Savunma Bilimleri Dergisi
The Journal of Defense Sciences
Kasım / Nov 2020, Sayı/Issue 38.
ISSN (Basılı) : 1303-6831 ISSN (Online): 2148-1776

Ortaokul Öğrencilerinin Bilgi Güvenliği Farkındalığı

M. Ali DERİN [*] ve M. Tuncay GENÇOĞLU[**]

Öz

Bilişim teknolojileri hayatın her alanını etkilemiş, özellikle de eğitimde önemli değişimlere sebep olmuştur. Bu değişimden en çok etkilenen grupların başında ortaokul öğrencileri gelmektedir. Gerek okulda gerek evde bilişim teknolojilerini çok yaygın bir şekilde kullanırken, diğer taraftan bu değişime öğrencilerin ne kadar hazır olduğu konusu ise bilinmemektedir. Bu çalışmanın amacı; hızla gelişen teknolojinin şekillendirdiği bilgi toplumu içerisinde ortaokul öğrencilerinin bilgi güvenliği farkındalığının ölçülmesidir. Araştırmanın örneklemini 2019-2020 eğitim öğretim yılında Akkapı Şehit Kemal Yüzgeç Ortaokulu beşinci, altıncı ve yedinci sınıflarda eğitim gören 400 öğrenci oluşturmaktadır. Öğrencilere uygulanan "Bilgi Güvenliği Farkındalığı Anketi" 30 soru ve iki bölümden meydana gelmektedir. Birinci bölümü öğrencilerin sosyo-ekonomik düzeyleri ve kişisel bilgilerini belirleyen sorular, ikinci bölümü ise Bilgi Güvenliği Anketi soruları oluşturmaktadır. Uygulanan anket SPSS programı kullanılarak analiz edilmiştir. Pilot uygulama yapılarak anketin güvenirlik katsayı 0,699 olarak belirlenmiştir. Yapılan araştırmanın güvenirlik katsayısının 0,50'nin üzerinde olması nedeniyle güvenilir bir ölçme yapıldığı kabul edilmiştir. Öğrencilerin teknoloji kullanımlarının ve bilgi güvenliği farkındalıklarının; cinsiyet, yaş ve sınıf, internet kullanım süresi ve internet kullanım amacı değişkenlerine göre farklılaşıp farklılaşmadıklarını belirlemek amacıyla bağımsız örneklemler için t testi ve tek yönlü ANOVA analizi uygulanmıştır. Farklılığın anlamlı olduğu grupların tespiti için ise Scheffe testi kullanılmıştır. Analiz sonuçlarına göre; katılımcıların bilgi güvenliği farkındalıkları

[*] AYÜ Siber Güvenlik Tezsiz YL Öğrencisi, maliderin@gmail.com, ORCID: 0000-0003-1768-5117.
[**]Dr. Öğr. Üyesi, Fırat Üniversitesi Teknik Bilimler MYO, mt.gencoglu@firat.edu.tr, ORCID: 0000-0002-8784-9634

Geliş Tarihi/Received : 01.05.2020
Kabul Tarihi/Accepted : 18.09.2020
Araştırma Makalesi/Research Article
DOI: 10.17134.khosbd.813459

arasında; cinsiyet, yaş, sınıf, internette geçirdiği süre ve interneti kullanmadaki amaç değişkenlerine göre farkın anlamlı olduğu görülmektedir.

Anahtar Kelimeler: *Bilişim Teknolojileri, Bilgi Güvenliği, Bilgi Güvenliği Farkındalığı.*

Information Security Awareness of Secondary School Students

Abstract

Information technologies have affected every area of life and have caused important changes especially in education. Secondary school students come first among the groups that are most affected by this change. As the use of information technologies is spreading rapidly both at school and at home, it is not known how ready students are for this change. The purpose of this study is the measurement of information security awareness of secondary school students within the information society shaped by the rapidly developing technology. The subjects of the study consist of 400 students studying in the fifth, sixth, and seventh grades of Akkapı Şehit Kemal Yüzgeç Secondary School in the 2019-2020 academic year. Information and Awareness Survey, with 30 questions and two parts, was applied to students. The first part contains the questions determining the socio-economic levels and personal information of the students and the second part includes the Information Security Questionnaire. The applied questionnaire was analyzed using the SPSS program. The reliability coefficient of the questionnaire was determined as 0.699 with a pilot application. Since the reliability coefficient of the research was over 0.50, it was accepted that a reliable measurement was made. Students' technology usage and information security awareness; t-test and one-way ANOVA analysis were applied for independent samples to determine whether they differ according to gender, age, and class, for the duration of internet usage and internet usage purpose. The Scheffe test was used to determine the groups in which the difference was significant. As a result of the results of the analysis among the information security awareness of the participants; accounting the variables of gender, age, class, time spent on the internet and the purpose of internet usage, it is seen that the difference was meaningful.

Keywords: *Information Technology, Information Security, Information Security Awareness.*

Giriş

Teknoloji, insanlık tarihi boyunca hayatın her alanında toplumların yaşam şeklini değiştirmiş, çağdaşlaşmanın ana unsuru olmuştur. Teknolojinin eğitimde, sağlıkta, üretimde ve sanayide kullanılmasıyla insan ve toplum yaşamında devrimsel nitelikte bir değişim yaşanmıştır. Bilişim teknolojilerinin ilerlemesi ile insanlık tarihinde insan ve makine gücü yerini bilişim teknolojilerine devretmiştir. Bilgi çağı olarak adlandırılan bu dönemde bilişim teknolojilerinin etkisi ile kültürel anlamda değişim de başlamıştır. Her teknoloji insan ve toplum yapısında önemli değişikliklere yol açmıştır. Bilişim teknolojileri ve özellikle internetin yaygınlaşması ile eğitimde bu teknolojilerin kullanılması kaçınılmaz olmuştur. Dolayısıyla bu gelişmeden en çok etkilenen tarafın öğrenciler olduğu bir gerçektir. Öğrenciler gerek okulda gerek evde yaşamın her alanında teknolojiye oldukça bağımlı hale gelmişlerdir. Teknolojinin öğrenciler tarafından bu kadar etkin kullanımı söz konusu iken bilgi güvenliği konusunun öğrenciler tarafından ne kadar önemsendiği ise merak konusudur.

1. Problem

Yapılan araştırmalar içinde bulunduğumuz çağda hayatlarının her alanında teknolojinin bütün nimetlerinden faydalanan bireylerin, bilgi güvenliği kavramı ile de mücadele etmelerinin gerektiğini göstermektedir. Çağlar boyunca korunmaya çalışılan doğru bilgiye hızlı ve zamanında ulaşmak bireyler için vazgeçilmez olmuşken, tehdit yaratabilecek unsurlar da yavaş yavaş hayatımıza girmiştir. Bilgi güvenliğinde insan faktörü güvenliğin garantilenmesinde kilit durumdadır. Bu noktada toplumun bilgi güvenliği farkındalığının oluşturulması şarttır. Literatürdeki çalışmalar incelendiğinde, bilginin önemi üzerinde durulmuş ve bilgi güvenliğine kasteden saldırıların, gün geçtikçe hem sayı hem de çeşitlilik bakımından arttığı bir ortamda etkin bir şekilde bilgi güvenliğinin sağlanabilmesi için gerekli olan güvenlik süreçleri özetlenmiştir (Canbek ve Sağıroğlu, 2006: 165). Yapılan araştırmalar göstermektedir ki bilgi güvenliği farkındalığı öncelikle okullarda yapılacak eğitim çalışmaları ile erken yaşta oluşturulmaya başlanmalıdır. Bilişim teknolojileri dersi müfredatında bu konuya daha fazla yer verilmeli, okullarda bilgi güvenliği konusunda sosyal kulüpler kurulması ve seminer çalışmaları yapılması sağlanmalıdır.

Bu çalışmada, öğrencilerin teknolojiyi kendilerine ne kadar adapte ettikleri ve teknolojiyi kullanırken karşılaştıkları güvenlik tehditleri karşısındaki farkındalık seviyeleri ölçülmeye çalışılmıştır. Bu çalışma ortaokul öğrencilerinin teknolojiyi kullanırken maruz kaldığı tehlikelerin görülmesi ve gerekli önlemlerin alınması açısından önem arz etmektedir.

2. Araştırmanın Amacı

Bu araştırmanın amacı, ortaokul öğrencilerinin bilgi güvenliği farkındalığını belirlemektir. Bu amaç doğrultusunda; öğrencilerin bilgi güvenliği farkındalıkları tespit edilmiş ve bilgi güvenliği farkındalığı üzerinde yaş, cinsiyet ve sınıf düzeyinin etkisi araştırılmıştır.

3. Kavramsal Çerçeve

Bu bölümde; ortaokul öğrencilerinin bilgi güvenliği farkındalığının önemini anlayabilmek için teknolojinin hayatımızdaki yeri, teknolojinin ortaokul öğrencilerinin hayatındaki yeri, bilginin önemi, bilginin gerekliliği, bilgi gizliliğinin önemi ve bilgi güvenliği farkındalığı ile ilgili çalışmalar üzerinde durulmuştur.

Bilgi Güvenliği

Kişilerin değerleri, barındırdıkları bilgi ile değerlendirilmektedir. Bireyler için bu kadar önemli olan ve her ortamda bulunan bir varlığın korunması ve onun güvenliğinin sağlanması olmazsa olmaz şartlardandır. Bilgi güvenliği, bilgi ve iletişim teknolojilerini de dikkate alarak şu şekilde tanımlanabilir; "bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önlemektir" (Canbek ve Sağıroğlu, 2006:165). Bilişim alanında en kritik konu bilgi güvenliğinin sağlanmasıdır. Bu nedenle bilgi güvenliği, bilginin izinsiz ya da yetkisiz bir şekilde erişim, kullanım, değiştirilme, ifşa edilme, ortadan kaldırılma, el değiştirme ve hasar verilmesini önlemek olarak tanımlanır. Ayrıca bilgi güvenliği; gizlilik, bütünlük ve erişilebilirlikten oluşan üç temel unsurdan mütevellittir. Bu üç temel güvenlik unsurundan herhangi biri zarar görürse, güvenlik zaafiyeti oluşur.

- Gizlilik (Confidentiality): Bilginin yetkisiz kişilerin eline geçmesinin ve yetkisiz erişilmesine karşı korunmasıdır.

- Bütünlük (Integrity): Bilginin yetkisiz kişiler tarafından değiştirilmemesidir.
- Erişilebilirlik (Availability): Bilginin yetkili kişilerce ihtiyaç duyulduğunda ulaşılabilir ve kullanılabilir durumda olmasıdır.

Yukarıda bahsettiğimiz bu üç temel unsur birbirleriyle ilişkili olarak düşünülmelidir. Bilgi gizliliğinin sağlanması bilginin erişilebilirliğini engellememekle birlikte aynı zamanda erişilebilen bilginin bütünlüğünün de korunması gerektiği anlamına gelmektedir. Bilginin gizliliği sağlanırken bilgiye erişim de engelleniyor ise bu bilgi kullanılamaz durumda olacağından bu bilginin bir değeri yoktur. Diğer taraftan erişim sağlanıyor ama bütünlük sağlanmıyor ise yanlış ya da eksik bilgi ihtimali olacağından ve olumsuz sonuçlar doğurabileceğinden yine bu bilginin bir değeri olmayacaktır. Bu nedenlerden dolayı bilgi güvenliği, temel olarak yukarıda ifade edilen üç unsurun bir arada bulunmasıyla mümkündür denebilir (Fussell, 2005:297).

1. Bilgi Güvenliğini Tehdit Eden Unsurlar

Bilişim alanında yeni teknolojilerin kullanılması toplumlara olabildiğince fazla yarar sağlamakla birlikte birtakım sorunları da beraberinde getirmektedir. Suç işlemenin kolaylaştığı bu ortamlarda, modern bilgi çağının istenmeyen bir ürünü olarak bilişim suçları da ortaya çıkmıştır. Bilgisayar korsanları; şirketlerin, bankaların, kamu kurumlarının sistemlerine sızarak büyük zararlar vermekte, bilgisayar ortamındaki bilgileri kullanılamaz hale getirmekte veya bu bilgileri kendilerininmiş gibi kullanarak bilişim suçu işleyebilmektedir. Bilişim teknolojileri topluma oldukça fazla fayda sağlamakla beraber, birçok tehdit de içermektedir. Tehdit, "bir sistemin veya kurumun zarar görmesine neden olan istenmeyen bir olayın arkasındaki gizli neden" olarak tanımlanabilir. Bununla birlikte internetteki olası tüm tehditlerin kökeninde gerçek hayatta da var olan tehditler yer almaktadır. Bu hususta tehditlerin bertarafı için toplum eğitilmeli ve bu konuda farkındalık oluşturulmalıdır. Tehditlerin bilişim sistemlerinde etkili olabilmesinin yolu bu sistemler üzerinde var olan açıklıkları ve zafiyetleri kullanmalarından geçer. Tehditlerin bilgi varlıklarına etkisi, tehlikenin oluşma olasılığı, bilgi varlığı üzerindeki zayıflıklar ve açıklar, varlığın değeri ile doğru orantılıdır. Tehditler ortamda uygun şartların oluşmasıyla bilgi sistemlerine zarar verecek kusurlar barındıran zafiyetlere yol açarlar. Bu zafiyetler de saldırganlar tarafından

kullanıldığında güvenlik ihlallerine sebep olup bilgi sitemlerine zarar vermelerine kapı aralarlar. Bunlara örnek olarak; doğal afetler neticesinde oluşabilecek; güç kaynaklarının, kamera sistemlerinin, telefon santrallerinin arızalanması, yazılım ve donanım hataları gibi engellenmesi zor olan tehditler verilebilir (Vural, 2007).

Yazılım tehditlerinin başlıca amacını ise şu şekilde özetleyebiliriz; yetkisiz olarak sisteme erişim, sistemi kullanılamaz kılmak, hizmetin engellenmesi, bilginin değiştirilmesi ve ortadan kaldırılması, bilgilerin açık edilmesi ve ele geçirilmesi (Ünver, Canbay ve Mirzaoğlu, 2009). Başlıca yazılım tehditleri şunlardır;

Hizmetin Engellenmesi Saldırıları (DDoS - Distributed Denial of Service); iletişim sistemlerini aşırı şekilde yüklenme ile devre dışı bırakmak için yapılan saldırılara verilen isimdir (Krause ve Tipton, 2007).

Truva Atı (Trojan); genellikle lisanslı programların yasa dışı kopyaları, mp3, oyun ve cinsel içerik indiren kullanıcıların indirdikleri içeriklere ekli olarak gelen dosyalar aracılığıyla bulaşan ve bilişim güvenliğine zarar veren programlardır (Krause ve Tipton, 2007).

Solucanlar (Worms); çoğalan, birbirinden bağımsız olarak çalışabilen ve ağ bağlantıları üzerinde hareket etme kabiliyetine sahip programlara verilen isimdir. Virüs ve solucanlar arasındaki temel farklılık ise; solucanların virüslerin aksine taşıyıcı bir dosyaya ihtiyaç duymamalarıdır (Nickolov, 2008).

Virüsler (Virus); e-postalar ve dosyalar aracılığı ile taşınarak bilgisayarların çalışmasını engelleyen, bilgilerin kaybolması, bozulması veya silinmesine sebep olan programlara verilen isimdir (Cohen, 1987: 22).

Bir sistemde virüs olduğunu anlamak için aşağıdaki belirtilere dikkat edilmelidir;

- İnternette işlem yapılmadığı zamanlarda başka kullanıcıların sistemde zarar verme amacıyla aktif olması,
- Güvenlik duvarı kurulu olmasına rağmen, bazı uygulamaların sisteme bağlanmak için zorlamaları,
- İnternette sörf yaparken reklam pencerelerinin açılması,
- Bilgisayarın düzgün çalışmaması,
- Telefonlardaki zararlı yazılımlar,
- Banka hesabına yetkisiz olarak erişim, kredi kartının habersiz kullanımı ya da herhangi bir casus yazılımın sisteme girişi (Nickolov, 2008).

Bir sisteme virüsün bulaşmasını önlemek için güncel bir antivirüs programıyla sistem taranmalıdır. Taramanın sonucunda bir virüs ya da truva atının tespiti halinde

virüslü dosyanın bir kopyasının antivirüs programı üreticisine iletilmesi, bu tür saldırılara karşı daha hızlı bir korumanın geliştirilmesine ve başka kullanıcıların da bu tür saldırılardan korunmasına vesile olacaktır (Nickolov, 2008).

Reklam Destekli Yazılımlar (Adware); belli firmaların reklamlarını yazılan programın içine yerleştirerek kullanıcının bu reklamlara yönlendirilmesini mümkün kılan uygulamalara verilen genel isimdir (Krause ve Tipton, 2007).

Casus Yazılımlar (Spyware); kullanıcının bilgisayarın da belirli firmaların reklamlarını görüntüleyerek bu sırada da bilgisayarda yapılan faaliyetleri belirli bir sunucuya gönderen programların ismidir (Krause ve Tipton, 2007).

Sazan Avlama (Phishing); internet kullanıcılarının aldatılması ya da inandırılması suretiyle sahte e-postalarla şahsa özel veriler ve kredi kartı bilgileri gibi gizli verilerin çalınması şeklinde bir sahtekârlık metodudur (Turhan, 2010). Ayrıca sosyal medya uygulamaları da sazan avlama (Phishing) ataklarından önemli derecede etkilenmektedir (APWG, 2019). Sazan avlama türü sahtekârlıklara maruz kalmamak için kimlik numarası, banka hesap numarası, kredi kartı numarası, kontrol şifresi, parola gibi önem arz eden şahsi bilgilerin yazılacağı ara yüzlerin güvenilirliği kontrol edilmelidir. Ayrıca sahte olduğu düşünülen mesajların ilgili yerlere bildirilmesi faydalı olur (Turhan, 2010).

Bu türden sahtekârlık faaliyetlerine karşı;

- İnternet bankacılığı işlemlerinde sanal klavye kullanılarak bilgi girişi, değişken karmaşık tuşlar ve tek kullanımlık SMS ile şifre gönderilmesi gibi uygulamaları tercih etmek güvenliğin teminat altına alınması açısından mühimdir. Bankalardan geldiği düşünülen e-postaların içerisindeki bağlantı aracılığıyla işlem yapılmamalı, kişisel bilgiler paylaşılmamalıdır.
- Lisanslı yazılımların şifrelerinin illegal olarak geçersiz kılınması amacıyla kullanılan aynı zamanda "crack" adıyla da bilinen yazılımların Truva atı, virüs gibi kötücül yazılımları da sisteme iliştirme olasılığı yüksektir. Buna ilaveten cracklar ile kullanılmaya devam edilen yazılımlar, güncellemeler tam ve doğru yapılmayacağından, düzgün çalışmayacaktır.
- Çevrimiçi alışverişlerde kullanılan sitelerin güvenli olup olmadıkları kontrol edilmelidir.
- Otomatik para çekme cihazları (ATM) kullanılırken dikkatli olunmalıdır. Bu cihazlara sahte tuşlar, kart okuyucu ve kamera gibi düzenekler yerleştirilebilmektedir.

- Kredi kartı ile ödeme yapılırken dikkatli olunmalıdır.
- Çevrimiçi ve anlık bellekler yardımıyla edinilen dosya ve programların virüs taramasından geçirilmesi oldukça önemlidir (Turhan, 2010).

İstem Dışı Elektronik Postalar (Spam); ihtiyacı olmayan kişilere birden çok kopyasını göndererek ticari olarak reklam yapmayı amaçlayan e-postalardır. Bugün için en büyük problemlerin başında e-postalar gelmektedir. Özellikle de istenmeyen mesajlar, zarar verme niyetiyle olmasalar dahi kontrolü ve ayıklanması ciddi bir zaman kaybıdır. Bununla birlikte sistem kaynaklarının etkin olarak kullanılmasına engel oluşturmaktadır. İstenmeyen mesajlar dolandırıcılık, sahtecilik ve kötü niyetli yazılımların yayılmasına da neden olmaktadır (Öztürk, 2009).

Zincir E-posta ve İnternet Aldatmacası (Hoax); birden fazla kişinin birbirine gönderdiği sömürü içerikli mesajların, gönderilenin listesindeki diğer kişilerle paylaşılması istenen mesajlardır. İnternet aldatmacası ise bir kurum, kuruluş ya da tanınmış bir kişi hakkında gerçek olmayan bilgiler ve haberler uydurarak zarara uğratmak, şahsi ya da toplumsal güvenliği tehdit eden bir ortamın olduğu algısı yayarak kargaşa oluşturmaktır. Zincir mesajlar ve internet aldatmacalarının temel amacı, iletilerin olabildiğince fazla sayıda şahsa iletilmesini sağlayıp, kişilerin e-posta adreslerinin ele geçirilmesidir. Bu şekilde elde edilen e-posta adresleri, üçüncü taraflara para karşılığı verilmekte ya da istenmeyen mesajların gönderilmesinde kullanılmaktadır (Schryen, 2007).

Diğer bir güvenlik tehdidi de insan kaynaklı tehditlerdir. Bu tehditler kullanıcının yeterli bilgi ve eğitime sahip olmadan bilinçsiz bir şekilde sisteme girmesi ya da sisteme zarar vermek maksadıyla yapılan eylemelerin sonucu ortaya çıkan tehditlerdir (Tekerek, 2008:132). İnterneti kullanan bireyler sanal ortamlarda cinsel istismar, müstehcenlik, rahatsız edilme, bağımlılık, kötü alışkanlıklar edinme, olumsuz etkilenme, kişisel bilgileri paylaşma ve özel hayata dair içeriklerin yayınlanması gibi ciddi problemlerle karşı karşıya kalmaktadırlar (Öztürk, 2009). Günümüzde internet kullanıcılarının yaklaşık %80'lik kısmı için olmazsa olmazlar arasında olan e-mail, internet bankacılığı, çevrimiçi alışveriş gibi birçok uygulama alanları, kötü niyetli kişi ve kurumlar tarafından suistimal edilmektedir (Arifoğlu, Kömes, Yazıcı, Akgül ve Ayvalı, 2002). İnternet bankacılığının güvenliğini tesis edecek en önemli unsurlar arasında önceliği kişiye özel verilen kullanıcı adı ve şifreler almaktadır. İnternet bankacılığı kullanıcısı mutlak suretle kullanıcı adı ve şifresinin bir başkası tarafından öğrenilmesini ve kullanılmasını engellemek için

tedbir almalıdır. Siber atakların ve siber saldırganların sayısı gün geçtikçe katlanarak artmaktadır. Bu artış kişilerin, kuruluşların, devletlerin ve siber ortamın güvenliği ve güvenilirliği açısından büyük problemlere yol açmaktadır. Siber güvenliğin garanti altına alınması bireysel bilgilerin ve özel hayatın güvence altına alınmasında, kritik altyapıların güvenliğinin ve güvenilirliğinin oluşturulmasında ve siber suçlarla mücadelede hayati öneme haiz bir öğedir (Turhan, 2010).

2. Bilgi Güvenliği Farkındalığı

Dünyada bilgi güvenliği farkındalığını oluşturmak için yapılan çalışmalara bakıldığında, ders içeriklerinin müfredatlara eklenmesi, bilgi güvenliği konusunda komisyonlar kurulması ve güvenliğe dikkat çekecek günler düzenlenmesi gibi etkinlikler yer alır. İngiltere ilköğretim müfredatında internetin güvenli kullanımı zorunlu bir ders olarak yer almaktadır. Daha önceden yalnızca ortaokul çağındaki öğrencilere verilen internetin güvenli kullanımı eğitimi günümüzde tüm ilköğretim çağındaki öğrencilere ders olarak verilmektedir (Ulaşanoğlu, Yılmaz ve Tekin, 2010).

2004 yılında bilgi güvenliği konusunda Avrupa koordinasyonunu sağlamak ve geliştirmek amacıyla Avrupa Şebeke ve Bilgi Güvenliği Kurumu (Europa Network and Information Security Agency - ENISA) kurulmuştur. Bilgi ve iletişim güvenliği hususunda temel güvenlik ihtiyaçlarının karşılanması için komisyona ve üye devletlere gerekli olan bütün katkıyı ve desteği sağlamakla görevlendirilen ENISA, bilgi güvenliği ile ilgili tüm taraflar ve aktörler arasında uluslararası işbirliğinin geliştirilmesine katkıda bulunmak üzere faaliyetlerini sürdürmektedir (Ulaşanoğlu, Yılmaz ve Tekin, 2010).

Diğer taraftan Birleşmiş Milletlere bağlı ITU (www.bilgiguvenligi.gov.tr) ve www.guvenliweb.org.tr gibi internet sayfaları aracılığıyla da farkındalık bilinçlendirme adına faaliyetler icra edilmektedir. Çocukların çevrimiçi ortamlarda korunmasını ana tema olarak benimseyerek, bu çerçevede Çocukların Çevimiçi Korunması (Child Online Protection – COP) etkinliği de yürütülmektedir. Bu etkinlik sınırları dâhilinde çevrimiçi ortamla ilgili tüm taraflara yönelik farkındalık, bilgilendirme ve bilinçlendirme faaliyetleri icra edilmeye başlanmıştır. Bu bağlamda internetin güvenli ve bilinçli kullanımı hususunda çocukların, gençlerin ve ailelerin bilinçlendirilmesi için basılı ve görsel yayımlar hazırlanmıştır. Tüm bunlara ilave olarak ülkemizde de Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından

çocukların interneti güvenli ve bilinçli kullanmalarına yönelik bir kitapçık hazırlanarak, toplam 12 milyon adet basılmış ve tüm ilköğretim öğrencileri ile öğretmenlere dağıtılmıştır. 2005 yılında Tunus'ta Bilgi Toplumu Zirvesi adıyla düzenlenen etkinlikte, internet güvenliğinin, sürekliliğinin ve istikrarının önemine vurgu yapılmış, interneti ve diğer Bilgi İletişim Teknolojileri ağlarını tehlikelerden ve güvenlik açıklarından korumanın hayati bir ihtiyaç olduğu deklare edilmiştir. Tüm bu gelişmeler şunu göstermektedir ki; siber güvenlik kültürünün ve farkındalığının oluşturulması ulusal olarak da hayati bir rol üstlenmektedir (Ulaşanoğlu, Yılmaz ve Tekin, 2010).

Metot

Bu bölümde araştırmanın modeli, örnek uzay ve örneklem, veri toplama araçları, ölçme aracının puanlaması ve verilerin incelenmesi üzerinde durulacaktır.

1. Araştırmanın Modeli

Toplumun gelişen bilişim teknolojileri ile bilgi ve iletişim kültürüyle ne kadar uyum içinde olduğunun belirlenmesi ve bu kültürle beraber bilgi güvenliği farkındalığının belirlenmesi amacıyla yürütülen bu çalışma gözden geçirme modeli niteliğinde tanımlayıcı bir çalışmadır.

Gözden geçirme modeli ile yapılan araştırmaların iki sınırlılığı vardır. Bu sınırlılıklar, veri bulma ile kontrol güçlükleridir. Çünkü tarama modeli ile yapılan araştırmalarda çok sayıda nesne ya da denek grubu kullanılmalıdır ve bu gruba belirli bir zaman diliminde ulaşmak oldukça güçtür.

2. Örnek Uzay ve Örneklem

Araştırmanın çalışma evrenini, Adana ili Seyhan İlçesi Akkapı Şehit Kemal Yüzgeç Ortaokulu öğrencileri oluşturmaktadır. Evrenin geniş olması sebebi ile örneklem uygulaması yapılmıştır. Araştırma, araştırmacı tarafından ulaşılması basit, olasılıksız örnekleme uygun olarak belirlenmiştir. Çalışma grubunu ortaokul 5-6-7 ve 8. sınıf öğrencileri oluşturmuştur.

3. Veri Toplama Araçları

Araştırmada Adana ili Seyhan İlçesi Akkapı Şehit Kemal Yüzgeç Ortaokulu öğrencilerinin bilgi güvenliği farkındalığını belirlemek için 30 sorudan oluşan bir anket hazırlanmıştır. Öğrencilere uygulanan "Bilgi Güvenliği Farkındalığı Anketi"

30 soru ve iki bölümden oluşmaktadır. Birinci bölümü öğrencilerin sosyo-ekonomik düzeyleri ve kişisel bilgilerini belirleyen sorular, ikinci bölümü ise Bilgi Güvenliği Anketi soruları oluşturmaktadır. Anket geliştirilirken bir grup öğrenci üzerinde pilot uygulama yapılmış ve anketin güvenirlik katsayısı (Cronbach Alpha) 0,699 olarak hesaplanmıştır. Yapılan çalışmanın güvenirlik katsayısı 0,50'nin üzerinde olduğundan anketin oldukça güvenilir bir ölçüm yaptığı kabul edilmiştir.

4. Verilerin Toplanması

Araştırma için yapılan planlama dâhilinde Akkapı Şehit Kemal Yüzgeç Ortaokulu öğrencilerden 400 tanesine okul bilişim teknolojileri sınıfında birebir ve çevrimiçi olacak şekilde Bilgi Güvenliği Belirleme Anketi uygulanmıştır.

5. Verilerin Analizi

Verilerin analizi ile ortaokul öğrencilerinin hızla gelişen teknoloji karşısında bilgi güvenliği konusunda ne seviyede olduğu belirlenecektir. Araştırmaya dâhil olan 400 öğrencinin sonuçları SPSS programında analiz edilerek tablolar oluşturulmuştur. Oluşturulan dağılım ve frekans tablolarında öğrencilerin bilgi güvenliği farkındalık seviyeleri araştırılmıştır. Ankette “Evet” cevabı 1, “Bazen” cevabı 2, “Hayır” cevabı 3 puan olarak belirlenmiştir. Bu analizde yüksek puan alan öğrencilerin bilgi güvenliği farkındalık seviyeleri düşük olarak kabul edilecektir. Araştırmada çıkan sonuçlarda ortaokul öğrencilerinin bilgi güvenliği farkındalıklarının ne seviyede olduğu belirlenmeye çalışılmış ilk başta verilerin normal bir dağılıma sahip olup olmadığı incelenmiş ve Shapiro Wilk testinin uygulanması sonucunda $p>0,05$ olduğu görülmüş ve verilerin homojen bir dağılıma sahip olduğu tespit edilmiştir.

Bulgular ve Yorum

1. Kişisel Bilgiler Anketiyle İlgili Sonuçlar

Öğrencilerin cinsiyet, yaş, sınıf, internet kullanım süresi, internet kullanım amacı, bilgisayar, tablet ve cep telefonu, internet, sosyal medya hesabı sahip olup olmaması ile ilgili elde edilen sonuçlar Tablo 1’de görülmektedir.

Tablo 1. Kişisel Bilgiler Tablosu

		Sayı	**Toplam N %**
Cinsiyet	Kız	194	48,5
	Erkek	206	51,5
	Toplam	400	
Yaş	10	82	20,5
	11	113	28,2
	12	119	29,8
	13	86	21,5
	Toplam	400	
Sınıf	5	100	25
	6	100	25
	7	100	25
	8	100	25
	Toplam	400	
Pc	Var	196	49
	Yok	204	51
	Toplam	400	
Cep Telefonu	Var	182	45,5
	Yok	218	54,5
	Toplam	400	
Tablet	Var	204	51
	Yok	196	49
	Toplam	400	
İnternet	Var	292	73
	Yok	108	27
	Toplam	400	
Kaç Saat	1’den az	144	36
	1-2 arası	135	33,8
	2-3 arası	71	17,8
	3’ten fazla	50	12,5
	Toplam	400	
Sosyal Medya	Var	220	55
	Yok	180	45
	Toplam	400	
Kullanım Amacı	ÖdevAraştırma	203	50,7
	Sosyal Medya	6	16,8
	Oyun	130	32,5
	Toplam	400	

Tablo 1'de görüldüğü gibi cinsiyet ve sınıf değişkenlerinin homojen dağılıma sahip olduğu, her iki öğrenciden birinde bilgisayar, cep telefonu veya tablet olduğu görülmektedir. Ayrıca çoğu öğrencinin internet erişiminin mevcut olduğu, çoğunlukla da interneti ödev ve araştırma yapmak için kullandığı ve interneti 1 saatten az veya 1-2 saat süreyle kullandığı görülmektedir.

2. Bilgi Güvenliği Anketiyle İlgili Sonuçlar

Öğrencilerin bilgi güvenliği farkındalıklarını belirlemek üzere uygulanan analizler aşağıdaki gibidir.

a. Cinsiyet Değişkenine Göre Bilgi Güvenliği Farkındalığı

Cinsiyete göre bilgi güvenliği farkındalığında farkın anlamlı olup olmadığını tespit etmek için bağımsız örnekleme t-testi uygulanmış ve sonuçların analizi yapılmıştır. Bu analiz sonuçları Tablo 2'deki gibidir.

Tablo 2. Cinsiyet Değişkenine Göre Bağımsız Örneklem t-Testi Sonuçları

		Varyans Eşitliği için Levene Testi		Ort. Eşitliği için t-Testi				
		F	Sig.	t	df	Sig.	Ort. Farkı	Std. Hata Farkı
Anket Puanı	Varyanslar Eşit	0,451	0,502	2,986	398	0,003	0,07439	0,02491
	Varyanslar Eşit Değil			2,983	394,428	0,003	0,7439	0,02494

Tablo 2 incelendiğinde Sig<0,05 olduğu görülmektedir. Buna göre öğrencilerin cinsiyetlerine göre bilgi güvenliği farkındalıklarının anlamlı bir şekilde değiştiği görülmektedir.

Cinsiyet değişkenine göre öğrenciler arasındaki farkı görmek için yapılan bağımsız örneklem t-testi grup istatistiği Tablo 3'te verilmiştir.

Tablo 3. Cinsiyete Göre Bağımsız Örneklem t-Testi Grup İstatistiği Sonuçları

Cinsiyet		N	Ort.	Std. Sapma	Std.Hata Ort.
Anket Puanı	Kız	194	2,5479	0,25346	0,01820
	Erkek	206	2,4735	0,24473	0,01705

Cinsiyet değişkenine göre öğrenciler arasındaki farkı görmek için yapılan bağımsız örneklem t testi grup istatistiğine göre ortalaması yüksek olan kız öğrencilerin erkek öğrencilere oranla bilgi güvenliği farkındalık seviyesinin yüksek olduğu görülmektedir.

b. Yaş Değişkenine Göre Bilgi Güvenliği Farkındalığı

Öğrencilerin yaş düzeylerine göre bilgi güvenliği farkındalığında anlamlı bir fark olup olmadığını tespit etmek için tek yönlü ANOVA analizi yapılmış ve elde edilen sonuçlar Tablo 4'te verilmiştir.

Tablo 4. Yaş Değişkenine Göre Tek Yönlü ANOVA Analizi Sonuçları

Anket Puanı					
	Kareler Top.	df	Ort. Kare	F	Sig.
Gruplar Arası	1,382	3	0,461	7,648	0,000
Gruplar İçi	23,849	396	0,060		
Toplam	25,230	399			

Tablo 4 incelendiğinde Sig<0,05 olduğu görülmektedir. Buna göre öğrencilerin yaşlarına göre bilgi güvenliği farkındalıklarının anlamlı bir şekilde değiştiği görülmektedir.

Yaş grupları arasındaki farkı incelemek için uygulanan Scheffe testi sonuçları ise Tablo 5'te görülmektedir.

Tablo 5. Yaş Değişkenine Göre Scheffe Testi Sonuçları

(I) Yaş	(J) Yaş	Ort. Fark (I-J)	Std.Hata	Sig.	%95 Güven Aralığı	
					Alt Sınır	Üst Sınır
10	11	-0,10900	0,03471	0,021	-0,2064	-0,0116
	12	-0,3950	0,03471	0,730	-0,1369	0,0579
	13	0,05200	0,03471	0,524	-0,0454	0,1494
11	10	0,10900	0,03471	0,021	0,0116	0,2064
	12	0,06950	0,03471	0,262	-0,0279	0,1669
	13	0,16100	0,03471	0,000	0,0636	0,2584
12	10	0,03950	0,03471	0,730	-0,0579	0,1369
	11	-0,06950	0,03471	0,262	-0,1669	0,0279
	13	0,09150	0,03471	0,075	-0,0059	0,1889
13	10	-0,05200	0,03471	0,524	-0,1494	0,0454
	11	-0,16100	0,03471	0,000	-0,2584	-0,0636
	12	-0,09150	0,03471	0,075	-0,1889	0,0059

Scheffe testi sonuçları incelendiğinde 11 yaş grubu öğrencilerin 13 yaş grubu öğrenciler lehine istatistiksel olarak anlamlı (Sig<0,01) bir farklılık saptanmıştır. Bu durum 10-11 yaş öğrenci grubunun bilgi güvenliği farkındalığı konusunda bilinçlendirilmesi gerektiğini göstermiştir. 12-13 yaş grubunda ise benzer bir ortalama olduğu görülmektedir.

c. Sınıf Değişkenine Göre Bilgi Güvenliği Farkındalığı

Sınıf düzeyine göre bilgi güvenliği farkındalığında anlamlı bir fark olup olmadığını tespit etmek için tek yönlü ANOVA analizi yapılmış olup bu testin sonuçları da Tablo 6'da verilmiştir.

Tablo 6. Sınıf Değişkenine Göre Tek Yönlü ANOVA Analizi Sonuçları

Anket Puanı					
	Kareler Top.	df	Ort. Kare	F	Sig.
Gruplar Arası	1,382	3	0,461	7,648	0,000
Gruplar İçi	23,849	396	0,060		
Toplam	25,230	399			

Tablo 6 incelendiğinde (Sig<0,05) öğrencilerin sınıflara göre bilgi güvenliği farkındalıklarının anlamlı bir şekilde değiştiği görülmektedir.

Öğrencilerin sınıf düzeyine göre aralarındaki farkı incelemek için uygulanan Scheffe testi sonuçları ise Tablo 7'deki gibidir.

Tablo 7. Sınıf Değişkenine Göre Scheffe Testi Sonuçları

		Ort. Fark	Std.Hata	Sig.	%95 Güven Aralığı	
(I) Yaş	(J) Yaş	(I-J)			Alt Sınır	Üst Sınır
5	6	-0,10900	0,03471	0,021	-0,2064	-0,0116
	7	-0,3950	0,03471	0,730	-0,1369	0,0579
	8	0,05200	0,03471	0,524	-0,0454	0,1494
6	5	0,10900	0,03471	0,021	0,0116	0,2064
	7	0,06950	0,03471	0,262	-0,0279	0,1669
	8	0,16100	0,03471	0,000	0,0636	0,2584
7	5	0,03950	0,03471	0,730	-0,0579	0,1369
	6	-0,06950	0,03471	0,262	-0,1669	0,0279
	8	0,09150	0,03471	0,075	-0,0059	0,1889
8	5	-0,05200	0,03471	0,524	-0,1494	0,0454
	6	-0,16100	0,03471	0,000	-0,2584	-0,0636
	7	-0,09150	0,03471	0,075	-0,1889	0,0059

Scheffe testi sonuçları incelendiğinde 6. sınıf öğrenciler ile 8. sınıf öğrenciler arasında, 8. sınıf öğrencilerin lehine istatistiksel olarak anlamlı (Sig<0,01) bir farklılık saptanmıştır. Bu durum 6. sınıf öğrenci grubunun bilgi güvenliği farkındalığı konusunda bilinçlendirilmesi gerektiğini göstermiştir.

ç. İnternet Kullanım Süresi Değişkenine Göre Bilgi Güvenliği Farkındalığı

İnternet kullanım sürelerine göre bilgi güvenliği farkındalığında anlamlı bir fark olup olmadığını tespit etmek için tek yönlü ANOVA analizi yapılmış ve testin sonuçları Tablo 8'de verilmiştir.

Tablo 8. İnternet Kullanım Süresi Değişkenine Göre Tek Yönlü ANOVA Analizi Sonuçları

Bilgi Güvenliği Puanı					
	Kareler Top.	df	Ort. Kare	F	Sig.
Gruplar Arası	1,440	3	0,480	7,993	0,000
Gruplar İçi	23,790	396	0,060		
Toplam	25,230	399			

Tablo 8 incelendiğinde (Sig<0,05) öğrencilerin internet kullanım sürelerine göre bilgi güvenliği farkındalıklarının anlamlı bir şekilde değiştiği görülmektedir.

İnternet kullanım sürelerine göre öğrenciler arasındaki farkı incelemek için uygulanan Scheffe testi sonuçları ise Tablo 9'daki gibidir.

Tablo 9. İnternet Kullanım Süresi Değişkenine Göre Scheffe Testi Sonuçları

BağımsızDeğ.:Bil.Güv.P.		Ort. Fark (I-J)	Std.Hata	Sig.	%95 Güven Aralığı	
(I)Kaçsaat	(J)Kaçsaat				Alt Sınır	Üst Sınır
1'den Az	1-2 Arası	0,06007	0,02936	0,244	-0,0224	0,1425
	2-3 Arası	0,17188	0,03554	0,000	0,0721	0,2717
	3'ten Fazla	0,08618	0,04023	0,206	-0,0268	0,1991
1-2 Arası	1'den Az	-0,06007	0,02936	0,244	-0,1425	0,0224
	2-3 Arası	0,11182	0,03593	0,023	0,0109	0,2127
	3'ten Fazla	0,02611	0,04058	0,937	-0,0878	0,1400
2-3Arası	1den Az	-0,17188	0,03554	0,000	-0,2717	-0,0721
	1-2 Arası	-0,11182	0,03593	0,023	-0,2127	-0,0109
	3'ten Fazla	-0,08570	0,04525	0,311	-0,2127	0,0413
3'ten Fazla	1'den Az	-0,08618	0,04023	0,206	-0,1991	0,0268
	1-2 Arası	-0,02611	0,04058	0,937	-0,1400	0,0878
	2-3 Arası	0,08570	0,04525	0,311	-0,0413	0,2127

Scheffe testi sonuçları incelendiğinde interneti günde 1 saatten daha az kullanan öğrencilerin interneti günde 2-3 saat ve üzeri kullanan öğrenciler lehine istatistiksel olarak anlamlı (Sig<0,01) bir farklılık saptanmıştır. Bu durum interneti daha az kullanan öğrenci grubunun bilgi güvenliği farkındalığı konusunda bilinçlendirilmesi gerektiğini göstermiştir.

d. İnterneti Kullanım Amacı Değişkenine Göre Bilgi Güvenliği Farkındalığı

İnternet kullanım amaçlarına göre bilgi güvenliği farkındalığında anlamlı bir fark olup olmadığını tespit etmek için tek yönlü ANOVA analizi yapılmıştır. Bu testin sonuçları da Tablo 10'dadır.

Tablo 10. İnternet Kullanım Amacı Değişkenine Göre Tek Yönlü ANOVA Analizi Sonuçları

Bilgi Güvenliği Puanı					
	Kareler Top.	df	Ort. Kare	F	Sig.
Gruplar Arası	0,609	2	0,304	4,907	0,008
Gruplar İçi	24,622	397	0,062		
Toplam	25,230	399			

Tablo 10 incelendiğinde (Sig<0,05) öğrencilerin internet kullanım amaçlarına göre bilgi güvenliği farkındalıklarının anlamlı bir şekilde değiştiği görülmektedir.

İnterneti kullanım amaçlarına göre gruplar arasındaki farkı incelemek için uygulanan Scheffe testi sonuçları da Tablo 11'de verilmiştir.

Tablo 11. İnternet Kullanım Amacı Değişkenine Göre Scheffe Testi Sonuçları

(I)Kul.Amacı	(J)Kul.Amacı	Ort. Fark(I-J)	Std.Hata	Sig.	%95 Güven Aralığı	
					Alt Sınır	Üst Sınır
Ödev/Araşt.	Sos. Med.	0,10830	0,03509	0,009	0,0221	0,1945
	Oyun	0,04113	0,02797	0,0340	-0,0276	0,1099
Sos. Med.	Ödev/Araşt.	-0,10830	0,03509	0,009	-0,1945	-0,0221
	Oyun	-0,06716	0,03745	0,202	-0,1592	0,0249
Oyun	Ödev/Araşt.	-0,04113	0,02797	0,340	-0,1099	0,0276
	Sos. Med.	0,06716	0,03745	0,202	-0,0249	0,1592

Scheffe testi sonuçları incelendiğinde interneti ödev-araştırma için kullanan öğrencilerin interneti sadece sosyal medya kullanmak amacıyla kullanan öğrenciler lehine istatistiksel olarak (sig<0,01) anlamlı bir farklılık saptanmıştır. Bu durum

interneti sosyal medya takip amaçlı kullanan öğrenci grubunun bilgi güvenliği farkındalığı konusunda bilinçlendirilmesi gerektiğini göstermiştir.

Sonuç, Tartışma ve Öneriler

Bu bölümde, yukarıda analiz edilen değişkenlere bağlı olarak elde edilen sonuçlar ve bu bağlamda uygulanabilecek öneriler bulunmaktadır.

Eğitim ve öğretimde teknolojinin bu denli yaygın kullanılması; teknolojinin günlük hayata hızla adapte edilmesi ve bunun sonucunda teknolojiye en hızlı şekilde maruz kalan kesimin öğrenciler olduğu düşünüldüğünde, konunun ne kadar önemli olduğu ortaya çıkmaktadır. Öğrencilerin, bilgisayar ve internet ile tanışma yaşının neredeyse ilk çocukluk dönemine kadar indiği dikkate alındığında, ortalama bilgisayar ve internet kullanımının uzun saatler olması bilgi güvenliği konusunda, çocukların da önemli bir paydaş olduğunu ortaya koymuştur.

Araştırma sonuçlarına göre; öğrencilerin yaşlarına, sınıflarına, cinsiyetlerine, bilgisayar kullanım sürelerine ve bilgisayarı kullanma amaçlarına göre anlamlı farklılıklar olduğu görülmektedir. Bunlara tek tek değinecek olursak; kız öğrencilerin erkeklere göre internette karşılaşacağı tehlikeli durumlardan daha çok haberdar olduğu söylenebilir. Yaş itibariyle üst sınıf olan (7. ve 8. sınıf) öğrencilerin alt sınıflara (5. ve 6. sınıf) göre bilgi güvenliği konusunda farkındalık seviyesinin daha iyi olduğu gözlemlenmiştir. İnternet kullanım süresi göz önüne alındığında, interneti daha uzun süre kullanan öğrencilerin, tehlikelerden daha fazla haberdar oldukları, daha az süre kullanan öğrencilerin ise bilgi güvenliği konusunda farkındalık eğitimi alması gerektiği tespit edilmiştir. İnterneti kullanım amaçlarına göre bilgi güvenliği farkındalığı seviyesine bakıldığında, sosyal medya takibi için kullanan öğrencilerin tehlikelerden daha az haberdar oldukları ve bu öğrencilerin bilgi güvenliği konusunda eğitim almaları gerektiği ortaya çıkmıştır.

Bu araştırma; hayatın her alanında kendini hissettiren teknolojinin, ortaokul öğrencilerinin hayatında teknolojiyi bu kadar etkin kullanırken tehlikeler karşısında ne kadar bilinçli olduklarını tespit etmeyi amaçlamıştır. Öğrencilerin, teknoloji kullanımını belirlemek için yapılan ankette öğrencilerin çoğunun bilgisayar sahibi olduğu ve interneti etkin bir şekilde kullandığı görülmektedir. Araştırma sonuçları, öğrencilerin internette rahatsız edici içeriklerle karşılaştığı ve bu durumda ne yapması gerektiğini bilmediğini ortaya koymuştur. Bu durumda bilgi güvenliği konusunda öğrencilerin aldıkları eğitimlerin yetersiz olduğu tespit edilmiştir.

Araştırma sonucunda ortaya çıkan analizler neticesinde ortaokul öğrencilerinin bilgi güvenliği farkındalık seviyesinin geliştirilmesi için sunulan öneriler şunlardır:

Öğrencilerde farkındalık yaratmak için bilgi güvenliği konusu ortaokul Bilişim Teknolojileri ve Yazılım dersi müfredatında ders sayısı bakımından daha uzun süre yer almalıdır. Bilişim Teknolojileri ve Yazılım dersi sadece ortaokulda değil ilkokulda da olmalıdır. Okullarda bilgi güvenliği konusunda sosyal kulüpler oluşturulmalı, sosyal kulüp panolarına bilgi güvenliği farkındalığı konusunda içerikler yerleştirilmelidir.

Extended Summary

Information technologies have affected every area of life and have caused important changes especially in education. Secondary school students come first among the groups that are most affected by this change. As the use of information technologies is spreading rapidly both at school and at home, it is not known how ready students are for this change. The purpose of this study is the measurement of information security awareness of secondary school students within the information society shaped by the rapidly developing technology. The subjects of the study consist of 400 students studying in the fifth, sixth, and seventh grades of Akkapı Şehit Kemal Yüzgeç Secondary School in the 2019-2020 academic year. Information and Awareness Survey was applied to students, which consists of 30 questions and two parts. The first part contains the questions determining the socio-economic levels and personal information of the students, and the second part includes the Information Security Questionnaire. The applied questionnaire was analyzed using the SPSS statistics software package. The reliability coefficient of the questionnaire was determined as 0.699 with a pilot application. Since the reliability coefficient of the research was over 0.50, it was accepted that it was a reliable measurement. t-test and one-way ANOVA analysis were applied for independent samples to determine whether students' technology usage and information security awareness differ according to gender, age, and class for the duration of internet utilization and internet usage purpose. The Scheffe test was used to present groups with meaningful discrepancies. We can say that the research topic in question is very important as the widespread use of technology in education causes students to adapt to daily life quickly and thus they become more exposed to

technology. The long average computer and internet use of children make them an important stakeholder in information security.

There are significant differences in terms of students' ages, classes, genders, computer usage times and purposes of using the computer. If we look at these differences separately, it can be said that female students are more aware of the dangerous situations on the internet than boys. It is seen that the awareness level of the upper-class students (7th and 8th grade) in regards to information security is higher than the lower classes (5th and 6th grade). Considering the internet usage period, it has emerged that students who use the internet for a longer period are aware of the dangers while students who use less time should receive awareness-training on information security. Considering the level of awareness of information security in terms of internet usage purposes, it has emerged that students who use the internet for social media are less aware of the dangers and should receive training on information security.

This research aims to determine how conscious secondary school students are in the face of the dangers of technology that make themselves felt in all areas of life while using technology so effectively. In the survey conducted to determine the use of technology, it was seen that most of the students had computers and used the internet effectively. The outcomes of the investigation emerged that the students encountered offensive content on the internet and did not know what to do in this situation. In this case, it was seen that the education received by the students on information security was insufficient.

As a consequence of the analysis, the suggestions for the improvement of the information security awareness level of secondary school students can be presented as follows:

- To raise awareness among students, the issue of information security should be included in the secondary school Information Technologies and Software lesson curriculum for a longer period of time.
- Information Technologies and Software lessons should be not only in secondary school but also in primary school.

Social clubs should be created on information security in schools, and remarks on social security awareness should be placed on social club boards.

Kaynakça

Kitaplar

Arifoğlu, A., Kömes, A., Yazıcı, A., Akgül, M.K., Ayvalı, A. (2002). *E-Devlet Yolunda.* Ankara: Türkiye Bilişim Derneği Yayınları.

Krause, M., Tipton, H. (2007). *Information Security Management Handbook.* London: CRC Press. ISDN: 0849319978.

Schryen, G. (2007). *Anti-Spam Measures: Analysis and Design.* Germany: Springer Science, Business Media. ISBN:9783540717485.

Ulaşanoğlu, M.E., Yılmaz, R., Tekin, M.A. (2010). *Bilgi Güvenliği: Riskler ve Öneriler.* Ankara: Bilgi Teknolojileri ve İletişim Kurumu.

Ünver, M., Canbay, C., Mirzaoğlu, A.G. (2009). *Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler.* Ankara: Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı.

Yurdakul, C., Çağlayan, M.U. (1997). *Bilgi Teknolojileri Türkiye İçin Nasıl Bir Gelecek Hazırlamakta.* Ankara: Türkiye İş Bankası Kültür Yayınları.

Makaleler

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

Cohen, F. (1987). Computer Viruses: Theory and Experiments. *Journal of Computers&Security,* 6(1), 22-23.

Fussell, R.S. (2005). Protecting Information Security Availability Via Self-adapting Intelligent Agents. *Military Communications Conference,* IEEE, 297s.

Tekerek, M. (2008). Bilgi Güvenliği Yönetimi. *KSÜ Fen ve Mühendislik Dergisi,* 11(1), 132.

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

Tezler

Öztürk, Ö. (2009). *E-Postalarda Spam Sorunu ve Çözüm Önerileri.* (Uzmanlık Tezi). Bilgi Teknolojileri ve İletişim Kurumu. Ankara.

Turhan, M. (2010). *Siber Güvenliğin Sağlanması, Dünya Uygulamaları ve Ülkemiz için Çözüm Önerileri.* (Uzmanlık Tezi). Bilgi Teknolojileri ve İletişim Kurumu. Ankara.

Vural, Y. (2007). *Kurumsal Bilgi Güvenliği ve Sızma (Penetrasyon) Testleri*. (Yüksek Lisans Tezi). Gazi Üniversitesi, Fen Bilimleri Enstitüsü. Ankara.

İnternet Kaynakları

APWG, (2019) Phishing Activity Trends Report, 10 Aralık 2019'da http://www.apwg.org adresinden alınmıştır.

Nickolov, E. (2008). Modern Trends in The Cyber Attacks Against The Critical Information Infrastructure, Regional Cybersecurity Forum. 10 Aralık 2019'da http://www.itu.int adresinden alınmıştır.

Türk Dil Kurumu, (2019). 12 Aralık 2019' da www.tdk.gov.tr adresinden alınmıştır.