlilik-Güvenirlik ..... 52
Normallik Testi Sonuçları ..... 53
Verilerin Toplanması ..... 54
Verilerin Çözümlenmesi ve Yorumlanması ..... 54
BÖLÜM IV ..... 57
BULGULAR VE YORUMLAR ..... 57
Açımlayıcı Faktör Analizi Bulguları ..... 57
Bağımsız Değişkenlere Ait Frekans ve Yüzde Değerleri ..... 59
Birinci Alt Probleme İlişkin Bulgular ..... 65
İkinci Alt Probleme İlişkin Bulgular ..... 71
Mağduriyet alt boyutunun frekans ve yüzdelik değerleri ..... 73
Davranış Alt Boyutunun Frekans Ve Yüzdelik Değerleri ..... 78
Kişisel Bilgi Gizliliği Alt Boyutunun Frekans ve Yüzdelik Değerleri ..... 80
Önlem Alma Alt Boyutunun Frekans Ve Yüzdelik Değerleri ..... 82
Koruma Bilinci Alt Boyutunun Frekans Ve Yüzdelik Değerleri ..... 87
Üçüncü Alt Probleme İlişkin Bulgular ..... 90

Öğretmenlerin Cinsiyet Değişkeni Açısından Bilgi Güvenliği Farkındalığı Düzeyleri ..... 90

Öğretmenlerin Yaş Değişkeni Açısından Bilgi Güvenliği Farkındalığı Düzeyleri ..... 91

Öğretmenlerin Öğrenim Durumu Değişkeni Açısından Bilgi Güvenliği Farkındalığı Düzeyleri ..... 92

Öğretmenlerin Bulundukları Bölge Değişkeni Açısından Bilgi Güvenliği Farkındalığı Düzeyleri ..... 92

Öğretmenlerin Görev Süresi Değişkeni Açısından Bilgi Güvenliği Farkındalığı Düzeyleri ..... 93

Öğretmenlerin İnterneti Kullanma Süreleri Değişkeni Açısından Bilgi Güvenliği Farkındalığı Düzeyleri ..... 94

Öğretmenlerin Bilgi Güvenliği Eğitimi Alma Değişkeni Açısından Bilgi Güvenliği Farkındalığı Düzeyleri ..... 95

Öğretmenlerin Branşlarına Göre Bilgi Güvenliği Farkındalığı Düzeyleri ... 97

BÖLÜM V ..... 99

SONUÇLAR VE ÖNERİLER ..... 99

Sonuçlar ..... 99

Öneriler ..... 103

KAYNAKÇA ..... 105

EKLER ..... 112

Ek-1 :Bilgi Güvenliği Farkındalığı Anketi ..... 113

EK-2 :Türkiye'de İBBS ya da (NUTS)'a Göre Sınıflandırılmış Bölgeler ..... 119

EK-3: Anketin Web Sayfasının Ekran Görüntüleri ..... 122

# TABLOLAR LİSTESİ

Tablo 1. *Araştırma Yapılan Bölgeler*.....49

Tablo 2. *Pilot Uygulamaya Katılan Öğretmenlerin Branş Dağılımı*.....51

Tablo 3. *KMO ve Bartlett Testi Sonuçları* .....52

Tablo 4. *Güvenirlik Katsayısı* .....53

Tablo 5. *Bilgi Güvenliği Farkındalığı Ölçeği için Güvenirlik*.....53

Tablo 6. *Katılımcıların Epostalerini Kontrol Etme Sıklığı*.....63

Tablo 7. *Katılımcıların Sosyal Medya Hesaplarının Olma Durumu*.....64

Tablo 8 *Anti Virüs Yazılımı Kullanımına Dair Betimsel İstatistikler* .....65

Tablo 9 *Bilgisayarlarda Kullanılan Anti Virüs Yazılım Türü*.....66

Tablo 10 *Eposta Kontrol Etme Sıklığı* .....66

Tablo 11 *Spam Eposta Nedir Soruna Verilen Cevaplar*.....67

Tablo 12 *"Bankanızdan gelen bir e-postada, bilgilerinizi güncellemeniz için bir adrese tıklamanız istense ne yaparsınız?" Sorusunun Betimsel İstatistik Bulguları* .....67

Tablo 13 *"Tanıdığınız birisinden dosya eklentili ve eposta adresi tuhaf bir eposta gelirse ne yaparsınız" Sorusunun Betimsel İstatistikleri* .....68

Tablo 14 *Aldatmaca Epostaleriyle İlgili Betimsel İstatistikler*.....69

Tablo 15 *Bir Sitenin Güvenli Olup Olmadığını Nereden Anlarsınız Sorusuyla İlgili Betimsel İstatistikler* .....70

Tablo 16 *Bilgi Güvenliği Farkındalığı Düzey Puanların Yorumlanması Amacıyla Kullanılan Puan Ortalama Aralıkları*.....72

Tablo 17 *Bilgi Güvenliği Farkındalığı Anketinin İstatistiksel Bulguları*.....72

Tablo 18 *"Kişisel Bilgilerimi İnternette Kullandığım İçin Sıkıntı Yaşadım." Maddesine İlişkin Frekans Ve Yüzde Değerleri* .....73

Tablo 19 *"Sosyal Ağlarda Yaptığım Bilgi Paylaşımı Hayatıma Zarar Verdi." Maddesine İlişkin Frekans Ve Yüzde Değerleri* .....73

Tablo 20 *"Kredi Kartı Bilgilerim Kopyalandı" Maddesine İlişkin Frekans Ve Yüzde Değerleri* .....74

Tablo 21 *"İnternette Kullandığım Hesaplarda Şifrem Ele Geçirildi." Maddesine İlişkin Frekans Ve Yüzde Değerleri* .....74

Tablo 22 *"Bilgisayarımdaki Bazı Dosyalarım Çalındı/Silindi." Maddesine İlişkin Frekans Ve Yüzde Değerleri* .....75

Tablo 23 *"İnternette Gezerken İsteğim Dışında Şiddet Ya Da Pornografik İçerikli Yayınlarla Karşılaştım." Maddesine İlişkin Frekans Ve Yüzde Değerleri*.....75

Tablo 24 *"Vatandaşlık Numaramın (T.C.) Başka Şahıslar Tarafından Bilinmesi Beni Rahatsız Etmez." Maddesine İlişkin Frekans Ve Yüzde Değerleri*.....76

Tablo 25 *"İnternetin Herkese Açık Olduğu Yerlerde İnternet Bankacılığı Kullanırım." Maddesine İlişkin Frekans Ve Yüzde Değerleri*.....76

Tablo 26 *Mağduriyet Alt Boyutuna İlişkin Verilerin Aritmetik Ortalama ve Standart Sapma Puanları* (n=1355) .....77

Tablo 27 *"Bütün Hesaplarımda Aynı Parolayı Kullanırım." Maddesine İlişkin Frekans Ve Yüzde Değerleri* .....78

Tablo 28 *"Kargo,Gsm Operatörü Gibi Kuruluşlarla Nüfus Cüzdanı Bilgilerimi Paylaşırım." Maddesine İlişkin Frekans Ve Yüzde Değerleri*.....78

Tablo 29 *"Parolalarımı Başkalarıyla Paylaşırım." Maddesine İlişkin Frekans Ve Yüzde Değerleri* .....79

Tablo 30 *"İnternet Bankacılığı Vs. Şifresini Yazarken Klavye Kullanırım." Maddesine İlişkin Frekans Ve Yüzde Değerleri* .....79

Tablo 31 *Davranış Alt Boyutuna İlişkin Verilerin Aritmetik Ortalama ve Standart Sapma Puanları* (n=1355) .....80

Tablo 32 *"Kişisel Bilgilerimin Başkaları Tarafından Kötü Amaçla Kullanılabileceğini Düşünürüm." Maddesine İlişkin Frekans Ve Yüzde Değerleri* .....80

Tablo 33 *"Kişisel Bilgisayarımda Otomatik Kullan Özelliğini Kullanırım." Maddesine İlişkin Frekans Ve Yüzde Değerleri* .....81

Tablo 34 *"Parolalarımı Yazılı Olarak Ulaşabileceğim Bir Yerde Saklarım." Maddesine İlişkin Frekans Ve Yüzde Değerleri* .....81

Tablo 35 *Kişisel Bilgi Gizliliği Alt Boyutuna İlişkin Verilerin Aritmetik Ortalama ve Standart Sapma Puanları (n=1355)* .....82

Tablo 36 *"İnternet Üzerindeki Hesaplarımda Kolay Tahmin Edilemeyecek Şekilde Karmaşık Ve Uzun Şifreler Kullanırım." Maddesine İlişkin Frekans Ve Yüzde Değerleri* .....82

Tablo 37 *"Aynı İletiyi Birden Fazla Kişiye Göndermem Gereken Durumlarda Gizli (BCC) Kısmını Kullanırım." Maddesine İlişkin Frekans Ve Yüzde Değerleri* .....83

Tablo 38 *"Bilgisayarımda Lisanslı Yazılım (Orijinal) Kullanmaya Dikkat Ederim." Maddesine İlişkin Frekans Ve Yüzde Değerleri*.....83

Tablo 39 *"Virüs Temizleme, Casus Yazılım Önleme Vb. Programları Kullanırım." Maddesine İlişkin Frekans Ve Yüzde Değerleri*.....84

Tablo 40 *"Kısa Bir İşim Olsa Dahi Çalışırken Ekran Koruyucu Kullanırım." Maddesine İlişkin Frekans Ve Yüzde Değerleri* .....84

Tablo 41 *"Kullandığım Programların Güncellemesini Düzenli Olarak Yaparım." Maddesine İlişkin Frekans Ve Yüzde Değerleri*.....85

Tablo 42 *"Güvenlik Duvarı, Reklam Önleyici Vb. Programlar Kullanırım." Maddesine İlişkin Frekans Ve Yüzde Değerleri* .....85

Tablo 43 *"Bulut Teknolojilerinde (Drive,Dropbox Vs.) Bilgilerimi Güvende Hissediyorum." Maddesine İlişkin Frekans Ve Yüzde Değerleri*.....86

Tablo 44 *Önlem Alma Alt Boyutuna İlişkin Verilerin Aritmetik Ortalama Ve Standart Sapma Puanları (N=1355)* .....86

Tablo 45 *"Önemli Dosyalarımı Şifrelerim." Maddesine İlişkin Frekans Ve Yüzde Değerleri* .....87

Tablo 46 *"Çocukları İstenmeyen İçeriklerden Koruyacak Filtre Programları Kullanırım." Maddesine İlişkin Frekans Ve Yüzde Değerleri*.....87

Tablo 47 *"Parolalarımı Sık Sık Değiştiririm." Maddesine İlişkin Frekans Ve Yüzde Değerleri*.....88

Tablo 48 *"Akıllı Telefonum Ve Bilgisayarım Bir Şifre İle Korunur." Maddesine İlişkin Frekans Ve Yüzde Değerleri*.....88

Tablo 49 *"Herkesin Kullanımına Açık Bir Bilgisayardan Ayrılmadan Önce Geçici İnternet Dosyalarını Ve Gezinme Geçmişini Silerim." Maddesine İlişkin Frekans Ve Yüzde Değerleri*.....89

Tablo 50 *Koruma Bilinci Alt Boyutuna İlişkin Verilerin Aritmetik Ortalama ve Standart Sapma Puanları (n=1355)*.....90

Tablo 51 *Bilgi Güvenliği Farkındalığının Cinsiyete Göre U-Testi Sonuçları*.....91

Tablo 52 *Bilgi Güvenliği Farkındalığının Yaş Değişkenine Göre Kruskal Wallis Testi Sonuçları*.....91

Tablo 53 *Bilgi Güvenliği Farkındalığının Öğrenim Durumu Değişkenine Göre Kruskal Wallis Testi Sonuçları*.....92

Tablo 54 *Bilgi Güvenliği Farkındalığının Bulunulan Bölge Değişkenine Göre Kruskal Wallis Testi* Sonuçları.....93

Tablo 55 *Bilgi Güvenliği Farkındalığının Görev Süresi Değişkenine Göre Kruskal Wallis Testi Sonuçları*.....94

Tablo 56 B*ilgi Güvenliği Farkındalığının İnternet Kullanım Süresi Değişkenine Göre Kruskal Wallis Testi Sonuçları*.....95

Tablo 57 *"Bilgi güvenliği veya internet güvenliğine yönelik eğitim aldınız mı?" Maddesine İlişkin Betimsel İstatistikler*.....95

Tablo 58 *Eğitim Alma Durumunun Branşlara Göre Dağılımı*.....96

Tablo 59 *Bilgi Güvenliği Farkındalığının Eğitim Alma Değişkenine Göre İncelenmesi*...97

Tablo 60 *Öğretmenlerin Bilgi Güvenliği Farkındalıklarının Branş Değişkenine Göre*.....98

# ŞEKİLLER LİSTESİ

*Şekil 1.* Bilgi güvenliğinin temel üç boyutu.....11

*Şekil 2*. Bilgi güvenliği boyutları.....13

*Şekil 3.* Bilgi gizliliği oluşturma bileşenleri.....15

*Şekil 4.* Casus yazılımların sınıflandırılması.....22

*Şekil 5*. Cryptologger virüs içeren e-posta.....35

Şekil 6. Katılımcıların İnterneti Kullanma Amaçları.....63

Şekil 7. Sosyal Ağlarda Paylaşılan Bilgiler.....65

Şekil 8. Bilgisayarın Çalınma Durumuna Karşı Alınabilecek Önlemler.....68

Şekil 9. Kişisel Haklara Saldırı Sorusu İle İlgili Betimsel İstatistikler.....70

Şekil 10. Sosyal Medyada Kullanılan Gizlilik Ayarları.....71

# SİMGELER VE KISALTMALAR

| | |
|---|---|
| İBBS | Türkiye İstatistiki Bölge Birimleri Sınıflandırması |
| TÜİK | Türkiye İstatistik Kurumu |

# BÖLÜM I

# GİRİŞ

Bu bölümde araştırma ile ilgili bilgilere, araştırmanın problemine, problem cümlesine, araştırmanın amacına, araştırmanın önemine, sayıltılara, sınırlılıklara ve tanımlara yer verilmiştir.

## Problem Durumu

Bilgi, veri'nin belirli bir çerçevede anlam ifade edecek şekilde düzenlenmiş halidir. İnsan yaşamında bilgi her zaman önemli olmuştur.Gelişen dünyada teknolojinin devamlı olarak ilerlemesiyle bilgi sürekli olarak yenilenmektedir ve bilginin önemi gelişen teknoloji ile hızla artmaktadır. John Naisbitt'e (1982) göre bilgi yeni bir güç kaynağıdır ve sosyal, ekonomik ve teknolojik alanlarda hayatın bütün sektörlerinde olduğu gibi önemini kabul ettirmiştir. Yine Kuçuradi (1995, s.97) felsefi açıdan bilgiyi, algılama, anlama, düşünme, yorumlama, doğrulama ve değerlendirme gibi birçok etkinliğin içerisinden oluştuğunu belirtmektedir.

Bilgi, içinde yaşanılan çağa damgasını vuran bir varlık olarak düşünüldüğünde, bu varlığı tanımlamak, kavramak ve bilgi ile ilgili hususları incelemek insanlığın başlangıcından itibaren ileriye yönelik gelişimi sağlamanın en önemli unsurudur (Canbek, 2005). Bilginin niteliğinde ve niceliğinde meydana gelen değişim toplumları bu dönüşüm sürecine hızlı bir şekilde uyum sağlamaya zorlamıştır ve bu dönemde bilgi toplumunun temel donanımlarına sahip olması önem taşımaktadır (Demiralay ve Karadeniz, 2010).

Bilgi ve teknoloji alanındaki birçok değişim ve gelişim eğitim alanında da kendini gösterdiği gözlemlenmektedir. 21.yy öğrencilerini yetiştirecek öğretmenlerden hem teknolojiyi kullanmalarını hem de becerileri öğrenme-öğretme süreçlerinde etkin bir şekilde öğretmeleri beklenmektedir. Bununla birlikte öğretmenin becerilerini çok boyutlu ve her duruma

uyarlanabilecek şekilde geliştirilmesi beklenmektedir (Tutkun ve Aksoyalp, 2010). Nitekim Milli Eğitim Bakanlığı, Eğitimi Araştırma ve Geliştirme Dairesi'nin 1999 yılında Çağdaş öğretmen profilini ortaya çıkarma amacıyla yaptığı çalışmasında, çağdaş öğretmenin çağın ihtiyaçlarını karşılayabilecek düzeyde 21. Yüzyılın bilgi teknolojisine hakim olması ve bilgi toplumundaki öğrencileri geleceğe hazırlayacak yeterlikte olması beklenmektedir (Meb, 2001).

Karalar ve Sarı'ya (2007) göre bilgi çağının en belirgin özelliği bilgi teknolojilerinin sıklıkla kullanılması ve maddi ürünün yerini bilgi üretiminin almasıdır.Gelişen teknoloji toplumun ihtiyaçlarını rahat karşılarken diğer taraftan da toplumun gelişimini olumlu yönde etkilemektedir. Teknoloji sayesinde yerleşen, günlük hayatta gerekli olan ihtiyaçların internet ile giderilmesi olarak tanımlanan e-yaşam sistemi, günlük hayatta karşılaşılabilecek durumları kolaylıkla çözebilmektedir (Mart, 2012).

Bilgi çağının oluşmasıyla bilgi ve iletişim teknolojileri alanında yaşanan gelişmeler, yalnızca bireylerin yaşamlarını kolaylaştırmakla kalmamış, iletişim engellerini de ortadan kaldırarak bireylerin daha kolay, hızlı ve etkileşimli iletişim kurmalarına imkân vermiştir. Böylece geçmiş zamanlarda kâğıt ortamında mekâna bağlı olarak gerçekleştirilen işlemler, bu yüzyılda dijital olarak gerçekleştirilmektedir. Yeni iletişim teknolojileri ile birlikte sosyal ağlar ve elektronik uygulamalarla insan hayatının önemli bir kısmı da dijital ortama taşınmıştır.

Hızla gelişen dijital ortama taşınma durumu tüm verileri korunması gerekli olan birer e-varlık şekline dönüştürmüştür. İnsan hayatının dijital ortama taşınmasından dolayı kişisel veriler bu ortamlarda birikmeye başlamıştır. Bundan dolayı teknolojinin uygunsuz kullanımı ile kişilerin bilgi güvenliği farkındalık seviyelerinin yetersiz olması sonucu, kişi ve kuruluşları tehdit eden bilgi güvenliği riskleri ve siber suçlar ortaya çıkmıştır. Yukarıda bahsedilen olumsuz durumlar kişilerin, teknolojiyi bilinçli kullanmak suretiyle kendilerini korumak zorunda oldukları gerçeği ile karşı karşıyadırlar ve tüm devletleri ilgili birimlerince vatandaşlarını bu tehditlerden koruyabilmek için yasalar düzenlemiştir (Öğütçü, 2010).

Bilgi toplumuna geçiş süreci sonucunda sosyo-ekonomik hayat, bankalar, devlet işleri, eğitim, sağlık, ticaret, kamu kurum ve kuruluşları gibi toplumun her kademesinde değişmeler meydana gelmiştir. Değişimin temeli olan bilişim teknolojilerinin topluma olan faydası dikkate alındığında, etkili ve yararlı kullanılmasının önemi görülmektedir (Çalık ve Çınar, 2009). Bununla birlikte kullanım yaygınlığı, etkin kullanım, kültür ve üretim gibi

konularda da oldukça gerilerdedir (Canbek ve Sağıroğlu, 2006).

Bilgi güvenliği, bilgilerin yetkisiz kişilerce erişiminden, kullanımından, değiştirilmesinden, açık edilmesinden, yok edilmesinden veya hasar verilmesinden koruma işlemi olarak tanımlanmaktadır. Kurumlarda bilgilerin istenmeyen kişiler tarafından ulaşılmasını engellemek için bilgi güvenliği sorumlusu belirlenir ve sorumlunun görevi, meydana gelen ve gelebilecek ihlalleri tespit edip kayıt altına alınması ve yetkili kişilere bildirilmesidir. Bilgi güvenliğinin amacı, bilgileri ve bilgilerin sağladıkları işleri sürekli olarak koruma altına almak ve bu çerçevedeki iş kazaları sonucu kaybolan bilgi miktarını düşürmek, ayrıca güvenlik olaylarından en düşük derece etkiyle kurtulabilmektir (Solms, 1998). Bu kapsamda, durumlara göre neler yapılacakların bir çerçevesini belirlemek ve olası tehditlerde nereye başvurulacağını belirlemek adına Cobit control hedefi ve ISO 27001 gibi Bilgi güvenliği yönetim sistemi standartları oluşturulmuştur (Altun, 2014). Değişen durumlara göre geliştirilen bu standartların toplumda her birey tarafından özelliklede eğiticiler tarafından bilgi güvenliği konusunda kişilerin ne türlü hak ve yetkilerinin bir standard içinde yürütülmesi gerektiğini bilmeleri büyük önem taşımaktadır.

Uluslararası denetim ve danışmanlık şirketi olan Ernst & Young her yıl Türkiye'nin de içinde bulunduğu 144 ülke ve çeşitli sektörlerde yaklaşık 1400 kuruluşun katılımıyla gerçekleştirdiği "2014 Küresel Bilgi Güvenliği Anketi'nde, bilgi güvenliğinin önemini belirten sonuçlar ortaya çıkarmıştır. Ankette sosyal medya kullanımı, mobil telefonlar, bulut bilişim ve diğer yeni teknolojilerin şirket sırlarının paylaşılmasını kolaylaştırdığı görülürken kurumların bilgi güvenliğinin korunması durumunu yönetim kurulunun ele alması ve bu konuda daha yüksek bütçe ayırması öneriliyor. Kurumların bilgi güvenliği konusundaki boşluklarının kapanması için önerilen yolun bilgi güvenliği altyapılarında köklü bir değişikliğe gitmek olduğu belirtilmiştir. Ankete katılanların %80'i dış tehditlerin artmasıyla risk faktörünün de yükseldiği konusunda hemfikir olması, kurumların bilgi güvenliği hakkındaki risk ortamlarının değiştiğinin farkında olduklarını göstermektedir. Buna ilaveten katılımcıların %10'u bilgi güvenliğini tehdit eden vakaların geçen yıla göre düşüş gösterdiğini, %59' u aynı oranda kaldığını ve %31'i ise artış gösterdiğini düşünmektedir. Bilgi güvenliğine yönelik tehditleri sıklığı ve güvenlik vakalarının artması bu konuda kurumların ve bireylerin görebileceği potansiyel zararında da arttığını göstermektedir (Global Information Security Awareness Survey, 2014).

Bilgi çağında bireyler, hayatlarının her aşamasında teknolojiyi kullanmaktadırlar ve bilgi güvenliği kavramı ile karşı karşıya kalmaktadırlar. Dolayısıyla bilgi güvenliğinin uygun ve yeterli seviyede olması için insan faktörü anahtar role sahiptir (Canbek ve Sağıroğlu, 2006; Siponen,2001 ;Tekerek, 2012 ;  Topal ve Akgün, 2015)

Teknolojinin hızla ilerlemesiyle bilgi, dökümanlarla kullanılır hale gelmiştir ve bunun sonucu olarak bilgi güvenliğinin önemi giderek artmıştır. Canbek ve Sağıroğlu'na (2006) göre; bilişim teknolojileri ve bu teknolojinin temel maddesi olan bilginin önemi tam olarak anlaşılmamıştır ve bilginin önemi ve sahip olduğu potansiyeli yeterince anlaşılmadığından, bilişim teknolojileri ve bilgi güvenliği gerekli ehemmiyeti görmemektedir.

Bu çalışmada, eğitim sisteminin temel bileşeni olan öğretmenlerin, bilgi güvenliği farkındalık seviyeleri belirlenmeye çalışılmıştır. Yalnızca parola güvenliği veya lisanslı yazılım kullanım güvenliği gibi durumlar güvenliği sağlamak için yeterli olmadığı için bilgi güvenliğini bir bütün olarak inceleme açısından, bireylerin olaylar karşısındaki davranışları ve maruz kaldıkları tehlikeleri değerlenmekte önemlidir. Öğretmenlerin bilgi güvenliğini tehdit edecek unsurları görmesi ve önlem alması, yetiştirdikleri yeni nesillerin korunması açısından önem arzetmektedir. Çalışmanın sonucunda, eğitim sisteminin şekillenmesinde kilit role sahip olan öğretmenlerin bilgi güvenliği farkındalık seviyelerini belirlemek amaçlanmıştır.

**Araştırmanın Amacı**

Bu araştırmanın amacı öğretmenlerin bilgi güvenliği farkındalığını ortaya koymak, gelişen yeni teknoloji paralelinde öğretmenlerin bilgi güvenliği farkındalığına olan ihtiyacını vurgulamaktır.

Çalışmanın amacını gerçekleştirmek için belirlenen alt problelmler şunlardır:

1. Öğretmenlerin bilişim teknolojilerini güvenli kullanmaları ile ilgili mevcut durum nedir?

2. Öğretmenlerin bilgi güvenliği farkındalık düzeyleri ne durumdadır?

3. Öğretmenlerin bilgi güvenliği farkındalıkları ile,

- Yaşları
- Cinsiyetleri
- Eğitim durumları
- Bulundukları bölge
- Bilgisayar kullanım süreleri
- İnternet kullanım süreleri
- Görev süresi
- Bilgi güvenliği eğitimi alma durumu
- Öğretmenlerin branşlarına göre farklılık göstermekte midir?

**Araştırmanın Önemi**

Bilgi ve teknolojilerin hızlı gelişmesi güvenlik tehditlerini de ortaya çıkarmıştır. Bu teknolojilerin insanlar tarafından kullanımı arttıkça insanların tehditlere maruz kalma olasılığı da artmıştır. Bu tehditler sonucunda maddi, manevi birçok zarar meydana gelmektedir. Bilgi güvenliğinin temel yapı taşı bireyler olduğu için ulusal güvenliğin sağlanabilmesi açısından öncelikle bireysel bilgi güvenliğinin sağlanması gerekmektedir.

Bilgi güvenliğinin sağlanması için, en yüksek seviyede önlemler alınmış olsa da insan faktörünün göz ardı edilmesi halinde, alınan önlemlerin sonuç veremeyeceği bilinmektedir (Albrectsen ve Hovden, 2008). Çünkü bilgi güvenliği bilinci ve korunma farkındalığı olmayan insanlar bu güvenlik sürecini ihmal edebileceklerdir.

Bilginin önemli olduğunun farkına varılıp korunmasına karar verilen zamanlardan bu yana güvenlik çemberinin en zayıf kısmı insanlar olmuşlardır. Gerekli yazılımsal ve donanımsal tedbirlerin yanında yönetsel güvenlik kontrolleri uygulansa da saldırganlar insanlar aracılığıyla güvenlik önlemlerini aşmışlardır. Alınan önlemleri bir güvenlik zinciri olarak düşünüldüğünde, en zayıf halkanın insan olması insanın eğitilme miktarı kadar bilgi güvenliği için önlem alınıldığını göstermektedir.

Mandiant'ın (2010) APT olarak adlandırılan hedef odaklı saldırılar tehdit raporuna göre, yapılan tüm APT atakları güvenliğin en zayıf halkası insanlar aracılığıyla başarılı olmuştur. Dolayısıyla, ne kadar ileri düzey teknoloji kullanılsa, güvenlik duvarı, antivirüs programları

ve koruma sistemleri kurulsa, saldırıları kolaylaştıracak olan insan faktörü eğitilmedikçe önlemler yeterli olmayacaktır.

Yapılan araştırmalar göstermektedir ki, (Albrechtsen,2007; Altun,2014; Şahinarslan, Kantürk,Şahinarslan ve Borandağ,2009) bilgi güvenliği ihlalleri genellikle bilgiyi kullanmakta yetkili olan bireyler tarafından yapılmıştır. Bunların çoğu bireylerin bilinçsizce davranışlarının sonucu olurken çok az bir bölümü kötü niyetli çalışanların bilgiyi dışarıya sızdırması, kötü amaçla kullanması veya yok edilmesi sonucu meydana gelmiştir. Bilgi güvenliğinin sağlanmasında insan faktörü önemli bir yere sahiptir. Saldırganlar açısından insan faktörünü kullanmak daha etkin sonuçların oluşmasını sağlayan önemli ve güncel bir saldırı aracıdır ve bu yöntemi kullanan saldırganlara sosyal mühendis olarak adlandırılmaktadır. Sosyal mühendisler, hedefledikleri bilgiye erişim yetkisi olan bireyleri kullanarak güvenlik önlemlerini atlatmaktadır. Bundan dolayı bireyleri sosyal mühendisliğe karşı korumayı hedefleyen eğitimler verilmelidir.
Yapılan çalışmalar, (Albrectsen ve Hovden, 2009; Durmuş, 2009; Mart,2012; Karakasiliotis, Furnell ve Papadaki, 2006; İlbaş, 2009 ;Schmidt, Johnston, Arnett, Chen ve Li, 2008 ; Tekerek, 2008; Tekerek, 2012; Tekerek ve Tekerek, 2013 ; Zhang, Reithe ve Li, 2009) bilgi güvenliğinin önemsenmesi ve insan faktörü açısından bilinçlendirilip, farkındalık oluşturulması gereken bir konu olduğunu göstermektedir. Öğütçü (2010) yaptığı çalışmasında; bilişim güvenliği bilincine sahip insanların, yapmakla yükümlü oldukları davranışları yerine getirip getirmediği anlamını taşımadığını belirtmektedir. Bundan dolayı bireylerin, bilişim güvenliğine doğrudan etkisi olan teknolojiyi kullanma davranışları da incelenmelidir. Bilişim güvenliği için hazırlanan politikaların sağlıklı ve etkili bir şekilde düzenlenebilmesi için bireylerin konuyla ilgili algılarının, değerlerinin ve davranışlarının belirlenmesi ve değerlendirilmesi gerekmektedir.

Eğitim sisteminde aktif role sahip olan öğretmenlerin, günümüzde yaşamın her alanında kullanılan teknolojinin barındırdığı tehditleri bilmesi ve yetiştirdiği nesiller için bu tehditleri analiz edip önlem alması gerekmektedir. Öğretmenlerin farkındalık seviyelerinin belirlenip, gerekli görüldüğü durumlarda eğitim verilmesi hem örgün eğitim verilen kurumların hem de öğrencilerin bilgilerinin güvence altına alınmasını sağlayacaktır. Bu eğitimde bilginin önemini, nasıl korunması gerektiğini ve neden korunması gerektiğini öğretmelidirler. Bu gibi eğitimlerle dikkatli ve iyi eğitimli bireyler yetiştirilir ve olası güvenlik tehditlerine karşı da önlem alınmış olacaktır.

Bu çalışma Türk eğitim sisteminin şekillenmesinde ve yürütülmesinde en önemli göreve sahip olan Öğretmenlerin, eğitim süreci içerisinde gelişen teknolojilerin doğurabilecekleri olumsuz sonuçlara hazırlıklı olmaları ve bu bilgileri yeni nesillere aktarabilmeleri açısından sahip oldukları bilgi güvenliği farkındalık seviyelerinin tespiti açısından önemlidir.

## Sayıltılar

Araştırmada aşağıdaki varsayımlar kabul edilmiştir.

1. Örnekleme alınan öğretmenlerin her bir branşın evrenini yeterince temsil edebilecek durumdadır.
2. Araştırmada görüşlerine başvurulan öğretmenlerin ankete verdikleri yanıtlar, öğretmenlerin gerçek görüşlerini yansıtmaktadır.

## Sınırlılıklar

1. Bu çalışmanın örneklemine anket, sosyal medya ve akademik paylaşımlar yoluyla ulaşılmıştır ve örneklem, anketi cevaplayanların sayısı ile sınırlıdır.

## Tanımlar

**Bilgi:** İnsan aklının erebileceği olgu, gerçek ve ilkelerin bütünü, malumat (Türk Dil Kurumu [TDK], 2016).

**Bilişim**: İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimidir (TDK,2016).

**Teknoloji**: İnsanın maddi çevresini denetlemek ve değiştirmek amacıyla geliştirdiği araç gereçlerle bunlara ilişkin bilgilerin tümüdür (TDK,2016).

**Bilgi Güvenliği:** Bilgiye sürekli olarak erişebilirliğin sağlandığı bir ortamda, bilginin göndericiden alıcıya gizlilikle, bozulmadan, değişime uğramadan ve başkaları tarafından ele

geçirilmeden bütünlüğünün sağlanması ve güvenli bir yolla iletilmesi sürecidir (Vural ve Sağıroğlu, 2008).

**Sosyal Mühendislik:** Temel olarak, insan ilişkilerini ve ya insanların dikkatsizliklerini kullanarak kurum hakkında bilgi toplamak olarak tanımlanabilir ve sosyal mühendisliğin asıl amacı kurum yapısı, kurumsal ağın yapısı, yöneticilerin kişisel bilgileri, şifreler ve saldırıda kullanılabilecek tüm bilgilerdir (Berkay, 2009).

**Bilgi Güvenliği Farkındalığı:** Bilişim teknolojileri kullanılırken, bireylerin kişisel bilgileri istenmeyen tehdit ve tehlikelerden korunması amacıyla gerekli güvenlik tedbirleri belirlenerek tehlikeler karşı farkında olma durumudur (Vural ve Sağıroğlu, 2008).

# BÖLÜM II

# KAVRAMSAL ÇERÇEVE

Bu başlık altında, araştırmanın kavramsal çerçevesinden bahsedilmiştir. Kavramsal çerçeve kapsamında; bilginin tanımı, bilgi güvenliği ve bilgi güvenliğinin önemi, bilgi ve bilgisayar güvenliği, sistemlere yapılan saldırı türleri, bilgi güvenliği farkındalığı ve eğitimi ile bilgi güvenliğindeki hukuksal süreçler ele alınmıştır.

**Bilgi Nedir?**

Yirmibirinci yüzyılın içinde bulunduğumuz döneme bilgi çağı denilmektedir ve bilgi çağı, hızla bilgi üreten, bilginin yoğun olduğu, bireylerin bilgiyi yaymak ve bilgiye ulaşmak için ileri düzey teknolojiye ihtiyaç duyduğu bir çağdır. Bilim ve teknolojideki meydana gelen hızlı değişim ve gelişmeler, toplumların yapısını ve eğitim sistemini değiştirmektedir. (Akkoyunlu,1998; Özer,1998).

Gelişen bilim ve teknoloji sonucu oluşan bu dönemde, bilgi önemli bir güç kaynağıdır. Mal ve hizmet üretiminde en önemli bileşen bilgidir. Bilgi yaşadığımız çağa damgasını vuran bir varlıktır ve çağın altın değerindeki hammaddesidir (Akkoyunlu,1998; Canbek,2005; Gökçen, 2002). Bu açılardan bakıldığında, bilgiyi tanımak, tanımlamak, kavramak ve bilgi ile ilgili durumları incelemek gerekmektedir. Bilgi, her ne kadar günümüzde ön plana çıkmış gibi görünsede dünün, bugünün ve geleceğin en temel bileşeni ve anahtarıdır (Canbek,2005). Bireyler daha nitelikli bir yaşam sağlayabilmek adına bilgiye ulaşma, bilgiyi kullanma gereksinimi içerisindedirler, dolayısıyla bilginin elde edilmesi ve saklanmasında kullanılan teknolojiler sürekli gelişmektedir.

Schuler bilgi çağında ilerlemeyi merdiven basamaklarından çıkmaya benzetmektedir ve merdiven basamaklarını ise; veri (data), bilgi (information), ve özbilgi (information)'dan oluşturmaktadır. Veri basamağından yukarıya doğru çıkıldıkça, eldeki şeyin miktarı azalırken değeri artar ve bir sonraki basamağa çıkmak aynı oranda zorlaşmaktadır. Genel olarak ölçme ile gerçeklikten veriye, ispat ile veriden bilgiye ulaşılır ve kavrama ile de bilgiden özbilgiye ulaşılmaktadır (aktaran Canbek, 2005).

Veri, birbiriyle bağlantısı kurulmamış, sayısal ortamlarda taşınan sinyallerken, bilgi verinin anlam ifade edecek şekilde düzenlenmiş halidir. İşlenmiş veri olarak da belirtilebilen bilgi, bir durum hakkındaki belirsizliği azaltmaktadır. Bilginin farkına varılması ve anlaşılmasıyla ise özbilgi oluşmaktadır. Yani, verileri biraraya getirip işlemek bilgiyi, daha fazla ve dikkatli olarak işlenmiş bilgi ise özbilgiyi oluşturmaktadır.

**Bilgi ve Bilgisayar Güvenliği**

Her geçen gün dünyada ve ülkemizde bilgisayar ve internet kullanımının arttığını yapılan çalışmalar göstermektedir. Teknoloji günlük hayatın birçok bölümüne artarak yerleşmektedir. Türkiye İstatistik Kurumu'nun [TUİK] yaptığı araştırmaya göre; Türkiye nüfusunun %54,8'i bilgisayar kullanırken, bu kullanıcıların %55,9'u internet kullanmaktadır. Ayrıca, 2015 yılı girişimlerde bilgisayar kullanım oranı %95,2 iken, hanelerde % 54,8'dir.İnternet erişimine bakıldığında ise girişimlerde %92,5 iken, hanelerde % 55,9'dur.Bu istatistikler sonucunda da görülmektedir ki ülkemizde bilgisayar ve internet kullanım oranı oldukça yüksektir.

Teknolojinin yaygınlaşması, kurumlarda teknolojiye bağımlı bilgi sistmeleri tasarlanmasını sağlamıştır. Bu sistemler işlevselliği arttırırken, maaliyeti azaltmakta ve kullanım kolaylığı sağlamaktadır. Bu sistemlerde bilgi güvenliği kavramı ilk sıralar mevcut değildi, ancak zamanla sistemlerdeki kırılganlıklar farkedildikçe, bilgi güvenliğinin öneminin farkına varılmıştır.

Dolayısıyla, gizli zayıf yönleri tanımlamak ve yönetmek için bir ihtiyaç doğmuştur ve sistemin güvenlik açıklarını belirlemekle bilgi sistemlerine verebileceği zararları sınırlamak için Gizlilik, Bütünlük ve Uygunluk alanları tanımlanmıştır. Ancak zamanla güvenlik açıkları, saldırganlar tarafından gittikçe daha hedefli ve karmaşık olarak kullanılmaktadır. Saldırganların teknikleri ve yöntemleri olağanüstü bir şekilde sürekli değişmektedir (Richardson & Director, 2008;Symantec,2009 ).

Bilgi güvenliğinin en büyük tehditlerinden biri de kurum çalışanlarıdır. Saldırganlar, kurumun altyapısına oldukça benzer sistemlerle, saldırıları içeriden gerçekleştirmektedirler. Yani çalışanları kullanarak içeriden saldırılar yapmaktadırlar. Yalnız bu saldırıda kullanılan çalışanlar her zaman işinden memnun olmayana ya da casusluk yapan kişiler değildir. Çoğu zaman kötü niyetli olmamakla birlikte bilgisiz davranan çalışanlardır (CTG, [Corporate Technology Group], 2008).

Birçok kurumda, bilgi güvenliği riskleri tanımlanmış, değerlendirilmiş, işlenmiş ve düzenli olarak rapor edilmiş olmak zorundadır. Kurumlar, kullandıkları teknolojiyle ilgili oluşabilecek güvenlik risklerini tanımlayamadıkları için, kullanıcılar ya da sistem beklenmedik bir şekilde birçok zarar görmüş olabiliyor (Blakley, McDermott ve Geer, 2002).Bundan dolayı, kurumların güvenilir bilgi güvenliği risk değerlendirilmesi yapacak ve risk yönetimindeki tehdit çerçevelerini belirlemelerini sağlayacak bir sisteme ihtiyaçları olmuştur.

Bilgi Güvenliği, varlık olarak düşünülen bilginin, doğru teknoloji, doğru amaç ve yöntemle hasarlardan korunarak doğru şekilde kullanılmasını sağlama ve istenmeyen kişilerce elde edilmesini önleme olarak tanımlanmaktadır. Bilgi güvenliğinin amacı, bilgileri ve bilgilerin sağladıkları işleri sürekli olarak koruma altına almak ve bu çerçevedeki iş kazaları sonucu kaybolan bilgi miktarını düşürmek, ayrıca güvenlik olaylarından en düşük derece etkiyle kurtulabilmektir (Solms, 1998).

Genellikle, bilgi güvenliği üç önemli açıyla değerlendirilir (C.Pfleeger, Pfleeger ve Margulies, 2015; Solms, 1998).

Bunlar;

**Gizlilik:** Bilgisayara ve içinde bulunan bilgilere, sadece yetkili kullanıcılar erişebilir.

**Bütünlük:** Verilerin yetkisiz kişilerce erişilmemesi, değiştirilmemesi durumudur.

**Kullanılabilirlik:** Bilgi ve ilişkili varlıklara, ihtiyaç halinde yetkili kullanıcının erişebilme hakkının olmasıdır.




*Şekil 1.* Bilgi güvenliğinin temel üç boyutu (C.Pfleeger, Pfleeger ve Margulies, 2015; Solms, 1998)

Teknolojinin getirdiği bilgiyi işleme ve iletişim araçları, bilginin üretilmesini, depolanmasını, kullanılmasını, korunmasını ve paylaşılmasını hızlı bir şekilde arttırmıştır. Bilgi yoğunluğu içinde kalan insanlar, aradıkları bilgiye doğrudan ulaşacak yöntemler aramaktadırlar. Bu durum bilginin taşıdığı değerin önemini ortaya koymuştur. Elde edilen bilginin taşıdığı değeri ölçmek, bilgi kadar önemlidir ve bu değeri ölçem için bilginin doğruluğuna, güncelliğine ve bütünlüğüne bakılması gerekmektedir. Ülkelerde olduğu gibi kişiler ve kurumlar için bilgi, elde edilmesi ve muhafaza edilmesi zor olan bir varlıktır. Bilgiyi muhafaza etme, kullanımındaki karmaşayı ve kötüye kullanımı önleyeceği gibi, bilgiyi bir emek sonucu elde eden gerçek ve tüzel kişlerin haklarının korunması da sağlanacaktır (Canbek, 2005).

Teknolojik aletlerde güvenliğin temel amacı, bu teknolojiyi kullanan kullanıcıların, karşılaşabilecekleri tehdit ve tehlikelerin analizini yapmak ve gerekli önlemleri almaktır. Bilgisayar güvenliği ise; kullanıcıların sadece izin verilen alanlarda etkinlik gösterebileceği güvenli bir bilgi işleme platformu oluşturma gayretleridir. Bu güvenlik durumu güvenlik politikasının belirlenmesi boyutunda değerlendirmektedir. İzin verilen alanlar yazılım, donanım, veriler, kullanıcı işlemleri ya da bunları birleşimidir. Bütün bunlardan önce de hangi bilginin kime karşı korunması belirlenmelidir (Pfleeger, Pfleeger ve Margulies, 2015). Güvenliğin en zayıf halkası, dolayısıyla en önemli bileşeni insan davranışıdır. Son yıllarda yapılan çalışmalarda, güvenliğin sağlanması için insan faktörünün öneminden bahsedilmiştir. (Brostoff ve Sasse, 2001; Scheier, 2000).

Trcek, Trobec, Pavešic ve Tasic'e (2007) göre; bilgi sistemlerinin ve bilginin güvenliğini korumak için en önemli çabanın teknolojileri geliştirmek olduğunu söylese de, son zamanlarda yapılan çalışmalar göstermiştir ki insan faktörü merkezdedir ve en önemli rolü oynamaktadır. Hatta kurumlardaki büyük güvenlik yaklaşımları ve koruma metotları hala dışarıdan gelen saldırılara odaklanmaktadır ve bu durum güvenlik olaylarını azaltmakta etkili olamamıştır (Pahnila, Siponen ve Mahmood, 2007). Onlar güvenlik farkındalığı düşük bireylerden dolayı saldırılara mağlup düşmektedirler.

Bilgisayar güvenliğindeki insan faktörü dikkate alınmadığında, kurumların yüklü miktarda harcama yaptıkları güvenlik duvarları, şifreleme ve güvenli erişim cihazları gibi teknik önlemler yeterli miktarda alınsa bile, en zayıf halka olan insan faktörünü kapsamadığı için güvenliğin sağlanamayacağı, ayrıca yapılan yatırımlarında etkisiz olacağı belirtilmiştir (Poulsen, 2000). Bu çerçevede bilgi güvenliği sistemleri tasarlanırken insan faktörü daha iyi

anlamaya çalışılmalı ve kullanıcıların bilinçlendirilmesi ve farkındalık oluşturulması için eğitim programları ile destek sağlanması gerekmektedir (Gonzales ve Sawicka, 2002).

**Bilgi Güvenliği İlkeleri**

Bilginin korunması için "Bilgi Güvenliğinin" temel boyutları tanımlanmıştır. Bunlar, bilginin gizliliğini, bütünlüğünü ve kullanılabilirlik ya da erişilebilirlik boyutlarını temin altına almayı amaçlamıştır.




*Şekil 2*. Bilgi güvenliği boyutları

Şekil 2'de gösterildiği gibi, Kullanılabilirlik (Availability), Gizlilik (Confidentiality), Bütünlük (Integrity), Kimlik Doğrulama (Authentication) ve İnkâr edememe (non-repudiation) bilgi güvenliğinin temel boyutlarındandır. Bunlara ek olarak Sorumluluk (Accountability), Erişim denetimi (Access control), Güvenirlilik (Reliability) ve Emniyet (Safety) gibi boyutlarda bilgi güvenliğini desteklemektedir.

**Kullanılabilirlik**

Kullanılabilirlik; yetkilendirilmiş kişilerin, insanların ya da bilgisayar sistemlerinin bilgilere zorlama ya da engel olmadan, gerekli formatlarla erişilebilmesidir. Araştırma kütüphanelerine girilmeden önce tanımlama yapıldığı gibi ve kütüphanecilerin kütüphane içeriğini koruyabilmek adına şifreleme politikası oluşturarak kütüphanedeki değerli bilgileri

yalnızca yetkilendirilmiş kişilerin görebilmesini sağladığı gibi, bilginin kullanılabilirlik boyutununda sağlanması gerekmektedir (Whitman ve Mattord, 2012).

Kullanılabilirlik farklı anlamlara gelebilmektedir. Ancak kısaca bir sistemin erişilebilir ya da kullanılabilir olması için;

- Kullanışlı bir yapıda olması,
- Servisin ihtiyaçlarını karşılayabilecek kapasitede olması,
- Sınırlı bir bekleme modunda, işlemini net yapması.
- Kabul edilen zaman peryodlarında işini tamamlaması gerekmektedir.

Bu basamaklar tamamlandığı zaman kullanılabilirliğin tanımı yapılmış olmaktadır (C.Pfleeger ve Pfleeger, 2015).

**Gizlilik**

Bazı bilgilerin özel korumaya ihtiyaçları vardır. Bu bilgiler, öğrencilerin notları, finansal kayıtlar, medikal kayıtlar ve vergi evrakları gibi hassas verilerdir. Bunlara ek olarak, diplomatik meseleler, askeri sırlar ve eğitim sınavları gibi verilerin gizliliğinin dikkatli bir şekilde kontrol edilmesi gerekmektedir. Bu bilgiler önemli olduklarından dolayı, herkese açık olmamaları gereken durumlar olabilmektedir. Örneğin, askeri bir kurumun yemek siparişi zararsız gibi görünebilir fakat sürekli ve normalden fazla yapılan siparişler, yakında bir çatışma çıkacağının belirtisi olabilmektedir. Dolayısıyla, gizlenmesi gerekiyorsa bazı durumları ortaya çıkaracak bilgiler olabilmektedir (C.Pfleeger ve Pfleeger, 2015).

Gizlilik, bilgi sistemlerinde korunması gereken bilgilere, sadece yetkili kişilerin ulaşabileceğini garanti altına alan sistem olarak tanımlanabilir. ISO tarafından yayınlanan ISO-17799 “Bilgi Güvenliği Yönetim Standardı” belgesinde gizliliğin sadece erişim izni olan birimlerce erişilebilmesini garanti etmek olarak tanımlanmaktadır.

Verilerin gizliliği;

- Yetkisiz bir kişinin verilere ulaşması durumunda,
- Verilerde yetkisiz bir yazılım çalıştığı zaman ya da işlem yapıldığı zaman,
- Verilerin bir boyutuna ulaşmak için yetkilendirilen kişinin, başka boyutlara da ulaşması ya da verilerin diğer parçalarının olduğunu öğrenmesi gibi durumlarda sağlanmamış olmaktadır.

Bilginin gizliliğini korumak için alınabilecek önlemler;

- Bilgiyi sınıflandırmak,
- Dokümanların saklandığı dosyaları güvence altına almak,

- Genel güvenlik politikalarını uygulamak,
- Bilgiyi yönetenleri ve kullanıcılarını güvenlik konusunda eğitmek olmalıdır.

Çalışanlar, müşteriler ve hastaların personel bilgilerinin gizliliği özellikle çok değerlidir. Gizli bilgilerin açığa çıkması problemleri meydana getirir. Bazı zamanlar bu ifşa etme kasıtlı olsa da çoğu zaman bir hata sonucu meydana gelir. Örneğin, kurum hakkındaki gizli bilgiler yanlışlıkla kurum içinden ziyade kurum dışına e-maille çıkarılması, birçok gizlilik ihlaline sebeb olmaktadır (Whitman ve Mattord, 2012).

Pfleeger (2015), bilginin gizlilik boyutunu sağlamanın yöntemini tanımlamak adına bir desen tarif etmiştir. Bu desende, veri parçalarına erişebilmek için özel kanallarla yetkilendirilmiş kişi, sistem ya da işlem vardır. Bu kişi, sistem ya da işlemi özne (Subject) olarak tanımlanmış, erişim çeşidini (veriyi okuma, yazma vs.) erişim modu olarak ve yetkilendirilmeyi politika olarak tanımlamıştır. Bu 4 bileşen, bilgisayar güvenliğinin temel boyutlarını oluşturmaktadır. Şekil 3'te bu boyutlar gösterilmiştir.

Ayrıca bilgisayar güvenliğinde, gizlilik istenilen bilgie erişmek yada ulaşmakdır ama değiştirmek değildir. Değiştirmek boyutu bütünlük kısmını ilgilendirmektedir.




*Şekil 3.* Bilgi gizliliği oluşturma bileşenleri (Pfleeger, 2015)

**Bütünlük**

Bilgi, hatalardan uzak olduğu zaman ya da son kullanıcıların hatalar konusunda uzmanlaştığı zaman bütünlük sağlar. Bilgi bilerek ya da bilmeyerek değiştirilirse, bütünlüğünü kaybetmiştir. Örneğin bir banka hesabı düşünüldüğünde, bu hesap finans sektöründe hesabın sahibi ve hesapta bulunan miktarı temsil eder. Bu hesaptaki yanlış bilgi, içerden ya da dışarıdan saldırılara sebeb olabilir. Banka görevlisi ya da hesabın sahibi, bu hesaba

yanlışlıkla birşeyler eklerse ya da değiştirirse hesabın bilgisi değişmiş olur. Her iki durumda da banka hesabı hisse senetlerinin yükselmesi gibi birçok hataya sebeb olabilir (Whitman ve Mattord, 2012).

Örnekte görüldüğü gibi, verilerin yetkisi olamayan kişilerce bilerek ya da bilmeyerek değiştirilmemesi, parçalanmaması ve kaybedilmemesi bilginin bütünlük boyutunun sağlanması anlamına gelmektedir. Bütünlük, bilgi ve bilgiyi işlemenin yöntemlerinin doğruluğunu ve bütünlüğünü garanti altına alma, ayrıca yetkisi olmayan kişiler tarafından da değiştirilmemesini sağlamaktır. Verilerin bir yerden başka bir yere iletilmesi veya taşınması sırasında belirlenen yolların değişmemesi, sırasının değişmemesi ve tekrarının yapılmaması durumunda veri bütünlüğü sağlanmış olmaktadır (Tekerek, 2008; Canbek, 2005; Gökmen, 2013; Vardar, 2009).

Bilginin bütünlüğünün sağlanmadığı durumlarda ortaya çıkabilecek zararlar konusunda geçmiş zamanlarda birçok hadise yaşanmıştır. Örneğin yıllar önce Word dökümanına kötücül bir makro yerleştirilmiş ve bu makro bazı rastgele kelimelerin mastar kısmına olumsuzluk eki getirmiştir. Belge söz dizimi olarak doğru olduğu için, uzun bir süre kullanıcılar tarafından farkedilmemiştir ve bu durum birçok zarara yol açmıştır (C.Pfleeger, Pfleeger ve Margulies, 2015). Yapılan saldırılar sonucu, son kullanıcıların farkında olmadan veya istemeden bir dosyayı silmesi, önemli dosyalardaki bilgilerin değişmesi ve bu dosyalara ya da sisteme virüs bulaşması veri bütünlüğünü bozacak örneklerdendir (Delialioğlu, 2011).

Bilginin bütünlüğünü sağlamak, gizliliğini sağlamaktan daha zor bir durum olduğunu söyleyen C. Pfleeger ve Pfleeger (2015), bütünlüğün farklı içerikleri ya da bileşenleri barındırması gerektiğinden bahsetmiştir.

Bu bileşenler;

- Kesinlik
- Doğruluk
- Değiştirilmemişlik
- Sadece kabul edilen yollarla değiştirilmiş olması
- Yetkili kişilerce değiştirilmiş olması
- Tutarlı
- Kendi içinde tutarlı
- Anlamlı ve kullanılabilir olmasıdır.

### Kimlik Tespiti

Sistemlere girmek isteyen kişilerin doğru kişi olduğundan emin olunma süreci kimlik kanıtlama sürecidir. Geçerli kullanıcı ve sistemlerin tanınması ve doğrulanması ve kullanıcıların hangi kaynaklara erişim hakkının olduğunun belirlenmesi işlemleri kimlik tanımayı oluşturmaktadır (Tekerek, 2008). Güvenliği sağlamak adına, neredeyse tüm teknolojik sistemlerde kimlik tespiti yapılmaktadır (Pfleeger ve Pfleeger, 2015). Parola, pin ve şifre gibi uygulamalar kimlik tespitini sağlamak içindir.

### İnkâr Edememe

İnkâr edememe, çalışan sistemde göndericinin mesajı gönderdiğini alıcının ise mesajı aldığını inkar edememesidir (Pfleeger, Pfleeger ve Margulies, 2015). Mesajı alan ve verenler sırasıyla tanımlanabilir (Canbek, 2005). Bankacılık gibi sektörlerde, gönderici ile alıcı arasında çıkabilecek anlaşmazlıkları önlemektedir.

### Sorumluluk

Eylemlerin yapılmasında kimlerin yetkili olduğunu belirleme sistemidir. Genel olarak, faaliyetlerin kayıtlarını tutmak için kayıt tutma sistemi ve bu kayıtları inceleyecek hesap inceleme sistemi gerekmektedir (Canbek, 2005).

### Süreklilik

Erişim yetkisi verilen kullanıcıların, erişmek istediği verilerin güncel kalabilmesi ve bu verilere sürekli olarak ulaşılabilinmesi sürekliliği oluşturmaktadır. Bilgi sistemlerinde meydana gelen yazılım hataları, kötü niyetli saldırganlar, sistem kullanıcılarının eğitimsiz ve bilgisiz olması veyahut fiziksel şartlarda meydana gelen ses, ışık, nem gibi değişiklikler sistem sürekliliğini etkileyebilmektedir. Sürekliliğin amacı, bilgi sistemlerini içeriden ya da dışarıdan gelebilecek arızalara karşı korumaktır.

Bilgi sistemlerinin sürekliliğini korumak için, kullanıcıların bilgi ve becerilerini artıracak eğitimlerin verilmesi ve sistemlerin çalışmasını engelleyecek durumların önceden analiz edilerek belirlenmesi ve çözümler üretilmesi gerekmektedir (Delialioğlu, 2011).

### Kayıt Tutma

Bilgi sistemleri üzerinde meydana gelen olayların ve ağ geçmişinin, daha sonra analizi yapılmak üzere kayıt altına alınmasıdır. Sistem üzerinde yapılan web sayfalarında gezinme,

e-posta gönderme, parola yazılarak kullanıcı girişi sağlama gibi faaliyetler kayıt altına alınarak, olası bir saldırı durumunda yöneticilere uyarı mesajı gönderilir veya saldırı izi takip edilir. Böylece, bu kayıtlar takip edilerek saldırıyı yapanların kimliğine ulaşılabilir (Tekerek, 2008).

**Güvenirlik**

Bilgi sistemlerinin planlanan davranışı sergilemesi, bilginin güvenirlik boyutunu oluşturmaktadır. Sistem tasarlanırken planlanan durumların, eksik ya da fazlası olmadan, sürekli ve kesin bir şekilde çalışması ve bu durumun hep aynı kalması güvenirlik olarak tanımlanmaktadır (Canbek, 2005).

**Emniyet** ise; bilgi sisteminin yerleştirildiği ortamda, kendisini ya da yerleştirildiği ortamı tehlikeye düşürecek isteyerek ya da istemeden yapılan etkinlik ve olaylara sebebiyet vermemesi durumudur.

**Erişim denetimi** ise, bir bilgi sistemine erişebilmek için belirli yetkilendirilme işlemlerinin yapılmasıdır.

**Bilgi Güvenliğini Sağlama Süreçleri**

Güvenlik, karşılaşılabilinecek tehditlere karşı önlem almaktır. Gelebilecek tehlikeleri önceden analiz edip önlem alma süreci ilk olarak önleme basamağıyla başlamaktadır. Önleme basamağı en dikkat edilmesi gereken adımdır. Bilgisayar sistemlerine karşı yapılan saldırı ve tehditlere karşı sistemlerin hazır olması için çeşitli önlemler geliştirilmektedir.

Bu önlemler şöyle olmalıdır;

- Kişisel bilgisayarlar için, kurulu bir virüs programı olması,
- İşletim sisteminin güncellemelerini düzenli aralıklarla yapıyor olması,
- Ekran koruyucunun şifreli olması ve bilgisayarda belirli bir süre işlem yapılmadığı zaman ekran koruyucunun devreye girecek şekilde ayarlanması güvenliğin temel prensiplerini oluşturmaktadır. Ayrıca;
- Bilgisayara erişmek için kullanılan şifrelerin tahminin zor olması ve belirli aralıklıklarla değiştirilmesi,
- Önemli olan dosyaların şifre ile saklanması ve önemli dosyaların sürekli yedeklerinin alınması,

- İnternetten indirilen dosyalar ve e-mail eklerinde emin olunmadığı durumda açılmaması,
- Güvenlik sertifikası olmayan sitelerde alışveriş yapılmaması,
- İnternetin kullanılmadığı durumlarda kapalı tutulması gibi sorunları önleyecek tedbirlerin alınması gerekmektedir (C. Pfleeger ve Pfleeger, 2015).

Ancak sadece önlemek güvenliği sağlamada yeterli olmayabilmektedir. Önleme yapılacak olan saldırıları herzaman engelleyememesine rağmen güçleştirebilmektedir. Saldırı girişimlerini de belirleyecek yöntemlerin kullanılması gerekmektedir. Saldırı belirleme yöntemi ile önceden bilinen ya da yeni ortaya çıkan saldırılar rapor edilip, uygun saldırıları karşılama yöntemleri kullanılır. Saptamanın yapılması için sistemin tüm hareketlerinin izlenmesi ve kaydının tutulması gerekmektedir. Güvenlik duvarları ve ağ trafiği izleyicileri bunları sağlayan bazı uygulamalardan bazılarıdır.

Önleme ile durdurulamayan ve tespit edilmiş saldırı girişimlerine en kısa sürede cevap verilmesi ve saldırı önlenmese bile sistemin eski haline dönmesi gerekmektedir.Ayrıca saldırının sebeblerini belirlenmesi süreci güvenliği sağlamanın en son basamağını oluşturmaktadır. Daha önceden yapılan saldırıların belirlenmesi ve alınacak önlemlerin iyi bir şekilde planlanması zaman ve para kaybını önleyecektir.

**Sistemlere Yapılan Saldırılar ve Türleri**

Sistemlere yapılacak saldırılan analiz edilerek sınıflandırılması, gelecekte gerçekleşebilecek saldırıların tahmin edilmesini kolaylaştırmaktadır.Saldırı türlerinin sınıflandırılarak, bu saldırılara karşı alınabilecek önlemlerin belirlenmesi gerekmektedir. Saldırılar; sayısına, türüne ve kullanılan aracına göre sınıflara ayrılabilmektedir.

Tek kişi ile yapılan saldırılar solo saldırı olurken, birden fazla kişilerin karıştığı saldırılar çoklu saldırı olarak sınıflandırılmaktadır. Yetkisiz erişim gibi saldırılar solo saldırıyken, IP kandırma, e-posta bombardımanı gibi saldırılar çoklu saldırı sınıfına girmektedir.

Başlıca saldırı çeşitleri ise;

- Arka kapılar,
- Doğrudan erişim saldırıları,
- Dolaylı saldırılar,
- Hizmet aksattırma saldırıları (DoS),
- Kaynak kod istismarı,

- Gizli dinleme,
- Sosyal Mühendislik.

**DOS Saldırıları (Denial of Service)**

Bu saldırının temel amacı, hedefteki bilgisayarın, sunucunun veya ağın kaldıramayacağı kadar yük binmesini sağlayarak, sistemleri kullanılmaz hale getirmektir. Bu işlemi genellikle, disk alanının tüketilmesi, bant genişliği ve işlemci gibi kaynakların bitmesi yöntemi ile ya da fiziksel ağ bileşenleri ile yapılandırma bilgilerinin bozulması gibi yöntemlerle yapılmaktadırlar.

Bu saldırılar, diğer tipik saldırılar gibi kontrolü ele geçirmek ya da bilgileri ele geçirmek amacıyla yapılmamaktadır. Sistemlerde önemli olan bir sunucunun böyle bir saldırıya uğraması, tüm sistemin işlemez hale gelmesini sağlamaktadır. Önlenmesi zor olan saldırı türlerindendir (Whitman ve Mattord, 2012; Canbek ve Sağıroğlu, 2007).

**Ddos Saldırıları (Distributed Denial Of Service)**

DDos saldırıları ise, birden fazla bilgisayarın koordineli olarak aynı anda kuvvetli bir sunucuya ya da sisteme saldırmasıdır. Bu saldırıyı yapan bilgisayarlar ele geçirilmiştir ve Zombi bilgisayara dönüşmüştür. Tek bir sistemle DDos ataklarını durdurmak çok zordur. DDos saldırılarının internet üzerinde, kitle imha silahlarına benzetildiği meşhur bir methapor bulunmaktadır ( Whitman ve Mattord, 2012).

**E-Posta Bombardımanı (e-mail Bomb)**

DoS saldırılarından biri olarak da adlandırılabilinen mail bombardımanı, hedef olarak belirlenen kişinin posta adresini binlerce e-posta ile doldurabilen ve böylece sistemin hafızasını ve işlem yapma durumu aksatan, hizmet durdurma saldırılarından biridir. Eğer bu gelen e-postalarda bir tuzak varsa ve kullanıcı bu tuzağa düşerse, sistemin bağlı olduğu diğer sistemlerde aynı posta saldırılarına maruz kalabilmektedir. Gönderilen e-postaların nereden geldiği ya da kim tarafından geldiğini bilmek de pek mümkün olamamaktadır (Whitman ve Mattord, 2012).

**Gizli Dinleme (eavesdropping)**

Kanal ya da bir ağ üzerinden iletimi sağlanan verilerin kötü niyetli üçüncü kişiler tarafından, araya girerek alınması veya değiştirilerek hedefe gönderilmesi olayıdır. Etkileşimsiz tek başına çalışan bir bilgisayar dahi ekran veya yazıcı gibi elektronik parçalarından yayılan

elektromanyetik dalgalarla gizlice dinlenilebilmektedir (Sağıroğlu ve Canbek, 2007).

### Kaynak Kod İstismarı (Code Exploit)

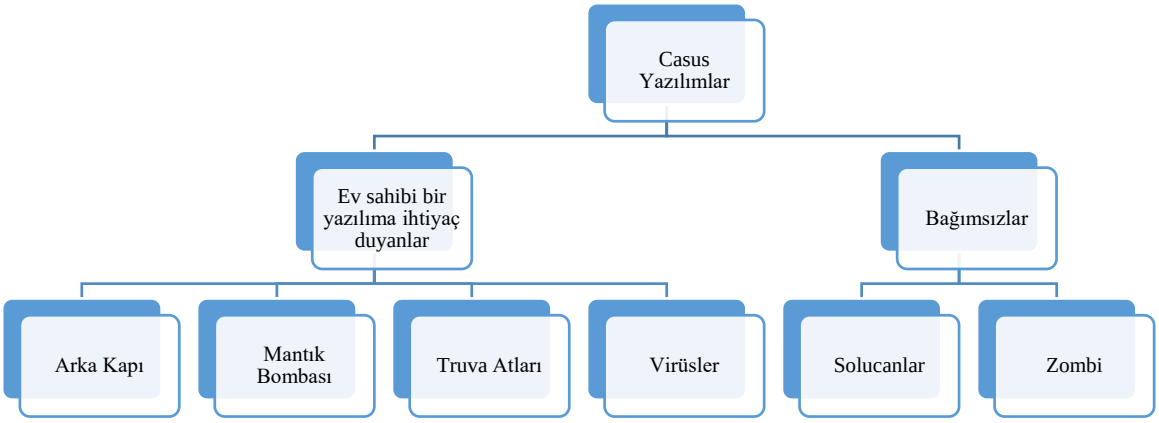
Bilgi sistemlerinde kullanılan yazlımlar üretilirken kod hatası ya da şifreleme hataları gibi yazılım kusurları bulunabilmektedir. Ayrıca sistem belleklerinde statik ve dinamik değişkenlerin tutulduğu sıralı hafıza blokları bulunmaktadır ve bu blokların taşıyabileceği veri miktarından daha fazlasını yüklemek bu hafıza bloklarının sınırlarının aşılmasına sebeb olmaktadır ve bu duruma bellek taşması (Buffer overflow) denilmektedir. Yazılım kusurları ve bellek taşması gibi durumlar, bilgisayar sisteminin beklenmedik şekilde çalışmasına ya da ele geçirilmesine sebeb olabilmektedir.

### Arka Kapılar (back doors)

Bilgisayar sistemlerinde incelemeler yapıldığında bulunamayan ancak o sistemin yazılımını yapan kişi tarafından gerektiğinde sisteme erişmek için konulan, bilgisayarla uzaktan bağlantı kurmayı sağlayan yöntemlere arka kapılar denilmektedir. Arka kapılar program şeklinde de olabilmektedir ( Whitman ve Mattord, 2012). Konulan arka kapılar sistemin kayıtlarına olağan düzeyde eklendikleri için fark edilmesi oldukça zor olmaktadır. Arka kapılar yıllardır sistem yöneticileri tarafından sistemi test etmek ya da bir hata olduğu zaman girip düzeltebilecekleri bir araç olarak tanıtılmıştır. Ancak her ne kadar sistem yazılımcısı yerleştirse de, saldırgan gruplar bu arka kapıları keşfederek sisteme sızabilmektedirler. Truva atları gibi gizliden çalışan program arka kapı amacıyla kullanılmaktadır. Ve arka kapıların girişlerinin tespiti de oldukça zor olmaktadır bu yüzden zararının büyüklüğünü engellemek için sistemlerin düzenli yedeğini almak gerekmektedir (Tak, Dixit ve Park, 2004).

## Bilgi Güvenliğini Tehdit Eden Unsurlar

Bilgisayar sistemlerine bulaşan ve bulaştığı makinelere zarar vermek için üretilen yazılımlara kötücül yazılımlar denilmektedir. Bilgi sistemlerine yapılabilecek bir saldırı, sistemdeki verilerin çalınmasına, değiştirilmesine veya yok edilmesine sebep olabilmektedir. Bu saldırılar, belli kötücül yazılımlar aracılığıyla gerçekleşmektedir.




*Şekil 4.* Casus yazılımların sınıflandırılması (William Stalling, 2011)

William Stalling (2011)'in yaptığı sınıflamaya göre, casus ve zarar veren yazılımlar konaklamak için bir yazılıma ihtiyaç duyanlar ve bağımsızlar olarak ikiye ayrılırken, birinci gruptakiler uygulama yazılımı ya da işletim sisteminin içine yerleşirler. Diğer grupta olanlar ise yerleşmek ve çoğalmak için herhangi bir yazılıma ihtiyaç duymazlar, kendiliğinden çoğalabilirler. Sadece birinci gruptaki virüsler kendiliğinden çoğalma konusunda ikinci gruba katılmaktadır.

Belli başlı kötücül yazılımlar;

- Virüsler,
- Solucanlar,
- Truva atları,
- Sömürücüler,

en geniş çerçevede bakılabilecek kötücül yazılımlardır.

**Virüsler (Viruses)**

Organizmadaki hücrelere bulaşan ve zarar veren küçük parçacık olarak bilinen biyolojik virüslerden esinlenerek isimlerine virüs denilmiştir. Kötücül yazılımlarının en tehlikeli ve en eskisi olarak kabul edilirler. Çünkü kendi kendilerine çoğalabilen kodlarla veya belgelerle yayılırlar ve bu kopyalarını çalıştırabilmektedirler. Ayrıca önemli dosyaları silmek ya da host sistemini tamamen çalışmaz hale getirmek gibi yıkıcı etkileri de bulunmaktadır. Disket, cd, flash bellek ve Dvd gibi ortamlarla ve e-posta ekleri ile yayılarak hedefledikleri sisteme bulaşırlar (Canbek ve Sağıroğlu, 2007).

Günümüzde virüslerin çoğalmasıyla birlikte virüs koruma programları da çoğalmış ve kendilerini geliştirmişlerdir. Artık koruma programları bilgisayarların vazgeçilmez bir parçası olmuştur. Bilgisayar kullanıcılarının virüslerin nasıl çalıştığını ve sistemlerine verebilecek zararları biliyor olması gerekmektedir. Çünkü birçok kurumda tüm bilgisayarların bir virüs programıyla korunması gerekirken, birçok kullanıcı koruma programlarını bilgisayarlara yüklememektedirler. Ayrıca kullanıcıların sadece düzenli olarak bilgisyarlarını taratmalarının yeterli olmadığını, indirdikleri dosyaları, mailleri ya da sürücüleri taratmaları gerektiğini bilmelidirler (Whitman ve Mattord,2012; Tak, Dixit ve Park, 2004).

Bilgisayar virüslerini dosya virüsleri, önyükleme virüsleri, makro virüsleri ve script virüsleri olarak dört bölümde değerlendirmek mümkündür.

- Çalıştırılabilir dosyalara kendini kodlayarak veya çoğalmak için kendini dizinlere kopyalabilen virüs türleridir.
- Önyükleme (boot) virüsleri ise sabit diskin ön yükleme kaydını değiştirerek, bilgisayar açıldığında virüslü olan kodun çalışmasını sağlayan virüslerdir.
- Makro virüsleri, Microsoft Word ve Excel gibi güçlü makro desteği bulunan ofis programlarını kullanan ve programların açılmasıyla çalışan makrolara bulaşan virüs türleridir.
- script virüsler ise, PHP, Visual Basic gibi script programlama dilleri kullanılarak yazılan virüs çeşitleri olmak üzere komut hizmet dosyalarına bulaşarak çok bileşenleri virüslerinin birer parçası olarak çalışmaktadırlar (Canbek,2005; Stalling, 2011)

**Truva Atları (Trojons)**

Truva atları, gizleme hilesini kullanan kötücül yazılımlar olarak bilinir ve yasal yazılım gibi görünen kötücül yazılımlardır.

Aktifleşmesi için çoğu zaman kullanıcının etkinleştirmesini gerektiren bu yazılımlar, kendi kendine çoğalmayan ve iyi programlara paketlenmektedirler ( Kissel, 2013; Stalling, 2011).

Truva atlarının;

- Bulaştıkları bilgisayarda bulunan şifreleri çalan,
- Bulaştığı makinenin uzaktan kontrolünü sağlayan,
- İnternet tarayıcısının ayarlarını değiştirerek kullanıcıyı belirli sitelere yönlendiren,
- Bulaştığı maddeye kullanıcının haberi olmadan kötücül yazılım yükleyip çalıştıran,
- Hizmet aksatma saldırıları için kullanılan,

- Tuş basımı, ekran görüntüleri gibi faaliyetleri kopyalayarak saldırgana gönderen, bulaştığı sistemin Ip adresi, e-posta adresi vb. gibi bilgileri saldırgana gönderen,
- Mesaj sağanağı için saldırgana, bulaştığı makinenin internet erişimi gibi imkânlar sunan türleri bulunmaktadır.

  Ayrıca, dosyaları sıkıştırmaya ve açmaya yarayan programları çalışmaz hale getirmek amacıyla hazırlanmış Truva atları da bulunmaktadır. Bu casus yazılımların amacı, sistemin belleğini gereksiz verilerle doldurarak, sistemi çalışmaz hale getirmektir. Arşivlenen dosyaların içeriğini tekrar ederek, arşivlerin dolmasına sebep olmaktadır (Canbek, 2005).

**Solucanlar (Worm)**

Yukarıda bulunan Şekil 4'de de görüldüğü gibi, solucanlar yayılmak için kendilerine konak bir ortam aramazlar zira yayılmak ve çoğalmak için başka bir programa ihtiyaçları yoktur. Yapısal olarak virüslere benzeseler de, bu konuda virüslerden ayrılmaktadırlar. E-postalar ve internet siteleri solucanların yayılması için kullandıkları en yaygın yöntemlerdendir. Ayrıca solucanların çalışmalarını sağlama amacıyla sosyal mühendisliğe de başvurulduğu olmuştur. Kendilerini sürekli kopyalarlar ve bellekte çoğalmaları sistemlerin işlemlerini yavaşlatır, bu yavaşlatma sonucu da fark edilebilmektedirler.

- e-posta solucanı olarak bilinen, zarar veren yazılımların en çok bulaştığı yöntem olan posta eki yöntemiyle yayılan ve son kullanıcıyı eki çalıştırdığı an kendini başlatıp bilgisayara bulaşan özellikte olan solucanlarda vardır. Bu solucanların en tipik özellikleri bulaştıkları bilgisayardaki kişiler bilgisini toplayarak bu bulduğu adreslere kendilerini göndermeleridir.
- Solucanların internet üzerinde tarama yaparak, güncelleştirmeleri kurulmamış, anti virüs programı ya da güvenlik duvarı olmayan bilgisayarlar bulmayı hedefleyen ve buldukları zaman kendilerini makineye kopyalayan internet türleri de bulunmaktadır.
- Paylaşılan klasörlerde, dikkat çeken bir isim formatında kendini kopyalayan ağ solucanları da bulunmaktadır ve bu dosyaların çalışmasıyla solucanlar bilgisayara yerleşmektedir (Stalling, 2011; Canbek, 2005).

**Reklam Destekli Yazılım (Adware)**

Reklam yazılımları ya da reklam destekli yazılımlar genelde, yazılımın maliyetini karşılamak ve düşük fiyatta yüksek kalite sunmak için yararlı yöntemlerde kullanılır. Ancak pop-up açılır pencere ve reklam bandında (banner) yer alan reklamların arka planda bilgileri

toplayan kötücül yönleri olanları bulunmaktadır. Ya da ekrana gelen açılır pencerenin bir kötücül yazılım yüklenmiş siteye yönlendirmesi gibi durumları bulunmaktadır (Brodie, 2008; Stalling, 2011).

### Tuş Kaydedici Yazılımlar (Keylogger)

Sistem kullanıcılarının klavyeyi kullanarak girdikleri bilgileri kopyalayarak saldırganlara gönderen casus yazılımlardır (Stalling, 2011).

### Casus Yazılım Ve İz Sürme Çerezleri (Spyware Cookie and Tracking Cookie)

Çerezler internet tarayıcının daha iyi hizmet vermesi için hazırlanmış hizmet ürünleridir. Fakat her zaman iyi yönde çalışmamaktadırlar. Örneğin, kullanıcıların bilgilerini elde etme ve paylaşma amacıyla yapılmış Casus çerezler bulunmaktadır. Ayrıca, Kullanıcıların internet üzerindeki gezinme geçmişini izlemek amacıyla iz sürme çerezleri de bulunmaktadır. Bu çerezlerin etkisini kırmak amacıyla Do not follow me tarzı çerezler de üretilmektedir.

### Damlatıcılar

Bu casus yazılım, otomatik yazılım indirme yöntemlerini kullanarak, arka planda gizli ve yavaş bir şekilde bir yazılımın bilgisayara indirilmesini ve kullanıcıya farkettirmeden kurulmasını sağlamaktadır. Kullanıcı bu yazılımı farkedip, ona ait bileşenleri silse dahi, eksik olan kısımlarını tekrar indirerek varlığını tekrar sürdürebilecek derece de tehlikeli bir yazılımdır (Sağıroğlu ve Canbek, 2007).

### Şifre ve Gizli Soru Tahmini

Sistemlerin yönetimini ele geçirmek için çeşitli teknik ya da sosyal yöntemler kullanılmaktadır. Teknik altyapı gerektirmeyen, kullanıcının kontrolünde olan saldırı yöntemlerinden biri ise şifreyi ya da gizli soruyu tahmin etme yöntemidir. Kullanıcının şifresi ya da gizli soruya verebileceği cevaplar tahmin yöntemiyle bulunarak sisteme girmeye çalışılır. Kullanıcıların kimlik bilgileri ya da ilgi, hobi vb. gibi özellikleri bilinirse tahmin kolaylaşmaktadır. Sosyal medyada yapılan paylaşımlar sonucu gizli sorunun tahmini kolaylaşmaktadır. Ayrıca, unutmak kaygısıyla kolay oluşturulan şifreler, saldırganların işlerini kolaylaştırmaktadır.

**Omuz Sörfü**

Kullanıcıların bilgisayar sistemlerinde ya da Atm, internet bankacılığı hesabı gibi ortamlarda sifrelerini yazarken gizlice izlenmesidir. Şifrelerini herhangi bir yere yazan kullanıcıların, bu yazdıkları yerlerden şifrelerin okunması durumunda da şifreler ele geçirilmektedir.

**Çöpe Dalma (Dumpster Diving)**

Şifrelerin ya da önemli verilerin, dijital olmayan malzemelerin üzerine yazıp, işlem bittikten sonra atılması sonucu bilgilerin ele geçirilme yöntemi ise çöpe dalma ya da çöp inceleme olarak tanımlanmaktadır. Dijital ortamlarda türetilen dosyaların, işi bittikten sonra çöp kutusuna atılmasıyla ya da silinse dahi geri getirme programlarıyla bu verilere ulaşılması da bu yöntemle gerçekleşmektedir. Bu saldırılara maruz kalmamak için, kullanıcıların şifrelerde ve önemli dosyaların saklanmasındaki hassasiyeti önemli bir bileşendir (Okenyi ve Owens, 2007).

**Mantık Bombaları**

En eski yazılım türlerinden birisi olan mantık bombaları, herhangi bir yazılıma gömülü olarak sisteme girmekte ve sisteme girdikten sonra da uygun şartların oluşmasını beklemektedir. Bahsedilen uygun şartlar, haftanın belirli bir tarihinin gelmesiyle ya da kullanıcıların belirlenen bir programı çalıştırmasıyla saplanmış olur. Daha sonra mantık bombaları patlar ve sistemdeki veriler silinebilir, değiştirilebilir ve sistem çalışmaz hale getirilebilmektedir (Tak vd., 2004).Mantık bombaları bir çeşit Truva atları gibi davrandıklarından dolayı, sistemde belirlenen şartlar gerçekleşinceye kadar faydalı bir yazılmmış gibi görünmektedir. Ancak belirlenen süre gelince kendini göstererek sürekli zarar vermeye başlamaktadır (Alaca, 2008).

**Sql İnjeksiyon (Sql Injection Attack)**

SQL injeksiyon, bir veritabanına sql üzerinden sızma ya da ulaşma olarak tanımlanabilir. Veri tabanında kayıt ekleme, silme, güncelleme vb. işlemlerin yapılmasını sağlayan bir yazılım dilidir. Web yazılımları veri tabanı işlemleri yapılırken sql komutları kullanılır ve çok basit düzeyde yazılan sql komutları yazılımcının istemediği sonuçlara ulaşabilir ya da saldırganlara açık verebilir. Veri tabanı kullanan web sitelerine yapılan bu saldırılar, veri tabanındaki kayıtları görüntülemekle beraber değiştirip silebilmektedir (Stalling, 2011).

### Rootkitler

Rootkitlerin Türkçe anlamı kök kullanıcı takımıdır. İlk olarak Unix işletim sisteminde ortaya çıkmışlardır. Unix işletim sisteminde root yönetici demektir ve saldırganlar bir sistemin kontrolünü ele geçirince sisteme kök kullanıcıları eklemektedirler. Diğer casus yazılımlarda olduğu gibi, rootkitleri sisteme yerleştiren saldırganlar sistem üzerinde her konuda yetkili olabilmektedirler. Kök kullanıcılarının ilk nesillerinin tek başına çok bir zararı yok gibi görünmektedir ancak, sonraki sürümleri fark ettirmeden sisteme büyük zararlar getirmektedir. Ayrıca truva atları ya da virüslerle birleşebilen yapılarından dolayı sistemlerde gizli dinleme, bilgi toplama ve sistemleri yok etme gibi zarar kombinasyonları sağlamaktadırlar. Sistem kayıtlarını silerek kendini gizleyebilen ve bu özelliğinden dolayı saldırganların istediği zaman sisteme girmelerini kolaylaştıran araçları da bulunmaktadır. Diğer yazılımlardan farkı, kendilerini gizleyebiliyor olmalarıdır ve sıradan virüs taramalarında izlerine rastlanmamaktadır. Tespit etmek için özel anti-rootkit yazılımları kullanılmaktadır (Stalling, 2011).

### Exploit

Belirli bir güvenlik korumasızlığını hedef alan türde saldırılar üretebilen kötücül yazılımlardır. Exploit'in kelime anlamı ise kötüye kullanmaktır. Saldırganların, sistemlerin zayıflığından faydalanmak için yetkisi olmayan kullanıcılara yönetici yetisi katarak kullandığı yöntemdir. Bu tür yazılımlar sadece bu korunmasızlığın varlığını bütün dünyaya göstermek amacıyla yazıldığı gibi; ağ solucanları gibi zararlı programların bulaşma yöntemi olarak da kullanılabilirler. Exploit'in yazılması için ileri düzey programlama bilgisi gerekmektedir ve yazılan exploid uygulamaları çok bilgili olmayan kullanıcılar tarafından bile kolaylıkla kullanılabilmektedir. Saldırganlar bu uygulamalardan yüksek miktarlar kazanmaktadırlar(Canbek,2005; Gökmen,2013; Whitman ve Mattord,2012; Stalling, 2011).

### Tarayıcı Soyma

URL enjeksiyonu (URL injection) olarak da adlandırılan tarayıcı soyma, İnternet tarayıcı ayarlarını her zaman veya sadece belirli bölgeler için, kullanıcının belirlediği tarzın dışında davranmasına yol açan yazılımlardır. Bu, en basit olarak, tarayıcı açıldığında gösterilen başlangıç sayfasını (home page) istenilen sitenin adresi yapmak olabilir. Bunun dışında uygunsuz içerik veya reklam içeren çıkıveren pencereler gösteren tarayıcı soyma türleri de bulunmaktadır.

### Telefon Çeviriciler

Telefon çeviriciler, kurbanlarına büyük miktarlarda telefon ücreti ödetmek amacıyla, genellikle milletler arası uzak mesafe telefon numaralarını, hedef bilgisayar modeminin İnternet servis sağlayıcısının bağlantı numarası ile değiştirirler. Her zamanki gibi İnternet'e bağlanan kişi aslında farklı bir hattı kullandığının farkına vardığında çok büyük miktarlarda telefon faturası ile karşılaşabilirler. Bazı telefon çeviriciler ise, tuş basım bilgilerini ve şifre gibi önemli bilgileri, kullanıcı belli bir süre aktif olmadığı bir anda, korsana telefon hattı kullanarak gönderirler.

### Hırsız Yazılım (Thiefware)

İnternet tarayıcılarının içinde bulunduğu trafiğini yeni tarayıcı pencereleri açarak farklı sitelerede yönlendirebilen yazılımlardır. Daha çok üye sayısı önemli olan siteler için, üyelik komisyonlarını çalan uygulamalar olarak kullanılmaktadır (Canbek, 2005).

### Web Böcekleri (Web Bugs)

İz sürme böceği veya temiz gif olarak bilinen web böceği, bir mesajın ya da web sayfasının kim tarafından ve kaç saniye görüntülendiğini bilmeye yarayan bir tekniktir. Kullanıcıların farkına varmadığı bu yöntemde, küçük bir resim mesajın içine gömüldüğü için harici bir adresten mesaja tıklandığında indirilir ve resim dosya olarak indirildiği bu ortamın bilgisini tutar. Bu teknikle, resmi indiren kişinin IP adresi, resmin gösterilme süresi ve gönderilen e-posta adresinin geçerli olması gibi birçok bilgi saldırganlar tarafından görülebilmektedir (Canbek, 2005).

### Uzaktan Yönetim Aracı, RAT (Remote Administration Tool)

Bilgi sistemlerinin en büyük zarara uğrayabileceği, en tehlikeli yazılımlardan biri olan RAT yani uzaktan yönetim aracı, hedeflenen bilgisayar çevrimiçi olduğu zaman bu bilgisayara sınırsız erişim hakkı vermektedir. Bilgisayarın yönetimini ele geçiren saldırgan, bu yazılım sayesinde dosyaları ya da programları ekleyip silebilir ya da klavye gibi donanımları kontrol altına alabilmektedir.

### Zombi Bilgisayar

DDOS saldırılarının ya da Botnet saldırılarının gerçekleştirilmesi için saldırganların birden çok sistemi aynı anda ele geçirmeleri ve bu geçirdikleri sistemlerle saldırı yapmaları gerekmektedir. Ele geçirdikleri sistemleri zombileştirecek yani istediklerini yaptırabilecek yazılımlar yüklemeleri gerekmektedir. Bu yazılımlar sayesinde saldırganlar bir sisteme

saldırı yapacakları zaman tek bir kodla zombi bilgisayarları harekete geçirerek istedikleri sistemlere yönlendirebilmektedirler (Stalling, 2011).

Saldırganlar, ele geçirdikleri bilgisayarların ilk bakışta farkedilmelerini istemedikleri için, zombi hale getiren yazıları özenle gizlemektedirler. Sistemlerin zombi hale gelip gelmediğini anlayabilmek için, işlemcilerin çalışma hızları kontrol edilmelidir. Zombi Ip adresleri "*http://www.robtex.com/ip/xxx.xxx.xxx.xxx.html#blacklists"* linkinde, genellikle kara listeye eklenmektedir.

### Bot Ağı (botnet)

Terim olarak "Bot", bilgisayar dilinde kendi başına çalışabilen ve bir insan faaliyetlerine benzetilmeye çalışılan yazılım robotlarının yerine kullanılmaktadır. Örneğin, internet tarayıcılarının arama yapıp, gerekli siteleri bulup getirme işlemi botlar aracılığıyla olmaktadır. Uzaktan yönetmeye yarayan yazılım türlerinden olan bot ağı, sık kullanılan DDOS saldırılarındandır. Birçok botun birleşerek hareket etmesine Botnet ya da Zombi ordusu denilmektedir. Botlar, üreticisinin kendisine tanıdığı komutlar aracılığıyla, sahte mesajlar gönderir, casus yazılımlar kurar ve çeşitli internet sitelerinde bulunan zararlı yazılımları otomatik olarak indirip kurmaktadırlar. Bilgisayar kullanıcısı gibi hareket edebilmektedirler.

Botnetlerin en tehlikeli olan noktası, bilgisayar kullanıcılarının haberi bile olmadan, bilgisayarıyla ciddi derecede suçların işlenmesidir. Botnet'e maruz kalan bilgisayarların en büyük ihmali bir güvenlik duvarının olmamasıdır. Bant genişliklerinin artması sonucu, bir korumaya sahip olmayan bilgisayarlar kolaylıkla botnetlerin bir parçası olabilmektedir (Botnet Zombie Army, 2016, Canbek, 2005).

### Ağ taşkını (flooder)

DDos saldırılarının yani sistemi aksatma saldırılarının sebeblerinden biri olarak seri paket internet yoklayıcı gibi yöntemler kullanılarak ağ bağlantılarının aşırı yüklenmesine sebeb olan yazılımlardır (Sağıoğlu ve Canbek, 2007).

### Şifre kırıcılar (password cracker)

Şifre kırıcılar, sözlük tabanlı deneme yanılma yöntemlerini içeren yazılımlardır. Güvenlik amaçlı olarak, kullanıcıların zayıf şifrelerinin bulunması için yasal olarak da kullanılabilmektedirler.

Ayrıca, sisteme girilen şifreleri yakalayıp kaydeden casus programlarda bulunmaktadır ve bunlar, şifre yakalayıcı ya da şifre soyguncusu olarak tanımlanmaktadır (Whitman ve Mattord, 2012).

**Sondaj Aracı (Probe Tool)**

Daha çok bir sistemde olabilecek açıkları bulmak için uğraşan güvenlik şirketleri tarafından kullanılmaktadır. Ayrıca bir sisteme saldırı yapmak isteyen saldırganlarda, sistemde ne gibi açıkların olduğunu öğrenmek için kullanabilmektedir.

**Arama Motoru Soyguncusu (Search Hijacker)**

Arama motoru soyguncusu olan kötücül yazılım, internet tarayıcısının varsayılan ayarlarını değiştirerek, arama motorunu kendi istediği yönde kullanabilmektedir. Değiştirilen ayarlar sayesinde, kullanıcının yaptığı arama sorgularını elde etmektedir ve yanlış girilen adres sonucu açılacak varsayılan arama sayfasını başka bir siteye yönlendirmektedir.

**Koklayıcı (Sniffer)**

Sniffer, bir ağdaki veri trafiğini izlemeye yarayan bir programdır. Sniffer'a ağ koklayıcı da denilmektedir. Ağ koklayıcıları sistem yöneticileri tarafından yasal olarak kullanıldığı gibi, saldırganlar tarafından da bilgilerin elde edilmesi amacıyla kullanılmaktadır. Ağa bağlı olan bilgisayarlar arasında veri alışverişi yaparlar ve bu ağdaki bilgisayarlardan birine erişebilen saldırganlar, sistem koklayıcı ile tüm ağ trafiğini izleyebilir, bu izleme sonucunda da kullanıcıların e-posta adreslerine, şifrelerine ve dosyalarına erişebilmektedirler. Saldırganların kullandığı bu yöntemle bilgileri ele geçirmesini önlemek için, ağ üzerinde kullanılan aktif cihazları ulaşılmak istenen adrese yönlendirmek gerekmektedir (Whitman ve Mattord, 2012; Canbek, 2005).

**Kandırıcı (Spoofer)**

Ip kandırıcıları bir saldırganın saldırı yaptığı hedef bilgisayarda izinin kalmaması adına sahte Ip adresleri üretmek için kullanılmaktadır. Ağlara bağlı olan bir bilgisayara, ağdaki başka bilgisayarmış gibi bağlanarak istediği verileri elde edebilmektedir. Güvenlik duvarları ve yönlendiriciler Ip saldırılarına engel olamamaktadır (Whitman ve Mattord, 2012).

**Pharming**

Pharming tek başına bir anlam ifade etmemekle birlikte, ingilize "phishing" ve "farming" kelimelerinin birleşimiyle oluşmuştur. Yapılan iş "Site trafiğini yönlendirmek " olarak

tanımlanabilir. Yasal bir internet sitesini ziyaret eden bir kullanıcının, saldırganın kendi hazırladığı yasal olmayan benzer bir siteye yönlendirilmesidir. Bu yönlendirmede amaç kullanıcının şifre gibi bilgilerini almaktır. Pharming saldırılarını yaparken, web sitenin URL'sini değiştirmek için genellikle trojenler, solucanlar ya da diğer virüs tekniklerini kullanmaktadırlar. Pharmin saldırıları Domain Name System (Dns) sunucuları aracılığıyla gerçekleşmektedir (Whitman ve Mattord, 2012).

Dns, Ip adreslerini isimlendirebilen veritabanı sistemine verilen isimdir.Web tarayıcısına bir isim yazıldığı zaman örneğin "www.gazi.edu.tr" yazıldığında, bir Dns sunucusu gazi.edu.tr'nin ıp adresine istek gönderir. Ancak saldırganlar çözümleme protokolünün ilk basamaklarını virüsler ya da trojenlerle etkisiz hale getirdiği zaman sunucu saldırganın istediği ıp adresine bağlanmaktadır. Tüm bu işlemleri çok kısa sürede sonuçlandığı için kullanıcılar durumu farketmemektedir. İnternet bankacılığına girmek isteyen bir kullanıcı tüm bilgilerini girer ve bankaya bağlanamaz ancak o sırada bilgileri saldırganın eline geçmektedir. Pharming'den korunmak için tarayıcıların SSL simgesini görmek büyük önem arz etmektedir. Ayrıca şüpheli web sitelerinden kaçınmak ve şüpheli e-posta iletilerini tıklamamak gibi önlemler gerekmektedir (Pharming, 2015).

**Zamanlı Saldırı (Timing Attack)**

Zamanlı saldırı yapmak isteyen saldırgan, web tarayıcısının önbelliğinin içeriğini sisteme zararlı bir çerez ekleyerek ulaşır. Eklenen çerez, kullanıcının şifre koruma sistemine nasıl ulaşacağının bilgilerini verir. Saldırgan kırmak istediği algoritmanın işlem süresini hesaplayarak açık kapı bulmaya çalışmaktadır ( Whitman ve Mattord,2012).

**Web Sayfası Hızsızlığı**

Kişi ya da kurumlar kendilerine özgü web sayfası oluşturmak için servis sağlayıcılarla görüşerek, kendilerine ait bir Ip adresi satın alırlar. Bu Ip adreslerinin kullanışlılığının artması için bir de alan adları verilmektedir. Alan adını alan kişiler ya da kurumlar, bu alan adlarını belirli bir süre kendileri için kiralamış olur. Ancak alan adları saldırganlardan tarafından ele geçirilmesi durumunda yüksek ücretlerle üçüncü kişilere satılarak web sayfası hırsızlığı gerçekleşmiş olmaktadır.

### Spam Mail

Spam istenmeyen elektronik postadır. Kullanıcıya çok fazla gelen spam mail, bir saldırıdan ziyade kullanıcıyı rahatsız eden kötü kod saldırılarının zenginleştirilmiş halidir. 2002 yılının mart ayında Pearce'nin yayınladığı "Security expert warns of MP3 danger" raporuna göre, spam maillerinin eklerinde olan MP3 dosyalarına zararlı kodların eklendiği görülmüştür (Pearce,2002). Spam maillerin yol açtığı en önemli sonuç bilgisayar ve insan kaynaklarının gereksiz yere kullanılmasıdır. Bundan dolayı spam maillerden korunmak için mail filtreleme teknikleri kullanılmaktadır (Whitman ve Mattord,2012). Gelen mesajlarda, içeriğin ve iletiyi gönderen kişinin mail adresinde tuhaflık olması spam mesaj olduğunu göstermektedir. Bu tür mesajlardan korunmak için güvenilmeyen web sitelerine mail adresinin verilmemesi de gerekmektedir.

### Sosyal Mühendislik

Sosyal mühendislik, bir bilgisayar korsanının elde etmek istediği bilgisayar sisteminin yönetimini elinde bulunduran kullanıcılar üzerinde, psikolojik numaralar kullanarak sisteme erişebilmek için gerekli olan bilgiyi elde etme tekniklerine verilen addır. Güvenlik çemberinde en önemli unsur insan faktörüdür bundan dolayı bilgisayar sistemlerinde karşılaşılan güvenlik meselelerinin temelinde insan faktörünün kasten veya bilerek devreye girmesi yatmaktadır (Granger,2001). Bu saldırı sisteminde amaçlanan, kurumun yapısı, kurumsal ağın yapısı, çalışanların ve yöneticilerin kişisel bilgileri, şifreler ve saldırılar için gerekli olan bilgilerin toplanmasıdır. Kuruma çalışan olarak girip, çalışanlarla arkadaş olmak ya da teknik destek gibi görünerek bilgi toplamak bilinen örnekler arasındadır (Berkay, 2009; Chitrey, Singh, Bag ve Singh, 2012).

Güvenliğin sağlanması konusunda en çok zorlanılan saldırı çeşidi sosyal mühendisliktir çünkü hedefte insan vardır. Ayrıca saldırganın böyle bir saldırı yapması için programlama ya da teknik bilgi sahibi olması gerekmemektedir. Saldırganın amacı, karşıdaki kullanıcıya kendisini inandırmasıdır. Saldırı yapılan kişinin güveni kazanıldıktan sonra kullanıcı adı ve şifre gibi bilgiler elde edilerek saldırı gerçekleştirilmektedir. Bu saldırının en güncel örneği telefonlara gönderilen ya da elektronik postalar verilebilmektedir. İletişim kurulmak istenen kişiye bir şeyler kazandığına inandırarak buna ulaşması için gerekli olan unsurunda kredi kartı bilgileri ya da kişisel bilgiler olduğu söylenmektedir (Delialioğlundan aktaran Gökmen,2013).

Sistemlere verilen hasar en çok bizzat kurum içi kullanıcılar olmakla birlikte, kurumlardan

ayrılan bir kişilerin daha sonra ayrıldığı şirkete zarar vermesi de olasılıklar içerisindedir. Bu durumu önleme yöntemi ise yine oluşturulan güvenlik politikalarında şirketten ayrılan kişiler içinde maddeler oluşturmak olmalıdır. Bunların yanı sıra sosyal mühendislik olarak saldırganlar, omuz sörfü, yetkisiz fiziksel erişim, yardım masası aramalarını taklit etme, şifre araklamak için intranet veya internet üzerinde sahte yazılımların oluşturulma ve koyma gibi belli başlı birçok saldırı düzenlemektedir.

Tüm bu korsan taktiklerinden yara almadan çıkmak için yapılması gereken en önemli adım ise, kullanıcıların sosyal mühendisliğe karşı farkındalıklarını arttırmak amacı için düzenli olarak eğitim verilmesi ve uyarılması gerekmektedir. Sistem hakkında önemli bilgi isteyenlere karşı nelerin yapılması, ayrıca yöneticileri de kapsayan bir çemberin, güvenlikle ilgili politikalara eksik vermeden uyması gerekmektedir.

Neden birçok saldırıyı sosyal mühendislikle yapılıyor ve yıllardır bu saldırı yöntemi yaygınlığını yitirmiyor sorusunun cevabı sosyal mühendislikte teknik altyapının gerekli olmamasıdır. Sosyal mühendislikle çoğu zaman saldırıya geçmek için teknik bir altyapı gerekmemektedir ve saldırganlar insanlarla etkileşime geçerek ve psikolojik yöntemler kullanarak güvenlik halkasını kırılabilmektedir. Bu saldırıya maruz kalmasının bağlı olduğu tek koşul insan davranışıdır (Kumar, Chaudhary ve Kumar,2015).

İnsan Tabanlı Yapılan Saldırı Yöntemleri, Bu saldırı yöntemini gerçekleştirmek, insanlarla etkileşime geçmeye bağlıdır ve kişi-kişi iletişim kurulması gerekmektedir.

**Kimliğine Bürünme (İmpersanation):** Bu yöntemle saldırganlar sistemde sahte bir kullanıcı hesabı ele geçirmektedirler. Bu ele geçirilen hesapla bir çalışan gibi görünen saldırganlar, korunan bilgilere ulaşabilmektedir.

**Önemli Bir Kullanıcı Gibi Görünme :** Sadırganlar, sistem yöneticisi ya da özel kullanıcı olarak görülebilerek sisteme erişebilmektedir.

**Üçüncü Taraf Olma:** Saldırgan, sistem yöneticisinden sistemi kullanmak için izin istiyor ve yönetici izin vermeye ikna olup izini verdiği zaman yönetimi artık kontrol edemiyor.

**Masaüstü Desteği :** Klasik sosyal mühendislik tekniği olan teknik destek servisidir. Personellere yardım etmek amacıyla oluşturulan yardım masasını ele geçirerek saldırganlar bilgileri ele geçirir. Masaüstü desteği sosyal mühendislik için vazgeçilmez bir kaynaktır (Kumar vd. 2015).

Bilgisayar Tabanlı Yapılan Saldırı Yöntemleri ise, istenilen bilgileri ele geçirmek için yazılım kullanarak yapılan saldırı yöntemleridir.

### Phishing

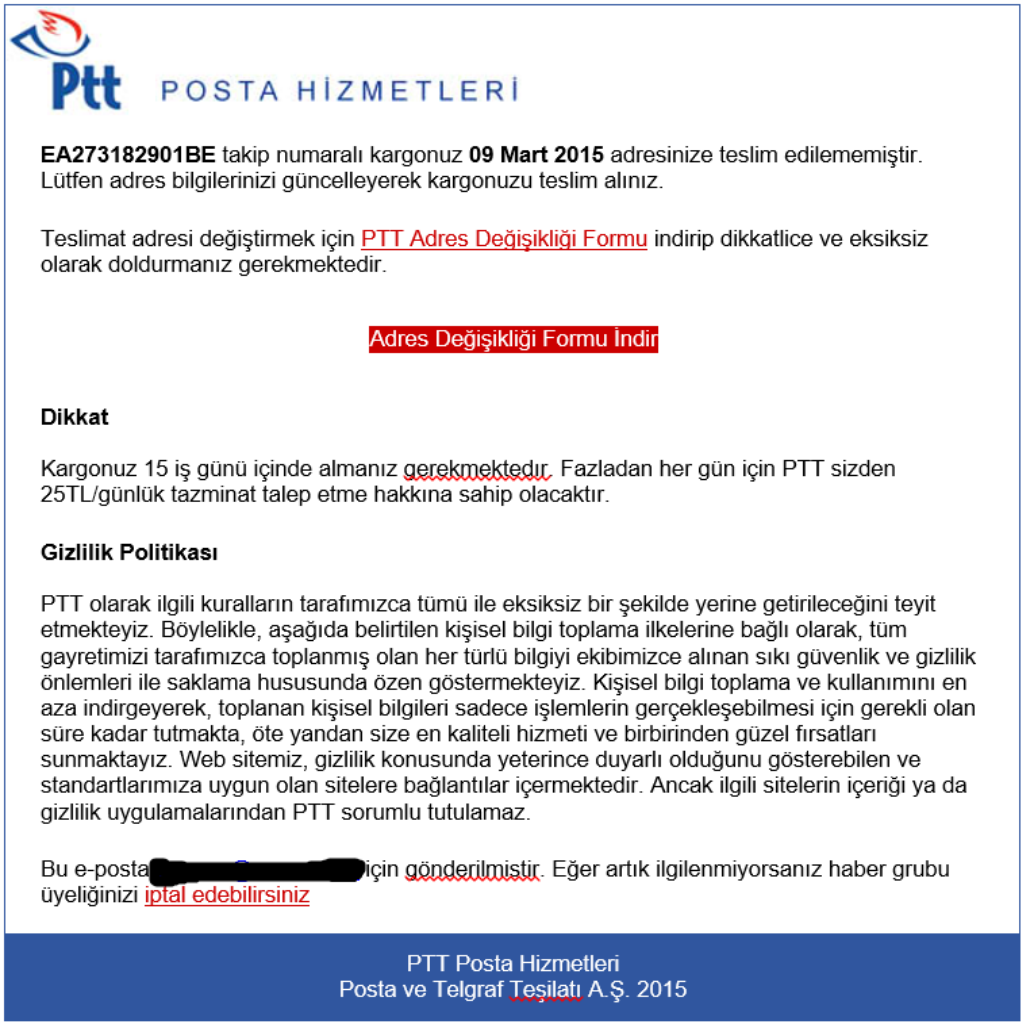
Phishing İngilizcede password (şifre) ve fishing (Balık tutmak) sözcüklerinin birleşmesinden meydana gelmiştir. Bilgileri ele geçirmek için yapılan bir çeşit sosyal mühendisliktir. Kredi kartı numaraları, banka hesap numaraları gibi kişisel bilgileri, gerçek kişiler tarafından gönderilmiş gibi e-posta ya da sitelerle ele geçirilmesidir (Strozer, Cohen, Moore, Mundie ve Cowley,2014).

Sosyal mühendisliğin bir uygulaması olarak kullanıcılara sahte e-postalar gönderilerek kişinin, ekteki linki tılayarak kredi kartı ya da kimlik bilgilerinin girmesi sağlanır ve bilgiler üçüncü şahısların eline geçmiş olmaktadır. Sonrasında hesapların boşaltılması ya da bilgilerin kullanılması gibi zararlara maruz kalınmaktadır (Canbek,2005).

Gönderilen postalarda, banka logosu, yazı tipi, posta arkaplanı rengi gibi sahte bileşenlerin eklenmesi kullanıcıların gönderen adrese bakmasını ya da bağlantının SSL olup olmadığını kontrol etmelerini engellemektedir. Karakasiliotis, Furnell ve Paradoki'nin(2006) yapmış olduğu çalışmada, belirli bir kitle hem yasal hem de yasal olmayan sahte 20 tane e-posta gönderilmiştir. Katılımcılardan hangisinin ve gerçek hangisinin sahte olduğunu anlamalarını istemişlerdir. Sahte gönderilen e-postaların yazı tipi, rengi, logosu gerçek olanlara benzediği için, katılımcıların çok az bir kesimi sahte e-postaları farketmiştir. Symantec(2013)'in tehdit raporuna göre; Phishing saldırılarının %69'u finans sektörüne olurken, %27'si bilgi sistemlerine yönelik yapılmaktadır.

Sosyal mühendislik saldırı çok uzun zamandır yapılmaktadır. Zamanla kullanıcıların bu yöntemler konusunda bilinçlenmasiyle yeni sosyal mühendislik yöntemleri çıkmaya başlamaktadır.

Örneğin 2015 yılında meşhur olan CryptoLocker virüs saldırılarıdır. Bu saldırıda, benzer şekilde e-posta içeriğinde bulunan ekleri indirilip açılması sistemi ele geçiren bir virüsün aktifleşmesi demektir.




*Şekil 5*. Cryptologger virüs içeren e-posta

Örneğin Şekil 5'de bir örneği gösterilen e-posta, ttnet fatura ya da Turkcell fatura gibi değişik şekillerde günümüzde birçok kişiye gönderilmektedir. Örnek e-posta'da gönderilen kişinin bir kargosu olduğu belirtilmekte ve takip için linkin tıklanması istenmektedir.Eski sosyal mühendislik yöntemlerine göre daha profesyonel olan bu yöntemde, e-postanın gerçekle pek bir farkının olmadığı görülmektedir.Ancak, gönderilen e-posta adresi güvenilir değilse linke tıklamamak gerekmektedir.Çözüm olarak bu tür e-postalarda linki tıklamak yerine, takip ya da ödemenin yapılacağı banka hesaplarının internet sitesini direk adres çubuğuna yazarak, güvenli yeşil kilit simgesini ve SSL etiketini görmek koruyucu olacaktır. Bu tür e-postalara karşı bilinçli ve dikkatli olmak gerekmektedir. İnternet tarayıcısının adres çubuğundaki adresin doğru adres olduğundan ve HTTPS güvenli protokolünün yazılı olmasından emin olunması gerekmektedir ( Delialioğlu, 2011). Phishing'e yönelik gönderilen e-postalar, farkedildiğinde ilgili banka ya da kuruma gönderilerek tedbir alınması istenmelidir.

### Pop Up Açılır Pencereler

Bir web sitesiyle bağlantı kurmak isteyen kullanıcının aniden karşısına çıkan reklam içerikli tarayıcı pencerelerine pop-up denir. Bu açılan pencereler kötü niyetli yazılımcılar tarafından kullanılabilir. Sahte vaadlerle kullanıcıların reklamı tıklamasını sağlayan pencereler, kullanıcıları sahte web sitelerine yönlendirerek bilgi hırsızlığı yapabilmektedirler (Kumar vd.2015) Yine aktifleşmek için kullanıcıyla etkişime girmesi gereken bir saldırı yöntemidir. Kullanıcıların bu içeriklere tıklaması bazı zararlara maruz kalmasına neden olmaktadır.

### E-Mail Ekleri

E-posta eklerine gizlenen programlar açıldığı zaman çeşitli zararlı yazılımlar yayılmakta ve bu durum bilgisayar sistemine zarar vermektedir. Bu zararlı yazılımlar; virüsler, solucanlar ve Truva atlarıdır. Kullanıcıların ekleri açması için çeşitli merak uyandıran yöntemler kullanılmaktadır (Kumar vd.2015). Örneğin, e-posta ekinde "Seni seviyorum" yazan bir solucan virüsü olabilmektedir. Kullanıcı eki tıkladığı zaman virüs aktifleşmektedir. Ya da çeşitli sanatçıların fotoğraflarını göndermiş gibi yaparak, ekte jipeg uzantılı dosya göndererek aynı sonuca ulaşmaktadırlar.

### Mail Zinciri Ve Aldatmacalar

Sosyal mühendisliğin bir çeşidi olan mail zinciri kurma yoluyla, kullanıcılar olmayan bir durumdan dolayı aldatılmakta ve bir mail zinciriyle birçok e-posta adresinin ele geçirilmesine neden olmaktadır. Bu aldatılma durumu genelde, gerçek olmayan bir virüs hakkında uyarı mesajı olarak ya da kanser hastası olan bir çocuk için yardım mesajı olarak kullanılmaktadır. Bu mesajların sahteliğinin farkına varmayan kullanıcılar, yardım amaçlı olarak mesajı kişi listelerine iletirler ve böylece aldatmanın daha fazla insana yayılmasına neden olmaktadırlar. Gereksiz internet trafiği ve zaman kaybına sebeb olan bu durumlar, bazen de ekte fotoğraf göndermek suretiyle zararlı bir yazılımın yayılmasına sebebiyet vermektedir. Ayrıca kişilerin mail adresleri gizlilik butonu dikkate alınmadan yazıldığı için, saldırgan tarafından görülebilmektedir. Bu tür e-postalara itibar edilmemesi ve tanınmayan kişilerden gelen ya da şüphe uyandıran postaların açılmaması gerekmektedir.(Canbek ve Sağıroğlu,2007; Whitman ve Mattord,2012; Stalling,2011; C.Pfleeger, Pfleeger ve Margulies, 2015)

### Sosyal Mühendislikten Korunmak

Sosyal mühendisliğe maruz kalmamak ve ataklarından kurtulmak için çeşitli araçlar ve teknikler geliştirilmektedir. Ancak temelden tedbir alınması, her gün değişen saldırı yöntemlerine karşı alınabilecek en büyük önlemdir. Bu ataklara karşı alınabilecek en önemli önlemler; eğitim, farkındalık ve seminer, politikalar ve uygulamaları denetlemedir.

Sosyal mühendislik saldırılarını en aza indirebilmek için;

- Kurumların ya da kişilerin bilgilerini yöneten kişilerin uyması gereken bir politika olmalıdır,
- Kişilerin verileriyle ilgilenen yetkililerin politikalara uyduklarından emin olmak amacıyla uygulamalar takip edilmelidir,
- Kişilerden kurumlardan ayrılmadan ya da işten atılmadan önce, kurumla ilgili olan tüm bilgi dokümanlarının alınması gerekmektedir. Bilgi güvenliğine zarar verecek en önemli adımlardan birisidir.
- Kurumda çalışanların kimlik bilgilerini ve kullandıkları sistemleri yöneten kişilerin eğitimli kişiler olması ve düzenli eğitimler alması gerekmektedir.
- Kurumların şirket web sitelerine çok dikkat edilmesi gerekmektedir çünkü şirketin detaylı bilgileri ve kullanıcıların bilgilerine bu sitelerden ulaşılabilinmektedir.

  Ayrıca;
- Bütün servisler için aynı şifrenin kullanılmaması, şifrenin her servis için değiştirilmesi ve tahmin edilemez bir şifre konulması,
- Hesapların ya da şifrelerin ele geçirilme ihtimaline karşı iki aşamalı doğrulayıcı kullanılması,
- Kolay tahmin edilemeyecek güvenlik sorularının kullanılması,
- Kredi kartlarının dikkatli kullanılması ve aracı kurumlarla ya da sanal kartlarla ödeme yapılması,
- Monitörden kişisel bilgilerin ve kişisel hesapların izlenerek ele geçirilebilme ihtimaline karşı dikkatli olunması,
- Herkese açık makinelerde kişisel bilgilerin (adres, doğum tarihi vb.) tutulduğu verilerin düzenli olarak silinmesi gerekmektedir.

Her geçen gün değişen sosyal mühendislik saldırılarına karşı olarak, bu adımlar saldırılardan kişileri tamamen korumasa da, riskleri en az sınıra indirmektedir. Çünkü bu saldırılara karşı koymak sadece teknoloji değil aynı zamanda kullanıcının farkındalık düzeyine göre değişmektedir.

**İlgili Araştırmalar**

Bilgi güvenliği alanında yapılan çalışmaların birçoğu sistem güvenliğini yazılım ve donanım güvenliğine odaklamış durumdadır. Alanyazın incelendiğinde sınırlı sayıda kişilerin bilgi güvenliği farkındalığı ve bu farkındalıklarının davranışlara yansıması durumu ile ilgili yapılmış çalışmalar mevcuttur.

Canbek ve Sağıroğlu'nun (2006) yaptığı inceleme çalışmasında, bilgi olgusu geniş bir açıdan irdelenmiş, veri, bilgi ve özbilgi kavramları açıklanmıştır. Bilgi güvenliğini oluşturan ana unsurların üzerinde durulmuş, geçen zaman boyunca artan bilgi güvenliğine yönelik saldırılara karşı etkin bir güvenlik oluşturabilmek için gerekli olan güvenlik süreçlerini özetlemişlerdir.

Karakasiliotis, Furnell ve Papadaki (2006), "Assessing End-User Awareness Of Social Engineering And Phishing" isimli çalışmalarında, kullanıcıların epostalarda sazan avlama (eposta phishing) saldırılarına karşı farkındalıklarını değerlendirmişlerdir. Web tabanlı uygulanan araştırmada katılımcılara karışık 20 tane yasal ve yasal olmayan epostalar gönderilmiş ve katılımcılardan gönderilen epostaları yasal olan ve olmayan olarak sınıflandırmalarını ve neden bu sınıflandırmayı yaptıklarına dair sebeblerini yazmalarını istemişlerdir. İki aşamada gerçekleştirilen araştırmada, birinci aşamada katılımcıların demografik özelliklerini belirlenirken, ikinci araştırmada 9'u yasal ve 11'i yasal olmayan 20 sorudan oluşan epostaların sınıflandırılması istenmiştir. Değerlendirme sonuçları göstermiştir ki,179 katılımcıdan %36'sı yasal epostalarını tanımada başarılı olurken %45'i yasal olmayan epostaları tespit etmiştir. Ancak yasal olmayan epostaları tespit edilme sebebi konusunda doğru cevabı verememiş, ikna edememişlerdir. Katılımcıların %55'i mesajlarda bulunan logo, banner, font ve copyright sembollerinden dolayı mesajların legal olduğunu düşündüklerini belirtmişlerdir.

Albrechtsen (2007) "A qualitative study of users' view on information security" isimli çalışmasında bilişim teknolojileri şirketlerini ve Norveç'teki bankalarda çalışan personelin güvenlik önlemlerine karşı bakış açılarını nitel bir çalışepostae incelemiştir. Kullanıcıların gündelik davranışlarıyla bilgi güvenliği farkındalıklarını ortaya koymayı amaçlamıştır. Katılımcıların bilgi güvenliğini anlama konusunda gönüllü olduğunu fakat uygulama noktasında yoksun olduklarını belirtmiştir. Bilinenlerle uygulama arasında olan boşluğu,

kullanıcıların iddia ettiği gibi yeterli bilgiye sahip olmadıklarına bağlamaktadır. Kullanıcıların mevcut bilgi güvenliği ile iş verimlilikleri arasında bir çatışması olabileceğini belirtirken, genel farkındalık kampanyalarının kullanıcılar üzerinde yeterli etkiye sahip olmadığnı belirtmiştir. Kullanıcıların dâhil edildiği kampanyaların kullanıcı farkındalığının ve davranışlarının üzerinde çok daha etkili olduğunun altını çizmektedir.

Schmidt, Johnston, Arnett, Chen ve Li (2008), "A Cross-Cultural Comparison of U.S. and Chinese Computer Security Awareness" isimli çalışmasında Amerika ve Çin kültürlerindeki bilgisayar güvenliği farkındalığını karşılaştırmak istemiştir. Bilgisayarlardaki Rootkitler, Casus yazılımlar ve virüsler'e karşı farkındalık seviyelerini karşılaştırmak için Amerika'dan 210 ve Çin'den 278 kişiye anket uygulanmıştır. Araştırma sonuçlarına göre Çin ve Amerika'daki kullanıcılar arasında casus yazılım ve bilgisayar virüsleri açısından anlamlı derece de farklılık olduğu görülmüştür. İnternetin hayatlara kattığı güzel yanlar yanında doğası gereği oluşturduğu tehlikelere, virüslere ve rootkitlere karşı eğitimler verilmesi gerektiği ve bu eğitimleri dünya genelinde yapmak gerektiği öneriler arasındadır.

Görkey (2008) "İnternet reklamcılığı: Etik ve Hukuk Sorunsalı" adlı yüksek lisans tez çalışmasında internette tüketiciye ulaşan reklamların etik ve hukuk kurallara uygunluğunu incelemektedir. Araştırmada bir ay boyunca farklı kategorilerde yer alan beş internet sitesinden kullanıcıya ulaşan reklamların içerik analizi yapılmış ve reklam iletilerinin kullanıcıya kullanıcının istediği dışında ulaştığını, bu durumla kişilerin mahremiyet alanına müdahale edildiğini belirtmiştir. Sonuç olarak, reklam yasalarının mevcut durumda kişilerin hak ve hürriyetlerini korumada yetersiz kaldığı sonucuna ulaşmıştır.

Tekerek (2008), "Bilgi Güvenliği Yönetimi" isimli çalışmasında, bilişim teknolojilerinde meydana gelen değişmeler sonucunda günlük hayatta kullanılan sistemlerin dijital ortamlara aktarıldığı ve e-dönüşüm sistemlerinin günlük yaşantımızın vazgeçilmez bir parçası haline geldiğini belirtmektedir. Bilişim ortamının sık kullanılması sonucu ortaya çıkan güvenlik risklerine karşı bilginin yönetilebileceğini belirtmiş ve bunun için bir model önermiştir. Bilgi güvenliğini yasal bir süreç olarak ele almıştır. Teknik önlemlerin yanı sıra kurallar, cezalar gibi idari önlemlerle de insan faktörünün önemini vurgulamıştır.

Albrechtsen ve Hovden (2008) "Improving information security awareness and behaviour by a user participative approach: an intervention study" isimli çalışmalarında kullanıcıların bilgi güvenliği farkındalıklarını ve davranışlarını geliştirmeyi hedefleyen bir eğitim programı önermiştir ve eğitim programının etkilerinden bahsetmiştir. Deneysel olarak

yürütülen çalışmada deney ve kontol grubu oluşturularak bilgi güvenliği eğitimi verilmiştir. Verilen eğitim sonucunda katılımcıların farkındalıklarının davranışa yansıdığı gözlemlenirken, eğitimden altı ay sonra tekrar yapılan anket davranışların kalıcı olduğunu göstermiştir. Deney grubu verilen eğitimin etkililiğini kanıtlamıştır.

Adıgüzel (2009), "Güvenlik Endişesinin İnternet Bankacılığı Kullanımına Etkisi ve Vakıfbank Müşterilerine Yönelik Bir Araştırma" isimli yüksek lisans tezinde, bankacılık işlemlerini büyük ölçüde kolaylaştıran internet bankacılığının müşterileriyle bir çalışma yapmıştır. Müşterilerin duyduğu güvenlik endişesinin internet bankacılığı kullanmalarına etkisini incelemiştir ve internet bankacılığının kullanma oranının kullanıcıların yaş, eğitim düzeyi ve gelir düzeyine göre değişiklik gösterdiğini sonucuna ulaşmıştır. Ayrıca ilginç bir şekilde internet bankacılığı aracılığıyla yaşanan dolandırıcılık vb. olayların internet bankacılığı kullanımına herhangi olumsuz bir etkisi olmadığını tespit etmiştir.

İlbaş (2009), çalışmasında öğretim elemanlarının ve öğrencilerin bazı bilişim suçlarına bakış açısını ve yasal düzenlemede nasıl gördüklerini belirlemeyi amaçlamış, demografik özelliklere göre değişimin nasıl olduğunu incelemiştir. Veri toplama aracında demografik özelliklerin yanısıra bilgisayar kullanımına yönelik ilgi, bazı bilişim suçlarının ahlaki ve hukuksal açıdan suç olup olmadığını belirleme ile farklı ülkelerin hukuk sistemlerinde bilişim suçu sayılan 14 hareketin kişisel algı düzeyinde suç şiddeti sayılma duruma yönelik sorular bulunmaktadır. Araştırma sonuçlarında, en çok suç olduğuna karar verilen bilişim suçu konuları çocuk pornografisi, özel hayatın gizliliği, siber hırsızlık ve akademik aşırmacılık olmuştur. Ayrıca araştırmacı bilişim suçlarına karşı bilinçlendirme adına eğitimler verilmesinin ve bu eğitimlerin yaygınlaştırılmasının gerekliliğine vurgu yapmıştır.

Şahinarslan, Kantürk, Şahinarslan ve Borandağ (2009), "Kurumlarda bilgi güvenliği farkındalığı" başlıklı çalışmalarında, kurumların sahip oldukları en değerli varlık olan bilginin; gizlilik, bütünlük ve erişilebilirlik özellikleri açısından korunması gerektiğini vurgulamış, koruma için fiziksel ve sistemsel önlemlerin yanı sıra bireylerin bilgi güvenliğine ilişkin tehdit ve risklerden, kurumun bilgi güvenliği politika ya da kurallarından haberdar olması gerektiğini belirtmiştir. Güvenliğin en zayıf halkası olarak belirtilen insan faktörü üzerinde çeşitli farkındalık programlarının uygulanması gerektiğini, bu programların başında ise bilgi güvenliği farkındalık eğitiminin gerektiğini belirtmiştir. Bilgi güvenliği farkındalık eğitimi için gerekli olan ana konuları belirleyen bir eğitim programı ve örneği sunmuşlardır.

Zhang, Reithe ve Li (2009) "Impact of perceived technical protection on security behaviors" isimli çalışmasında bilgi güvenliğinde ve güvenlik politikalarında insan faktörünü incelemeyi amaçlamıştır. Oluşturulan güvenlik politikaları ile çalışanların davranışlarının uyumunu incelemek amacıyla 176 teknik çalışana anket uygulanmıştır. Sonuç olarak, güvenlik politikalarının davranış biçimini ve tutumları önemli ölçüde etkilediği gözlenmiştir. Uygulama sırasında dikkat çeken bir nokta ise, teknik koruma mekanizmalarının kapasitesi ve gücünün abartılı olması yerine daha sınırlı ve direk sorunlara vurgu yapan güvenlik politikalarına kullanıcıların adapte olmasının daha kolay olabileceği görülmüştür.

Öğütçü (2010) "E-dönüşüm sürecinde kişisel bilgi güvenliği davranışı ve farkındalığın analizi" adlı yüksek lisans tezinde, e-dönüşüm sürecinde bilgi sistemini aktif olarak kullanan bireylerin, bilişim güvenliğine yönelik risk içeren teknolojileri kullanımları ve kendilerini risklerden ne şekilde koruduklarını araştırmıştır. Bununla birlikte bireylerin herhangi bir bilişim suçuna maruz kalıp kalmadıkları ya da olumsuz bir deneyim yaşayıp yaşamadıkları ve bazı bilişim teknolojilerini hangi ölçüde tehlikeli algıladıklarını araştırmıştır. Araştırma kapsamında geliştirilen anket formu Türkiye genelindeki Başkent üniversitesi kurum ve kuruluşlarında çalışan akademi ve idari personel ile Başkent üniversitesi öğrencilerine uygulanmıştır. Ankette demografik sorular, katılımcıların bilişim teknolojileri ve bilgisayar güvenliği ile ilgili profillerinin belirlenmesine yönelik sorular, katılımcıların bilişim teknolojilerini yönelik risk içeren davranış profillerinin belirlenmesine yönelik sorular, bilişim tehditlerine yönelik korumacı davranış düzeylerini belirleyen sorular ve katılımcıların bilişim suçlarına maruziyet düzeylerinin belirlenmesine yönelik sorular yer almıştır. Araştırma sonuçlarına göre, ne kadar yazılımsal ve donanımsal önlemler alınsa da en büyük tehlikenin bireyin kendisi olduğu, bireylerin bir sorunla karşılaştıklarında bunu hangi makama ileteceklerini bilmediklerini ve risk içeren teknolojilerin kullanımı arttıkça suça maruziyet oranının da arttığı ortaya çıkmıştır. Araştırmanın sonucunda bireylerin bilişim güvenliği farkındalık oranlarının çok yüksek olmadığı, kişisel açıdan korumacı davranışların henüz tam olarak gelişmediği belirtilmiştir. Bunun yanı sıra suça maruziyet oranının düşük olduğu ve konu hakkında eğitim alan bireylerin eğitim almayanlara oranla farkındalıklarının yüksek olduğu görülmüştür. Araştırmacı bu çalışma sonucunda, riskleri en aza indirmenin kaçınılmaz olduğunu bu konularda çeşitli eğitimlerin ve kampanyaların düzenlenmesi gerektiği ve bilişim savcılığı ve bilişim mahkemelerinin kurulması gerektiğini

önermiştir.

Dijle ve Doğan (2011) çalışmalarında Dünya'da ve Türkiye'de bilişim suçlarında meydana gelen artışa vurgu yapmış ve eğitimli insanlar kategorisinde öğrenciler ve öğretim elemanları ile bilişim suçu ve bilişim suçlarıyla mücadele konusunda görüşmeler yapmıştır. 766 kişiyle yapılan çalışmada elde edilen verilere göre; katılımcıların %72,5' nin lisanssız yazılım kullandığı, %75,3' ünün internet bankacılığını güvenilir bulmadığını, %34,9' unun maliyet düşüklüğü nedeniyle internetten indirme yaptıklarını, %29,6'sının internetten film, müzik ve oyun indirmenin suç olduğunu bildiklerini ve %35,6'sı bilişim suçu kavramını daha önce hiç duymadığını belirtmiştir. Araştırma sonuçları, katılımcıların konuyla ilgili yeterli bilgiye sahip olmadıklarını ve öğrencilerle bilgisayar eğitimi olmayanların bilişim suçu işleme oranının yüksek olduğunu göstermektedir. Dijle ve Doğan, bilişim suçlarının takibini yapabilecek özel ve kamu kuruluşlarının kurulmasını, bilişim suçlarını işleyenlerin aldıklarını cezanın kamuoyuna duyurulmasını ve bilişim teknolojilerini iyi bilecek uzaman personelin yetiştirilmesinin gerekli olduğunu belirtmişlerdir. Ayrıca, toplumun bilişim suçları konusunda bilgilendirilmesini ve nasıl mücadele edileceğinin anlatılmasını önermiştir.

Mart (2012) teknolojinin toplumda hızla yaygınlaşması ile oluşan bilişim kültürü içinde bireylerin bilgi güvenliği farkındalıklarını ölçen bir çalışma yapmıştır. Tarama niteliğinde betimsel bir çalışma olan araştırmanın örneklemini 2011-2012 yıllarında öğretmen, avukat mühendis ve sağlık personeli olmak üzere farklı meslek gruplarından oluşan 501 katılımcı oluşturmaktadır. Çalışmada bilgi güvenliğini tehdit eden unsurlardan, bilişim teknolojilerinin doğuşundan ve bilişim kültürünün oluşmasından söz edilmiştir. Katılımcılara 60 soru ve 3 bölümden oluşan " Bilişim Kültüründe Bilgi Güvenliği Anketi" uygulanmıştır. Birinci bölümde katılımcıların demografik özelliklerini belirleyen sorular, ikinci bölümde bilgi güvenliği ve üçüncü bölümde teknoloji kullanımını belirleyen sorular bulunmaktadır. Araştırma sonuçlarına göre, katılımcıların teknoloji kullanımları arasında yaşlarına ve bilgisayar ve internet kullanım sürelerine göre anlamlı bir farklılık olduğu görülürken, cinsiyetlerine, eğitim durumlarına ve mesleklerine göre anlamlı bir fark olmadığı görülmektedir. Katılımcıların bilgi güvenliği farkındalıkları arasında ise yaşlarına, cinsiyetlerine ve mesleklerine göre anlamlı bir farklılık olduğu görülürken, eğitim durumlarına, mesleklerine ve bilgisayar ve internet kullanım sürelerine göre anlamlı bir farklılık olmadığı görülmektedir. Katılımcıların bilişim kültürü ve bilgi güvenliği

farkındalıkları arasında zayıf düzeyde, pozitif ve anlamlı bir ilişki olduğu belirtilmiştir. Mart bireylerde bilgi güvenliği farkındalığı yaratmak için küçük yaşlardan itibaren eğitim verilmesi gerektiğini ve zorunlu bir ders olarak okulda uygulanması gerektiğini önermektedir. Yetişkin bireyler için ise bilgi güvenliği ile ilgili seminerler vererek farkındalık oluşturulmasını önermektedir.

Tekerek (2012) çalışmasında, ilköğretim ve lise öğrencilerinin bilgi ve bilgisayar güvenliği farkındalık düzeylerini ortaya koymuştur. Araştırmanın örneklemini Kahramanmaraş ili, il merkezi, ilçe, kasaba ve köylerinde öğrenim gören 2447 öğrenci oluşturmaktadır ve katılımcılara bilgi ve bilgisayar güvenliği farkındalık ölçeği uygulanmıştır. Verilerin analizi sonucunda, temel olarak öğrencilerin etik konularında yeterli farkındalık düzeyine sahip olduğu görülürken, kurallar ve bilgi gerektiren konularda farkındalık düzeylerinin düşük olduğu belirlenmiştir. Araştırmacı, bu sonuçlardan bilgi ve bilgisayar güvenliği farkındalık ve etkinliklerinin yetersiz olduğu sonucunu çıkarmıştır. Ayrıca araştırmacı, haftada bir saat ve seçmeli olarak okutulan bilişim teknolojileri dersinde bilgi ve bilgisayar güvenliği farkındalığının kazandırılması gerektiğini önermiştir.

Kınay (2012) "Lise Öğrencilerinin Siber Zorbalık Duyarlılığının Riskli Davranış, Korumacı Davranış, Suça Maruziyet Ve Tehlike Algısı İle İlişkisi ve Çeşitli Değişkenler Açısından Değerlendirilmesi" isimli yüksek lisans tez çalışmasında, öğrencilerin bilgisayar ve internet kullanımında riskli davranış durumlarını incelemeyi amaçlamıştır. İlişkisel tarama modeli ile yürütülen çalışma 368 öğrenciye uygulanmıştır. Araştırmada tehlike algısının ve suça maruziyet durumunun siber zorbalığa ilişkin duyarlılığı anlamlı düzeyde yordadığı görülürken, erkek öğencilerin kadın öğrencilere göre bilgisayar ve internet kullanımında daha riskli davranış sergilediği sonucuna ulaşılmıştır. Buna paralel olarak siber duyarlılık konusunda kadın öğrenciler erkek öğrencilere göre daha duyarlıyken, erkek öğrencilerin tehlike algısının kadın öğrencilere göre daha yüksek olduğu da tespit edilmiştir. Araştırmacı bu bulgular ışığında, lise öğrencilerine bilgi güvenliği konusunda eğitimler verilmesi gerektiğinin ve farkındalıklarının arttırılması için etkin siteler ve yazılımlar hazırlanması gerektiğinin altını çizmiştir.

Al-Ahmad ve Mohammad (2012), "Addressing Information Security Risks by Adopting Standards" adlı çalışmalarında uygun bilgi güvenliği risk yönetimini kurmak için girişmde bulunan kurumların, kapsamı ve standartları kendilerine göre uyarlarken karşılaştıkları güçlükleri vurgulamışlardır. Bilgi güvenliği risk yönetimini kullanmak için en uygun yapıyı

seçmeye yardımcı olmayı amaçlarken en çok seçilen ve en yaygın kullanılan standartların üzerinde durmuşlardır. Uygun standart ve seçim kriterlerini belirlerken fırsatları ilerletmek amacyla bir dizi öneri bulunmuşlardır.

Bilek (2012), çalışmasında teknolojinin yaygınlaşmasıyla hayatımızın elektronik sistemlere dönüşmesiyle ortaya çıkabilecek zafiyetlere değinmiş ve oluşan bilişim suçlarından bahsetmiştir. Bilişim suçundan, bu şuçlara yönelik oluşturulan yasalardan ve 2006-2011 yılları arasındaki bilişim suçlarından bahsedilmiştir. Araştırma da nicel ve nitel veri toplama yöntemi kullanmıştır. Ceza evlerindeki eğitim bürosundan 30 mahkûmla 19 sorudan oluşan nitel bir çalışma yaparken, Bilgisayar ve Öğretim Teknolojileri eğitimi bölümünde okuyan 312 öğrenciyle 49 sorudan oluşan nicel bir çalışma gerçekleştirilmiştir. Katılımcıların bilişim suçları konusunda bilgi düzeyleri ve tutumlarını ölçmek planlanmıştır. Sonuç olarak böte üniversite öğrencilerinin bilişim suçları farkındalık düzeyleri yüksek olurken teknik konularda eksik bilgilerinin olduğu tespit edilmiştir. Araştırmacı bilişim suçlarıyla mücadele konununun çıkarılması gerektiğini ve bu alanda uzman personelin yetiştirilmesi gerektiğini vurgulamış ve kurumsal farkındalığın arttırılması için alınması gereken önlemlerden bahsetmiştir.

Tekerek ve Tekerek (2013) yaptıkları çalışmada ilköğretim ve lise düzeyinde öğrenim görmekte olan öğrencilerin bilgisayar ve internet güvenliği farkındalıklarını incelemeyi amaçlamışlardır. 2449 öğrenci ile yürütülen çalışmada araştırmacı tarafından geliştirilen bilgi güvenliği farkındalık ölçeği uygulanmıştır. Araştırma sonuçlarına göre öğrencilerin güvenli şifre kullanımı, kişisel bilgisayar güvenliği, filtreleme yazılımları vb. konularda farkındalıklarının düşük olduğu ve bilgi güvenliği konusunda da yeterli bilgiye sahip olmadıkları gözlenmiştir. Araştırmaya katılan öğrenciler etik konularında yeterli bilgi birikimine sahipken kurallar ve bilgi gerektiren konularda gerekli bilgilere sahip değillerdir. Araştırmacı, bilgi güvenliği konusunda öğrencilere, velilere ve öğretmenlere eğitim verilmesi gerektiğini vurgulamaktadır.

Akın, Çınar, Karaman ve Bilekyiğit'in (2013) "Siber Durum Farkındalığını Artırmada Etkili Bir Yöntem: Bayrağı Yakala" isimli çalışmalarında siber tehditlerin getirdiği risklere karşı farkındalık oluşturmak amaçlanmıştır.Durum farkındalığını arttırma amaçlı bayrağı yakala (BY) yarışmaları ayrıntılı olarak incelenmiş ve kurum içi farkındalık oluşturmak amacıyla hazırlanmış bir yarışmanın sonuçlarına yorumlanarak yer verilmiştir. Bu yarışmanın sonuçlarına göre, siber güvenlik alanında çalışan ve gerçekte bir sisteme saldırı yapma

imkanı olmayan personel için bu yarışmalar önemli ilerlemeler kaydettirmiştir. Ayrıca bilgi düzeyinde ve farkındalıklarında artış olduğu gözlemlenmiştir. Bu yarışmayla beraber, bir personelin siber güvenlik alanında görevli olsa dahi uygulamalı olarak yaşayabileceği tecrübelerin teorik olarak öğrenilen bilgiden çok daha etkili olduğu da görülmüştür.

Altun (2014), yüksek lisans tezinde belirli kısıtlara göre bilgi güvenliği ihlallerini incelemiştir. Teknolojinin ilerlemesi sonucu, bilgilere erişimin kolaylaştığı ve bu durumun iziniz erişimlere, kullanımlara ve ifşa edilmelere sebebiyet vermektedir. Kurum bilgilerinin istenmeyen kişiler tarafından ele geçmesini engellemek ve güvenliğin sağlanmasını sağlamak amacıyla ihlal tespiti yapılıp, ihlallerin kayıt altına alınması gerekmektedir. Bu çalışma da bilgi güvenliği konusunda yapılması gerekenlerin çerçevesinin çizilmesi ve güvenlik ihlallerinin tespit edilip Bilgi güvenliği yönetim sisteminin kullanılması amaçlanmıştır. Bu sayede bilgi güvenliğinde yaşanabilecek güvenlik zafiyetlerini azaltmak planlanmıştır.

Durmuş (2014) çalışmasında beş farklı örnek küme üzerinde bilgi güvenliği farkındalığını incelemiştir. Bu incelemeyi web tabanlı olarak genel konuları içeren bir anketle yaparken, daha büyük ve karmaşık bir anketle de yedi devlet kurumunda çalışan bilgi işlem personelinin bilgi güvenliği farkındalığını ele almıştır. Çalışma sonucunda kullanıcıların bilgi güvenliği konularında gösterdikleri zayıf ve güçlü davranışlar vurgulanmakla beraber, teknik anketin analizi sonucunda da devlet kurumlarında ki eksik güvenlik önlemleri tespit edilmiştir. Çalışmanın sonucunda katılımcıların farkındalık düzeylerini arttırmak adına bir doküman eklenmiştir.

# BÖLÜM III

# YÖNTEM

Bu bölümde araştırmanın modeli, evren ve örneklemi, verilerin toplanmasında faydalanılan araçlar ve verilerin çözümlenmesinde kullanılan istatistiksel yöntem ve teknikler ile ilgili bilgiler verilmiştir.

**Araştırmanın Modeli**

Bu araştırmada öğretmenlerin bilgi güvenliği farkındalıkları ve interneti güvenli kullanım düzeylerini belirlemek amaçlamıştır. Bu yönüyle araştırma betimsel bir çalışma olup belirlenen konunun özelliğine, araştırmanın amacına, evren ve örneklemine uygun olan tarama modeli ile gerçekleştirilmiştir. Tarama araştırması bir grubun belirli özelliklerini belirlemek amacıyla verilerin toplanmasıdır. Bu araştırma türünün amacı genel olarak var olan durumu betimlemektir (Büyüköztürk, Kılıç Çakmak, Akgün, Karadeniz ve Demirel, 2012, s.147).

Karasar'a (1999, s.77) göre tarama modelleri geçmişte ya da halihazırda var olan bir durumu var olduğu haliyle betimlemeyi amaçlayan bir araştırma yaklaşımıdır.

**Araştırmanın Evreni**

Bu araştırmanın evrenini araştırmanın amacı doğrultusunda Türkiye'de yaşayan Türkçe, Matematik, Bilişim Teknolojileri, Fen ve Teknoloji, Sosyal Bilimler ve Sınıf öğretmenleri gibi farklı branştaki eğitimciler oluşturmaktadır.

**Araştırmanın Örneklemi**

Bu araştırmanın örneklemini; TÜİK[1] (Türkiye İstatistik Kurumu)'in oluşturduğu bölge birimleri sınıflandırılmasında Türkiye'nin 12 bölgeye ayrılmasından oluşan Düzey 1 (12 Bölge Birimleri) sınıflaması dikkate alınarak, her bölgedeki illerde, 2015-2016 eğitim-öğretim yılında görev yapan 1355 öğretmen oluşturmaktadır.

Olasılıklı örnekleme, birimlerin evrenden her seferinde eşit olasılıkla seçilmesidir ve ayırt edici özelliği olan elemanların evrenden rastgele seçilmesi işlemidir. Bu araştırmada örneklem seçimi için, olasılıklı örnekleme yöntemleriden küme örnekleme yöntemi kullanılmıştır. Küme örnekleme yönteminde birimleri gruplar oluşturmaktadır. Araştırma yapılacak bireyler geniş bir alana dağıldıkları için, bireylere ulaşmak küme örnekleme yöntemi ile daha kolay olması düşünülmüştür. Örnekleme yöntemlerinde hatalar bulunabilir fakat bu örnekleme yönteminde hatayı en aza indirebilmek adına grupların sayısının çok olması ve bu grupların heterojen olmasına özen gösterilmiştir.

Küme örneklemesi, örnekleme gruplarının birden fazla grup içermesini ifade eder. Örneklem coğrafi olarak çok geniş alana yayıldığında ve alandan rastgele çekilen n adet elemandan veri elde etme maliyetinin yüksek olması durumunda, veri toplamada maliyeti azaltabilmek için öncelikle kümeler belirlenir. Küme örneklemesinde 4 olası durum vardır. Bunlar;

- Pratikte uygulması zor olsa da, eşit sayıda eleman içeren kümeler oluşturarak, her bir kümeden eşit sayıda örnek eleman seçilebilir.
- Değişen sayıda eleman içeren kümeler oluşturularak, her bir kümeden eşit sayıda örnek eleman seçilebilir.
- Eşit sayıda eleman içeren kümeler oluşturularak, her bir kümeden değişen sayıda örnek eleman seçilebilir.
- Değişen sayıda eleman içeren kümeler oluşturularak, her bir kümeden değişen sayıda örnek eleman seçilebilir (TOBB,[Türkiye Odalar ve Borsalar Birliği], 2013).

[1] Ülkemizde, Avrupa Birliği İstatistik Ofisi tarafından 1970'li yıllarda Avrupa Birliği'ne detaylı veriler sunmak üzere İstatistiki Bölge Birimleri Sınıflandırılması (İBBS) oluşturulmuştur. İBBS'nin temel amacı istatistikleri bölgesel olarak toplamak, sosyo-ekonomik analizler yapmak ve topluma yönelik bölgesel politikaların sınırlarını oluşturmaktır.İBBS, Avrupa Birliği genelinde tek bir veri tabanı oluşurmayı planlamıştır ve bu plan dâhilinde bölgesel istatistikleri standartlaştırmıştır. Bunu yaparken de, bölgelerin sahip oldukları benzer niteliklere göre bir tablo ortaya çıkarmayı amaçlamıştır. Böylece Türkiye'de de örnek bölge birimi uygulaması olarak, (TUIK)'in desteği ile Devlet Planlama Teşkilatı (DPT) tarafından 2002 yılında tamamlanmış ve kabul edilmiştir. İller 3 Düzey olarak tanımlanmış; ekonomik, sosyal ve coğrafi yönden benzerlik gösteren komşu illler, bölgesel kalkınma planları ve nüfus büyüklükleri dikkate alınarak 1. Düzey ve 2. Düzey olarak hiyerarşik bir şekilde sıralanmıştır.

Bu araştırmada, değişen sayıda eleman içeren kümeler oluşturularak, her bir kümeden değişen sayıda örnek eleman seçilmiştir. TÜİK'in oluşturduğu Düzey1 sınıflamasındaki 12 bölgeyi kapsayan tüm illerden öğretmenler araştırma kapsamına dahil edilmiştir. Düzey1 sınıflamasını kapsayan iller EK-2'de verilmiştir.

Tablo 1.

*Araştırma Yapılan Bölgeler*

| İstanbul |
|---|
| Batı Marmara |
| Ege |
| Doğu Marmara |
| Batı Anadolu |
| Akdeniz |
| Orta Anadolu |
| Batı Karadeniz |
| Doğu Karadeniz |
| Kuzeydoğu Anadolu |
| Orta Doğu Anadolu |
| Güney Doğu Anadolu |

**Veri Toplama Aracı**

Bu başlık altında öğretmenlerin bilgi güvenliği farkındalık seviyelerini belirlemek amacıyla oluşturulan Bilgi Güvenliği Farkındalığı anketinin özellikleri ve geliştirme aşamalarıyla ilgili bilgiler verilmiştir.

Araştırmanın verileri anket tekniğinden yararlanılarak toplanmıştır. Anket "Posta ile ölçme kâğıdı gönderilerek ya da kişilere gidilerek görüşlerin saptanması işlemidir (Kaptan, 1993; s.34). Anket'in diğer veri toplama tekniklerine göre, farklı bölgelerden ve büyük gruplardan veri toplama konusunda büyük avanatajları bulunmaktadır (Büyüköztürk vd., ,2012).

Veri toplama aracı olarak kullanılan anketin geliştirilmesi aşamasında Büyüköztürk (2008) tarafından belirtilen aşamalar dikkate alınmıştır. Aşamalar şöyledir;

- Problemi Belirleme (Amaç ve Soru belirleme)
- Madde Yazma (Taslak Form)
- Uzman Görüşü alma
- Pilot uygulama ve Ankete Son Şeklini Verme

Araştırmada Türkiye'nin farklı bölgelerinde yaşayan öğretmenlerin Bilgi güvenliği

farkındalığını belirleyebilmek için katılımcılara uygulanmak üzere 76 sorudan oluşan bir anket geliştirilmiştir. Literatür taraması ve güncel maruz kalınan tehlikeler (Sazan avlama, Spam eposta, Pharming, Sosyal mühendislik) incelenmiş ve 76 sorudan oluşan bir soru havuzu oluşturulmuştur.

Ölçme aracı üç ana bölümden oluşmaktadır. Birinci bölüm Kişisel Bilgileri kapsamakta ve farklı branşlardaki öğretmenlerin cinsiyet, yaş, şehir, eğitim düzeyi, branş, görev süresi, internet kullanım süresi, interneti kullanım amaçları, bilgi güvenliğine yönelik eğitim alma durumu ve sosyal medya kullanım durumu bilgilerini içermektedir. Bu bölümde öğretmenlerin demografik özelliklerini betimlemeye yönelik olgusal sorular yer almaktadır. İkinci bölüm, farklı branşlardaki öğretmenlerin bilgisayar ve interneti güvenli kullanma durumunu ölçmektedir ve dijital ortamlarda bilginin korunma düzeyini ölçmeyi amaçlayan maddeler bulunmaktadır. Katılımcıların güvenli bilgisayar kullanımı konusunda ne bildiklerini belirlemeye yönelik bilgi soruları yer almaktadır.

Üçüncü ve son bölüm öğretmenlerin bilgi güvenliği konusunda farkındalık düzeylerini ölçmek amacıyla 32 madde bulunmaktadır.

Öğretmenlerin Bilgisayar ve İnterneti güvenli kullanması konusundaki mevcut bilgi durumlarını ölçmek amacıyla çoktan seçmeli şeklinde maddeler oluşturulurken, öğretmenlerin ne derece katıldıklarını ortaya koymak amacıyla Bilgi Güvenliği Farkındalık Düzeyi boyutlarına ilişkin maddeler "Her zaman", "sık sık", "Bazen", "Nadiren", ve "Hiçbir zaman" biçiminde derecelendirilmiştir. Ölçme aracı kapsam geçerliliğinin yanı sıra yapı ve görünüş geçerliliği anlamında, uzman görüşüne başvurularak gözden geçirilmiştir.

**Uzman Görüşü Alma**

Taslak veri toplama aracı hazırlanırken maddelerin açık, anlaşılır ve kısa olmasına dikkat edilmiştir ayrıca her bir maddenin, bir davranışı veya durumu yansıtmasına özen gösterilmiştir. Taslak anketteki ifadelerin kapsam ve görünüş geçerliğine uygunluğu ve ifadelerin doğruluğu için alanında uzman 3 öğretim üyesi (1 Ölçme ve değerlendirme bölümünden, 2 Bilgisayar ve Öğretim Teknoloji bölümünden) ve bilgi güvenliği alanında deneyimli, devlet kurumlarında uzman olarak görev yapan 2 kişinin görüşlerine başvurulmuştur. Uzman görüşleri çevrimiçi ortamda sunulan uzman değerlendirme formu aracılığıyla alınmıştır. Kapsam geçerliğini test etmede kullanılan yöntemlerden biri de uzman görüşüne başvurmaktır (Eroğlu, 2009). Uzmanların görüşüne göre 4 madde ölçekten çıkarılmış ve 3 maddenin anlamı düzenlenmiştir.

**Pilot Uygulama Ve Ölçeğe Son Şeklini Verme**

Uzman değerlendirmesi sonucunda, hazırlanan anket geçerlik ve güvenirlik çalışması yapmak için pilot uygulama aşamasında hazır hale getirilmiştir. Pilot uygulama aşamasında 54 maddelik taslak anket belirlenen örneklem dışında, Ankarada bulunan 121 Öğretmen üzerinde online olarak gerçekleştirilmiştir.

Tablo 2.

*Pilot Uygulamaya Katılan Öğretmenlerin Branş Dağılımı*

| **Branşlar** | **N** | **%** |
|---|---|---|
| Matematik | 25 | 21 |
| Bilişim Teknolojileri [BT] | 19 | 16 |
| Türkçe | 23 | 19 |
| Sınıf Öğretmenliği | 24 | 20 |
| Fen ve Teknoloji | 18 | 15 |
| Sosyal bilgiler | 12 | 10 |
| Toplam | 121 | 100,0 |

Ön uygulamaya katılan öğretmenlerin 80 (% 66,1)'i kadın, 41 (% 33,8)'i erkektir. Tablo 2'de görüldüğü üzere, katılımcıların %25'i matematik, %19'u Bilişim Teknolojileri, %23'ü Türkçe, %24'ü Sınıf Öğretmenliği, %18'i Fen ve Teknoloji ve % 12'si Sosyal bilgiler branşlarındandır.

**Açımlayıcı faktör analizi**

Açımlayıcı faktör analizi, birbiriyle ilişkili birden fazla değişkeni bir araya getirerek, kavramsal olarak anlamlı ve az sayıda yeni değişkenler bulmayı ve keşfetmeyi amaçlayan çok değişkenli bir istatistiktir (Büyüköztürk, 2002, s.130).

Green vd. (1997)'den aktaran Çokluk, açımlayıcı faktör analizinin değişken azaltma ve belirlenen faktörlerin davranışının azalmasına yardımcı olan kuramın yapıları ile benzerlik gösterip gösterdiğini ortaya koyduğunu belirtmektedir. Yani, faktör analiziyle belirli bir faktör altında toplanan maddelerin, kuramsal yapının göstergeleri olup olmadığına ilişkin sorgulama yapılmaktadır (Çokluk, Şekercioğlu ve Büyüköztürk, 2014).

Araştırmacı tarafından geliştirilen Öğretmenlerin Bilgi Güvenliği Farkındalığı anketinin yapı geçerliliğini saptamak amacıyla açımlayıcı faktör analizi yapılmıştır. Açımlayıcı faktör analizi için SPSS 23 paket programı kullanılmıştır. Bu faktör analizinden önce verilerin faktör analizine uygunluğunu belirlemek amacıyla KMO katsayısı hesaplanmış, Bartlett's Sphericity testi uygulanmıştır. Örneklemin yeterliliğini test eden Kaiser- Meyer-Olkin (KMO) testi'nin değeri 0.839 olarak bulunmuştur.

Tablo 3.

*KMO ve Bartlett Testi Sonuçları*

| **KMO and Bartlett's Test** | | |
|---|---|---|
| Kaiser-Meyer-Olkin Measure of Sampling Adequacy. | | ,839 |
| Bartlett's Test of Sphericity | Ki-kare | 4793,715 |
| | Serbestlik derecesi | 496 |
| | Sig. | ,000 |

Tablo 3'de gösterildiği gibi, KMO değerinin .70'den büyük olması, bu veriler üzerinde faktör analizinin yapılabileceğini göstermektedir. Ayrıca Bartlett Sphericity testi ($p<.01$) anlamlı farklılık gösterdiği için faktör analizinin yapılmaya uygun olduğu tespit edilmiştir (Büyüköztürk, 2008).

Açımlayıcı Faktör analizi uygulmasında, faktör yük değeri ,40'tan düşük olan maddelerin görünmemesi istenmiştir ve varimax döndürme tekniği uygulanmıştır. Ölçeklerde yapı geçerliliğinin sağlanması için, yüksek olan iki faktör yükü arasındaki farkın en az (,10) olması ve faktör yük değerinin (,45) ve daha yüksek olması gerekmektedir (Büyüköztürk,2008). Dolayısıyla, birden fazla faktör altında yer alan ve yükleri arasında .10'dan daha düşük fark bulunan maddeler binişik kabul edilerek 5 madde ölçme aracından çıkarılmıştır. Her bir madde çıkarma işleminden sonra analiz tekrarlanmıştır.

Açımlayıcı faktör analizi sonuçları bulgular bölümünde verilmiştir.

### Geçerlilik-Güvenirlik

Veri toplama aracının pilot uygulaması yapılmış ve güvenirlik analizi için cronbach alpha iç tutarlılık katsayısı hesaplanmışır. Cronbach alpha 0 ve 1 arasında değişmektedir. Güvenirlik katsayısının değerleri aşağıdaki ölçütlere göre değerlendirmeye alınır.

$0.0 \leq \alpha < 0.40$ ise ölçek güvenilir değildir.

$0.40 \leq \alpha < 0.60$ ise ölçek düşük güvenirliktedir

$0.60 \leq \alpha < 0.80$ ise orta düzeyde güvenilirdir.

$0.80 \leq \alpha < 1.00$ ise ölçek yüksek derecede güvenilir bir ölçektir.

Tablo 4.

*Güvenirlik Katsayısı*

| **Güvenirlik** | |
|---|---|
| Cronbach's Alpha | Madde sayısı |
| ,741 | 28 |

Güvenirlik analizi için cronbach alpha değeri .741 olarak bulunmuştur (Bkz. Tablo 4). Bu sonuç geliştirilen ölçme aracının güvenilir olduğunu göstemektedir.

Tablo 5.

*Bilgi Güvenliği Farkındalığı Ölçeği için Güvenirlik*

| ***Faktör*** | ***Madde Sayısı*** | ***Cronbach Alfa*** |
|---|---|---|
| Mağduriyet | 8 | .836 |
| Önlem Alma | 8 | .702 |
| Koruma Düzeyi | 5 | .753 |
| Davranış | 4 | .741 |
| Kişisel Bilgi Gizliliği | 3 | .762 |
| Ölçek | 28 | .741 |

Ayrıca, Tablo 5'de görüldüğü üzere 8 maddeden oluşan mağduriyet ölçeği için cronbach alfa katsayısı .836, 8 maddeden oluşan Önlem alma ölçeği için .702, 5 maddeden oluşan Koruma Düzeyi ölçeği için .753, 4 maddeden oluşan Davranış ölçeği için .741 ve Kişisel Bilgi Gizliliği ölçeği için .762 bulunmuştur.

Güvenirlik katsayısının ölçeğinin geneli ile faktörlerde orta düzeyde güvenilir seviyede olması, ölçme aracının maddelerinin belirli bir amacı ölçmek için biraraya getirildiğinin bir göstergesidir. Ayrıca veri toplamak için geliştirilen anketler çevrimiçi ortamda web sayfası üzerinden sunulmuştur. Bu web sayfasında, anketi aynı kişilerin doldurmaması temin etmek adına Ip kontrolü eklenmiştir. Yani anket tek bir Ip adresinden doldurulabilmektedir. Böylece bir bilgisayardan sadece bir kişi anketi doldurma imkânı bulabilmektedir. Bu durumda ölçme aracının güvenirliliğini olumlu yönde etkilemiştir.

**Normallik Testi Sonuçları**

Geliştirilen ölçekle toplanan verilerin analizinde parametrik testlerin kullanılabilmesi için

verilerin normal bir dağılım göstermesi gerekmektedir. Verilerin dağılımının normal olmadığı durumlarda parametrik olmayan testlerin kullanılması gerekmektedir. Bundan dolayı araştırmada Öğretmenlerin Bilgi Güvenliği Farkındalığı adlı ölçme aracından elde edilen verilere Kolmogorov-Simirnov testi ve Sharpiro-Wilk normallik testi uygulanmıştır. Her iki dağılımı hesaplayan testlerde de p değeri 0 olarak bulunmuştur ve bu değer 0,05 anlamlılık değerinden düşük olduğu için "Veriler normal dağılmaktadır" hipotezi reddedilmiştir.

**Verilerin Toplanması**

Katılımcıların Bilgi Güvenliği Farkındalıklarını ölçmek için veri toplama aracı olarak, araştırmacı tarafından geliştirilen "Öğretmenlerin Bilgi Güvenliği Farkındalığı Anketi" kullanılmıştır. Pilot uygulama ve geçerlik-güvenirlik çalışmalarından sonra hazır duruma gelen ölçme aracını uygulmak için bir çevrimiçi ortam tasarlanmıştır. Bu ortamda bilgiguvenligifarkindaligi.com isimli web sayfası, sosyal ağlarda ve akademik ve mesleki formlarda açıklayıcı bilgilerle birlikte paylaşılmıştır. Akademik çevrelerce de paylaşılması sağlanmıştır. Ölçme aracının uygulama süresi Eylül-Kasım 2015 tarihleri arasında gerçekleşmiştir. Ölçme aracının çevrimiçi durumu Ek-2'de gösterilmektedir.

**Verilerin Çözümlenmesi ve Yorumlanması**

Farklı branşlardaki öğretmenlerin bilgi güvenliği farkındalıklarını belirlemek amacıyla yapılan bu çalışmadan elde edilen veriler bilgisayar ortamında SPSS (Statistical Package for the Social Sciences) 23.0 paket programı yardımıyla analiz edilip çözümlenerek yorumlanmıştır.

Araştırmaya katılan öğretmenleri tanıma amaçlı hazırlanan demografik özellikler frekans ve yüzde gibi betimsel istatistiklerle analiz edilmiştir. Aynı şekilde, öğretmenlerin bilgisayar ve interneti güvenli kullanım durumlarını ölçen 11 çoktan seçmeli soru için de frekans ve yüzde alınarak durum betimlenmiştir.

Farklı branşlardaki öğretmenlerin bilgi güvenliği farkındalık düzeyini tespit etmeye yönelik yapılan ankette, her madde için ortalama puanlar hesaplanmıştır. Bu puanlar ölçme aracının alt bölümlerinden alınabilecek en düşük ve en yüksek puanları ile derecendirilerek belirlenmiştir. Belirlenmiş puan aralıklarının karşılık geldiği bilgi güvenliği farkındalık düzeyi bulgular bölümünde gösterilmiştir.

Bu anket kapsamında sorularda bulunan “Her Zaman” seçeneğinin puanı 5, “Sık Sık” seçeneğinin puanı 4, “Bazen” seçeneğinin puanı 3, “Nadiren” seçeneğinin puanı 2, “Hiçbir Zaman” seçeneğinin puanı ise 1 olarak belirlenerek, katılımcıların toplam puanı hesaplanmıştır.

Bu durumda;

Mağduriyet alt ölçeğinden alınabilecek en yüksek puan 40 (8x5), en düşük puan ise 8 (8x1); Önlem alma alt ölçeğinden alınabilecek en yüksek puan 40 (8x5), en düşük puan ise 8 (8x1); Koruma bilinci alt ölçeğinden alınabilecek en yüksek puan 25 (5x5), en düşük puan ise 5 (5x1); Davranış alt ölçeğinden alınabilecek en yüksek puan 20 (4x5), en düşük puan ise 4 (4x1); Kişisel Bilgi Gizliliği alt ölçeğinden alınabilecek en yüksek puan 15 (3x5), en düşük puan ise 3 (3x1) olarak belirlenmiştir.

Öğretmenlerin bilgi güvenliği farkındalığı ölçeğinin verileri toplanarak, Kolmogorov-Simirnov testi ve Sharpiro-Wilk normallik testi uygulanmıştır ve verilerin normal dağılmadığı görülmüştür. Bu durumda, normallik varsayımının karşılanmadığı durumlarda ilişkisiz iki örneklem için Mann-Whitney U testi, ikiden fazla ilişkisiz örneklem için Kruskal- Wallis H-testi uygulanmıştır. Bu testlerle öğretmenlerin bilgi güvenliği farkındalığı toplam puanlarının; yaş, cinsiyet, eğitim durumu, bulundukları bölge, bilgisayar kullanım süresi, internet kullanım süresi ve meslekte geçirdikleri süreye göre farklılık gösterip göstermediği incelenmiştir.

Öğretmenlerin bilgi güvenliği farkındalık puanlarının, bilgi güvenliği ile ilgili eğitim alıp almama durumuna göre anlamlı bir farklılık gösterip göstermediği durumu Mann- Whitney U testi ile incelenmiştir.

Öğretmenlerin bilgi güvenliği farkındalık puanlarının, öğretmenlerin branşları ile anlamlı bir farklılık gösterip göstermediği durumu ise yine Mann Whitney U testi ile incelenmiştir. Araştırmada verilerin yorumlanmasında anlamlılık düzeyi $p$=0,05 olarak alınmış ve analiz sonucunda elde edilen bulgular 0,95 güven aralığında değerlendirilmiştir.

# BÖLÜM IV

# BULGULAR VE YORUMLAR

Bu bölümde, araştırmanın amacına yönelik belirlenen alt amaçlara ait; toplanan verilerle ilgili bulgular ve bulgulara ilişkin yorumlar bulunmaktadır.

**Açımlayıcı Faktör Analizi Bulguları**

Açımlayıcı faktör analizi yapılan ölçeğin, özdeğeri 1,00 ve üstünde olan 5 faktörden oluştuğu ve 5 faktörün açıkladığı varyans oranı %43,726 olarak ölçülmüştür. Faktör analizi sonucunda farkındalık ölçme aracındaki maddelerden 8'i 1.faktörde, 8'i 2.faktörde, 5'i 3'cü faktörde, 3'ü 4'cü faktörde ve 4'ü 5.faktörde toplanmıştır. 1. faktör Mağduriyet**,** 2.faktör Önlem Alma, 3.faktör Koruma Düzeyi 4.faktör Davranış ve 5.faktör Kişisel Bilgi Gizliliği Olarak adlandırılmıştır.

Tablo 6.*Öğretmenlerin Bilgi Güvenliği Farkındalığı Anketinin Maddelerine ilişkin Faktör Yükleri*

| Madde No | Mağduriyet | Önlem Alma | Koruma Bilinci | Davranış | Kişisel Bilgi Gizliliği |
|---|---|---|---|---|---|
| **22** | ,814 | | | | |
| **23** | ,811 | | | | |
| **27** | ,791 | | | | |
| **21** | ,738 | | | | |
| **24** | ,737 | | | | |
| **19** | ,486 | | | | |
| **10** | ,473 | | | | |
| **25** | ,557 | | | | |
| **29** | | ,610 | | | |

| | | | | |
|---|---|---|---|---|
| **30** | ,598 | | | |
| **6** | ,549 | | | |
| **11** | ,547 | | | |
| **14** | ,544 | | | |
| **9** | ,487 | | | |
| **18** | ,484 | | | |
| **31** | ,424 | | | |
| **17** | | ,708 | | |
| **16** | | ,657 | | |
| **3** | | ,526 | | |
| **4** | | ,456 | | |
| **28** | | ,417 | | |
| **20** | | | ,688 | |
| **26** | | | ,671 | |
| **7** | | | ,552 | |
| **13** | | | ,437 | |
| **1** | | | | ,690 |
| **8** | | | | ,470 |
| **5** | | | | ,417 |

Yapılan Scree Plot grafiğiyle; ikinci noktadan üçüncü noktaya keskin bir düşüş olduğu ve beşinci noktadan sonra çizginin eğimi yatay bir seyre geçtiği görülmüştür. Dolayısıyla, beşinci noktanın üzerinde kalan nokta sayısı faktör sayısı olarak belirlenmiştir.

**Bağımsız Değişkenlere Ait Frekans ve Yüzde Değerleri**

Bu bölümde araştırmaya katılan öğretmenlerin kişisel profillerini belirlemek amacıyla toplanan; cinsiyet, yaş, öğrenim durumu, şehir, branş ve görev süresi değişkenleriyle ilgili frekans değerleri ve yüzde hesaplamalarına yer verilmiştir. Araştırmaya katılan öğretmenlerin bu değişkenlere ilişkin sayısal değerleri aşağıda tablolar şeklinde sunulmuştur.

Tablo 7.

*Katılımcıların Cinsiyet Dağılımı*

| **Cinsiyet** | **N** | **%** |
|---|---|---|
| Kadın | 840 | 62,0 |
| Erkek | 515 | 38,0 |
| Toplam | 1355 | 100,0 |

Araştırmanın örneklemini 1355 öğretmen oluşturmaktadır. Tablo 7'de görüldüğü üzere, katılımcıların %62'si kadın (N=840) ve % 38'i (N=515) erkektir.

Tablo 8.

K*atılıcıların Yaş Aralığı*

| **Yaş Aralığı** | **N** | **%** |
|---|---|---|
| 21-30 | 945 | 69,7 |
| 31-40 | 315 | 23,2 |
| 41-50 | 85 | 6,3 |
| 51-60 | 10 | 0,7 |
| Toplam | 1355 | 100,0 |

Araştırmaya katılan öğretmenlerin yaş gruplarıyla ilgili Tablo 8 incelendiğinde, öğretmenlerin %69,7'si (N=945) 21- 30 yaş arasında, %23,2'si (N=315) 31-40 yaş arasında, %6,3'ü (N=85) 41-50 yaş arasında ve %7'si (N=10) 51-60 yaşları arasında olduğu görülmektedir.

Tablo 9.

*Katılıcıların Bölgelere Göre Dağılımı*

| **Düzey 1** | **N** | **%** |
|---|---|---|
| Tra Kuzeydoğu Anadolu | 102 | 7,5 |
| Trb Ortadoğu Anadolu | 111 | 8,2 |
| Trc Güneydoğu Anadolu | 155 | 11,4 |
| Tr1 İstanbul | 105 | 7,7 |
| Tr2 Batı Marmara | 81 | 6,0 |
| Tr3 Ege | 119 | 8,8 |
| Tr4 Doğu Marmara | 84 | 6,2 |
| Tr5 Batı Anadolu | 122 | 9,0 |
| Tr6 Akdeniz | 145 | 10,7 |
| Tr7 Orta Anadolu | 112 | 8,3 |
| Tr8 Batı Karadeniz | 91 | 6,7 |
| Tr9 Doğu Karadeniz | 128 | 9,4 |
| Toplam | 1355 | 100,0 |

Katılımcıların yaşadıkları bölgeyle ilgili Tablo 9'a bakıldığında görüleceği üzere, %7,5 (N= 102) Kuzeydoğu Anadolu bölgesinden, %8,2'si (N=111) Ortadoğu Anadolu bölgesinden, %11,4'ü (N=155) Güneydoğu Anadolu bölgesinden, %7,7'si (N=105) Düzey 1'e göre tek başına bir bölge olarak belirlenen İstanbul'dan, %6'sı (N=81) Batı Marmara bölgesinden, %8,8'i (N=119) Ege bölgesinden, %6,2'si (N=84) Doğu Marmara bölgesinden, %9'u (N=122) Batı Anadolu bölgesinden, %10,7'si (N=145) Akdeniz bölgesinden, %8,3'ü (N=112) Orta Anadolu bölgesinden, % 6,7'si (N=91) Batı Karadeniz bölgesinden, %9,4'ü (N=128) Doğu Karadeniz bölgesinden olmak üzere, Devlet Planlama Teşkilatının düzenlediği Düzey 1 olarak Türkiye'yi temsil eden 12 bölgeden toplamda 1355 öğretmen katılmıştır.

Tablo 10.

*Araştırmaya Katılan Öğretmenlerin Eğitim Durumu*

| **Eğitim Durumu** | **N** | **%** |
|---|---|---|
| Ön Lisans | 30 | 2,2 |
| Lisans | 805 | 59,4 |
| Yüksek Lisans | 395 | 29,2 |
| Doktora | 125 | 9,2 |

Araştırma örnekleminde bulunan öğretmenlerin eğitim düzeyleriyle ilgili olarak Tablo 10'a bakıldığında, katılımcıların %2,2'si (N=30) ön lisans mezunu iken, %59,4'ü (N=805) lisans mezunu, %29,2'si (N=395) yüksek lisans mezunu ve %9,2'si (N=125) doktora eğitimini tamamlamış bulunmaktadır.

Tablo 11.

*Araştırmaya Katılan Öğretmenlerin Branşlara Göre Dağılımı*

| **Branşlar** | **N** | **%** |
|---|---|---|
| Matematik | 264 | 19,5 |
| Bilişim Teknolojileri | 335 | 24,7 |
| Türkçe | 192 | 14,2 |
| Sınıf Öğretmenliği | 197 | 14,5 |
| Fen ve Teknoloji | 195 | 14,4 |
| Sosyal Bilgiler | 172 | 12,7 |
| Toplam | 1355 | 100,0 |

Araştırmaya katılan öğretmenlerin branşlarına bakıldığı zaman, Tablo 11'in incelenmesinden de anlaşılacağı üzere, çalışmaya 6 farklı branşta öğretmenler katılmıştır. Bunlardan %19,5'ini (N=264) Matematik öğretmeni, %24,7'sini (N=335) Bilişim Teknolojileri öğretmeni, %14,2'sini (N=192) Türkçe öğretmeni, %14,5'ini (N=197) Sınıf öğretmeni, %14,4'ünü (N=195) Fen ve Teknoloji öğretmeni ve %12,7'sini (N=172) Sosyal bilgiler öğretmeni oluşturmaktadır.

Tablo 12.

*Öğretmenlerin Görevdeki Geçirdikleri Zamanla İlgili Betimsel İstatistikler*

| **Görev Süresi** | **N** | **%** |
|---|---|---|
| 0-4 yıl | 830 | 61,3 |
| 5-9 yıl | 287 | 21,2 |
| 10-14 yıl | 105 | 7,7 |
| 15-19 yıl | 63 | 4,6 |
| 20 yıl ve üzeri | 70 | 5,2 |
| Toplam | 1355 | 100,0 |

Öğretmenlerin görev sürelerine bakıldığında Tablo 12'de görüldüğü üzere, % 61,3'ü (N=830) 0-4 yıl arasında görev yaparken, % 21,2'si (N=287) 5-9 yıl arasında, % 7,7'si (N=105) 10-14 yıl arasında, %4,6'sı (N=63) 15-19 yıl arasında ve %5,2'si (N=70) 20 yıl ve üzerinde görev yapmaktadır.

Tablo 13.

*Katılımcıların Akıllı Cep Telefonu Bulundurma Durumu*

| **Akıllı cep telefonu** | **N** | **%** |
|---|---|---|
| Evet | 1320 | 97,4 |
| Hayır | 35 | 2,6 |
| Toplam | 1355 | 100,0 |

Katılımcıların teknolojiyi kullanma profillerini belirlemek adına yöneltilen sorulara bakıldığında, öğretmenlerin akıllı cep telefonu olma durumu Tablo 13'de görüldüğü üzere, %97,4'ünün (N=1320) akıllı cep telefonu bulunurken, %2,6'sının (N=35) akıllı bir cep telefonunun olmadığı görülmektedir.

Tablo 14.

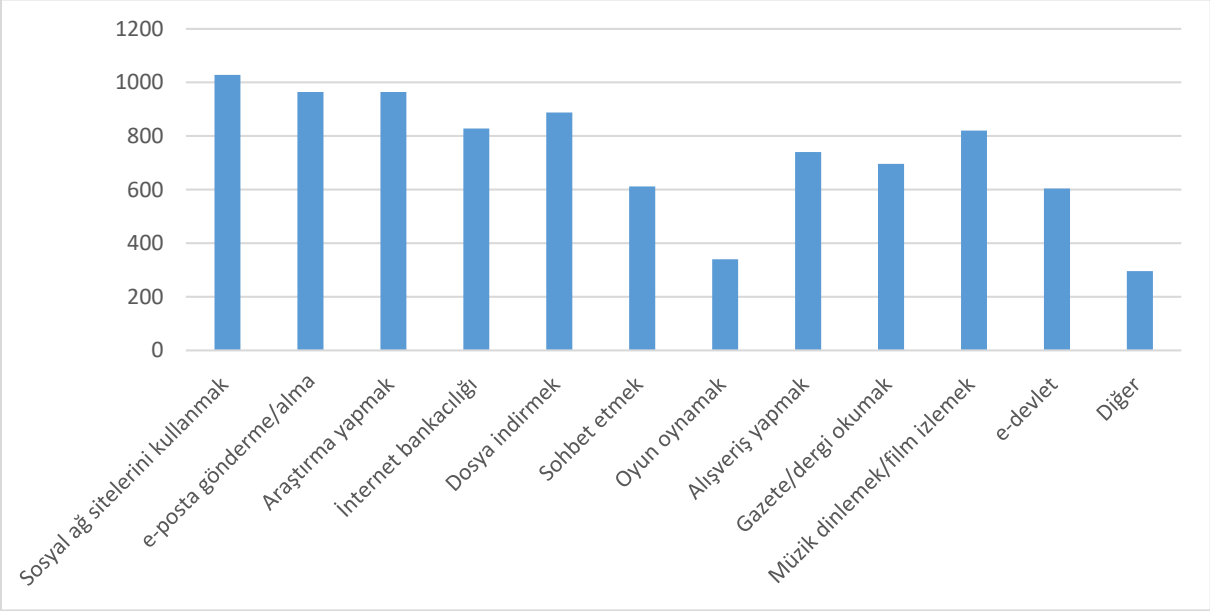
*Katılımcıların İnterneti Kullanma Süresi*

| **İnternet Kullanım Süresi** | **N** | **%** |
|---|---|---|
| 0-4 yıl | 100 | 7,4 |
| 5-9 yıl | 475 | 35,1 |

| | | |
|---|---|---|
| 10-14 yıl | 605 | 44,7 |
| 15-19 yıl | 175 | 12,9 |

Araştırmaya katılan öğretmenlerin internet kullanma durumuna bakıldığında, Tablo 14'de inceleneceği üzere, % 7,4'ü (N=100) 4 yıla kadar internet kullanırken, %35,1'i (N=475) 5-9 yıl arasında kullanmakta, %44,7'si (N=605) 10-14 yıl arasında, %12,9'u (N=175) 15-19 yıl arasında internet kullanmaktadır.

*Katılımcıların İnterneti Kullanma Amaçları*




Şekil 6. Katılımcıların İnterneti Kullanma Amaçları

Katılımcıların interneti hangi amaçlarla kullandıkları incelendiğinde en çok sosyal ağ sitelerini kullanmak, e-posta göndermek/almak, araştırma yapmak, dosya indirmek ve müzik dinlemek/ film izlemek olduğu görülmektedir. Ayrıca, internet bankacılığı, dosya indirmek, sohbet etmek, e-devlet, alışveriş yapmak ve oyun oynamakta diğer interneti kullanma amaçlarındandır (Bkz. Şekil 6).

Tablo 6.

*Katılımcıların Epostalerini Kontrol Etme Sıklığı*

| **Eposta Kutusu Kontrol Sıklığı** | **N** | **%** |
|---|---|---|
| Ayda bir kez | 90 | 6,6 |
| Haftada bir | 290 | 21,4 |

| | | |
|---|---|---|
| Hergün bir kez | 390 | 28,8 |
| Hergün birden fazla | 535 | 39,5 |
| Yılda bir kez | 30 | 2,2 |
| Bir yıldan fazla süredir | 20 | 1,5 |

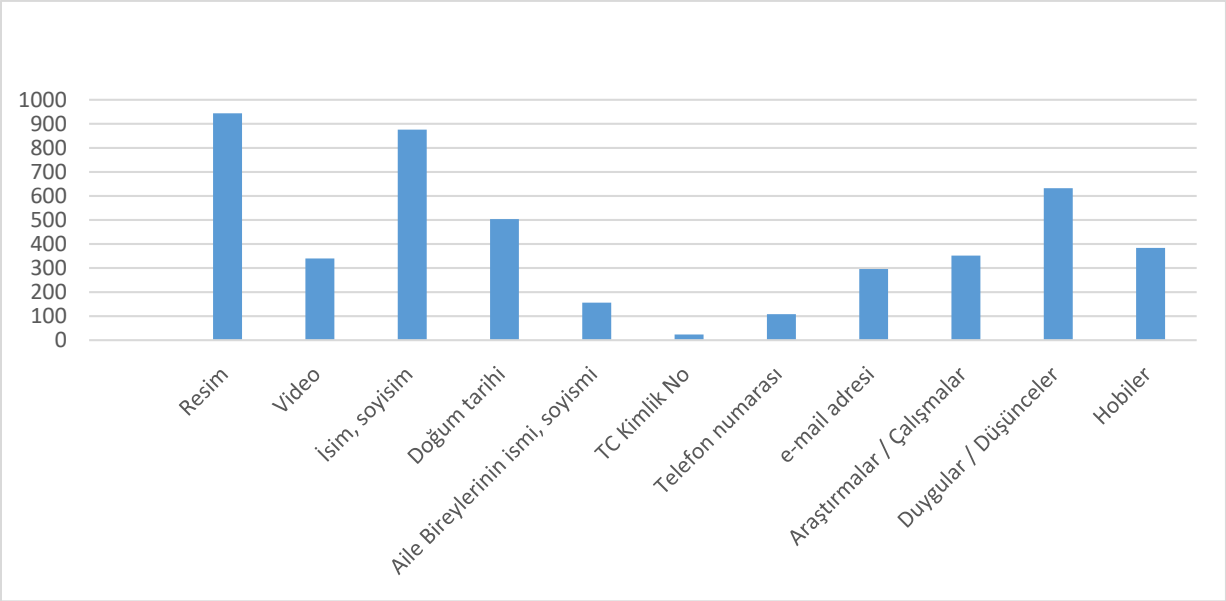
Katılımcıların epostalarını kontrol etme durumları için Tablo 6'ya bakıldığında, öğretmenlerin % 39,5'i (N=535) eposta kutusunu her gün günde birden fazla kontrol ederken, %28,8'i (N=390) her gün bir kez, %21,4'ü (N=290) haftada bir kez, %6,6'sı (N=90) ayda bir kez, %2,2'si (N=30) bir kez ve %1,5'i (N=20) bir yıldan fazla sürede eposta kutusunu kontrol ettiğini belirtmektedir.

Tablo 7.

*Katılımcıların Sosyal Medya Hesaplarının Olma Durumu*

| **Sosyal Medya platformlarında bir hesabınız var mı? (Facebook, Twitter, Instagram vs.)** | **N** | **%** |
|---|---|---|
| Evet | 1275 | 94,1 |
| Hayır | 80 | 5,9 |
| Toplam | 1355 | 100,0 |

Araştırmaya katılan öğretmenlerin bir sosyal ağ'a üyelik durumları Tablo 7'den anlaşılacağı üzere, öğretmenlerin %94,1'inin (N=1275) bir sosyal ağa üyeliği varken, %5,9'unun (N=80) herhangi bir sosyal ağa üyeliği bulunmamaktadır.




Şekil 7. Sosyal Ağlarda Paylaşılan Bilgiler

Katılımcı öğretmenlerin sosyal ağlarda paylaştıkları bilgiler için Şekil 7'de incelendiğinde, katılımcılar en çok resimlerini, isim/soyisimlerini, duygu/düşüncelerini, doğum tarihlerini, hobilerini, araştırmalarını ve eposta adreslerini paylaşmaktadırlar. Ayrıca, telefon numarası, aile bireylerinin ismi-soyismi ve TC vatandaşlık numaralarını paylaşan katılımcılar bulunmaktadır.

**Birinci Alt Probleme İlişkin Bulgular**

Araştırmanın birinci alt probleminde, Öğretmenlerin bilişim teknolojilerini güvenli kullanım düzeylerini belirlemek hedeflenmiştir. Bu amacı gerçekleştirmek için katılımcıların güvenli kullanım davranış durumlarını belirlemek amacıyla bilgi soruları sorulmuştur. Bu sorulara verilen cevaplar betimsel istatistik yöntemiyle frekans ve yüzde olarak analiz edilmiştir.

Tablo 8

*Anti Virüs Yazılımı Kullanımına Dair Betimsel İstatistikler*

| **Madde** | **N** | **%** |
|---|---|---|
| Evet | 1105 | 81,5 |
| Hayır | 250 | 18,5 |

Araştırmaya katılan öğretmenlerin teknolojik aletlerinde anti virüs yazılımı kullanma durumları Tablo 9'da görüldüğü üzere, %81,5'i (N=1105) bir anti virüs yazılımı kullanırken, %18,5'i (N=250) anti virüs yazılımı kullanmamaktadır.

Tablo 9

*Bilgisayarlarda Kullanılan Anti Virüs Yazılım Türü*

| **Madde** | **N** | **%** |
|---|---|---|
| Ücretsiz antivirüs yazılımı kullanırım | 725 | 53,5 |
| Korsan (şifresi kırılmış) antivirüs yazılımı kullanırım | 290 | 21,4 |
| Lisansı ödenmiş antivirüs yazılımı kullanırım | 325 | 24,0 |
| Diğer | 15 | 1,1 |

Katılımcılardan anti virüs kullandığını belirten %81,5'lik kısmının, %53,5'i (N=725) ücretsiz anti virüs yazılımı kullanırken, %24'ü (N=325) lisansı ödenmiş anti virüs yazılımı kullanmakta,%21,4'ü (N=290) şifresi kırılmış anti virüs yazılımı kullanmakta iken %1,1'i (N=15) diğer anti virüs yazılım türlerini kullanmaktadır.

Tablo 10

*Eposta Kontrol Etme Sıklığı*

| **Madde** | **N** | **%** |
|---|---|---|
| Günlük | 165 | 12,2 |
| Haftalık | 285 | 21,0 |
| Ayda bir kez | 305 | 22,5 |
| Yılda bir kez | 110 | 8,1 |
| Sadece kurduğum zaman | 55 | 4,1 |
| Bilgisayarda yavaşlama olduğu zaman | 330 | 24,4 |
| Diğer | 105 | 7,7 |

Öğretmenlerin virüs taraması sıklıkları incelendiğinde, Tablo 10'dan anlaşıldığı üzere katılımcıların %24,4'ü (N=330) virüs taramasını bilgisayarda yavaşlama olduğu zaman yaparken, %22,5'i (N=305) virüs taramasını ayda bir kez, %21'i (N=285) haftada bir kez, %12,2'si (N=165) günlük, % 8,1'i (N=110) yılda bir kez ve % 7,7' si (N=105) diğer olarak belirtmektedir. Bu sonuçlar, öğretmenlerin virüs taraması sıklıklarının bilgisayarlarında yavaşlama olduğunda veya ayda bir kez olduğunu göstermektedir. Gökmen (2014) böte öğretmen adaylarıyla yaptığı çalışmasında, adayların kısa zaman aralıklarıyla virüs taraması yaptıklarını belirtmektedir.

Tablo 11

*Spam Eposta Nedir Soruna Verilen Cevaplar*

| **Madde** | **N** | **%** |
|---|---|---|
| Spam server tarafından gönderilen bir e-postadır | 120 | 8,9 |
| Spam bir çeşit güvenlik duvarıdır | 145 | 10,7 |
| Spam, istenmeyen postadır | 1015 | 74,9 |
| Spam bir eposta ekidir | 45 | 3,3 |
| Spam, bilinen bir kişi tarafından gönderilen postadır | 30 | 2,2 |

Katılımcıların güvenli kullanım boyutlarını ölçen bilgi sorularından olan "spam nedir?" sorusuna Tablo 11'de görüldüğü gibi, öğretmenlerin %74,9'u (N=1015) doğru cevap olan istenmeyen postadır şıkkını seçmişlerdir. % 10,7'si (N=145) spam'ı bir çeşit güvenlik duvarı olarak tanımlarken, %8,9'u (N=120) spam'ı server tarafından gönderilen bir e-posta olarak, %3,3'ü spam'ı bir eposta eki olarak ve % 2,2'si (N=30) spamı bilinen bir kişi tarafından gönderilen e-posta olarak tanımlamışlardır. Bu sonuçlar, öğretmenlerin eposta güvenliği konusunda en önemli bileşen olan spam eposta hakkında yeterli bilgiye sahip olduklarını göstermektedir. Aynı şekilde Durmuş (2014) farklı sektörlerden katılımcılarla yaptığı çalışmasında, katılımcıların büyük bir çoğunluğunun spam'ı istenmeyen posta olarak değerlendirdiğini belirtmiştir.

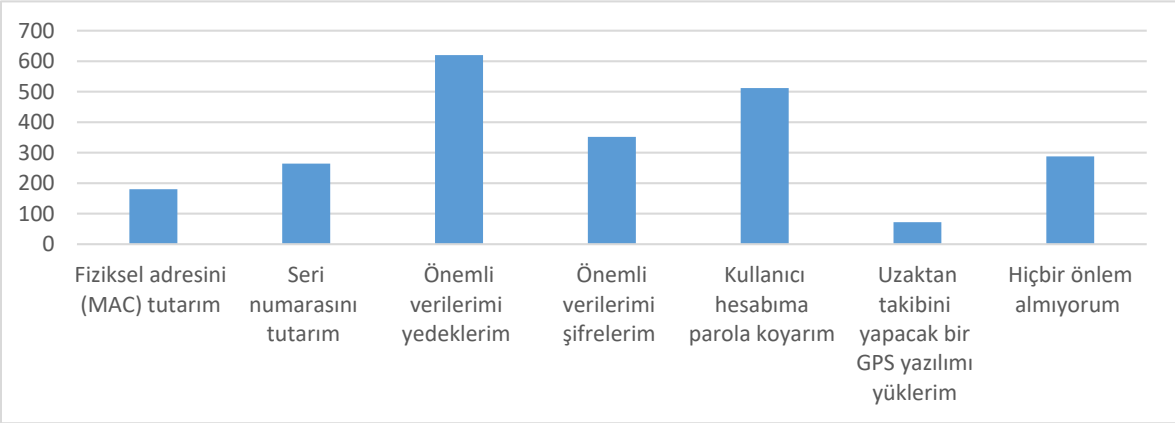
Tablo 12

*"Bankanızdan gelen bir e-postada, bilgilerinizi güncellemeniz için bir adrese tıklamanız istense ne yaparsınız?" Sorusunun Betimsel İstatistik Bulguları*

| **Madde** | **N** | **%** |
|---|---|---|
| Eğer bankanın logo'su ve adresi doğru ise linki tıklarım | 405 | 29,9 |
| Yakın arkadaşlarım bilgilerini güncellerse ben de aynısını yaparım | 50 | 3,7 |
| Eposta hakkında bilgi almak için bankayı ararım | 590 | 43,5 |
| Diğer | 310 | 22,9 |

Katılımcılara yöneltilen bir diğer bilgi sorusu olan, "Bankanızdan gelen bir e-postada, bilgilerinizi güncellemeniz için bir adrese tıklamanız istense ne yaparsınız? " sorusuna

katılımcıların %43,5'i (N=590) doğru seçenek olan "eposta hakkında bilgi almak için bankayı ararım" ı seçmişlerdir. Bununla birlikte, öğretmenlerin % 29,9'u (N=405) "Eğer bankanın logo'su ve adresi doğru ise linki tıklarım" seçeneğini seçerken, % 22,9'u (N=310) diğer seçeneğini ve % 3,7'si (N=50) "Yakın arkadaşlarım bilgilerini güncellerse ben de aynısını yaparım" seçeneğini seçmiştir. Durmuş (2014) çalışmasında da katılımcıların büyük çoğunluğunun (%75) "eposta hakkında bilgi almak için bankayı ararım" cevabını verdiklerini belirtmektedir.




Şekil 8. Bilgisayarın Çalınma Durumuna Karşı Alınabilecek Önlemler

Araştırma katılımcılarına, "Bilgisayarınızın çalınabilme durumuna karşı hangi önlemleri alırsınız " sorusu yöneltilmiştir ve birden fazla cevap verebileceği belirtilmiştir. Bu soruyla ilgili bulgular Şekil 8'de verilmiştir. Şöyle ki, öğretmenlerin büyük bir çoğunluğunun, bilgisayarının çalınabilme durumuna karşı alacağı önlem önemli verileri yedeklemek olmuştur. Çalınma ihtimaline karşı alınan diğer seçilen önlemler ise, sırasıyla kullanıcı hesabına parola koymak, önemli verileri şifrelemek, bilgisayarın seri numarasını almak, fiziksel adresi olan MAC adresini almak ve uzaktan takibini yapacak GPS yazılımı yüklemek olarak belirtilmiştir. Bilgisayarın çalınma ihtimaline karşı hiçbir önlem almayan büyük bir kitle de bulunmaktadır.

Tablo 13

*"Tanıdığınız birisinden dosya eklentili ve eposta adresi tuhaf bir eposta gelirse ne yaparsınız" Sorusunun Betimsel İstatistikleri*

| **Madde** | **N** | **%** |
|---|---|---|
| Gönderen kişi tanıdığımsa eklentiyi açmak güvenlidir | 110 | 8,1 |

| | | |
|---|---|---|
| epostayı tanıdığımın gönderdiğini doğrularsam cevap veririm | 492 | 36,3 |
| Teyit etmek için tanıdığıma yeni bir eposta atarım | 448 | 33 |
| Diğer | 305 | 22,5 |

Öğretmenlerin eposta güvenliği bilgisini ölçmeyi amaçlayan bir diğer soru ise, "Tanıdığınız birisinden dosya eklentili ve eposta adresi tuhaf bir eposta gelirse ne yaparsınız? "'dir. Öğretmenlerin %36,3'ü (N=492) "Epostayı tanıdığımın gönderdiğini doğrularsam cevap veririm" seçeneğini seçerken,%33'ü (N=448) doğru seçenek olan "Teyit etmek için tanıdığıma yeni bir eposta atarım" seçeneğini seçmiştir. Katılımcıların %22,5'i (N=305) diğer seçeneğini, %8,1'i (N=110) "Gönderen kişi tanıdığımsa eklentiyi açmak güvenlidir" seçeneğini seçmiştir.

Tablo 14

*Aldatmaca Epostaleriyle İlgili Betimsel İstatistikler*

| **Madde** | **N** | **%** |
|---|---|---|
| Tüm arkadaşlarıma gönderirim | 90 | 6,6 |
| Sadece yakın arkadaşlarıma gönderirim | 55 | 4,1 |
| Eposta zincirine katılmadan yeni bir eposta oluştururum ve gönderen kişiye cevap veririm | 115 | 8,5 |
| Sakıncalı olduğunu düşünerek önemsemem | 908 | 67,0 |
| Diğer | 181 | 13,4 |

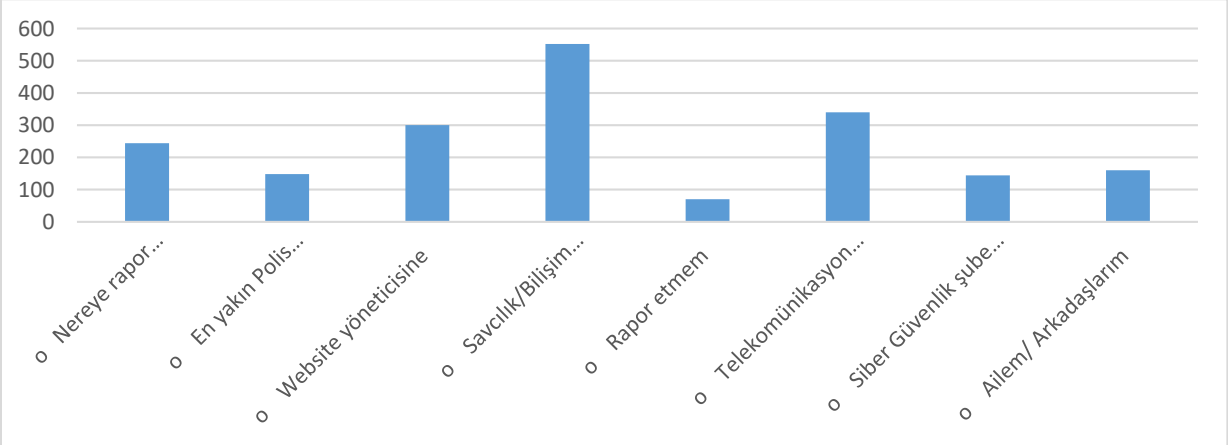
İnternet dünyasında en çok aldatma yöntemi olarak kullanılan örneklere, araştırmaya katılan öğretmenlerin tavrının nasıl olduğunu anlamak için sorulan "Size küçük bir kız çocuğunun kaçırıldığına dair veya acil kan ihtiyacı olduğu belirtilen vb. bir eposta gelse ve bu epostayı tüm arkadaşlarınıza göndermeniz istense ne yaparsınız" sorusuna, katılımcıların %67'si (N=908) "Sakıncalı olduğunu düşünerek önemsemem" cevabını verirken, %13,4'ü diğer seçeneğini işaretlemiştir. Bunun yanı sıra % 8,5'i (N=115) "Eposta zincirine katılmadan yeni bir eposta oluştururum ve gönderen kişiye cevap veririm" seçeneğini ve % 4,1'i (N=55) "Sadece yakın arkadaşlarıma gönderirim" seçeneğini işaretlemişlerdir.

Tablo 15

*Bir Sitenin Güvenli Olup Olmadığını Nereden Anlarsınız Sorusuyla İlgili Betimsel İstatistikler*

| **Madde** | **N** | **%** |
|---|---|---|
| Ücretsiz yazılım sunan bir web sitesi ise güvenlidir | 26 | 1,9 |
| Güvenlidir logosu varsa güvenlidir | 130 | 9,6 |
| İnternet adresi "http:// " yerine "https:// " ile başlıyorsa güvenlidir | 525 | 38,7 |
| Popüler görünüyorsa güvenlidir | 102 | 7,5 |
| Ayırt etmekte zorlanırım | 566 | 41,8 |

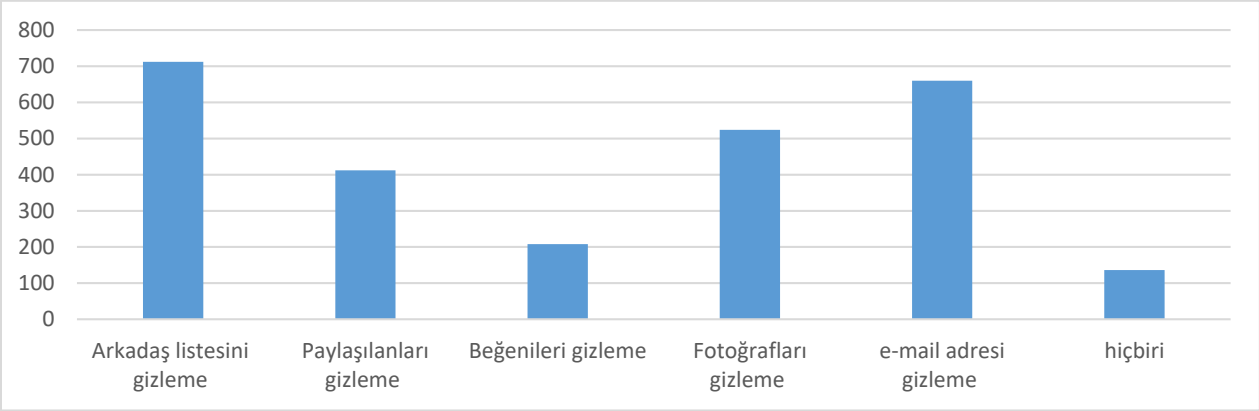
Araştırmaya katılan öğretmenlerin bir sitenin güvenli olduğunu nasıl anladıkları sorusuna verilen cevaplar Tablo 15'de görüldüğü üzere, öğretmenlerin %41,8'i bir web sitesinin güvenli olup olmadığını ayırt etmekte zorlandığını belirtirken, % 38,7'si sitenin https etiketine bakılabileceğini, %9,6'sı bir sitenin güvenli olabilmesi için güvenlidir logosunun yeterli olabileceğini, % 7,5'i site popüler görünüyorsa güvenli olabileceğini ve % 1,9'u ücretsiz yazılım sunan bir web sitesi ise güvenli olabileceğini belirtmektedir.




Şekil 9. Kişisel Haklara Saldırı Sorusu İle İlgili Betimsel İstatistikler

Katılımcılara, sosyal medyalarda veya web sitelerinde kişisel haklarına yönelik bir saldırıyla karşılaştıklarında nereye başvurabilecekleri sorulmuş ve birden fazla seçeneği işaretleyebilecekleri belirtilmiştir.1355 öğretmenin katıldığı ankette, Şekil 9'da belirtildiği gibi bu soruya en çok savcılık ve bilişim suçları birimine başvurulması gerektiği yönünde

yanıt verilmiştir. Ardından sırası ile Telekomünikasyon İletişim Başkanlığı, İnternet Bilgi İhbar Merkezine, web sitenin yöneticisine başvurulması gerektiğini, En yakın polis merkezine, Siber güvenlik şube ofisine ve Aile ya da arkadaşlara başvurulabileceğini belirtilmişlerdir. Katılımcıların 5'te 1'i ise nereye rapor edileceğini bilmediklerini belirtmişlerdir.




Şekil 10. Sosyal Medyada Kullanılan Gizlilik Ayarları

Araştırmaya katılan öğretmenlerin %94,1'inin bir sosyal ağ üyeliği bulunmaktadır. Bu sosyal ağlara kullanılan gizlilik ayarları Şekil 10'da inceleneceği üzere, en çok kullanılan gizlilik ayarından en azına doğru arkadaş listesini gizleme, e-eposta adresini gizleme, fotoğrafları gizleme, paylaşılanları gizleme ve beğenileri gizleme olarak belirtilmiştir. Hiçbir gizlilik ayarını kullanmayan bir kesimde mevcuttur.

**İkinci Alt Probleme İlişkin Bulgular**

Bu araştırmada öğretmenlerin bilgi güvenliği farkındalık düzeylerini belirlemek planlanmıştır. Farklı branşlardaki öğretmenlerin (Türkçe, Matematik, Fen ve Teknoloji, Sosyal Bilgiler, Bilişim teknolojileri ve Sınıf öğretmenliği) Bilgi güvenliği farkındalık düzeyleri uygulanan ölçek ile belirlenmiştir. Bilgi Güvenliği Farkındalık anketi 5'li likert tipinde olup 28 madde içermektedir. Öğretmenlerin bilgi güvenliği farkındalığını belirlemek için, betimleyici istatistikten yararlanarak, veri toplama aracına verilen cevapların ortalama değerleri hesaplanmıştır. Tablo 34'te belirtildiği üzere bulguların yorumlanması ise, ortalama değerleri 5-4.21 arasında olanları bilgi güvenliği farkındalığı konusunda Tam Yeterli, ortalama değeri 4.20- 3.41 arasında olanları bilgi güvenliği farkındalığı konusunda Yeterli, 3.40-2.61 arasında olanları Orta Düzeyde Yeterli, 2,60- 1.81 arasında olanları Az Yeterli ve 1.80- 1.00 arasında değer alanlar da Hiç Yeterli Değil şeklinde değerlendirilmiştir. Bulgular ayrı tablolar halinde sunulmuştur.

Tablo 16

*Bilgi Güvenliği Farkındalığı Düzey Puanların Yorumlanması Amacıyla Kullanılan Puan Ortalama Aralıkları*

| **Puan Aralığı** | **Farkındalık Düzeyi** |
|---|---|
| 4.21 – 5.00 | Tam Yeterli |
| 3.41 – 4.20 | Yeterli |
| 2.61 – 3.40 | Orta Düzeyde Yeterli |
| 1.81 – 2.60 | Az Yeterli |
| 1.00 – 1.80 | Hiç Yeterli Değil |

Öğretmenlerin bilgi güvenliği farkındalık düzeylerinin yer aldığı Tablo 16'da görüldüğü üzere, öğretmenlerin ölçeğin bütününden aldıkları toplam puanın aritmetik ortalaması 3,04'tür. Anketin bütünü için belirlenen puan aralıkları dikkate alındığında bu puan, Orta Düzeyde Yeterli düzeyine karşılık gelmektedir.

Tablo 17

*Bilgi Güvenliği Farkındalığı Anketinin İstatistiksel Bulguları*

| N | Minimum | Maximum | Ortalama | SS |
|---|---|---|---|---|
| 1355 | 1,89 | 4,18 | 3,0493 | ,35204 |
| | 53,00 | 117,00 | 85,3801 | 9,857 |

Tablo 17'de anket için alınan toplam puanlara bakıldığında ise, katılımcıların aldıkları puanların en yükseği 117 olurken en düşüğü 53'tür ve ortama puan 85,3 olduğu görülmektedir.

Öğretmenlerin bilgi güvenliği farkındalıklarının ölçüldüğü ve Kişisel bilgi gizliliği, Davranış, Koruma bilinci, Önlem alma ve Mağduriyet olarak belirlenen alt boyutlara verilen cevaplara ilişkin frekans ve yüzdelik değerler, ortalama ve standart sapma aşağıda tablolar halinde verilmiştir.

**Mağduriyet alt boyutunun frekans ve yüzdelik değerleri**

Tablo 18

*"Kişisel Bilgilerimi İnternette Kullandığım İçin Sıkıntı Yaşadım." Maddesine İlişkin Frekans Ve Yüzde Değerleri*

| | f | % |
|---|---|---|
| hiçbir zaman | 950 | 1,9 |
| Bazen | 180 | 9,6 |
| nadiren | 155 | 38,7 |
| sık sık | 45 | 7,5 |
| her zaman | 25 | 41,8 |
| Toplam | 1355 | 100 |

Mağduriyet alt boyutuna göre, Tablo 18'da görüldüğü üzere araştırmaya katılan öğretmenlerin "Kişisel bilgilerimi internette kullandığım için sıkıntı yaşadım." maddesine %1,9'u (N= 950) hiçbir zaman, %9,6'sı (N=180) bazen, %38,7'si (N=155) nadiren, %7,5'i (N=45) sık sık ve %41,8'i (N=25) her zaman cevabını vermişlerdir.

Tablo 19

*"Sosyal Ağlarda Yaptığım Bilgi Paylaşımı Hayatıma Zarar Verdi." Maddesine İlişkin Frekans Ve Yüzde Değerleri*

| | f | % |
|---|---|---|
| hiçbir zaman | 990 | 73,1 |
| Bazen | 185 | 13,7 |
| nadiren | 120 | 8,9 |
| sık sık | 40 | 3,0 |
| her zaman | 20 | 1,5 |
| Toplam | 1355 | 100,0 |

Tablo 19'dan anlaşıldığı gibi araştırmaya katılan öğretmenlerin "Sosyal ağlarda yaptığım bilgi paylaşımı hayatıma zarar verdi" maddesine %73,1'i (N= 990) hiçbir zaman, %13,7'si

(N=185) bazen, %8,9'u (N=120) nadiren, %3'ü (N=40) sık sık ve %1,5'i (N=20) her zaman cevabını vermişlerdir.

Tablo 20

*"Kredi Kartı Bilgilerim Kopyalandı" Maddesine İlişkin Frekans Ve Yüzde Değerleri*

| | **f** | **%** |
|---|---|---|
| hiçbir zaman | 1095 | 80,8 |
| Bazen | 95 | 7,0 |
| nadiren | 90 | 6,6 |
| sık sık | 35 | 2,6 |
| her zaman | 40 | 3,0 |
| Toplam | 1355 | 100,0 |

Mağduriyet alt boyutuna göre, Tablo 20'de görüldüğü üzere araştırmaya katılan öğretmenlerin "Kredi kartı bilgilerim kopyalandı" maddesine ilişkin verdikleri cevaplar, %80,8'i (N= 1095) hiçbir zaman, %7'si (N=95) bazen, %6,6'sı (N=90) nadiren, %2,6'sı (N=35) sık sık ve %3'ü (N=40) her zaman şeklindedir.

Tablo 21

*"İnternette Kullandığım Hesaplarda Şifrem Ele Geçirildi." Maddesine İlişkin Frekans Ve Yüzde Değerleri*

| | **f** | **%** |
|---|---|---|
| hiçbir zaman | 990 | 73,1 |
| Bazen | 145 | 10,7 |
| nadiren | 105 | 7,7 |
| sık sık | 35 | 2,6 |
| her zaman | 80 | 5,9 |
| Toplam | 1355 | 100,0 |

Tablo 21'den anlaşıldığı gibi araştırmaya katılan öğretmenlerin "İnternette kullandığım hesaplarda şifrem ele geçirildi" maddesine %73,1'i (N= 990) hiçbir zaman, %10,7'si

(N=145) bazen, %7,7'si (N=105) nadiren, %2,6'sı (N=35) sık sık ve %5,9'u (N=80) her zaman cevabını vermişlerdir.

Tablo 22

*"Bilgisayarımdaki Bazı Dosyalarım Çalındı/Silindi." Maddesine İlişkin Frekans Ve Yüzde Değerleri*

| | **f** | **%** |
|---|---|---|
| hiçbir zaman | 975 | 72,0 |
| Bazen | 165 | 12,2 |
| nadiren | 105 | 7,7 |
| sık sık | 70 | 5,2 |
| her zaman | 40 | 3,0 |
| Toplam | 1355 | 100,0 |

Katılımcı öğretmenlerin "Bilgisayarımdaki bazı dosyalarım çalındı/silindi." Maddesine verdikleri cevaplar, Tablo 22'de görüldüğü üzere %27'si (N=975) hiçbir zaman, %12,2'si (N=165) bazen, %7,7'si (N=105) nadiren, %5,2'sı (N=70) sık sık ve %3'ü (N=40) her zaman şeklindedir.

Tablo 23

*"İnternette Gezerken İsteğim Dışında Şiddet Ya Da Pornografik İçerikli Yayınlarla Karşılaştım." Maddesine İlişkin Frekans Ve Yüzde Değerleri*

| | **f** | **%** |
|---|---|---|
| hiçbir zaman | 285 | 21,0 |
| Bazen | 300 | 22,1 |
| nadiren | 410 | 30,3 |
| sık sık | 230 | 17,0 |
| her zaman | 130 | 9,6 |
| Toplam | 1355 | 100,0 |

Mağduriyet alt boyutunda katılımcılara "İnternette gezerken isteğim dışında şiddet ya da pornografik içerikli yayınlarla karşılaştım." maddesi yöneltilmiştir ve Tablo 23'de görüldüğü üzere cevaplardan %21'i (N= 285) hiçbir zaman, %22,1'i (N=300) bazen,

%30,3'ü (N=410) nadiren, %17'si (N=230) sık sık ve %9,6'sı (N=130) her zaman şeklindedir.

Tablo 24

*"Vatandaşlık Numaramın (T.C.) Başka Şahıslar Tarafından Bilinmesi Beni Rahatsız Etmez." Maddesine İlişkin Frekans Ve Yüzde Değerleri*

| | **f** | **%** |
|---|---|---|
| hiçbir zaman | 160 | 11,8 |
| Bazen | 65 | 4,8 |
| nadiren | 160 | 11,8 |
| sık sık | 115 | 8,5 |
| her zaman | 855 | 63,1 |
| Toplam | 1355 | 100,0 |

Katılımcı öğretmenlerin "Vatandaşlık numaramın (T.C.) başka şahıslar tarafından bilinmesi beni rahatsız etmez." maddesine verdikleri cevaplar, Tablo 24'da görüldüğü üzere %11,8'i (N=160) hiçbir zaman, %4,8'i (N=65) bazen, %11,8'i (N=160) nadiren, %8,5'i (N=115) sık sık ve %63,1'i (N=855) her zaman şeklinde olmuştur.

Tablo 25

*"İnternetin Herkese Açık Olduğu Yerlerde İnternet Bankacılığı Kullanırım." Maddesine İlişkin Frekans Ve Yüzde Değerleri*

| | **f** | **%** |
|---|---|---|
| hiçbir zaman | 65 | 4,8 |
| bazen | 90 | 6,6 |
| nadiren | 165 | 12,2 |
| sık sık | 235 | 17,3 |
| her zaman | 800 | 59,0 |
| Toplam | 1355 | 100,0 |

Öğretmenlere sunulan ölçek maddelerinden biri de "İnternetin herkese açık olduğu yerlerde internet bankacılığı kullanırım." maddesidir ve alınan cevaplar Tablo 25'de belirtilmiştir.

Şöyle ki; cevapların %4,8'i (N= 65) hiçbir zaman olurken, %6,6'sı (N=90) bazen, %12,2'si (N=165) nadiren, %17,3'ü (N=235) sık sık ve %59'u (N=800) her zaman olarak belirtilmiştir.Öğretmenlerin Bilgi güvenliği farkındalık düzeylerini belirleyen Mağduriyet alt boyutunun ortalamaları ve standart sapmaları maddelerine göre Tablo 26'da verilmiştir.

Tablo 26

*Mağduriyet Alt Boyutuna İlişkin Verilerin Aritmetik Ortalama ve Standart Sapma Puanları* (n=1355)

| **Madde** | **X** | **ss** |
|---|---|---|
| Kişisel bilgilerimi internette kullandığım için sıkıntı yaşadım. | 1,53 | ,948 |
| Sosyal ağlarda yaptığım bilgi paylaşımı hayatıma zarar verdi. | 1,46 | ,883 |
| Kredi kartı bilgilerim kopyalandı. | 1,39 | ,939 |
| İnternette kullandığım hesaplarda şifrem ele geçirildi. | 1,57 | 1,124 |
| Bilgisayarımdaki bazı dosyalarım çalındı/silindi. | 1,54 | 1,033 |
| İnternette gezerken isteğim dışında şiddet ya da içerikli yayınlarla karşılaştım. | 2,71 | 1,240 |
| Vatandaşlık numaramın (T.C) başka şahıslar tarafından bilinmesi beni rahatsız etmez. | 4,06 | 1,414 |
| İnternetin herkese açık olduğu yerlerde internet bankacılığı kullanırım. | 4,19 | 1,172 |

Tablo 26 incelendiğinde Öğretmenlerin maruz kaldığı olayları incelemek için oluşturulan Mağduriyet Boyutuna ait aritmetik ortalamaların 4,19 ile 1,39 arasında değiştiği görülmektedir. En düşük ortalama 1,39 ile "Kredi kartı bilgilerim kopyalandı." maddesine aitken en yüksek ortalama 4,19 ile "İnternetin herkese açık olduğu yerlerde internet bankacılığı kullanırım" maddesine aittir.

**Davranış Alt Boyutunun Frekans Ve Yüzdelik Değerleri**

Tablo 27

*"Bütün Hesaplarımda Aynı Parolayı Kullanırım." Maddesine İlişkin Frekans Ve Yüzde Değerleri*

| | f | % |
|---|---|---|
| hiçbir zaman | 145 | 10,7 |
| bazen | 190 | 14,0 |
| nadiren | 370 | 27,3 |
| sık sık | 345 | 25,5 |
| her zaman | 305 | 22,5 |
| Toplam | 1355 | 100,0 |

Katılımcı öğretmenlerin "Bütün hesaplarımda aynı parolayı kullanırım." maddesine verdikleri cevaplar, Tablo 27'de görüldüğü üzere %10,7'si (N=145) hiçbir zaman, %14'ü (N=190) bazen, %27,3'ü (N=370) nadiren, %25,5'i (N=345) sık sık ve %22,5'i (N=305) her zaman şeklinde olmuştur.

Tablo 28

*"Kargo,Gsm Operatörü Gibi Kuruluşlarla Nüfus Cüzdanı Bilgilerimi Paylaşırım." Maddesine İlişkin Frekans Ve Yüzde Değerleri*

| | f | % |
|---|---|---|
| hiçbir zaman | 135 | 10,0 |
| bazen | 205 | 15,1 |
| nadiren | 250 | 18,5 |
| sık sık | 225 | 16,6 |
| her zaman | 540 | 39,9 |
| Toplam | 1355 | 100,0 |

Tablo 28'den anlaşıldığı gibi araştırmaya katılan öğretmenlerin "Kargo,Gsm operatörü gibi kuruluşlarla nüfus cüzdanı bilgilerimi paylaşırım" maddesine %10'u (N= 135) hiçbir zaman, %15,1'i (N=205) bazen, %18,5'i (N=250) nadiren, %16,6'sı (N=225) sık sık ve %39,9'u (N=540) her zaman cevabını vermişlerdir.

Tablo 29

*"Parolalarımı Başkalarıyla Paylaşırım." Maddesine İlişkin Frekans Ve Yüzde Değerleri*

| | **f** | **%** |
|---|---|---|
| hiçbir zaman | 35 | 2,6 |
| bazen | 35 | 2,6 |
| nadiren | 85 | 6,3 |
| sık sık | 215 | 15,9 |
| her zaman | 985 | 72,7 |
| Toplam | 1355 | 100,0 |

Davranış alt boyutuna göre, Tablo 29'da görüldüğü üzere araştırmaya katılan öğretmenlerin "Parolalarımı başkalarıyla paylaşırım" maddesine ilişkin verdikleri cevaplar, %2,6'sı (N= 35) hiçbir zaman olurken, %2,6'sı (N=35) bazen, %6,3'ü (N=85) nadiren, %15,9'u (N=215) sık sık ve %72,7'si (N=985) her zaman şeklindedir.

Tablo 30

*"İnternet Bankacılığı Vs. Şifresini Yazarken Klavye Kullanırım." Maddesine İlişkin Frekans Ve Yüzde Değerleri*

| | **f** | **%** |
|---|---|---|
| hiçbir zaman | 365 | 26,9 |
| bazen | 335 | 24,7 |
| nadiren | 310 | 22,9 |
| sık sık | 165 | 12,2 |
| her zaman | 180 | 13,3 |
| Toplam | 1355 | 100,0 |

Tablo 30'dan anlaşıldığı gibi araştırmaya katılan öğretmenlerin "İnternet bankacılığı vs. şifresini yazarken klavye kullanırım" maddesine ilişkin verdikleri cevaplar, %26,9'u (N= 365) hiçbir zaman, %24,7'sı (N=335) bazen, %22,9'u (N=310) nadiren, %12,2'si (N=165) sık sık ve %13,3'ü (N=180) her zaman şeklindedir.

Tablo 31

*Davranış Alt Boyutuna İlişkin Verilerin Aritmetik Ortalama ve Standart Sapma Puanları* (n=1355)

| Madde | X | ss |
|---|---|---|
| Bütün hesaplarımda aynı parolayı kullanırım. | 3,35 | 1,26 |
| Kargo,Gsm operatörü gibi kuruluşlarla nüfus cüzdanı bilgilerimi paylaşırım. | 3,61 | 1,39 |
| Parolalarımı başkalarıyla paylaşırım. | 4,53 | 0,91 |
| İnternet bankacılığı vs. şifresini yazarken klavye kullanırım. | 2,60 | 1,34 |

Öğretmenlerin davranışlarını incelemek için oluşturulan Davranış Alt Boyutuna ait aritmetik ortalamaların 4,53 ile 2,60 arasında değiştiği görülmektedir. En düşük ortalama 2,60 ile "İnternet bankacılığı vs. şifresini yazarken klavye kullanırım." maddesine aitken en yüksek ortalama 4,53 ile "Parolalarımı başkalarıyla paylaşırım" maddesine aittir.

**Kişisel Bilgi Gizliliği Alt Boyutunun Frekans ve Yüzdelik Değerleri**

Tablo 32

*"Kişisel Bilgilerimin Başkaları Tarafından Kötü Amaçla Kullanılabileceğini Düşünürüm." Maddesine İlişkin Frekans Ve Yüzde Değerleri*

| | **f** | **%** |
|---|---|---|
| hiçbir zaman | 90 | 6,6 |
| bazen | 95 | 7,0 |
| nadiren | 300 | 22,1 |
| sık sık | 305 | 22,5 |
| her zaman | 565 | 41,7 |
| Toplam | 1355 | 100,0 |

Öğretmenlerin kişisel bilgi gizliliği farkındalığını belirlemek için oluşturulan alt boyutunun "İnternet bankacılığı vs. şifresini yazarken klavye kullanırım" maddesine ilişkin verdikleri cevaplar, Tablo 32'de görüldüğü üzere %6,6'sı (N= 90) hiçbir zaman, %7'si (N=95) bazen, %22,1'i (N=300) nadiren, %22,5'i (N=305) sık sık ve %41,7'si (N=565) her zaman şeklinde olmuştur.

Tablo 33

*"Kişisel Bilgisayarımda Otomatik Kullan Özelliğini Kullanırım." Maddesine İlişkin Frekans Ve Yüzde Değerleri*

| | f | % |
|---|---|---|
| hiçbir zaman | 175 | 12,9 |
| bazen | 200 | 14,8 |
| nadiren | 320 | 23,6 |
| sık sık | 250 | 18,5 |
| her zaman | 410 | 30,3 |
| Toplam | 1355 | 100,0 |

Tablo 33'den anlaşılacağı üzere araştırmaya katılan öğretmenlerin "Kişisel bilgisayarımda otomatik kullan özelliğini kullanırım" maddesine verdikleri cevaplar, %12,9'u (N=175) hiçbir zaman, %14,8'i (N=200) bazen, %23,6'i (N=320) nadiren, %18,5'i (N=250) sık sık ve %30,3'ü (N=410) her zaman şeklinde olmuştur.

Tablo 34

*"Parolalarımı Yazılı Olarak Ulaşabileceğim Bir Yerde Saklarım." Maddesine İlişkin Frekans Ve Yüzde Değerleri*

| | f | % |
|---|---|---|
| hiçbir zaman | 155 | 11,4 |
| bazen | 195 | 14,4 |
| nadiren | 210 | 15,5 |
| sık sık | 145 | 10,7 |
| her zaman | 650 | 48,0 |
| Toplam | 1355 | 100,0 |

Katılımcı öğretmenlerin "Parolalarımı yazılı olarak ulaşabileceğim bir yerde saklarım." maddesine verdikleri cevaplar, Tablo 34'den anlaşılacağı üzere %11,4'ü (N=155) hiçbir zaman, %14,4'ü (N=195) bazen, %15,5'i (N=210) nadiren, %10,7'si (N=145) sık sık ve %48'i (N=650) her zaman şeklinde olmuştur.

Tablo 35

*Kişisel Bilgi Gizliliği Alt Boyutuna İlişkin Verilerin Aritmetik Ortalama ve Standart Sapma Puanları (n=1355)*

| **Madde** | **X** | **ss** |
|---|---|---|
| Kişisel bilgilerimin başkaları tarafından kötü amaçla kullanılabileceğini düşünürüm. | 3,85 | 1,223 |
| Kişisel bilgisayarımda otomatik kullan özelliğini kullanırım. | 3,38 | 1,383 |
| Parolalarımı yazılı olarak ulaşabileceğim bir yerde saklarım. | 3,69 | 1,465 |

Öğretmenlerin kişisel bilgi gizliliği farkındalığını incelemek için oluşturulan Kişisel bilgi gizliliği alt boyutuna ait aritmetik ortalamaların 3,85 ile 3,38 arasında değiştiği görülmektedir. En düşük ortalama 3,38 ile "Kişisel bilgisayarımda otomatik kullan özelliğini kullanırım." maddesine aitken en yüksek ortalama 3,85 ile "Kişisel bilgilerimin başkaları tarafından kötü amaçla kullanılabileceğini düşünürüm." maddesine aittir.

**Önlem Alma Alt Boyutunun Frekans Ve Yüzdelik Değerleri**

Tablo 36

*"İnternet Üzerindeki Hesaplarımda Kolay Tahmin Edilemeyecek Şekilde Karmaşık Ve Uzun Şifreler Kullanırım." Maddesine İlişkin Frekans Ve Yüzde Değerleri*

| | **f** | **%** |
|---|---|---|
| hiçbir zaman | 85 | 6,3 |
| bazen | 105 | 7,7 |
| nadiren | 325 | 24,0 |
| sık sık | 360 | 26,6 |
| her zaman | 480 | 35,4 |
| Toplam | 1355 | 100,0 |

Tablo 36'dan anlaşıldığı gibi araştırmaya katılan öğretmenlerin "İnternet üzerindeki hesaplarımda kolay tahmin edilemeyecek şekilde karmaşık ve uzun şifreler kullanırım" maddesine %6,3'ü (N= 85) hiçbir zaman, %7,7'si (N=105) bazen, %24'ü (N=325) nadiren, %26,6'sı (N=360) sık sık ve %35,4'ü (N=480) her zaman cevabını vermişlerdir.

Tablo 37

*"Aynı İletiyi Birden Fazla Kişiye Göndermem Gereken Durumlarda Gizli (BCC) Kısmını Kullanırım." Maddesine İlişkin Frekans Ve Yüzde Değerleri*

| | f | % |
|---|---|---|
| hiçbir zaman | 210 | 15,5 |
| bazen | 175 | 12,9 |
| nadiren | 355 | 26,2 |
| sık sık | 230 | 17,0 |
| her zaman | 385 | 28,4 |
| Toplam | 1355 | 100,0 |

Önlem alma alt boyutuna göre, Tablo 37'de görüldüğü üzere araştırmaya katılan öğretmenlerin "Aynı iletiyi birden fazla kişiye göndermem gereken durumlarda gizli (BCC) kısmını kullanırım." maddesine ilişkin verdikleri cevaplar, %15,5'i (N= 210) hiçbir zaman olurken, %12,9'u (N=175) bazen, %26,2'si (N=355) nadiren, %17'si (N=230) sık sık ve %28,4'ü (N=385) her zaman şeklindedir.

Tablo 38

*"Bilgisayarımda Lisanslı Yazılım (Orijinal) Kullanmaya Dikkat Ederim." Maddesine İlişkin Frekans Ve Yüzde Değerleri*

| | f | % |
|---|---|---|
| hiçbir zaman | 185 | 13,7 |
| bazen | 190 | 14,0 |
| nadiren | 325 | 24,0 |
| sık sık | 290 | 21,4 |
| her zaman | 365 | 26,9 |
| Toplam | 1355 | 100,0 |

Tablo 38'de görüldüğü üzere araştırmaya katılan öğretmenlerin "Bilgisayarımda lisanslı yazılım (orijinal) kullanmaya dikkat ederim." maddesine %13,7'si (N=185) hiçbir zaman, %14'ü (N=190) bazen, %24'ü (N=325) nadiren, %21,4'ü (N=290) sık sık ve %26,9'u (N=365) her zaman cevabını vermişlerdir.

Tablo 39

*"Virüs Temizleme, Casus Yazılım Önleme Vb. Programları Kullanırım." Maddesine İlişkin Frekans Ve Yüzde Değerleri*

| | f | % |
|---|---|---|
| hiçbir zaman | 105 | 7,7 |
| bazen | 150 | 11,1 |
| nadiren | 290 | 21,4 |
| sık sık | 360 | 26,6 |
| her zaman | 450 | 33,2 |
| Toplam | 1355 | 100,0 |

Katılımcı öğretmenlerin "Virüs temizleme, casus yazılım önleme vb. programları kullanırım." maddesine verdikleri cevaplar, Tablo 40'da görüldüğü üzere %7,7'si (N=105) hiçbir zaman, %11,1'i (N=150) bazen, %21,4'ü (N=290) nadiren, %26,6'sı (N=360) sık sık ve %33,2'si (N=450) her zaman şeklinde olmuştur.

Tablo 40

*"Kısa Bir İşim Olsa Dahi Çalışırken Ekran Koruyucu Kullanırım." Maddesine İlişkin Frekans Ve Yüzde Değerleri*

| | f | % |
|---|---|---|
| hiçbir zaman | 535 | 39,5 |
| bazen | 250 | 18,5 |
| nadiren | 265 | 19,6 |
| sık sık | 140 | 10,3 |
| her zaman | 165 | 12,2 |
| Toplam | 1355 | 100,0 |

Tablo 40'da görüldüğü üzere araştırmaya katılan öğretmenlerin "Kısa bir işim olsa dahi çalışırken ekran koruyucu kullanırım." maddesine %39,5'i (N=535) hiçbir zaman, %18,5'i (N=250) bazen, %19,6'sı (N=265) nadiren, %10,3'ü (N=140) sık sık ve %12,2'si (N=165) her zaman cevabını vermişlerdir.

Tablo 41

*"Kullandığım Programların Güncellemesini Düzenli Olarak Yaparım." Maddesine İlişkin Frekans Ve Yüzde Değerleri*

| | **f** | **%** |
|---|---|---|
| hiçbir zaman | 75 | 5,5 |
| bazen | 200 | 14,8 |
| nadiren | 420 | 31,0 |
| sık sık | 350 | 25,8 |
| her zaman | 310 | 22,9 |
| Toplam | 1355 | 100,0 |

Öğretmenlerin önlem alma farkındalığını belirlemek için oluşturulan alt boyutunun "Kullandığım programların güncellemesini düzenli olarak yaparım" maddesine ilişkin verdikleri cevaplar, Tablo 41'de görüldüğü üzere %5,5'i (N= 75) hiçbir zaman, %14,8'i (N=200) bazen, %31'i (N=420) nadiren, %25,8'i (N=350) sık sık ve %22,9'u (N=310) her zaman şeklinde olmuştur.

Tablo 42

*"Güvenlik Duvarı, Reklam Önleyici Vb. Programlar Kullanırım." Maddesine İlişkin Frekans Ve Yüzde Değerleri*

| | **f** | **%** |
|---|---|---|
| hiçbir zaman | 265 | 19,6 |
| bazen | 235 | 17,3 |
| nadiren | 345 | 25,5 |
| sık sık | 215 | 15,9 |
| her zaman | 295 | 21,8 |
| Toplam | 1355 | 100,0 |

Tablo 42'de görüldüğü üzere araştırmaya katılan öğretmenlerin "Güvenlik duvarı, reklam önleyici vb. programlar kullanırım." maddesine %19,6'sı (N=265) hiçbir zaman, %17,3'ü (N=235) bazen, %25,5'i (N=345) nadiren, %15,9'u (N=215) sık sık ve %21,8'i (N=295) her zaman cevabını vermişlerdir.

Tablo 43

*"Bulut Teknolojilerinde (Drive,Dropbox Vs.) Bilgilerimi Güvende Hissediyorum." Maddesine İlişkin Frekans Ve Yüzde Değerleri*

| | f | % |
|---|---|---|
| hiçbir zaman | 350 | 25,8 |
| bazen | 330 | 24,4 |
| nadiren | 400 | 29,5 |
| sık sık | 180 | 13,3 |
| her zaman | 95 | 7,0 |
| Toplam | 1355 | 100,0 |

Araştırmaya katılan öğretmenlerin "Bulut teknolojilerinde (Drive,Dropbox vs.) bilgilerimi güvende hissediyorum " maddesine %25,8'i (N=350) hiçbir zaman olarak cevap verirken, %24,4'ü (N=330) bazen, %29,5'i (N=400) nadiren, %13,3'ü (N=180) sık sık ve %7'si (N=95) her zaman cevabını vermişlerdir.

Tablo 44

*Önlem Alma Alt Boyutuna İlişkin Verilerin Aritmetik Ortalama Ve Standart Sapma Puanları (N=1355)*

| **Madde** | **X** | **SS** |
|---|---|---|
| Bilgisayarımda lisanslı yazılım (orijinal) kullanmaya dikkat ederim. | 3,77 | 1,19 |
| Virüs temizleme, casus yazılım önleme vb. programları kullanırım. | 3,29 | 1,40 |
| Aynı iletiyi birden fazla kişiye göndermem gereken durumlarda gizli (BCC) kısmını kullanırım. | 3,33 | 1,36 |
| İnternet üzerindeki hesaplarımda kolay tahmin edilemeyecek şekilde karmaşık ve uzun şifreler kullanırım. | 3,66 | 1,25 |
| Kullandığım programların güncellemesini düzenli olarak yaparım. | 2,37 | 1,40 |
| Kısa bir işim olsa dahi çalışırken ekran koruyucu kullanırım. | 3,45 | 1,15 |
| Güvenlik duvarı, reklam önleyici vb. programlar kullanırım. | 3,02 | 1,40 |
| Bulut teknolojilerinde (Drive,Dropbox vs.) bilgilerimi güvende hissediyorum. | 2,51 | 1,20 |

Öğretmenlerin Önlem alma farkındalığını incelemek için oluşturulan Önlem Alma alt boyutuna ait aritmetik ortalamaların 3,77 ile 2,37 arasında değiştiği görülmektedir. En düşük ortalama 2,37 ile "Kullandığım programların güncellemesini düzenli olarak yaparım." maddesine aitken en yüksek ortalama 3,77 ile "Bilgisayarımda lisanslı yazılım (orijinal) kullanmaya dikkat ederim." maddesine aittir.

**Koruma Bilinci Alt Boyutunun Frekans Ve Yüzdelik Değerleri**

Tablo 45

*"Önemli Dosyalarımı Şifrelerim." Maddesine İlişkin Frekans Ve Yüzde Değerleri*

| | **f** | **%** |
|---|---|---|
| hiçbir zaman | 295 | 21,8 |
| bazen | 185 | 13,7 |
| nadiren | 305 | 22,5 |
| sık sık | 270 | 19,9 |
| her zaman | 300 | 22,1 |
| Toplam | 1355 | 100,0 |

Öğretmenlerin "Önemli dosyalarımı şifrelerim" maddesine verdikleri cevaplar, %21,8'i (N=295) hiçbir zaman, %13,7'si (N=185) bazen, %22,5'i (N=305) nadiren, %19,9'u (N=270) sık sık ve %22,1'i (N=300) her zaman olarak belirlenmiştir.

Tablo 46

*"Çocukları İstenmeyen İçeriklerden Koruyacak Filtre Programları Kullanırım." Maddesine İlişkin Frekans Ve Yüzde Değerleri*

| | **f** | **%** |
|---|---|---|
| hiçbir zaman | 300 | 22,1 |
| bazen | 225 | 16,6 |
| nadiren | 345 | 25,5 |
| sık sık | 230 | 17,0 |
| her zaman | 255 | 18,8 |
| Toplam | 1355 | 100,0 |

Araştırmaya katılan öğretmenlerin "Çocukları istenmeyen içeriklerden koruyacak filtre programları kullanırım" maddesine verdikleri cevaplar, %22,1'i (N=300) hiçbir zaman, %16,6'sı (N=225) bazen, %25,5'i (N=345) nadiren, %17'si (N=230) sık sık ve %18,8'i (N=255) her zaman olarak belirlenmiştir.

Tablo 47

*"Parolalarımı Sık Sık Değiştiririm." Maddesine İlişkin Frekans Ve Yüzde Değerleri*

| | **f** | **%** |
|---|---|---|
| hiçbir zaman | 245 | 18,1 |
| bazen | 250 | 18,5 |
| nadiren | 425 | 31,4 |
| sık sık | 210 | 15,5 |
| her zaman | 225 | 16,6 |
| Toplam | 1355 | 100,0 |

Tablo 47'de görüldüğü üzere araştırmaya katılan öğretmenlerin "Parolalarımı sık sık değiştiririm" maddesine %18,1'i (N=245) hiçbir zaman, %18,5'i (N=250) bazen, %31,4'ü (N=425) nadiren, %15,5'i (N=210) sık sık ve %16,6'sı (N=225) her zaman cevabını vermişlerdir.

Tablo 48

*"Akıllı Telefonum Ve Bilgisayarım Bir Şifre İle Korunur." Maddesine İlişkin Frekans Ve Yüzde Değerleri*

| | **f** | **%** |
|---|---|---|
| hiçbir zaman | 255 | 18,8 |
| bazen | 85 | 6,3 |
| nadiren | 185 | 13,7 |
| sık sık | 195 | 14,4 |
| her zaman | 635 | 46,9 |
| Toplam | 1355 | 100,0 |

Öğretmenlerin koruma bilinci farkındalığını belirlemek amacıyla oluşturulan Koruma Bilinci Alt boyutunun "Akıllı telefonum ve bilgisayarım bir şifre ile korunur" maddesine ilişkin verdikleri cevaplar, Tablo 48'de görüldüğü üzere %18,8'i (N= 255) hiçbir zaman, %6,3'ü (N=85) bazen, %13,7'si (N=185) nadiren, %14,4'ü (N=195) sık sık ve %46,9'u (N=635) her zaman şeklinde olmuştur.

Tablo 49

*"Herkesin Kullanımına Açık Bir Bilgisayardan Ayrılmadan Önce Geçici İnternet Dosyalarını Ve Gezinme Geçmişini Silerim." Maddesine İlişkin Frekans Ve Yüzde Değerleri*

| | **f** | **%** |
|---|---|---|
| hiçbir zaman | 140 | 10,3 |
| bazen | 95 | 7,0 |
| nadiren | 255 | 18,8 |
| sık sık | 250 | 18,5 |
| her zaman | 615 | 45,4 |
| Toplam | 1355 | 100,0 |

Tablo 49'dan anlaşılacağı üzere araştırmaya katılan öğretmenlerin "Herkesin kullanımına açık bir bilgisayardan ayrılmadan önce geçici internet dosyalarını ve gezinme geçmişini silerim" maddesine %10,3'ü (N=140) hiçbir zaman, %7'si (N=95) bazen, %18,8'i (N=255) nadiren, %18,5'i (N=250) sık sık ve %45,4'ü (N=615) her zaman cevabını vermişlerdir.

Tablo 50

*Koruma Bilinci Alt Boyutuna İlişkin Verilerin Aritmetik Ortalama ve Standart Sapma Puanları (n=1355)*

| **Madde** | **X** | **SS** |
|---|---|---|
| Önemli dosyalarımı şifrelerim. | 3,07 | 1,44 |
| Çocukları istenmeyen içeriklerden koruyacak filtre programları kullanırım. | 2,93 | 1,40 |
| Parolalarımı sık sık değiştiririm | 2,94 | 1,31 |
| Akıllı telefonum ve bilgisayarım bir şifre ile korunur | 3,64 | 1,55 |
| Herkesin kullanımına açık bir bilgisayardan ayrılmadan önce geçici internet dosyalarını ve gezinme geçmişini silerim. | 3,81 | 1,34 |

Öğretmenlerin Koruma bilinci farkındalığını incelemek amacıyla düzenlenen Koruma Bilinci Alt boyutuna ait aritmetik ortalamaların 3,81 ile 2,93 arasında değiştiği görülmektedir. En düşük ortalama 2,93 ile "Çocukları istenmeyen içeriklerden koruyacak filtre programları kullanırım." maddesine aitken en yüksek ortalama 3,81 ile "Herkesin kullanımına açık bir bilgisayardan ayrılmadan önce geçici internet dosyalarını ve gezinme geçmişini silerim." maddesine aittir.

**Üçüncü Alt Probleme İlişkin Bulgular**

Araştırmanın üçüncü alt amacında, öğretmenlerin bilgi güvenliği farkındalığı anketi maddelerine ilişkin verdikleri cevaplar değerlendirilerek, faktörler bazında yaş, cinsiyet, eğitim durumu, bulundukları bölge, internet kullanma süreleri ve görev süreleri açısından istatistiksel olarak herhangi bir anlamlı farklılık olup olmadığı araştırılmıştır.

**Öğretmenlerin Cinsiyet Değişkeni Açısından Bilgi Güvenliği Farkındalığı Düzeyleri**

Araştırmaya katılan öğretmenlerin cinsiyet değişkeni açısından Bilgi Güvenliği Farkındalık düzeylerini belirlemek amacıyla Mann Whitney U-testi uygulanmıştır. Tablo 51'de öğretmenlerin bilgi güvenliği farkındalık düzeyleriyle cinsiyetleri arasında anlamlı bir farklılık olmadığı görülmektedir.

Tablo 51

*Bilgi Güvenliği Farkındalığının Cinsiyete Göre U-Testi Sonuçları*

| Cinsiyet | N | Sıra Ortalaması | Sıra Toplamı | U | p |
|---|---|---|---|---|---|
| Kadın | 840 | 678,98 | 570345,00 | 215475,000 | ,906 |
| Erkek | 515 | 676,40 | 348345,00 | | |
| Toplam | 1355 | | | | |

Tablo 51 incelendiğinde araştırmaya katılan öğretmenlerin bilgi güvenliği farkındalık düzeylerinin cinsiyetlerine göre anlamlı bir farklılık göstermediği [U: 215475,0, p<.05] yapılan Mann Whitney U-testi sonucuna görülmektedir. Sıra ortalamaları dikkate alındığında, ankete katılan kadınlar ve erkeklerin bilgi güvenliği farkındalıkları arasında çok az bir fark olduğu görülmektedir.

**Öğretmenlerin Yaş Değişkeni Açısından Bilgi Güvenliği Farkındalığı Düzeyleri**

Öğretmenlerin Bilgi güvenliği farkındalık düzeylerinin yaş değişkenine göre farklılaşmasını belirlemek amacıyla Kruskall Wallis testi uygulanmıştır.

Tablo 52

*Bilgi Güvenliği Farkındalığının Yaş Değişkenine Göre Kruskal Wallis Testi Sonuçları*

| Yaş | N | Sıra Ortalaması | sd | $X^2$ | *p* |
|---|---|---|---|---|---|
| 21-30 | 945 | 709,42 | 3 | 29,5 | .000 |
| 31-40 | 315 | 596,81 | | | |
| 41-50 | 85 | 594,03 | | | |
| 51-60 | 10 | 980,50 | | | |
| Toplam | 1355 | | | | |

Tablo 52'den anlaşılacağı üzere öğretmenlerin bilgi güvenliği farkındalık düzeyleriyle yaşları arasında anlamlı bir şekilde farklılaştığı görülmektedir [$X^2$(sd=3, n=1355)=29,5, $p$<.05]. Bu sonuç, yaş değişkeninin öğretmenlerin bilgi güvenliği farkındalıkları üzerinde önemli etkilere sahip olduğunu göstermektedir. Yaş gruplarının sıra ortalamaları dikkate

alındığında, farkındalık düzeyleri en yüksek olan 51-60 yaş aralığı iken en düşük olan 41-50 yaş aralığıdır.

**Öğretmenlerin Öğrenim Durumu Değişkeni Açısından Bilgi Güvenliği Farkındalığı Düzeyleri**

Öğretmenlerin Bilgi güvenliği farkındalık düzeylerinin öğrenim durumu değişkenine göre farklılaşmasını belirlemek amacıyla Kruskall Wallis testi uygulanmıştır.

Tablo 53

*Bilgi Güvenliği Farkındalığının Öğrenim Durumu Değişkenine Göre Kruskal Wallis Testi Sonuçları*

| **Eğitim Düzeyiniz** | **N** | **Sıra Ortalaması** | **sd** | $X^2$ | ***p*** |
|---|---|---|---|---|---|
| Ön Lisans | 30 | 779,25 | 3 | 10,0 | ,018 |
| Lisans | 805 | 693,21 | | | |
| Yüksek Lisans | 395 | 667,56 | | | |
| Doktora | 125 | 588,70 | | | |
| Toplam | 1355 | | | | |

Tablo 53'den verilen sonuçlar, bilgi güvenliği farkındalık düzeyleri bakımından öğretmenlerin öğrenim durumları arasında anlamlı bir farklılık oluşturduğu şeklinde yorumlanabilir. Katılımcıların yaş gruplarına göre karşılaştırılması, anketten aldıkları toplam puanlar aracılığıyla yapılmıştır [$X^2$(sd=3, n=1355)= 10, $p$<.05]. Sıra ortalamaları dikkate alındığında ön lisans mezunlarının sıra ortalaması [779,25] en yüksek çıkmaktadır. Bu sonuca göre Ön lisans mezunu öğretmenlerin bilgi güvenliği farkındalık düzeyleri diğer öğrenim durumlarına göre istatistiksel olarak anlamlı düzeyde daha yüksek olduğu söylenebilmektedir.

**Öğretmenlerin Bulundukları Bölge Değişkeni Açısından Bilgi Güvenliği Farkındalığı Düzeyleri**

Öğretmenlerin Bilgi güvenliği farkındalık düzeylerinin bulundukları bölge değişkenine göre farklılaşma durumunu belirlemek amacıyla Kruskall Wallis testi uygulanmıştır.

Tablo 54

*Bilgi Güvenliği Farkındalığının Bulunulan Bölge Değişkenine Göre Kruskal Wallis Testi* Sonuçları

| **Yaşanılan Şehir** | **N** | **Sıra Ortalaması** | **sd** | $X^2$ | ***p*** |
|---|---|---|---|---|---|
| Kuzeydoğu Anadolu | 102 | 660,65 | 11 | 27,3 | ,004 |
| Ortadoğu Anadolu | 111 | 715,91 | | | |
| Güneydoğu Anadolu | 155 | 710,00 | | | |
| İstanbul | 105 | 741,21 | | | |
| Batı Marmara | 81 | 609,91 | | | |
| Ege | 119 | 621,51 | | | |
| Doğu Marmara | 84 | 737,20 | | | |
| Batı Anadolu | 122 | 644,19 | | | |
| Akdeniz | 145 | 723,78 | | | |
| Orta Anadolu | 112 | 725,43 | | | |
| Batı Karadeniz | 91 | 678,47 | | | |
| Doğukaradeniz | 128 | 563,64 | | | |
| Toplam | 1355 | | | | |

Tablo 54'de verilen sonuçlara göre, öğretmenlerin bulundukları bölge ile bilgi güvenliği farkındalık düzeyleri arasında anlamlı bir farklılık oluşturduğu görülmektedir [$X^2$(sd=11, n=1355)= 27,3, $p$<.05]. Sıra ortalamaları dikkate alındığında İstanbul bölgesinde bulunan öğretmenlerin sıra ortalaması [741,21] en yüksek çıktığı görülmektedir. Sıra ortalamaları sırası ile Doğu Marmara, Orta Anadolu, Akdeniz, Ortadoğu Anadolu, Güneydoğu Anadolu, Batı Anadolu, Batı Karadeniz,Kuzeydoğu Anadolu, Ege, Batı Marmara, Doğu Karadeniz olarak sıralanmaktadır.

## Öğretmenlerin Görev Süresi Değişkeni Açısından Bilgi Güvenliği Farkındalığı Düzeyleri

Öğretmenlerin Bilgi güvenliği farkındalık düzeylerinin görev süresi değişkenine göre farklılaşma durumunu incelemek için Kruskall Wallis testi uygulanmıştır.

Tablo 55

*Bilgi Güvenliği Farkındalığının Görev Süresi Değişkenine Göre Kruskal Wallis Testi Sonuçları*

| **Görev Süresi** | **N** | **Sıra Ortalaması** | **sd** | $X^2$ | ***p*** |
|---|---|---|---|---|---|
| 0-4 yıl | 830 | 736,95 | 4 | 58,2 | ,000 |
| 5-9 yıl | 287 | 582,78 | | | |
| 10-14 yıl | 105 | 554,07 | | | |
| 15-19 yıl | 63 | 510,98 | | | |
| 20 yıl ve üzeri | 70 | 705,68 | | | |
| Toplam | 1355 | | | | |

Tablo 55'de verilen sonuçlara göre, öğretmenlerin görev süresi ile bilgi güvenliği farkındalık düzeyleri arasında anlamlı bir farklılık oluşturduğu görülmektedir [$X^2$(sd=4, n=1355)= 58,2, $p$<.05]. Sıra puanlarına dikkat edildiğinde, görev süresi 0-4 yıl arasında olan öğretmenlerin bilgi güvenliği farkındalık düzeylerinin en yüksek olduğu görülmektedir [736,95]. [510,98] sıra puanıyla 15-19 yıl arasında görev yapan öğretmenlerin farkındalık düzeylerinin en düşük olduğu görülmektedir.

**Öğretmenlerin İnterneti Kullanma Süreleri Değişkeni Açısından Bilgi Güvenliği Farkındalığı Düzeyleri**

Araştırmaya katılan öğretmenlerin Bilgi güvenliği farkındalık düzeyleri ile interneti kullanma süreleri arasında anlamlı bir farklılık olup olmadığını incelemek için Kruskall Wallis testi uygulanmıştır.

Tablo 56

B*ilgi Güvenliği Farkındalığının İnternet Kullanım Süresi Değişkenine Göre Kruskal Wallis Testi Sonuçları*

| **Görev Süresi** | **N** | **Sıra Ortalaması** | **sd** | $X^2$ | **p** |
|---|---|---|---|---|---|
| 0-4 yıl | 100 | 623,50 | 3 | 5,98 | ,112 |
| 5-9 yıl | 485 | 709,52 | | | |
| 10-14 yıl | 600 | 663,29 | | | |
| 15-19 yıl | 170 | 672,04 | | | |
| Toplam | 1355 | | | | |

Tablo 56'dan anlaşılacağı üzere, öğretmenlerin internet kullanım süreleri ile bilgi güvenliği farkındalık düzeyleri arasında anlamlı bir farklılık olmadığı görülmektedir [$X^2$(sd=3, n=1355)= 5,98, p>.05]. Grupların ortalama sıra puanlarına bakıldığında aralarındaki farkın çok az olduğu görülmektedir.

**Öğretmenlerin Bilgi Güvenliği Eğitimi Alma Değişkeni Açısından Bilgi Güvenliği Farkındalığı Düzeyleri**

Araştırmaya katılan öğretmenlerin bilgi güvenliği eğitim alma durumları ile bilgi güvenliği farkındalıkları arasında istatistiksel olarak anlamlı bir ilişki olup olmadığı incelenmiştir. Normallik testi sonucu verilerin normal dağılmadığı tespit edilmiş ve parametrik olmayan testlerden ilişkisiz ölçümler için Mann Whitney U-testi uygulanmıştır.

Tablo 57

*"Bilgi güvenliği veya internet güvenliğine yönelik eğitim aldınız mı?" Maddesine İlişkin Betimsel İstatistikler*

| **Eğitim Alma Durumu** | **N** | ***f*** |
|---|---|---|
| Evet | 145 | 10,7 |
| Hayır | 1210 | 89,3 |
| Toplam | 1355 | 100 |

Tablo 57'de görüldüğü üzere, katılımcı öğretmenlerden %10,7'si (N=145) bilgi güvenliği eğitimi almıştır.

Bilgi güvenliği eğitimi aldıklarını beyan edenlerin aldıkları eğitimler,

- Güvenli İnternet Kullanımı,

- Yazılım Geliştirme ve Güvenliği,
- Site, eposta güvenliği, spam, spy, face pages, post ve get metotları vb,
- Güvenli internet semineri,
- Cisco,
- Bilge adam seminerleri,
- İnternet güvenliği,
- İnternetin güvenli kullanımı eğitimi,
- Bilgi Güvenliği Semineri-Çankaya halk eğitim merkezi bilişim günleri,
- Linux kullanıcıları derneği etkinlikleri,
- Farklı kongre ve sempozyumlardaki programlar,
- Bilişim etiği,
- Lisans dersleri

şeklindedir.

Gökmen (2014) yaptığı çalışmasında, örnekleminin %69,9'sı bilgi güvenliğine dair bir eğitim almadıklarını belirtirken %30,4'ünün bu konuda bir ders veya kurs aldıklarını belirtmişlerdir. Öğretmen kitlesinin bu konuda daha duyarlı oldukları görülmektedir. Öğütçü (2010) ise, öğrencilerin %30,5'inin bilgi güvenliğine yönelik ders aldıklarını belirtmişlerdir.

Tablo 58

*Eğitim Alma Durumunun Branşlara Göre Dağılımı*

| **Eğitim Alma Durumu** | **Matematik** | **Bilgisayar** | **Türkçe** | **Sınıf Öğretmenliği** | **Fen ve Teknoloji** | **Sosyal bilgiler** | **Toplam** |
|---|---|---|---|---|---|---|---|
| Evet | 19 | 69 | 26 | 18 | 0 | 13 | 145 |
| Hayır | 245 | 266 | 166 | 179 | 195 | 159 | 1210 |
| Toplam | 264 | 335 | 192 | 197 | 195 | 172 | 1355 |

Bilgi güvenliği eğitim alma durumlarının branşlara göre dağılımı Tablo 58'de belirtilmektedir.Eğitim alan öğretmenlerin %48'i Bilgisayar öğretmenleri iken, %18'i Türkçe Öğretmenleri, %13'ü Matematik Öğretmenleri, %12'sini Sınıf öğretmenleri ve %9'unu Sosyal Bilgiler öğretmenleri oluşturmaktadır. Fen ve Teknoloji öğretmenlerinin bilgi güvenliği ile ilgili hiç ders almadıkları görülmektedir.

Tablo 59
*Bilgi Güvenliği Farkındalığının Eğitim Alma Değişkenine Göre İncelenmesi*

| **Eğitim Alma Durumu** | **N** | **Sıra Ortalaması** | **sd** | $X^2$ | **p** |
|---|---|---|---|---|---|
| Evet | 145 | 853,69 | 1 | 32,7 | ,000 |
| Hayır | 1210 | 656,95 | | | |
| Toplam | 1355 | | | | |

Öğretmenlerin bilgi güvenliği farkındalık düzeyleri ile bilgi güvenliği eğitimi alma durumları arasında anlamlı bir ilişki olduğu yapılan Kruskal Wallis testi ile görülmüştür. Tablo 59'a göre $P<.05$ olup $X^2$(sd=1, n=1355)= 32,7'dır. Sıra ortalamaları dikkate alındığında, bilgi güvenliği eğitimi alan öğretmenlerin, almayanlara göre bilgi güvenliği farkındalığı yüksek çıkmıştır.

Ancak Gökmen (2014) çalışmasında, katılımcılarının bilişim güvenliği puanlarıyla bu konuda eğitim alıp almama durumun arasında anlamlı farklılık göstermediğini belirtmektedir. Ancak yine de bilişim güvenliğine yönelik verilen eğitimlerin adayların bilgilerine ve farkındalıklarını arttırabilineceğini eklemektedir.

**Öğretmenlerin Branşlarına Göre Bilgi Güvenliği Farkındalığı Düzeyleri**

Katılımcı öğretmenlerin branşları ile bilgi güvenliği farkındalıkları arasında istatistiksel olarak anlamlı bir ilişki olup olmadığı incelenmiştir. Normallik testi sonucu verilerin normal dağılmadığı tespit edilmiş ve parametrik olmayan testlerden ilişkisiz ölçümler için Kruskall Wallis testi uygulanmıştır.

Tablo 60

*Öğretmenlerin Bilgi Güvenliği Farkındalıklarının Branş Değişkenine Göre İncelenmesi*

| **Branşlar** | **N** | **Sıra Ortalaması** | **sd** | $X^2$ | **p** | **Anlamlı Fark** |
|---|---|---|---|---|---|---|
| Matematik | 264 | 693,02 | 5 | 38,8 | ,000 | M-T,M-S,B-S, B-S,T-S,T-S |
| Bilgisayar | 335 | 745,55 | | | | |
| Türkçe | 192 | 731,31 | | | | |
| Sınıf Öğretmenliği | 197 | 582,90 | | | | |
| Fen ve Teknoloji | 195 | 680,83 | | | | |
| Sosyal Bilgiler | 172 | 569,58 | | | | |
| Toplam | 1355 | | | | | |

Tablo 60'da görüldüğü üzere, öğretmenlerin branşları ile bilgi güvenliği farkındalık düzeyleri arasında anlamlı bir farklılık olduğu görülmektedir [$X^2$(sd=5, n=1355)= 38,8, $p$>.05]. Grupların sıra ortalamalarına bakıldığında, bilgi güvenliği farkındalığı en yüksek olan branşın bilgisayar öğretmenliği olduğu görülürken, bu branşı sırasıyla Türkçe, Matematik, Fen ve Teknoloji, sınıf öğretmenliği ve sosyal bilgiler öğretmenliği takip etmektedir. Hangi branşlar arasında anlamlı farklılık olduğuna bakmak için Mann Whitney U-testi uygulanmıştır. Bölümler arası anlamlı farklılıklar olanlar sırasıyla; Matematik-Türkçe, Matematik- Sosyal bilgiler, Bilgisayar- Sınıf öğretmenliği, Bilgisayar- Sosyal Bilgiler, Türkçe- Sınıf öğretmenliği ve Türkçe- Sosyal Bilgiler öğretmenliği branşları arasında anlamlı farklılıklar bulunmaktadır.

# BÖLÜM V

# SONUÇLAR VE ÖNERİLER

Bu araştırmada öğretmenlerin bilgi güvenliği farkındalık düzeylerinin belirlenmesi amaçlanmıştır. Araştırma sürecinde araştırmacı tarafından geliştirilen, "Bilgi Güvenliği Farkındalığı Anketi" kullanılarak araştırma verileri toplanmış ve bu veriler bulgular ve yorumlar kısmında değerlendirilmiştir. Bu bölümde ise araştırma bulgularının ortaya koyduğu sonuçlara ve bu sonuçlar çerçevesinde, ileri çalışmalar için geliştirilen önerilere yer verilmiştir.

**Sonuçlar**

Araştırma bulgularının ortaya koyduğu en genel sonuç, 1355 katılımcıdan oluşan farklı alanlarda uzmanlaşmış öğretmenlerin bilgi güvenliği farkındalık düzeyleri Orta Düzeyde Yeterli olarak değerlendirilmesidir.

Farklı branşlardan toplam 1355 öğretmenin katıldığı araştırmada katılımcıların %62'sini kadın ve %38'ini erkek öğretmenler oluşturmaktadır. Katılımcıların çoğunluğu (%69,7) 21-30 yaş aralığındadır.

Katılımcılar sosyal ağlarda en çok resimlerini, isim/soyisimlerini, duygu/düşüncelerini, doğum tarihlerini, hobilerini, araştırmalarını ve eposta adreslerini paylaşmaktadırlar. Ayrıca, telefon numarası, aile bireylerinin ismi-soyismi ve TC vatandaşlık numaralarını paylaşan katılımcılar bulunmaktadır. Bilgi güvenliğini sağlamada en önemli bileşenlerden birisi internet üzerinde paylaşım yapmaktır ve öğretmenlerin hem kendileri hemde öğrencileri için bu konuda dikkatli olmaları gerekmektedir. Nitekim, Mert, Bülbül ve Sağıroğlu'nun (2012) Milli Eğitim Bakanlığına bağlı okullarda güvenli internet kullanımını inceledikleri çalışmalarında öğrencilerin sosyal paylaşım sitelerinde doğum tarihini, şehirini ve durum bilgisini paylaştıkları görülmüştür.

Araştırmaya katılan öğretmenlerin bilgisayar ve interneti güvenli kullanım durumlarına bakıldığında teknolojik aletlerinde %81,5'i bir anti virüs yazılımı kullanırken, %18,5'i anti

virüs yazılımı kullanmamaktadır. Kullananların ise, %53,5'i ücretsiz anti virüs yazılımı kullanırken, %24'ü lisansı ödenmiş anti virüs yazılımı kullanmakta,%21,4'ü şifresi kırılmış anti virüs yazılımı kullanmakta iken %1,1'i diğer anti virüs yazılım türlerini kullanmaktadır. Öğretmenlerin %24,4'ü virüs taramasını bilgisayarda yavaşlama olduğu zaman yaparken, %22,5'i virüs taramasını ayda bir kez, %21'i haftada bir kez, %12,2'si günlük, % 8,1'i yılda bir kez ve % 7,7' si diğer olarak belirtmektedir. Bu sonuçlar, öğretmenlerin virüs taraması sıklıklarının bilgisayarlarında yavaşlama olduğunda yaptıklarını veya ayda bir kez olduğunu göstermektedir. Gökmen (2014) böte öğretmen adaylarına üzerinde yaptığı çalışmasında, adayların kısa zaman aralıklarıyla virüs taraması yaptıklarını belirtmektedir.

Güvenli kullanım boyutlarını ölçen bilgi sorularından olan spam nedir? sorusuna öğretmenlerin %74,9'u doğru cevap olan istenmeyen postadır şıkkını seçmişlerdir. Bu sonuçlar, öğretmenlerin eposta güvenliği konusunda en önemli bileşen olan spam eposta hakkında yeterli bilgiye sahip olduklarını göstermektedir. Benzer şekilde Durmuş (2014) farklı sektörlerden katılımcılarla yaptığı çalışmasında, katılımcıların büyük bir çoğunluğunun spam'ı istenmeyen posta olarak değerlendirdiğini belirtmiştir.

Öğretmenlere yöneltilen bir diğer bilgi sorusu olan, "Bankanızdan gelen bir e-postada, bilgilerinizi güncellemeniz için bir adrese tıklamanız istense ne yaparsınız?" sorusuna katılımcıların %43,5'i doğru seçenek olan eposta hakkında bilgi almak için bankayı ararım'ı seçmişlerdir. Durmuş (2014) çalışmasında da katılımcıların büyük çoğunluğunun (%75) "eposta hakkında bilgi almak için bankayı ararım" cevabını verdiklerini belirtmektedir.

Katılımcılara, "Bilgisayarınızın çalınabilme durumuna karşı hangi önlemleri alırsınız " sorusu yöneltilmiştir ve birden fazla cevap seçeneği sunulmuştur. Öğretmenlerin büyük bir çoğunluğunun bilgisayarının çalınabilme durumuna karşı alacağı önlem önemli verileri yedeklemek olmuştur.

Öğretmenlerin eposta güvenliği bilgisini ölçmeyi amaçlayan bir diğer soru ise, "Tanıdığınız birisinden dosya eklentili ve eposta adresi tuhaf bir eposta gelirse ne yaparsınız? "'dir. Öğretmenlerin %33'ü doğru seçenek olan "Teyit etmek için tanıdığıma yeni bir eposta atarım" seçeneğini seçmiştir. Bununla beraber Durmuş'un (2014) çalışmasında da katılımcıların tanıdık birisinden geliyor gibi görünen ancak tuhaf görünen epostalarda nasıl davranacağı yönünde yöneltilen maddeye verilen cevaplardan en çok tercih edileni "arkadaşımın eposta adresine doğrulamak için yeni bir eposta atarım" olmuştur. Ancak Gökmen'in (2014) çalışmasında ise öğretmen adaylarının %63,7'si güvenilir kaynaktan

geldiği zaman e-posta eki içindeki bağlantıya tıklamanın güvenliği olduğu cevabını vermişlerdir.

Araştırmaya katılan öğretmenlerin bir sitenin güvenli olduğunu nasıl anladıkları sorusuna öğretmenlerin %41,8'i bir web sitesinin güvenli olup olmadığını ayırt etmekte zorlandığını cevabını vermişlerdir. Bu durum öğretmenlerin güvenli internet durumlarının farkında olmadıklarının bir göstergesi olabilir. Küçükali ve Bülbül'ün (2015) yaptığı çalışmasında da öğretmenlerin büyük çoğunluğu internetin ve internet sitelerinin bilinçli kullanımı konusunda web sitelerinden ve diğer internet kullanıcılarından destek aldıklarını belirtmişlerdir.

Katılımcılara, sosyal medyalarda veya web sitelerinde kişisel haklarına yönelik bir saldırıyla karşılaştıklarında nereye başvurabilecekleri sorulmuş ve birden fazla seçeneği işaretleyebilecekleri belirtilmiştir. Katılımcılar en çok savcılık ve bilişim suçları birimine başvurulması gerektiği yönünde yanıt verilmiştir. Katılımcıların 5'te 1'i ise nereye rapor edileceğini bilmediklerini belirtmişlerdir. Benzer şekilde Öğütçü'nün (2010) yapmış olduğu çalışmada, katılımcılar nerdeyse yarısı karşılaştıkları bilişim suçlarını hiçbir makama iletmediklerini ifade etmişlerdir. Ayrıca katılımcıların %40,4'ünün karşılaştıkları sorunları kime ifade edebileceklerini bilmedikleri sonucuna ulaşılmıştır.

Araştırmaya katılan öğretmenlerin Bilgi Güvenliği Farkındalık düzeylerinin cinsiyetlerine göre anlamlı bir farklılık göstermediği sonucuna ulaşılmıştır. Mart (2012) ise, çalışmasına katılanların bilgi güvenliği farkındalıkları ile cinsiyetleri arasında anlamlı bir farklılık olduğunu ve kadın katılımcıların erkek katılımcılara oranla farkındalıklarının daha yüksek olduğunu belirtirken, Gökmen (2014)'de bilişim güvenliği bilgi puanlarının cinsiyete göre anlamlı olarak farklılaştığını belirtmektedir. Bu çalışmada ise erkek öğretmen adayların kadın öğretmen adaylara göre bilgi puanlarının daha yüksek olduğunu belirtmektedir.

Öğretmenlerin bilgi güvenliği farkındalık düzeyleriyle yaşları arasında anlamlı bir farklılık görülmektedir. Bu sonuç, yaş değişkeninin öğretmenlerin bilgi güvenliği farkındalıkları üzerinde önemli etkilere sahip olduğunu göstermektedir.Aynı şekilde Mart(2012) çalışmasının katılımcılarının bilgi güvenliği farkındalıklarının yaşları ile arasında anlamlı bir farklılık olduğunu belirtirken, 35-44 yaş aralığının 45-üzeri ve 25-34 yaş aralığına oranla bilgi güvenliği farkındalıklarının daha yüksek olduğu sonucuna ulaşmıştır. Ancak buna karşın, Gökmen (2014) Böte öğretmen adaylarının bilişim güvenliği bilgileri ile yaşları arasında anlamlı bir farkındalığı olmadığı sonucuna ulaşmıştır.

Bilgi güvenliği farkındalık düzeyleri bakımından öğretmenlerin öğrenim durumları arasında anlamlı bir farklılık oluşturduğu görülmüştür. Sıra ortalamaları dikkate alındığında ön lisans mezunlarının sıra ortalaması en yüksek çıkmaktadır. Bu sonuca göre Ön lisans mezunu öğretmenlerin bilgi güvenliği farkındalık düzeyleri diğer öğrenim durumlarına göre istatistiksel olarak anlamlı düzeyde daha yüksek olduğu söylenebilmektedir. Buna karşın Mart 2012 yılında yaptığı çalışmasında farklı meslek gruplarından oluşan katılımcılarının eğitim durumları ve bilgi güvenliği farkındalıkları arasında anlamlı bir farklılık olmadığını sonucuna ulaşmıştır.

Öğretmenlerin bulundukları bölge ile bilgi güvenliği farkındalık düzeyleri arasında anlamlı bir farklılık oluşturduğu görülmektedir. Sıra ortalamaları dikkate alındığında İstanbul bölgesinde bulunan öğretmenlerin farkındalıklarının en yüksek çıktığı görülmektedir. Sıra ortalamaları sırası ile Doğu Marmara, Orta Anadolu, Akdeniz, Ortadoğu Anadolu, Güneydoğu Anadolu,Batı Anadolu, Batı Karadeniz, Kuzeydoğu Anadolu, Ege, Batı Marmara, Doğu Karadeniz olarak sıralanmaktadır.

Katılımcı öğretmenlerin görev süresi ile bilgi güvenliği farkındalık düzeyleri arasında anlamlı bir farklılık oluşturduğu sonucuna ulaşılmıştır. Görev süresi 0-4 yıl arasında olan öğretmenlerin bilgi güvenliği farkındalık düzeylerinin en yüksek olduğu gözlemlenirken, 15-19 yıl arasında görev yapan öğretmenlerin farkındalık düzeylerinin en düşük olduğu görülmüştür.

Öğretmenlerin internet kullanım süreleri ile bilgi güvenliği farkındalık düzeyleri arasında anlamlı bir farklılık olmadığı görülmektedir. Grupların ortalama sıra puanlarına bakıldığında aralarındaki farkın çok az olduğu görülmektedir. Mart (2012) da yaptığı çalışmasında farklı meslek gruplarının internet kullanım süreleri ile bilgi güvenliği farkındalıkları arasında anlamlı bir farklılık olmadığı sonucuna ulaşmıştır. Aynı şekilde Gökmen'de (2014) böte öğretmen adaylarının günlük internet kullanım süreleri ile bilişim güvenliği bilgileri arasında anlamlı bir farkın olmadığını belirtmektedir.

Katılımcı öğretmenlerden %10,7'si (N=145) bilgi güvenliği eğitimi almıştır. Gökmen (2014) yaptığı çalışmasında, örnekleminin %69,9'sı bilgi güvenliğine dair bir eğitim almadıklarını belirtirken %30,4'ünün bu konuda bir ders veya kurs aldıklarını belirtmişlerdir. Öğretmen kitlesinin bu konuda daha duyarlı oldukları görülmektedir. Öğütçü (2010) ise, öğrencilerin %30,5'inin bilgi güvenliğine yönelik ders aldıklarını belirtmişlerdir. Öğretmenlerin bilgi güvenliği farkındalık düzeyleri ile bilgi güvenliği eğitimi alma durumları arasında anlamlı bir ilişki vardır. Bilgi güvenliği eğitimi alan öğretmenlerin,

almayanlara göre bilgi güvenliği farkındalığı yüksek çıkmıştır. Ancak Gökmen (2014) çalışmasında, katılımcılarının bilişim güvenliği puanlarıyla bu konuda eğitim alıp almama durumun arasında anlamlı farklılık göstermediğini belirtmektedir. Ancak yine de bilişim güvenliğine yönelik verilen eğitimlerin adayların bilgilerine ve farkındalıklarını arttıra bilineceğini eklemektedir.Ayrıca, Erol, Ceyhan ve Sağıroğlu (2015) yaptıkları çalışmalarında bu eğitimlerin düzenli aralıklarla da yapılması gerektiğini ve buna rağmen ortaya çıkan yeni gelişmelerle verilen eğitimler ve oluşturulan farkındalıklar geçersiz sayılabileceğini belirtmişlerdir.Eğitimin düzenli ve güncellenmiş olarak verilmesi bu açıdan önemlidir.

Öğretmenlerin branşları ile bilgi güvenliği farkındalık düzeyleri arasında anlamlı bir farklılık olduğu sonucuna ulaşılmıştır. Bilgi güvenliği farkındalığı en yüksek olan branşın bilgisayar öğretmenliği olduğu görülürken, bu branşı sırasıyla Türkçe, Matematik, Fen ve Teknoloji, sınıf öğretmenliği ve sosyal bilgiler öğretmenliği takip etmektedir. Ayrıca bölümler arası anlamlı farklılıklar olanlar sırasıyla; Matematik- Türkçe, Matematik- Sosyal bilgiler, Bilgisayar- Sınıf öğretmenliği, Bilgisayar- Sosyal Bilgiler, Türkçe- Sınıf öğretmenliği ve Türkçe- Sosyal Bilgiler branşlarıdır.

## Öneriler

- Teknolojinin son haliyle insanlığın bilgileri dijital ortamlara aktarılmış durumdadır. Bu durum riskleri ve tehlikeleri beraberinde getirmektedir. Bu çalışmada öğretmenler örneği görülmüştür ki mevcut durumda bilginin güvenliğini koruma düzeyi yeterli değildir. Nesilleri yetiştiren öğretmenlerin bu konuda yeterli bilgiye sahip olmaması, gelecek nesillerinde yeterli şekilde eğitilmediği anlamadına gelebilmektedir. Bu sebeple öğretmenlere bilgi güvenliği farkındalıklarını arttırmak adına düzenli eğitimler, çalıştaylar düzenlenmeli ve seminerler verilmelidir.
- Bu çalışmanın örneklemini öğretmenler oluşturmuştur. Bundan sonraki çalışmalar farklı meslek grupları ve topluluklar üzerinde de uygulanabilir.
- Çocukları ve öğretmenleri korumak adına okullarda ortak kullanabilecek etkileşimli bilgi güvenliği web siteleri yapılabilir.
- Bu çalışma deneysel bir çalışma olarak yapılabilir. Kontrol ve deney grubu oluşturularak deney grubuna verilen farkındalık eğitiminin davranışa ne kadar yansıdığı belirli aralıklarla yapılan testlerle ölçülebilir.

- 8. Uluslararası Bilgi Güvenliği Konferansı sonuç bildirgesinde de belirtildiği gibi, bilgi güvenliği konusu ilköğretimden itibaren müfredata dahil edilmeli ve sürekli olarak yenilerek gündemde kalması sağlanmalıdır. Böylece bilgi güvenliğinin farkında olan nesilleri yetiştirilmelidir. Ayrıca, farkındalık sağlayan projeler, sosyal projeler, araştırmalar ve açık bilgilendirme platformlarının sayıları arttırılmalı ve sorumlu kurumlarca desteklenmelidir.
- Okullarda öğretmenlere farkındalıklarının arttırma fırsatı bulabilecekleri bilgimikoruyorum.org.tr yada güvenlikiçinbirdakika.org gibi internet sitelerinin tanıtımı yapılabilir.
- Bilgi güvenliği farkındalığını arttırmak ve tehlikelerden haberdar olmak adına öğrencilere belirli aralıklarla izletilebilecek animasyonlar geliştirilebilir ya da kamu spotları yayınlanabilir.

# KAYNAKÇA


Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*.*33(3). 237-248.*

Adıgüzel, Ö.(2010). *Eğitimde Yaratıcı Drama*. I. Basım, Ankara: Naturel.

Adıgüzel, G. C., (2009). *Güvenlik endişesinin internet bankacılığı kullanımına etkisi ve vakıfbank müşterilerine yönelik bir araştırma*. Yüksek Lisans Tezi, Gazi Üniversitesi Eğitim Bilimleri Enstitüsü. Ankara.

Al-Ahmad, W., & Mohammad, B. (2013). Addressing information security risks by adopting standards. International Journal of Information Security Science, 2(2), 28-43.

Albrechtsen, E. (2007). "A qualitative study of users' view on information security". *Computers & Security*. *26(4). 276-289*.

Albrechtsen, E., & Hovden, J. (2008). "Improving information security awareness and behaviour by a user participative approach: an intervention study". Accepted for review in Information & Management. Friend or foe? *Information security management of employees.*

Altun, R. (2014). *Belirli kısıtlara göre bilgi güvenliği ihlallerinin tespiti*. Yüksek Lisans Tezi, Beykent Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Akkoyunlu, B. (1998). *Eğitimde teknolojik gelişmeler.* B. Özer (Ed.), Çağdaş eğitimde yeni teknolojiler (s.3-8). Eskişehir: Anadolu Üniversitesi.

Akın, O., Cınar, I., Karaman, M., & Bilekyigit, F. (2013). *Siber Durum Farkındalıgını Artırmada Etkili Bir Yontem: Bayragı Yakala (Capture the Flag)*. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı ODTÜ, Ankara.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & security*. *26(4). 276-289.*

Agamba, J. & Keengwe, J. (2012). Pre-Service Teachers' Perceptions of Information Assurance and Cyber Security. *International Journal of Information and Communication Technology Education*. 8(2). 94-101.

Başbakanlık Kanunlar ve Kararlar Genel Müdürlüğü, *Kişisel Veri Güvenliği Kanun Tasarısı*,(2014).http://www.kgm.adalet.gov.tr/Tasariasamalari/Tbmmkms/Tbmmkom/ki%C5%9Fisel%20veriler.pdf, 2014 adresinden erişilmiştir.

Berkay, A. (2009). *Hack Teknikleri*. Gebze yüksek teknoloji enstitüsü. http://bilmuh.gyte.edu.tr/~ispinar/BIL673/Hacktek.pdf sayfasından erişilmiştir.

Büyüköztürk Ş. (2002). Faktör Analizi: Temel Kavramlar ve Ölçek Geliştirmede Kullanımı. *Kuram ve Uygulamada Eğitim Yönetimi Dergisi*. *8 (32).*

Büyüköztürk, S. (2008). *Sosyal bilimler için veri analizi el kitabı*. Ankara: Pegem A Yayıncılık.

Büyüköztürk, Ş., Kılıç Çakmak, E., Akgün, Ö. E., Karadeniz, Ş. ve Demirel, F. (2012). *Bilimsel araştırma yöntemleri (13.Baskı)*. Ankara: Pegem Akademi.

Bilek, B.T. (2012). *Bilişim suçları ve üniversite lisans öğrencilerin bilişim suçlarına yönelik görüşleri*. Yüksek lisans tezi, Gazi Üniversitesi, Bilişim Enstitüsü, Ankara.

Blakley, B., McDermott, E., & Geer, D. 2001. *Information security is information risk management.* Proceedings of the 2001 Workshop on New Security Paradigms, 97-104.

Brostoff, S., & Sasse, M. A.,2001. *Safe And Sound: A Safety-Critical Approach To Security.* In Proceedings of the 2001 workshop on New security paradigms (s. 41-50). NewYork:The Association for Computing Machinery press.

Brodie, C. (2008). *The importance of security awareness training*.

Canbek, G. (2005). *Klavye dinleme ve önleme sistemleri analiz, tasarım ve geliştirme*. Yüksek Lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Ankara.

Canbek, G. ve Sağıroğlu, Ş. (2007). Kötücül Casus Yazılımlar Kapsamlı Bir Araştırma. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*. 22 (1). 121-136.

Canbek, G. ve Sağıroğlu, Ş. Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme. (2006). *Politeknik Dergisi. 9(3). 165-174.*

Chitrey, A., Singh, D., & Singh, V. (2012). A comprehensive study of social engineering based attacks in india to develop a conceptual model. *International Journal of Information and Network Security*. *1(2). 45.*

Chitrey, A., Singh, D., & Singh, V. (2012). A comprehensive study of social engineering based attacks in india to develop a conceptual model. *International Journal of Information and Network Security*. *1(2). 45.*

Corporate Technology Group (2008). *The threat within: is your company safe from itself?* http://www.ctgyourit.com/newsletter.php sayfasından erişilmiştir.

Çalık, D., ve Çınar, Ö.P. (2009) *Geçmişten günümüze bilgi yaklaşımları bilgi toplumu ve internet.* 14.Türkiye'de İnternet Konferansı'nda sunulmuş bildiri, İstanbul Bilgi Üniversitesi, İstanbul.

Çokluk, Ö., Şekercioğlu G., & Büyüköztürk, Ş. (2014). *Sosyal bilimler için çok değişkenli istatistik: SPSS ve LISREL Uygulamaları.* Ankara: Pegem Akademi.

Demiralay, R. ve Karadeniz, Ş. (2010). Bilgi ve iletişim teknolojileri kullanımının, ilköğretim öğretmen adaylarının bilgi okuryazarlığı öz-yeterlik algılarına etkisi, *Kuram ve Uygulamada Eğitim Bilimleri*. *10(2). 819-851.*

Delialioğlu, Ö. (2011). *Bilişim Sistemleri Güvenliği ve İlgili Etik Kavramlar.* A.Şentürk (Ed.), Temel bilgi teknolojileri ve bilgisayar kullanımı içinde (s. 509-538). Bursa: Ekin.

Dijle, H. ve Doğan, N. (2011). Türkiye'de Bilişim Suçlarına Eğitimli İnsanların Bakışı. *Bilişim Teknolojileri Dergisi. 4(2). 43-53.*

Durmuş, A., (2014). *Türkiye'de bilgi güvenliği farkındalığının incelenmesi.* Yüksek Lisans Tezi, Çankaya Üniversitesi Fen Bilimleri Enstitüsü. Ankara.

Dülger, M. V. (2004). *Bilişim şuçları*. Ankara: Seçkin.

Ersoy, E. (2011). *Gizlilik, bireysel haklar, kişisel verilerin korunması*. Telekomünikasyon Kurumu, Ankara.

Erol, E., Ceyhan, E.B., Sagiroglu, S.,(2015). "*Kişisel, Kurumsal ve Ulusal Bilgi Güvenliği Farkındalığı Üzerine Bir İnceleme",* Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı ODTÜ, Ankara.

Global Information Security Awareness Survey. (2014) http://www.ey.com/GL/en/Services/Advisory/EY-cybersecurity sayfasından erişilmiştir.

Granger, S. (2001). *Social Engineering Fundamentals, Part I: Hacker Tactics.* http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics sayfasından erişilmiştir.

Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D., & Cowley, J. (2014). *Analysis of unintentional insider threats deriving from social engineering exploits*. In Security and Privacy Workshops (SPW), IEEE. 236-250.

Gonzalez, J. J., & Sawicka, A. (2002). *A framework for human factors in information security.* In WSEAS International Conference on Information Security, Rio de Janeiro .448-187.

Görkey,D., (2008). *İnternet reklamcılığı: etik ve hukuk sorunsalı*. Yüksek Lisans Tezi, İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü.

Gökmen, Ö. F., (2014). *Bilgisayar Ve Öğretim Teknolojileri Eğitimi Öğretmen Adaylarının Bilişim Güvenliği Eğitimi Verebilme Yeterliklerinin İncelenmesi.* Yüksek Lisans Tezi, Sakarya Üniversitesi Eğitim Bilimleri Enstitüsü. Sakarya.

İlbaş, Ç. (2009). *Bilişim suçlarının sosyo-kültürel seviyelere göre algı analizi*. Yüksek lisans tezi, Başkent Üniversitesi Fen Bilimler Enstitüsü, Ankara.

Kaptan, S.(1993), *Bilimsel araştırma ve istatistik teknikleri*. Ankara: Rehber.

Karakasiliotis, A., Furnell, S. M., & Papadaki, M. (2006). *Assessing end-user awareness of social engineering and phishing.*

Karasar, N. (1999), *Bilimsel araştırma yöntemi*. Ankara: Nobel.

Karalar, H. ve Sarı, Y. (2007) *Bilgi Teknolojileri Eğitiminde BDÖ Yazılımı Kullanma ve Uygulama Sonuçlarına Yönelik Bir Çalışma*. Akademik Bilişim 2007 Konferansı, Dumlupınar Üniversitesi, Kütahya.

Kuçuradi, I. (1995). *Knowledge and its object*. In The Concept of Knowledge, Springer Netherlands, s.97-102.

Kurt, L. (2005). *Bilişim suçları*. Ankara: Seçkin.

Kumar, A.,Chaudhary, M., & Kumar, N., (2015). Social Engineering Threats and Awareness: A Survey. *European Journal of Advances in Engineering and Technology*.2(11). 15-19

Küçükali, M., & Bülbül, H. İ. (2015). Fatih Projesi Kapsamında İnternetin Bilinçli, Güvenli Kullanımının Artırılması. *TÜBAV Bilim Dergisi*. 8(2). 1-17.

Kınay, H. (2012). *Lise öğrencilerinin siber zorbalık duyarlılığının riskli davranış, korumacı davranış, suça marüziyet ve tehlike algısı ile ilişkisi ve çeşitli değişkenler açısından incelenmesi.* Yüksek lisans tezi, Sakarya Üniversitesi, Eğitim Bilimler Enstitüsü. Sakarya.

Kissel, R. (2013). *Glossary of key information security terms*. NIST Interagency Reports NIST IR, 7298(3).

Mart, İ. (2012). *Bilişim kültüründe bilgi güvenliği farkındalığı*. Yüksek lisans tezi. Kahramanmaraş Sütçü İmam Üniversitesi, Fen Bilimleri Enstitüsü, Kahramanmaraş.

MEB.*Çağdaş Öğretmen Profili.(2001).*Ankara

Mert, M., Bülbül, H. İ., & Sağıroğlu, Ş. (2012). Milli eğitim bakanlığına bağlı okullarda güvenli internet kullanımı. *Türk Bilim Araştırma Vakfı Bilim Dergisi*,5(4), *1-12.*

Naisbitt, J. (1982). *Megatrends*, New York, Warner Bookss.

Okenyi, P. O., & Owens, T. J. (2007). On the anatomy of human hacking.*Information Systems Security*. *16(6). 302-314.*

Öğütçü, G. (2010). *E-dönüşüm sürecinde kişisel bilişim güvenliği davranışı ve farkındalığın analizi.* Yüksek lisans tezi. Başkent Üniversitesi, Fen Bilimleri Enstitüsü, Ankara.

Özer, B. (1998). *Teknoloji yoğunluklu eğitim yaklaşımı olarak uzaktan eğitim*. B. Özer (Ed.), Çağdaş eğitimde yeni teknolojiler (s.121-135). Eskişehir: Anadolu Üniversitesi.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). *Employees' behavior towards IS security policy compliance.* In System sciences, 2007. HICSS 2007. 40Th annual hawaii international conference on IEEE.

Pearce, J. (2002). Security Expert Warns of MP3 Danger. ZDNet News Online,18.

Pfleeger, C. P., & Pfleeger, S. L. (2015). *Security in computing*. 5th ed., Prentice Hall Upper Saddle River, NJ.

Margulies, J., Pfleeger, C., & Pfleeger, S. L. (2015). Security in Computing.

Pharming (2015). *Site trafiği yönlendirme nedir?* http://www.kaspersky.com/tr/internet-security-center/definitions/pharming sayfasından erişilmiştir.

Poulsen, K. (2000). *Mitnick to lawmakers: People, phones and weakest links*. http://www.politechbot.com/p-00969.html sayfasından erişilmiştir.

Rights, R. F. (2001). *SANS Institute InfoSec Reading Room*.

Richardson, R., & Director, C. S. I. (2008). CSI computer crime and security survey. *Computer Security Institute*, *1*, *1-30.*

Schuler, A. J.(2003) "How to Build Wisdom and Prosper in an "Information Age"",

"What's Up, Doc?" *e-Newsletter,* 3(6). 5-7.

Schultz, E. E., Proctor, R. W., Lien, M. C., & Salvendy, G. (2001). Usability and security an appraisal of usability issues in information security methods. *Computers & Security*. 20 (7). 620-634.

Schmidt, M. B., Johnston, A. C., Arnett, K. P., Chen, J. Q., & Li, S. (2008). A cross-cultural comparison of us and chinese computer security awareness.*Journal of Global Information Management, 16(2), 91*.

Siponen, M. (2001). Five dimensions of information security awareness.*Computers and society*. 31(2). 24-29.

Spıtzner, L., (2010). *The "people problem" continues to hamper information security efforts; what can be done about it ?*

http://searchsecurity.techtarget.com/magazineContent/How-to-build-an-effective-information-security-awareness-program sayfasından erişilmiştir.

Stallings, W. (2011). *Network Security Essentials- Applications and Standards.* Pcarson Educational İnternational India.

Solms, R. V. (1998). Information security management (3): the Code of Practice for Information Security Management (BS 7799). *Information Management & Computer Security*. 6(5). 224-225.

Symantec. (2009).Symantec global internet security threat report–trends for 2009. http://eval. symantec. com/mktginfo/enterprise/white papers/b-whitepaper internet security threat report adresinden erişilmiştir.

Symantec. (2013). *Internet Security Threat Report 2013.*http://www.symantec.com/content/en/us/enterprise/other_resources/bistr_main_report_v18_2012_21291018.en-us.pdf adresinden erişilmiştir.

Şahin, L., Çetin, B.I. ve Yıldırım, K. (2009). Bilişim Teknolojilerindeki Gelişmelerin İşletmelerin Strateji ve Maliyet Üzerine Etkileri. *Sosyal Siyaset Konferansları Dergisi*. *56(1). 45.*

Şahinaslan, E., Kantürk, A., Şahinaslan., Ö. ve Borandağ, E. (2009). *Kurumlarda Bilgi Güvenliği Farkındalığı, Önemi ve Oluşturma Yöntemleri.* 11. Akademik Bilişim Konferansı Bildirileri. Harran Üniversitesi, Şanlıurfa.

Tak, S., Dixit, S., & Park, E. K. (2004). An end-to-end home network security framework. *Computer Communications*. *27(5). 412-422.*

Tandoğan, M. (1998). *Öğretmen ve teknoloji*. B. Özer (Ed.), Çağdaş eğitimde yeni teknolojiler (s.15-24). Eskişehir: Anadolu Üniversitesi.

Tekin, M., Zerenler, M. ve Bilge, A. (2005). Bilişim Teknolojileri Kullanımının İşletme Performansına Etkileri: Lojistik Sektöründe Bir Uygulama. *İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi. 4(8). 115-129.*

Tekerek, M., (2012). *İlköğretim ve Lise Öğrencilerinin Bilgi ve Bilgisayar Güvenliği Farkındalığı: Kahramanmaraş Örneği.* Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı ODTÜ, Ankara.

Tekerek, M. (2008). Bilgi Güvenliği Yönetimi. *Kahramanmaraş Sütçü İmam Üniversitesi Fen ve Mühendislik dergisi*. *11(1). 132-137*.

Tekerek, M., & Tekerek, A. (2013). Öğrencilerin Bilgi Güvenliği Farkındalığı Üzerine Bir Araştırma. *Turkish Journal of Education, 2(3).*

Trček, D., Trobec, R., Pavešić, N., & Tasič, J. F. (2007). Information systems security and human behaviour. Behaviour & Information Technology, 26(2), 113-118.

Tutkun, Ö. F., & Aksoyalp, Y. (2010). 21. Yüzyilda Ögretmen Yetistirme Egitim Programinin Boyutlari/Dimensions of Teacher Training Curricula in The 21st Century. *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*. (24). 361.

Türk Ceza KanunuMadde Gerekçeleri.(2015) www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc adresinden erişilmiştir.

Türk Dil Kurumu. (2015). Genel Türkçe Sözlüğü, http://tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.52 ab0a9de06dc8.51022261 adresinden 13.10.2015 tarihinde erişilmiştir.

Türkiye Odalar ve Borsalar Birliği (TOBB), 2013. Sorularla Örnekleme, Araştırma ve Veri Denetleme, Yayın No: 189, İskitler, Ankara.

Topal, M. Ve Akgün, Ö., E., (2015). Eğitim Fakültesinde Okuyan Öğretmen Adaylarının Eğitim Amaçlı İnternet Kullanımı Öz-Yeterlik Algılarının İncelenmesi: *Sakarya Üniversitesi Örneği. Kastamonu Eğitim Dergisi . 23(1). 343-364.*

Vardal, N. (2009).*Yükseköğretimde bilgi güvenliği: Bilgi güvenlik yönetim sistemi için bir model önerisi ve uygulaması.* Yüksek Lisans Tezi, Gazi Üniversitesi Eğitim Bilimleri Enstitüsü. Ankara.

Vural, Y., ve Sağıroğlu, Ş. (2008). Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*. *23 (2). 507-522.*

Whitman, M., & Mattord, H.(2012). *Prıncıples of information security*. Cengage Learning.

Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security*. *17(4). 330-340.*

# EKLER

**Ek-1 :Bilgi Güvenliği Farkındalığı Anketi**

Sayın Hocam;

Bu anket, Gazi üniversitesi Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı'nda yürütülen yüksek lisans programı kapsamında hazırlanmıştır. Araştırmada bilgi güvenliği farkındalık seviyelerini ölçmek hedeflenmektedir. Bu anketi online olarak dolduran kişinin mail adresi dahil hiçbir kişisel bilgisi araştırmacı tarafından görülememektedir. Bu doğrultuda kişisel bilgilerinizin üçüncü şahıslarla paylaşılması söz konusu değildir. Çalışmanın amacına ulaşması değerli katkılarınıza bağlıdır. Lütfen size en uygun olan seçeneği işaretleyiniz. Anketi cevaplama süresi ortalama 10 dk sürmektedir.

Kıymetli zamanınızı paylaştığınız için teşekkür eder, saygılar sunarım.

Arş. Gör. Gülsüm KAPANOĞLU

gulsumkapanoglu@gmail.com

Gazi Üniversitesi, Gazi Eğitim Fakültesi,
Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü,
Beşevler, Ankara, Türkiyesunarım.

**BÖLÜM I: Kişisel Bilgiler**

**1.**Cinsiyetiniz. ( ) Kadın ( ) Erkek
**2**.Yaşınız. ( ) Ön lisans ( ) Lisans ( ) Yüksek Lisans ()Doktora
**3**.Yaşadığınız Şehir.....
**4**.Eğitim Düzeyiniz ( ) Ön lisans ( ) Lisans ( ) Yüksek Lisans ( )Doktora
**5**.Branşınız.....
**6.**Görev Süreniz
( ) 0-4 yıl ( ) 5-9 yıl ( ) 10-14 yıl ( )15-19 yıl ( ) 20 yıl ve üzeri
**7.**Akıllı cep telefonunuz var mı? ( )Evet ( ) Hayır
**8.** Günlük internet kullanım sıklığınız nedir?
( ) 0-1 sa ( ) 2-3 sa ( ) 4-5 sa ( )5+ sa
**9.**Kaç yıldır internet kullanıyorsunuz?
( ) 0-4 yıl ( ) 5-9 yıl( ) 10-14 yıl ()15-19 yıl
**10**.İnterneti hangi amaçlarla kullanırsınız? (Birden fazla seçenek işaretleyebilirsiniz)
( ) Sosyal ağ sitelerini kullanmak
( ) e-posta gönderme/ alma
( ) Araştırma yapmak
( ) İnternet bankacılığı
( ) Dosya indirmek
( ) Sohbet etmek
( ) Oyun oynamak

( ) Alışveriş yapmak
( ) Gazete/ dergi okumak
( ) Müzik dinlemek/film izlemek
( ) e-devlet
( ) Diger
**11.** Bilgi güvenliği veya internet güvenliğine yönelik eğitim aldınız mı?
( )Evet ( ) Hayır
**12.** Aldığınız eğitimleri belirtir misiniz?.....
**13.** Hangi sıklıkla eposta kutunuzu kontrol edersiniz?
( ) Her gün birden fazla
( ) Her gün bir kez
( ) Haftada bir kez
( ) Ayda bir kez
( ) Yılda bir kez
( ) Bir yıldan fazla süredir
**14.**Sosyal Medya platformlarında bir hesabınız var mı? (Facebook, Twitter, instagram vs.)
( )Evet ( ) Hayır
**15.** Sosyal Medya hesaplarınızda hangi kişisel bilgilerinizi paylaşırsınız?
(Birden fazla seçenek işaretleyebilirsiniz.)
( ) Resim
( ) Video
( ) İsim, Soyisim
( ) Doğum tarihi
( ) Aile bireylerinin ismi, soyismi
( ) T.C kimlik no
( ) Telefon numarası
( ) eposta adresi
( ) Araştırmalar/ Çalışmalar
( ) Duygular/Düşünceler
( ) Hobiler
( ) Diger

**Bölüm II: Güvenli Kullanım**

| MADDELER | EVET | HAYIR |
|---|---|---|
| 1.Bir Antivirüs yazılımı kullanıyor musunuz? (Cevabınız Hayır ise .soruyu geçiniz.)<br>( )Evet ( ) Hayır | | |
| 2.Bilgisayarınızda ne tür antivirüs yazılımı kullanırsınız?<br>( ) Ücretsiz antivirüs yazılımı kullanırım<br>( )Korsan (şifresi kırılmış) antivirüs yazılımı kullanırım<br>( )Lisansı ödenmiş antivirüs yazılımı kullanırım<br>( )Diğer | | |
| 3. Hangi sıklıkla virüs tarama yazılımlarını güncellersiniz?<br>( )Günlük ( ) Haftalık ( )Ayda bir kez ( ) Yılda bir kez ( )Sadece kurduğum zaman ( )Bilgisayarda yavaşlama olduğu zaman ( ) Diğer | | |
| 4.Spam mail nedir?<br>( )Spam server tarafından gönderilen bir e-postadır<br>( )Spam bir çeşit güvenlik duvarıdır<br>( )Spam, istenmeyen postadır<br>( )Spam bir email ekidir<br>( )Spam, bilinen bir kişi tarafından gönderilen postadır | | |
| 5.Bankanızdan gelen e-postada, bilgilerinizi güncellemeniz için bir adrese tıklamanız istense ne yaparsınız?<br>( )Eğer bankanın logo'su ve adresi doğru ise linki tıklarım<br>( )Yakın arkadaşlarım bilgilerini güncellerse ben de aynısını yaparım<br>( )e-mail hakkında bilgi almak için bankayı ararım<br>( )Diğer | | |
| 6.Bilgisayarınızın çalınabilme durumuna karşı hangi önlemleri alırsınız?<br>( )Fiziksel adresini (MAC) tutarım<br>( )Seri numarasını tutarım<br>( )Önemli verilerimi yedeklerim<br>( )Önemli verilerimi şifrelerim<br>( )Kullanıcı hesabıma parola koyarım<br>( )Uzaktan takibini yapacak bir GPS yazılımı yüklerim<br>( )Hiçbir önlem almıyorum | | |
| 7.Tanıdığınız birisinden dosya eklentili ve mail adresi tuhaf bir mail gelirse ne yaparsınız?<br>( )Gönderen kişi tanıdığımsa eklentiyi açmak güvenlidir<br>( )Maili tanıdığımın gönderdiğini doğrularsam cevap veririm<br>( )Teyit etmek için tanıdığıma yeni bir mail atarım | | |

| | | |
|---|---|---|
| ( )Diğer | | |
| 8.Size küçük bir kız çocuğunun kaçırıldığına dair veya acil kan ihtiyacı olduğu belirtilen v.b bir mail gelse ve bu maili tüm arkadaşlarınıza göndermeniz istense ne yaparsınız?<br>( )Tüm arkadaşlarıma gönderirim<br>( )Sadece yakın arkadaşlarıma gönderirim<br>( )Mail zincirine katılmadan yeni bir mail oluştururum ve gönderen kişiye cevap veririm<br>( )Sakıncalı olduğunu düşünerek önemsemem<br>( )Diğer | | |
| 9.Bir websitesinin güvenli olup olmadığını nasıl anlarsınız?<br>( )Ücretsiz yazılım sunan bir websitesi ise güvenlidir<br>( )Güvenlidir logosu varsa güvenlidir<br>( )İnternet adresi "http:// " yerine "https:// " ile başlıyorsa güvenlidir<br>( )Popüler görünüyorsa güvenlidir<br>( )Ayırt etmekte zorlanırım | | |
| 10.Sosyal medyalarda veya websitelerinde, kişisel haklarınıza yönelik bir saldırıyla karşılaştığınızda nereye başvurursunuz?<br>( )Ailem/ Arkadaşlarım<br>( )En yakın Polis Merkezine<br>( )Website yöneticisine<br>( )Telekomünikasyon İletişim Başkanlığı, İnternet Bilgi İhbar Merkezi<br>( )Siber Güvenlik şube ofisi<br>( )Savcılık/Bilişim Suçları<br>( )Nereye rapor etmem gerektiğini bilmiyorum<br>( )Rapor etmem | | |
| 11.Sosyal Medya hesaplarınızda hangi gizlilik ayarlarını aktif kullanırsınız?<br>(Birden fazla seçenek işaretleyebilirsiniz.)<br>( )Arkadaş listesini gizleme<br>( )Paylaşılanları gizleme<br>( )Beğenileri gizleme<br>( )Fotoğrafları gizleme<br>( )e-mail adresi gizleme<br>( )Hiçbiri | | |

**Bölüm III: Bilgi Güvenliği Farkındalığı**

| MADDELER | HİÇBİR ZAMAN | NADİREN | BAZEN | SIK SIK | HER ZAMAN |
|---|---|---|---|---|---|
| 1.Kişisel bilgilerimin başkaları tarafından kötü amaçla kullanılabileceğini düşünürüm. | | | | | |
| 2.Parolalarımı sık sık değiştiririm. | | | | | |
| 3.Akıllı telefonum bir şifre ile korunur. | | | | | |
| 4.Parolalarımı yazılı olarak ulaşabileceğim bir yerde saklarım. | | | | | |
| 5.Bilgisayarımda lisanslı yazılım (orijinal) kullanmaya dikkat ederim. | | | | | |
| 6.Bütün hesaplarımda aynı parolayı kullanırım. | | | | | |
| 7.Kişisel bilgisayarımda otomatik kullan özelliğini kullanırım. | | | | | |
| 8.Kısa bir işim olsa dahi çalışırken ekran koruyucu kullanırım. | | | | | |
| 9.İnternetin herkese açık olduğu yerlerde internet bankacılığı kullanırım. | | | | | |
| 10.Virüs temizleme, casus yazılım önleme vb. programları kullanırım. | | | | | |
| 11.Kargo,Gsm operatörü gibi kuruluşlarla nüfus cüzdanı bilgilerimi paylaşırım. | | | | | |
| 12.Kullandığım programların güncellemesini düzenli olarak yaparım. | | | | | |
| 13.Çocukları istenmeyen içeriklerden koruyacak filtre programları kullanırım. | | | | | |
| 14.Önemli dosyalarımı şifrelerim. | | | | | |
| 15.Güvenlik duvarı, reklam önleyici vb. programlar kullanırım. | | | | | |
| 16.Vatandaşlık numaramın (T.C) başka şahıslar tarafından bilinmesi beni rahatsız etmez. | | | | | |
| 17.Parolalarımı başkalarıyla paylaşırım. | | | | | |
| 18.İnternette kullandığım hesaplarda şifrem ele geçirildi. | | | | | |
| 19.Kişisel bilgilerimi internette kullandığım için sıkıntı yaşadım. | | | | | |
| 20.Sosyal ağlarda yaptığım bilgi paylaşımı hayatıma zarar verdi. | | | | | |
| 21.Bilgisayarımdaki bazı dosyalarım çalındı/silindi. | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| 22.İnternette gezerken isteğim dışında şiddet ya da pornografik içerikli yayınlarla karşılaştım. | | | | | |
| 23.İnternet bankacılığı vs. şifresini yazarken klavye kullanırım. | | | | | |
| 24.Kredi kartı bilgilerim kopyalandı. | | | | | |
| 25.Herkesin kullanımına açık bir bilgisayardan ayrılmadan önce geçici internet dosyalarını ve gezinme geçmişini silerim. | | | | | |
| 26.İnternet üzerindeki hesaplarımda kolay tahmin edilemeyecek şekilde karmaşık ve uzun şifreler kullanırım. | | | | | |
| 27.Aynı iletiyi birden fazla kişiye göndermem gereken durumlarda gizli (BCC) kısmını kullanırım. | | | | | |
| 28.Bulut teknolojilerinde (Drive,Dropbox vs.) bilgilerimi güvende hissediyorum. | | | | | |

## EK-2 :Türkiye'de İBBS ya da (NUTS)'a Göre Sınıflandırılmış Bölgeler

| **DÜZEY 1** (12 Bölge Birimi NUTS-1) | | **DÜZEY 2** (26 Bölge Birimi) | | **DÜZEY 3** (81 İl Düzeyinde) | |
|---|---|---|---|---|---|
| **Kod** | **Tanım** | **Kod** | **Tanım** | **Kod** | **Tanım** |
| **TRA** | KUZEYDOĞU ANADOLU | TRA1 | ERZURUM | TRA11 | ERZURUM |
| | | | | TRA12 | ERZİNCAN |
| | | | | TRA13 | BAYBURT |
| | | TRA2 | AĞRI | TRA21 | AĞRI |
| | | | | TRA22 | KARS |
| | | | | TRA23 | IĞDIR |
| | | | | TRA24 | ARDAHAN |
| **TRB** | ORTADOĞU ANADOLU | TRB1 | MALATYA | TRB11 | MALATYA |
| | | | | TRB12 | ELAZIĞ |
| | | | | TRB13 | BİNGÖL |
| | | | | TRB14 | TUNCELİ |
| | | TRB2 | VAN | TRB21 | VAN |
| | | | | TRB22 | MUŞ |
| | | | | TRB23 | BİTLİS |
| | | | | TRB24 | HAKKÂRİ |
| **TRC** | GÜNEYDOĞU ANADOLU | TRC1 | GAZİANTEP | TRC11 | GAZİANTEP |
| | | | | TRC12 | ADIYAMAN |
| | | | | TRC13 | KİLİS |
| | | TRC2 | ŞANLIURFA | TRC21 | ŞANLIURFA |
| | | | | TRC22 | DİYARBAKIR |
| | | TRC3 | MARDIN | TRC31 | MARDİN |
| | | | | TRC32 | BATMAN |
| | | | | TRC33 | ŞIRNAK |
| | | | | TRC34 | SİİRT |
| **TR1** | İSTANBUL | TR10 | İSTANBUL | TR100 | İSTANBUL |
| **TR2** | BATI MARMARA | TR21 | TEKİRDAĞ | TR211 | TEKİRDAĞ |
| | | | | TR212 | EDİRNE |
| | | | | TR213 | KIRKLARELİ |
| | | TR22 | BALIKESİR | TR221 | BALIKESİR |
| | | | | TR222 | ÇANAKKALE |
| **TR3** | EGE | TR31 | İZMİR | TR310 | İZMİR |
| | | TR32 | AYDIN | TR321 | AYDIN |

| | | | | | |
|---|---|---|---|---|---|
| | | | | TR322 | DENİZLİ |
| | | | | TR323 | MUĞLA |
| | | TR33 | MANİSA | TR331 | MANİSA |
| | | | | TR332 | AFYONKARAHİSAR |
| | | | | TR333 | KÜTAHYA |
| | | | | TR334 | UŞAK |
| **TR4** | DOĞU MARMARA | TR41 | BURSA | TR411 | BURSA |
| | | | | TR412 | ESKİŞEHİR |
| | | | | TR413 | BİLECİK |
| | | TR42 | KOCAELİ | TR421 | KOCAELİ |
| | | | | TR422 | SAKARYA |
| | | | | TR423 | DÜZCE |
| | | | | TR424 | BOLU |
| | | | | TR425 | YALOVA |
| **TR5** | BATI ANADOLU | TR51 | ANKARA | TR510 | ANKARA |
| | | TR52 | KONYA | TR521 | KONYA |
| | | | | TR522 | KARAMAN |
| **TR6** | AKDENİZ | TR61 | ANTALYA | TR611 | ANTALYA |
| | | | | TR612 | ISPARTA |
| | | | | TR613 | BURDUR |
| | | TR62 | ADANA | TR621 | ADANA |
| | | | | TR622 | MERSİN |
| | | TR63 | HATAY | TR631 | HATAY |
| | | | | TR632 | K.MARAŞ |
| | | | | TR633 | OSMANİYE |
| **TR7** | ORTA ANADOLU | TR71 | KIRIKKALE | TR711 | KIRIKKALE |
| | | | | TR712 | AKSARAY |
| | | | | TR713 | NİĞDE |
| | | | | TR714 | NEVŞEHİR |
| | | | | TR715 | KIRŞEHİR |
| | | TR72 | KAYSERİ | TR721 | KAYSERİ |
| | | | | TR722 | SİVAS |
| | | | | TR723 | YOZGAT |
| **TR8** | BATI KARADENİZ | TR81 | ZONGULDAK | TR811 | ZONGULDAK |
| | | | | TR812 | KARABÜK |
| | | | | TR813 | BARTIN |
| | | TR82 | KASTAMONU | TR821 | KASTAMONU |

| | | | | | |
|---|---|---|---|---|---|
| | | | | TR822 | ÇANKIRI |
| | | | | TR823 | SİNOP |
| | | TR83 | SAMSUN | TR831 | SAMSUN |
| | | | | TR832 | TOKAT |
| | | | | TR833 | ÇORUM |
| | | | | TR834 | AMASYA |
| **TR9** | DOĞUKARADENİZ | TR90 | TRABZON | TR901 | TRABZON |
| | | | | TR902 | ORDU |
| | | | | TR903 | GİRESUN |
| | | | | TR904 | RİZE |
| | | | | TR905 | ARTVİN |
| | | | | TR906 | GÜMÜŞHANE |

## EK-3: Anketin Web Sayfasının Ekran Görüntüleri

bilgiguvenligifarkindaligi.com



**Farklı Branşlardaki Öğretmenlerin Bilgi Güvenliği Farkındalığı Düzeylerinin Belirlenmesi Anketi**

**Sayın Hocam;**

Bu anket, Gazi üniversitesi Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı'nda yürütülen yüksek lisans programı kapsamında hazırlanmıştır. Araştırmada bilgi güvenliği farkındalık seviyelerini ölçmek hedeflenmektedir. Bu anketi online olarak dolduran kişinin mail adresi dahil hiçbir kişisel bilgisi araştırmacı tarafından görülememektedir. Bu doğrultuda kişisel bilgilerinizin üçüncü şahıslarla paylaşılması söz konusu değildir. Çalışmanın amacına ulaşması değerli katkılarınıza bağlıdır. Lütfen size en uygun olan seçeneği işaretleyiniz. Anketi cevaplama süresi ortalama 10 dk sürmektedir.

Kıymetli zamanınızı paylaştığınız için teşekkür eder, saygılar sunarım.

Arş. Gör. Gülsüm KAPANOĞLU

gulsumkapanoglu@gmail.com

Gazi Üniversitesi, Gazi Eğitim Fakültesi,
Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü,
Beşevler, Ankara, Türkiye

Ankete Başla

bilgiguvenligifarkindaligi.com/b1

**Farklı Branşlardaki Öğretmenlerin Bilgi Güvenliği Farkındalığı Düzeylerinin Belirlenmesi Anketi**

* Gerekli

**I. Kişisel Bilgiler**

**1. Cinsiyetiniz ***

- Kadın
- Erkek

**2. Yaşınız ***

- 21-30
- 31-40
- 41-50
- 51-60
- 61 ve üstü

**3. Yaşadığınız Şehir ***

**4. Eğitim Düzeyiniz ***

- Ön Lisans
- Lisans
- Yüksek Lisans
- Doktora

**5. Branşınız ***

**6. Görev Süreniz ***

- 0-4 yıl
- 5-9 yıl

## Farklı Branşlardaki Öğretmenlerin Bilgi Güvenliği Farkındalığı Düzeylerinin Belirlenmesi Anketi

### II. Güvenli Kullanım

**1. Bir Antivirüs yazılımı kullanıyor musunuz? ***

- Evet
- Hayır

**2. Bilgisayarınızda ne tür antivirüs yazılımı kullanırsınız?**

- Ücretsiz antivirüs yazılımı kullanırım
- Korsan (şifresi kırılmış) antivirüs yazılımı kullanırım
- Lisansı ödenmiş antivirüs yazılımı kullanırım
- Diğer

**3. Hangi sıklıkla virüs tarama yazılımlarını güncellersiniz? ***

- Günlük
- Haftalık
- Ayda bir kez
- Yılda bir kez
- Sadece kurduğum zaman
- Bilgisayarda yavaşlama olduğu zaman
- Diğer

**4. Spam mail nedir? ***

- Spam server tarafından gönderilen bir e-postadır
- Spam bir çeşit güvenlik duvarıdır
- Spam, istenmeyen postadır
- Spam bir email ekidir
- Spam, bilinen bir kişi tarafından gönderilen postadır

**5. Bankanızdan gelen e-postada, bilgilerinizi güncellemeniz için bir adrese tıklamanız istense ne yaparsınız? ***

- Eğer bankanın logo'su ve adresi doğru ise linki tıklarım
- Yakın arkadaşlarım bilgilerini güncellerse ben de aynısını yaparım
- e-mail hakkında bilgi almak için bankayı ararım



## Farklı Branşlardaki Öğretmenlerin Bilgi Güvenliği Farkındalığı Düzeylerinin Belirlenmesi Anketi

**Hiçbir Zaman <- 1 - 2 - 3 - 4- 5 -> Her Zaman**

Aşağıda Bilgi güvenliği ve Bilgi güvenliğine yönelik tutumlarınızı ölçmek amacıyla sorular sorulmaktadır.Size yöneltilen her soru için size en uygun seçeneği işaretleyiniz.(Size en çok uyan soru için Her zaman, uymayan sorular için Hiçbir zaman olmak üzere)

### III. Bilgi Güvenliği Farkındalığı

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| **1.** Kişisel bilgilerimin başkaları tarafından kötü amaçla kullanılabileceğini düşünürüm. | ○ | ○ | ○ | ○ | ○ |
| **2.** Bilgisayarım bir şifre ile korunur. | ○ | ○ | ○ | ○ | ○ |
| **3.** Parolalarımı sık sık değiştiririm. | ○ | ○ | ○ | ○ | ○ |
| **4.** Akıllı telefonum bir şifre ile korunur. | ○ | ○ | ○ | ○ | ○ |
| **5.** Parolalarımı yazılı olarak ulaşabileceğim bir yerde saklarım. | ○ | ○ | ○ | ○ | ○ |
| **6.** Bilgisayarımda lisanslı yazılım (orijinal) kullanmaya dikkat ederim. | ○ | ○ | ○ | ○ | ○ |
| **7.** Bütün hesaplarımda aynı parolayı kullanırım. | ○ | ○ | ○ | ○ | ○ |
| **8.** Kişisel bilgisayarımda otomatik kullan özelliğini kullanırım. | ○ | ○ | ○ | ○ | ○ |
| **9.** Kısa bir işim olsa dahi çalışırken ekran koruyucu kullanırım. | ○ | ○ | ○ | ○ | ○ |
| **10.** İnternetin herkese açık olduğu yerlerde internet bankacılığı kullanırım. | ○ | ○ | ○ | ○ | ○ |



*GAZİ GELECEKTİR…*