



HACETTEPE ÜNİVERSİTESİ
EĞİTİM BİLİMLERİ ENSTİTÜSÜ

Bilgisayar ve Öğretim Teknolojileri Eğitimi Ana Bilim Dalı

SAYISAL AYAK İZİ DERS TASARIMININ ÖĞRENCİLERİN SAYISAL
VATANDAŞLIK KONUSUNDAKİ AKADEMİK BAŞARILARINA ETKİSİ



Gizem KUH

Yüksek Lisans Tezi

Ankara, 2018



Liderlik, araştırma, inovasyon, kaliteli eğitim ve değişim ile

Daha ileriye ... En İyiyeye ...



HACETTEPE ÜNİVERSİTESİ
EĞİTİM BİLİMLERİ ENSTİTÜSÜ

Bilgisayar ve Öğretim Teknolojileri Eğitimi Ana Bilim Dalı

SAYISAL AYAK İZİ DERS TASARIMININ ÖĞRENCİLERİN SAYISAL
VATANDAŞLIK KONUSUNDAKİ AKADEMİK BAŞARILARINA ETKİSİ

THE EFFECT OF DIGITAL FOOTPRINT COURSE DESIGN ON STUDENTS'
ACADEMIC ACHIEVEMENT ABOUT DIGITAL CITIZENSHIP

Gizem KUH

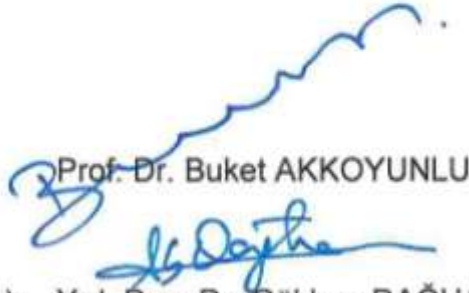
Yüksek Lisans Tezi

Ankara, 2018

Kabul ve Onay

Eğitim Bilimleri Enstitüsü Müdürlüğüne,
Gizem KUH'un hazırladığı "Sayısal Ayak İzi Ders Tasarımının Öğrencilerin Sayısal Vatandaşlık Konusundaki Akademik Başarılarına Etkisi" başlıklı bu çalışma jürimiz tarafından **Bilgisayar ve Öğretim Teknolojileri Eğitimi Ana Bilim Dalında Yüksek Lisans Tezi** olarak kabul edilmiştir.

Jüri Başkanı


Prof. Dr. Buket AKKOYUNLU

Jüri Üyesi (Danışman)

Yrd. Doç. Dr. Gökhan DAĞHAN

Jüri Üyesi


Doç. Dr. G. Alev ÖZKÖK

Jüri Üyesi


Doç. Dr. Ahmet Naci ÇOKLAR

Jüri Üyesi


Yrd. Doç. Dr. Salih BARDAKCI

Bu tez Hacettepe Üniversitesi Lisansüstü Eğitim, Öğretim ve Sınav Yönetmeliği'nin ilgili maddeleri uyarınca yukarıdaki jüri üyeleri tarafından 05 / 03 / 2018 tarihinde uygun görülmüş ve Enstitü Yönetim Kurulunca / / tarihinde kabul edilmiştir.

Prof. Dr. Ali Ekber ŞAHİN
Eğitim Bilimleri Enstitüsü Müdürü

*Sonsuz Destekleri ve Sevgileriyle
Her Daim Yanımda Olan
SEVGİLİ ANNEM ve BABAM'a*

Öz

Bu araştırmada önemi günden güne artan, öğretim programlarında eksikliği görülen ve internet ortamında yapılan her türlü faaliyeti kapsayan sayısal ayak izi konulu bir ders tasarlanmıştır. Bu araştırmanın amacı sayısal ayak izi adı verilen ders tasarımının öğrencilerin sayısal vatandaşlık konusundaki akademik başarılarına etkisini incelemektir. Sayısal ayak izinin, bireylerin sanal ortamdaki kimliğini oluşturduğu ve bilinçsiz bir internet kullanımı ile yanlış ve kötü kimlik oluşturabilecekleri, bu kimliğin asla silinemeyeceği ve hayatın her alanında bireyleri olumlu ya da olumsuz yönde etkileyebileceği söylenebilir. Çalışma grubu 2016-2017 Eğitim-Öğretim yılında özel bir ortaokulun 5. ve 6. sınıflarında öğrenim gören 49 öğrenciden oluşmaktadır. Tasarlanan sayısal ayak izi konulu dersin uygulaması Bilişim Teknolojileri ve Yazılım dersi kapsamında ilk hafta ön test, 7 hafta ders anlatımı ve son hafta son test olmak üzere toplam 9 hafta sürmüştür. Uygulama öncesi ve sonrası bir farklılık olup olmadığını test etmek amacıyla öğrencilerin ön test ve son test puanlarından elde edilen veriler ilişkili örneklem t testi ile sınanmıştır. Yapılan analizin etki büyüklüğünü incelemek için ise Cohen's d değeri hesaplanmıştır. Araştırmanın sonucunda ön test ve son test puanları arasında anlamlı bir fark olduğu ve son test puanlarının ön test puanlarına göre çok geniş etkili bir artış gösterdiği görülmüştür. Bu sonuçlara göre, sayısal ayak izi ders tasarımının öğrencilerin sayısal vatandaşlık konusundaki akademik başarılarına olumlu yönde bir etkisinin olduğu ve bu etkinin anlamlı olduğu söylenebilir. Elde edilen bulgular ve sonuçların ışığında araştırmaya ve uygulamaya yönelik birtakım önerilerde bulunulmuştur.

Anahtar sözcükler: güvenli internet, sayısal ayak izi, sayısal kimlik, sayısal vatandaşlık, siber zorbalık

Abstract

In this research, a lesson was designed about digital footprint. The importance of digital footprint which covers all kinds of activities carried out in the internet environment is increasing day by day, and the lack of this concept is seen in the curriculum. The aim of this research is to examine the effect of the digital footprint course design on the academic achievement of students about the subject of digital citizenship. It can be put forward that digital footprint constitutes individuals identities in the virtual environment and they can create false and evil identities through the use of an unconscious internet that this identity can never be erased and individuals in all areas of life can affect positively or negatively. The research group consisted of 49 students in the 5th and 6th grades of a college during the 2016-2017 academic year. The implementation of the designed digital footprint course lasted for a total of 9 weeks including the first week pre-test, 7 week implementation process and last week post-test within the scope of Information Technologies and Software course. In order to test whether there is a difference before and after the implementation process, the data obtained from pre-test and post-test scores of the students were tested by paired samples t-test. Cohen's d value was calculated to examine the effect size of the analysis performed. It was observed that there was a meaningful difference between pre-test and post-test scores in the result of the research and post-test scores showed a very large effective increase compared to pre-test scores. According to these results, it can be said that the design of the digital footprint course has positive effect on the academic achievement of the digital citizenship and this effect is meaningful. In the light of the findings and results obtained, some suggestions were made for research and further implementation.

Keywords: safety internet, digital footprint, digital identity, digital citizenship, cyberbullying

Teşekkür

Işığ, bilgisi ve tecrübesiyle bana yol gösteren, hatalarıma karşı sabırlı ve anlayışlı tutumlar sergileyen, bana yeni bakış açıları kazandıran, değerli zamanını büyük bir özveriyle bana ayıran, kendisiyle çalıştığım süre boyunca hep “iyi ki” dediğim sevgili danışmanım ve hocam Yrd. Doç. Dr. Gökhan DAĞHAN’a ve tezimin yapı taşlarını oluşturmama yardımcı olan ve oluşumunda büyük katkıları bulunan, desteğini, sevgisini ve şefkatini her daim hissettiğim, onu tanıdığım için kendimi şanslı hissettiğim sevgili hocam Prof. Dr. Buket AKKOYUNLU’ya sevgi, saygı ve teşekkürlerimi sunarım.

Tez savunma sınavında getirmiş oldukları katkılar nedeniyle, Doç. Dr. G. Alev ÖZKÖK’e, Doç. Dr. Ahmet Naci ÇOKLAR’a ve Yrd. Doç. Dr. Salih BARDAKCI’ya teşekkür ederim.

Görev yaptığım okulda tezimin uygulanması için bana gerekli izinleri sağlayan ve desteklerini esirgemeyen sevgili müdürüm Kasım SİNOPLU ve müdür yardımcım M. Arif TOLU’ya teşekkür ederim.

Araştırmama katılan Özel Arı Okulları ve Özel Reyhanlı Şahika Koleji öğrencilerine ve başarı testini hazırlamamda yardımcı olan Özel Arı Okulları Bilişim Teknolojileri ve Yazılım dersi öğretmenlerine de ayrıca teşekkür ederim.

Hazırlanan ders tasarımıyla ilgili kazanımlarda görüşlerini esirgemeyen sevgili hocalarım Prof. Dr. S. Sadi SEFEROĞLU, Prof. Dr. Şirin KARADENİZ, Doç. Dr. Yasemin DEMİRASLAN ÇEVİK ve Yrd. Doç. Dr. Gökhan DAĞHAN ile sevgili arkadaşlarım Arş. Gör. Fulya TORUN, Arş. Gör. Mehmet TEMİZKAN ve Arş. Gör. Sinan KESKİN’e katkılarından dolayı teşekkür ederim.

Araştırmanın uygulama sürecinde bana destek olarak yardımlarını esirgemeyen, iş yükümü hafifleten ve bana zaman kazandıran sevgili yengem Aylin KUH ve kardeşim Ahmet KUH’a teşekkür ederim.

Hayatıma girdiği günden beri her daim bana destek veren, sabır ve sonsuz sevgiyle her zaman yanımda olduğunu hissettiren sevgili nişanlım, koca yürekli hayat arkadaşım Cihan KARYELİ’ye sonsuz sevgimi ve teşekkürlerimi sunarım.

Bugünlere kadar gelmemde en büyük emeđi olan, hayatımın her adımında yanımda olan, bana güç veren, her konuda desteklerini esirgemeyen, uęsuz bucaksız sevgi ve şefkatleri ile son nefesime kadar yanımda olacaklarından emin olduđum, sevgili annem, babam, abim ve kardeşime sonsuz sevgi, saygı ve teşekkürlerimi sunarım.



İçindekiler

Öz.....	iii
Abstract.....	iv
Teşekkür.....	v
Tablolar Dizini.....	ix
Şekiller Dizini.....	x
Simgeler ve Kısaltmalar Dizini.....	xi
Bölüm 1 Giriş.....	1
Problem Durumu.....	1
Araştırmanın Amacı ve Önemi.....	24
Araştırma Problemi.....	25
Sınırlılıklar.....	25
İşlevsel Tanımlar.....	25
Bölüm 2 İlgili Araştırmalar.....	27
Bölüm 3 Yöntem.....	35
Araştırmanın Yöntemi.....	35
Çalışma Grubu.....	36
Veri Toplama Araçları.....	36
Uygulama Süreci.....	40
Verilerin Analizi.....	42
Araştırmanın İç ve Dış Geçerliği.....	42
Bölüm 4 Bulgular.....	44
Araştırmanın Problemine Ait Bulgular.....	44
Bölüm 5 Sonuç, Tartışma ve Öneriler.....	49
Sonuç ve Tartışma.....	49
Öneriler.....	51
Kaynaklar.....	52

EK-A: Sayısal Ayak İzi Ders Kazanımları	58
EK-B: Ön Test Ve Son Test Olarak Uygulanan Başarı Testi	59
EK-C: Ders Planları	64
EK-Ç: Sayısal Ayak İzi Sunusu Ekran Görüntüleri	79
EK-D: Sayısal Vatandaşlık Sunusu Ekran Görüntüleri	82
EK-E: Güvenli İnternet Sunusu Ekran Görüntüleri.....	84
EK-F:İnternette Etkili Arama Yapma Sunusu Ekran Görüntüleri.....	87
EK-G: İnternette Etkili Arama Yapma Afişi	90
EK-Ğ: Web Sayfası Değerlendirme Formu	91
EK-H: Siber Taciz Sunusu Ekran Görüntüleri.....	92
EK-I: Siber Tuzaklar Afişi.....	95
EK-İ: Çevrimiçi İtibar Kontrol Listesi Afişi	96
EK-J: Etik Komisyonu Onay Bildirimi	97
EK-K: Etik Beyanı.....	98
EK-L: Yüksek Lisans Tez Çalışması Orijinallik Raporu	99
EK-M: Thesis Originality Report	100
EK-N: Yayımlama ve Fikrî Mülkiyet Hakları Beyanı.....	101

Tablolar Dizini

Tablo 1 2012 Yılı ve Sonrasında Uygulamaya Konan Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programının Ünite ve Konuları	13
Tablo 2 2012 Yılı ve Sonrasında Uygulamaya Konan Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programının Bilişim Okur-Yazarlığı ile Araştırma, Bilgiyi Yapılandırma ve İşbirlikli Çalışma Ünitesinde Yer Alan Kazanımlar	15
Tablo 3 Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programının 5. Sınıf Ünite, Konu ve Ders Süreleri	17
Tablo 4 Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programının, 5. Sınıf Etik ve Güvenlik Ünitesi ve İletişim, Araştırma ve İşbirliği Ünitesinin Araştırma Alt Başlığında Yer Alan Kazanımlar.....	19
Tablo 5 Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programının, 6. Sınıf Ünite Konu ve Süreleri.....	20
Tablo 6 Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programının, 6. Sınıf Etik ve Güvenlik Ünitesi ve İletişim, Araştırma ve İşbirliği Ünitesinin Araştırma Alt Başlığında Yer Alan Kazanımlar.....	21
Tablo 7 Sayısal Ayak İzi Ünitesi Kazanımlarının Öğretim Programına Eklenmesi	23
Tablo 8 Araştırma Deseni.....	35
Tablo 9 Çalışma grubunun cinsiyetlerine ilişkin demografik bilgiler.....	36
Tablo 10 Ön Test- Son Test Konu-Soru Dağılımı.....	37
Tablo 11 Başarı Testine İlişkin Betimsel İstatistikler.....	38
Tablo 12 Testin Madde Analizi	39
Tablo 13 Çalışma Grubunun Ön Test ve Son Test Puanlarına İlişkin Ortalama ve Standart Sapma Değerleri.....	44
Tablo 14 Normallik Testi Sonuçları.....	46
Tablo 15 Çalışma Grubunun Ön Test ve Son Test Puanlarına İlişkin İlişkili Örneklem T-Testi Sonuçları.....	47

Şekiller Dizini

Şekil 1. 16-74 yaş grubundaki bireylerin bilgisayar ve internet kullanım durumları ile internet erişimine sahip olma durumları (TÜİK, 2017).....	2
Şekil 2. Öğrencilerin başarı testi puanlarının dağılımı	38
Şekil 3. Ön test puanlarının dağılımı	44
Şekil 4. Son test puanlarının dağılımı	45
Şekil 5. Fark istatistiğine ilişkin histogram	46
Şekil 6. Fark istatistiğine ilişkin Q-Q grafiği	47



Simgeler ve Kısaltmalar Dizini

BİT: Bilgi ve İletişim Teknolojileri

BTK: Bilgi Teknolojileri ve İletişim Kurumu

CCTV: Closed-Circuit Television (Kapalı Devre Televizyon)

DIGCOMP: Digital Competence (Sayısal Yeterlilik)

GPS: The Global Positioning System (Küresel Konumlama Sistemi)

ISTE: International Society for Technology in Education / Uluslararası Eğitimde Teknoloji Topluluğu

JRC-IPTS2: Joint Research Centre Institute for Prospective Technological Studies

Max: Maximum

MEB: Milli Eğitim Bakanlığı

Min: Minimum

N: Kişi Sayısı

NETS: National Educational Technology Standards / Ulusal Eğitim Teknolojileri Standartları

NETS-S: National Educational Technology Standards for Students / Öğrenciler için Ulusal Eğitim Teknolojileri Standartları

Ort: Ortalama

p: Anlamlılık Düzeyi

P21: Partnership For 21st Century Learning

sd: Serbestlik Derecesi

SS: Standart Sapma

TTKB: Talim ve Terbiye Kurulu Başkanlığı

TÜİK: Türkiye İstatistik Kurumu

Bölüm 1

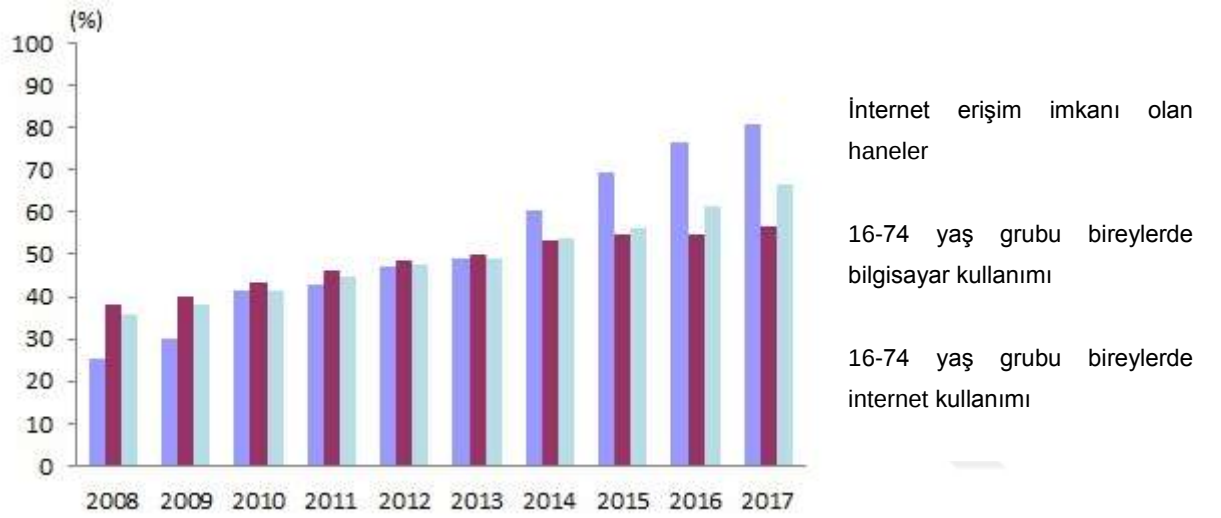
Giriş

Bu bölümde araştırmanın problem durumu, amacı ve önemi, problem cümlesi, alt problemleri ve sınırlılıkları yer almaktadır.

Problem Durumu

İnternete dayalı iletişim ve bilgi paylaşımının (elektronik posta, mesajlaşma, sohbet odaları, sosyal medya araçları vb.) giderek artması, bireylerin birbirleriyle etkileşim iletişimlerini, öğrenme süreçlerini ve eğlence biçimlerini gün geçtikçe değiştirmektedir. Dolayısıyla internet, yaşamın her alanında öne çıkmış, gündelik yaşantıların vazgeçilmezleri arasına girmiştir. Gelineen noktada insanlar yaşantılarını sanal ortama aktarmaya başlamışlardır. Sayısal pazarlama ajansı We Are Social'ın, bir sosyal medya yönetim aracı olan Hootsuite iş birliği ile hazırlanan ve 238 ülkeden toplanan verilerle ortaya konan "Digital in 2017 Global Overview" raporu, dünya nüfusunun yarıdan fazlasının internet kullandığını ve 2017 yılındaki internet kullanımının bu bağlamda sayısal dünyada önemli bir kilometre taşı oluşturduğunu göstermektedir (We Are Social, 2017). Bu rapora göre, küresel internet kullanıcı sayısı 3.77 milyar iken, Türkiye'de nüfusun % 60'ının, yani 48 milyon kişinin internete bağlandığı söylenebilir. Artık dünya nüfusunun 2.80 milyarı aktif olarak sosyal medya kullanmaktadır. Türkiye'de 2016 yılı Ocak ayından bu yana internet kullanımındaki büyüme incelendiğinde, internet kullanıcı sayısının 2 milyon civarında arttığı (Türkiye nüfusunun % 4'ü) görülmektedir. Türkiye'de en çok kullanılan sosyal medya kanalı Youtube iken, ikinci sırada Facebook bulunmaktadır. Diğer popüler sosyal medya kanalları ise Instagram ve Twitter'dır. Yine bu rapora göre, dünya nüfusunun neredeyse üçte ikisinin bir cep telefonu sahibi olduğu, yine nüfusun yarıdan çoğunun bir akıllı telefon kullandığı ve dünyanın web trafiğinin yarıdan fazlasının cep telefonlarından geldiği ortaya konmaktadır. Dünyanın dört bir yanındaki mobil bağlantıların yarıdan çoğunun artık geniş bant bağlantısı olduğu ve nüfusun beşte birinden fazlasının son 30 gün içinde çevrimiçi alışveriş yaptığı belirtilmektedir. Bu istatistikler insanların yaşamlarında internetin, sosyal medyanın ve mobil araçların ne kadar büyük bir yere sahip olduğunu göstermektedir.

Türkiye İstatistik Kurumu'nun (TÜİK, 2017) Hanehalkı Bilişim Teknolojileri Kullanım Araştırması sonuçları, We Are Social'ın Hootsuite iş birliği ile hazırladığı sonuçlarla benzerlik göstermektedir. TÜİK (2017) sonuçlarına göre internet kullanan bireylerin oranı % 66,8'dir. 2017 yılında 16-74 yaş grubundaki bireylerde bilgisayar ve internet kullanımının sırasıyla %56,6 ve %66,8 olduğu görülmüştür. Yine aynı araştırmanın 2017 yılı Nisan ayı sonuçlarına göre hanelerin %80,7'si evden internete erişim sağlayabilmektedir. 16-74 yaş grubundaki bireylerin bilgisayar ve internet kullanım durumları ile internet erişimine sahip olma durumları Şekil 1'de ortaya konmaktadır.



Şekil 1. 16-74 yaş grubundaki bireylerin bilgisayar ve internet kullanım durumları ile internet erişimine sahip olma durumları (TÜİK, 2017)

Şekil 1 incelendiğinde gerek internete sahip olan hane sayısındaki, gerek bilgisayar ve internet kullanımındaki artış dikkat çekmektedir.

TÜİK (2017) Hanehalkı Bilişim Teknolojileri Kullanım Araştırması sonuçlarına göre kişisel amaçla kamu kurum ve kuruluşları ile iletişime geçmek ya da kamu hizmetlerinden yararlanmak amacıyla 2016 yılı Nisan ayı ile 2017 yılı Mart aylarını kapsayan on iki aylık dönemde internet kullanan bireylerin oranının % 42,4 olduğu ortaya konmuştur. Bu oranın önceki yılın aynı döneminde (2015 Nisan-2016 Mart) %36,7 olması ve kullanım amaçları arasında kamu kuruluşlarına ait web sitelerinden bilgi edinmenin %37,6 ile ilk sırayı alması, son dönemde sayısal vatandaşlık uygulamalarına olan talebin arttığının bir göstergesidir.

İnternette Yer Alan Riskler. Çubukçu ve Bayzan (2013) internet güvenliğinin öneminin gün geçtikçe arttığını ifade etmektedirler. İnsanların yaşantısında oldukça önemli bir yere sahip olan teknoloji ile internetin getirdiği birçok kolaylık ve katkı olmasına rağmen, internetin, doğru ve etkili kullanılmamasından veya bilinçsiz kullanımından kaynaklanan riskleri de bulunmaktadır. Bireylerin internette yer alan bilgilere ne kadar güveneceklerini, yani siber tuzaklardan nasıl korunacaklarını bilmemeleri internetin bilinçsiz kullanımı olarak tanımlanabilir. İnternetin bilinçsizce kullanımı söz konusu olduğunda insanların yaşantısı zorlaşmakta, kişisel bilgileri tehlikeye girmektedir. Kim ve arkadaşları (2011) internette yer alan riskleri; internetin karanlık taraflarını, teknoloji merkezli ve teknoloji merkezli olmayan riskler olarak iki gruba ayırmaktadır. Teknoloji odaklı olan riskler; kötü amaçlı yazılımlar, bilgisayar korsanlığı, hizmeti engelleme saldırıları, tıklama hileleri, istenmeyen e-postalar, oltalama faaliyetleri (phishing) ve dijital hakların ihlalidir. Teknoloji odaklı olmayan riskler ise; çevrimiçi hırsızlık, çevrimiçi dolandırıcılık, fiziksel şiddet, siber zorbalık, aşağılama ve gizliliğe saldırı, yasadışı çevrimiçi kumar ve suça yardım etmedir (Kim, Jeong, Kim, & So, 2011).

Bilgi Teknolojileri ve İletişim Kurumu (BTK, 2016) internette yer alan riskleri; yanlış ya da zararlı bilgiye erişim, siber zorbalık, sanal dolandırıcılık, kişisel bilgilerin paylaşımı ve kimlik hırsızlığı (identity theft), zararlı yazılımlar, oltalama, pornografi / çocuk istismarı ve fuhuş, yasadışı kumar, internet bağımlılığı, sağlık sorunları (internetin başında aşırı zaman geçirmeye bağlı olarak görülebilecek fiziki rahatsızlıklar), yabancılarla çevrimiçi ve çevrimdışı iletişim, şiddet / nefret / ırkçılık faaliyetleri, silah ve madde kullanımı, telif hakları ihlali olarak sıralamıştır. Bu risklerden en çok etkilenebilecek gruplar, internet okuryazarlığı ile bilgi okuryazarlığını da içeren sayısal okuryazarlık becerilerini henüz edinmemiş çocuklar ve gençlerdir.

Geleneksel olarak okuryazarlığa sahip olmak, bir bireyin belirli bir kültürde paylaşılan dili okuyup yazabilmesi iken, sayısal okuryazarlık sayısal teknolojileri kullanarak bilgiye ulaşma, bilgiyi düzenleme, analiz etme, yorumlama, değerlendirme, iletme ve bilgi üretme süreciyle birlikte, sayısal metinlerin okunup yazılmasını içermektedir (Akkoyunlu & Yılmaz Soylu, 2010). Sayısal okuryazarlık kuşkusuz bilgisayarı kullanmak ya da e-posta gönderebilmek değildir. Sayısal

okuryazar bir birey, bilgi ve iletişim teknolojilerinin dünyayı nasıl etkilediğini bilir ve sayısal teknolojileri bu amaçla kullanabilir. Ayrıca, sayısal teknolojileri kullanabilenlerden daha etkili bir şekilde bu teknolojileri kullanabilir ve bu araçlar vasıtasıyla iletişim kurabilmek için gerekli olan tüm becerilere sahiptir. İş dünyası artık sayısal okuryazarlık becerilerine sahip bireylere ihtiyaç duymakta ve onları tercih etmektedir. Vasıflı iş gücüne sahip olabilmek de, sayısal okuryazarlık becerilerine sahip olmayı gerektirmektedir. Bireylere sayısal okuryazarlık becerilerinin kazandırılması, sadece ayrıcalıklı olanların değil, tüm bireylerin teknolojiyi anlamlı bir şekilde kullanmalarını ve sayısal kültüre bütünüyle dahil olmalarını sağlamanın yollarından biridir. Sayısal okuryazarlık becerilerini kazanmamış bireylerin karşılaşılabileceği risklerin en az düzeye indirilmesi ise bireylerin doğru ve etkili internet kullanımı konusunda bilinçlendirilmeleri ile mümkün olabilir. Bu risklerin kontrol altına alınabilmesi için öncelikle bu riskler tanınmalı ve risklerin nedenleri belirlenmelidir. Alanyazında yer alan çalışmalar incelendiğinde en yaygın karşılaşılan risklerin, siber zorbalık ve siber tuzaklar olduğu görülmüştür.

Siber zorbalık son yıllarda toplumsal bir sorun haline gelmiştir. Bu kavram, günlük yaşamda karşılaşılan zorbalık davranışlarının internet ortamında boy göstermesi sonucu ortaya çıkmıştır. İlk olarak Belsey (2007) tarafından tanımlanan siber zorbalık, bilgi ve iletişim teknolojilerini kullanarak karşısındakine zarar vermeyi amaçlayan, bir grup ya da kişi tarafından kasıtlı olarak yapılmış, tekrar eden düşmanca bir davranıştır. Patchin ve Hinduja (2006) siber zorbalığı, elektronik metin aracı vasıtasıyla, kasıtlı ve tekrarlanan zarar verme olarak tanımlarken, Commonwealth of Australia (2014) bir kişiye ya da gruba toplumsal, psikolojik ya da fiziksel olarak zarar vermek amacıyla zorbalık yapmak için teknolojinin kullanılması olarak tanımlamaktadır. Arıca (2009) ise siber zorbalığı, diğer kişilere zarar vermek amacıyla, bir birey ya da grup tarafından, elektronik posta, cep telefonu, çağrı cihazı, kısa mesaj servisi ve web siteleri gibi bilgi ve iletişim teknolojilerinin kullanımını içeren; kasten, tekrarlayıcı bir şekilde ve düşmanca davranışları destekleyen etkinlikler olarak daha kapsamlı bir biçimde ifade etmektedir. Tanımlardan da görülebileceği gibi, küfürlü metinler ve e-postalar, kırıcı mesajlar, resimler ya da videolar, çevrimiçinde başkalarını taklit etmek, dışlamak, küçük düşürmek, hoş olmayan dedikodu ve sohbet gibi

davranışlar siber zorbalığı içermektedir (Milosevic, 2016). Kamerayla siber zorbalık kurbanının fotoğrafını çekmek, genellikle haberi ve rızası olmadan görüntülerini sosyal medyada paylaşmak, elektronik posta ya da mesaj yoluyla aşağılayıcı, alay edici, tehdit, cinsel taciz ya da şiddet içerikli mesajlar göndermek, kurbanı yönelik karalayıcı, aşağılayıcı web sayfaları hazırlamak gibi davranışları da kapsamaktadır (Akça, Sayımer, Salı ve Başak, 2014).

Bilinçsiz internet kullanımında karşılaşılan diğer bir tehlike de siber tuzaklardır. Siber tuzak, siber dolandırıcılık ve siber hırsızlık olarak da isimlendirilebilir. Siber tuzak insanların internet üzerinden dolandırılmasıdır. Kimlik bilgilerinin istenerek “tatil kazandınız”, “telefon kazandınız” gibi mesajların gelmesi, açılır pencerelerle (pop up) yarışmaya katılımın istenmesi siber tuzaklara örnek olarak verilebilir (Keşf@ Bilinçli İnternet Hareketi Projesi, 2017).

Gençler ve çocuklar kişisel mahremiyetlerini koruma konusunda dikkatsiz davranabilmekte, interneti güvenli bir şekilde kullanmaktan uzaklaşabilmekte ve farkında olmadan risk alabilmektedirler. Odabaşı ve arkadaşları (2015) tarafından yapılan araştırmada gençlerin % 9'u hediye kazandığını belirten bir e-postadaki yönergeleri izlemekte bir sakınca görmediklerini, % 16'sının internetteki bir yarışma ilanında güvenilir bir şirketin adı geçiyorsa, yarışmaya katılmakta bir sakınca görmediklerini, % 18'inin ise güvendiği bir kişiden zincirleme bir e-posta gelmiş ise e-postanın güvenilir olduğunu düşündüklerini ortaya koymuşlardır. Siber tuzaklar bireylerin önünde bir tehdit oluşturmakta, interneti doğru ve etkili kullanmalarını engellemektedir. Bu nedenle öğrencilerin bu konuda eğitilmesi ve bilinçlendirilmesi gerekmektedir.

Bireylerin, çevrimiçi kullanıcı profilinin yani sayısal ayak izinin siber dünyada ve internetin etkili ve verimli kullanımında çok önemli olduğunu bilmeleri de ele alınması gereken diğer bir konudur. Çünkü internetteki risklerin bireylerin geleceği ve itibarı açısından ortaya çıkardığı bir diğer tehdit de, hem bu risklere sebep olan kişilerin, hem de bu risklerin mağdurlarının sayısal kimliklerinde olumsuz ayak izleri bıraktığıdır.

Sayısal Ayak İzi. Bireylerin internet ortamında bıraktıkları ize ya da ipucuna *sayısal ayak izi* ya da *dijital ayak izi* denir. Birey tarafından paylaşılan e–posta mesajları, yüklenen ya da indirilen dosyalar (metin, video ve sayısal imajlar vb.) ve sosyal ağ ortamlarının kullanımları, bireylerin çevrimiçi ortamda bıraktıkları izlerdir (Hewson, 2013). Bu nedenle, çevrimiçi ortamlarda yapılan her türlü aktivite bir iz bırakır ve bu iz sayısal ayak izini oluşturur. Klavyeden, fareden ya da ekrandan, tuşlayarak, tıklayarak ya da dokunarak elektronik ortama aktarılan bireyle ilgili her türlü bilgi bir izdir. Web etkinliklerinin sürekli olarak devam eden kaydının toplamı sayısal ayak izidir. Düşünmeden ve deneyimsiz yapılan fare ve klavye tıklamaları gelecekteki iş hayatında ya da üniversite kabulünde gençlerin önüne bir engel olarak çıkabilmektedir (O'Keeffe, Pearson, & Council on Communications and Media, 2011). Richardson (2008), öğretmenlere yönelik olarak, kendilerinin, okullarındaki meslektaşlarının ve öğrencilerinin özel bilgilerinin, okul bilgilerinin, blog yazılarının, YouTube videolarının, Flickr fotoğraflarının, Facebook ya da Instagram gibi sosyal medya ortamlarında paylaştıklarının Google tarafından okunduğunu ifade etmektedir. Ayrıca, cep telefonları, GPS verileri, internet kullanımı, CCTV kameralar üzerindeki doğrudan kayıtlar ile kredi kartı işlemleriyle üretilen veriler de bir kişiye etiketlenerek kişinin sayısal ayak izine katkıda bulunmaktadır (Fletcher, Griffiths, & Kutar, 2011).

Değiştirilmesi kolay olmayan sayısal ayak izi, bireylerin ekran ile etkileşimlerinin, sayısal ortamdaki paylaşımlarının, internet arşivlerinin ve arama motoru sonuçlarının bir bileşkesinden oluşmaktadır (Thompson, 2012). Thompson'a (2012) göre, bireylerin internet ortamındaki bulunuşlukları, internet ortamında ifade ettikleri, yaptıkları ve paylaştıkları zamanla sayısal ayak izine doğru evrilmektedir.

Çevrimiçi sosyal medyadaki hızlı büyüme nedeniyle kullanıcıların çevrimiçi sayısal ayak izlerinin büyüklüğü de artmaktadır (Malhotra, Totti, Meira, Kumaraguru, & Almeida, 2012). Sayısal ayak izi bireylerin yaşamlarıyla ilgili önemli bilgiler içermekte, bazen de onların aleyhine kullanılabilir. Bireyin sayısal ayak izini doğru yönetebilmesi hem interneti doğru ve etkili kullanması hem de bilinçli bir sayısal vatandaş olması için önemlidir. Başka bir deyişle, iyi bir sayısal vatandaş olmanın yolu olumlu sayısal ayak izi bırakmaktan geçmektedir. Bireyler, internet dünyasında söyledikleri her şeyi kaydedebilen ve dağıtabilen, dünyaya

genel bir seslendirme sistemiyle bağlanmış olan bir konferans salonu içindedirler. Bütün dünyanın dinlediği bir sistemin içinde söylenilen ve yapılanların daha ilgi çekici ve olumlu olduğundan emin olunarak yapılması, olumlu bir kimlik oluşturma bakımından daha doğru olacaktır (Digital Citizenship Adventures, 2017).

Kuehn (2012) sayısal ayak izi ve itibarın 2 yolla oluştuğunu ileri sürmektedir. Bunların birincisi aktiftir ve aktif sayısal ayak izi kişinin bloglarda kendisinin yazmış olduğu yazılar, paylaştığı fotoğraflar, videolar ve her türlü paylaşımlarıdır. Diğeri ise pasiftir ve pasif sayısal ayak izi başkalarının kendi dışında bir kişi hakkında oluşturduğu paylaşımlardır. İnternetin doğasından dolayı bunların hepsi kalıcıdır (Kuehn, 2012). Bireylerin kendisiyle ilgili ne paylaşıldığını kontrol etmesinin yanı sıra hakkında söylenen ve paylaşılanları da düzenli olarak izlemesi gerekmektedir. Buna ilk olarak hakkında hangi içeriklerin bulunduğu belirlenerek başlanmalıdır. Daha sonra Google aracılığı ile kişinin kendiyle ilgili bir şey yayımlandığında haber verilmesi için uyarı oluşturulabilir (Hengstler, 2017).

Katkıda bulunma ve iş birliği kaygısı ile insanlar, internette çok fazla ve çeşitli alanlarda paylaşım yapmaktadır. Sayısal ayak izlerinin kapsamı ve derinliği ise günden güne artmaktadır (Hengstler, 2017). Madden, Fox, Smith ve Vitak (2007), yetişkinleri çevrimiçi ayak izlerini sınırlamak için attıkları adımlara göre gruplara ayırmışlardır. Bu gruplar ve özellikleri aşağıda ifade edilmektedir.

- Kendine Güvenen Yaratıcılar: Çevrimiçindeki yetişkinlerin %17'sini oluşturmaktadırlar. Çevrimiçi bilgilerinin ulaşılabilirliği konusunda endişelenmediklerini ve aktif olarak içerik yüklediklerini, ama yine de kişisel bilgilerini sınırlamak için adımlar attıklarını söylemektedirler.
- Endişeli ve Dikkatli: Çevrimiçindeki yetişkinlerin %21'i bu gruptadır. Çevrimiçi bilgilerini sınırlamak için adımlar atmaktadırlar ve çevrimiçindeki bilgileri konusunda endişeli ve dikkatli davranmaktadırlar.
- Yol Kenarından Endişelenenler: Kendileri hakkında internette ne kadar bilgi olduğu konusunda endişe duysalar da, çevrimiçi bilgilerini aktif olarak sınırlamamaktadırlar. Çevrimiçi yetişkinlerin %18'idirler.
- Korkusuz ve Pasif: Çevrimiçi yetişkinlerin %43'ünü oluşturan gruptur. Kişisel bilgileriyle ilgili endişe duymamakta ve çevrimiçinde

kendileriyle ilgili bulunabilecek bilgi miktarını sınırlamak için adımlar atmamaktadırlar.

Boyle (2017) öğrencilere sayısal ayak izlerini yönetmeleri için 11 ipucu önermiştir. Bu ipuçları aşağıda sıralanmaktadır:

1. Sosyal medya hesaplarının gizlilik ve güvenlik ayarlarını düzenli olarak kontrol etmek,
2. Kullanılmayacak hesapları silmek ve hangi hesaplara sahip olunduğunu unutmamak için bir hesap listesi tutmak,
3. Fazla paylaşım yapmamak ve böylece fazla kişisel bilgi yaymamak,
4. Her site türünde farklı bir şifre kullanmak gerektiği için bir şifre tutucu edinmek,
5. Herhangi bir sürprize karşı kendini Google'da aratmak,
6. Hesapları birbirine bağlayarak bağlı hesaplardaki izinleri kontrol etmek zor olacağından ikinci bir e-posta hesabı kullanmak,
7. Farklı sosyal medya hesapları ya da farklı kişilerle iletişim kurmak için ikinci bir e-posta hesabı kullanmak,
8. Yönetebilecek kadar e-posta hesabı kullanmak,
9. İnternette paylaşılan şeylerin sonsuza dek orada kaldığının farkında olmak,
10. Yapılan aramaların kontrol edildiğini bilmek ve kullanıcıların tarama gizliliğini koruyan arama motorları kullanmak,
11. Kişisel bilgilerin gizliliği konusunda sınırlandırma yapılmasını sağlayan tarayıcı uzantıları ve uygulama eklentileri gibi araçlardan faydalanmak.

İnterneti güvenli ve etkili bir şekilde kullanan; sayısal vatandaşlığın önemini bilen; sayısal vatandaşlık kurallarına ve ilkelerine uygun davranan; siber zorbalık, siber taciz ve siber tuzak gibi risklerin farkında olan ve bu tür davranışlarda bulunmayan; çevrimiçindeki davranışlarında empati kuran, kişisel hesaplarında güçlü şifreler kullanan bireyler *olumlu sayısal ayak izine ve itibara* sahip bireylerdir.

Sayısal Vatandaşlık. Çevrimiçi olarak zaman geçiren, bir ya da birden fazla cihazla bağlantı kuran, arkadaşları, ailesi ve meslektaşlarıyla dijital yoldan irtibat kuran herkes birer *sayısal vatandaş*tır (eTwinning, 2016).

Mossberger, Tolbert ve McNeal (2007) sayısal vatandaşlığı teknoloji kullanımına ilişkin davranış normları olarak, başka bir deyişle, teknolojiyi kullanırken etik ve uygun davranışlarda bulunma ve bu konuda bilgilenme olarak tanımlamaktadırlar. Sayısal vatandaş, teknolojiyi ahlaki sınırlar içinde kullanan, ortamdaki bilgiyi sorgulayabilen, sanal ortamda iletişim kurabilen, çevrimiçi yapılan davranışların etik sonuçlarını bilen, ahlaki olarak çevrimiçi kararlar alan ve teknolojiyi kötüye kullanmayarak başkalarına zarar vermeyen kişidir. Başka bir deyişle, sayısal ortamda iletişim kurabilen, bilgi üretebilen, bilgiyi kullanabilen ve kullanırken eleştirebilen, sayısal ortamda alışveriş yapabilen, sayısal ortamdaki eğitim alabilen ve bu davranışları yaparken etik kurallara uyan, hak ve sorumluluklarının bilincinde olan bireyler sayısal vatandaşlardır. Council of Europe (2018) sayısal vatandaşlığın öğrencilere dijital ortamlarda çalışmayı, yaşamayı ve paylaşmayı olumlu bir şekilde öğretmeye odaklanan yeni bir vatandaşlık eğitimi boyutunu temsil ettiğini ileri sürmektedir. Tamayo (2016) yayımladığı raporda sayısal vatandaşlığın tanımını teknolojinin uygun kullanım normları olarak tanımlamıştır ve sayısal vatandaşlığı, etik (sayısal toplumda davranış kurallarına uyma), iletişim (elektronik bilgi alışverişi yapma fırsatına sahip olma), okuryazarlık (teknoloji ve teknoloji kullanım bilgisine sahip olma), ticaret (e-ticaret ile ilgili risklerin ve problemlerin farkında olma), hukuk (sayısal dünyadaki eylemlerden sorumlu olma), erişim (sayısal toplumun bir parçası olma), güvenlik (sayısal ortamlarda güvenlik önlemlerini alma) ile haklar ve sorumluluklar (sayısal dünyada herkesin sahip olduğu özgürlükler) olmak üzere 8 stratejik alana bölmüştür. Tanımlardan da görülebileceği gibi sayısal vatandaşlık, teknolojinin doğru ve etkili kullanımı ile ilgili standartların belirlenmesidir.

Ribble (2011) çocuklara çok erken yaşlardan itibaren sayısal araçların doğru ve etkili kullanımının öğretilmesi gerektiğini ve ancak bu şekilde sayısal vatandaşlık algısının oluşturulabileceğini vurgulamaktadır. Ayrıca Ribble ve Bailey (2004), sayısal vatandaşlığın okulda sadece bir ders ya da konu olarak işlenmesinin değil, okul kültürünün bir parçası haline gelmesinin gerekliliğini vurgulamaktadır. Toplumun gereksinim duyduğu insan profiline uygun bireyler

yetiřtirme sorumluluęu olan eęitim kurumlarında ocukların sayısal vatandaşlık becerilerini kazanmaları, yanlış teknoloji kullanımından kaynaklanacak tehlikeleri ortadan kaldıracıdır (Hollandsworth, Dowdy, & Donovan, 2011). Bu nedenle birçok lke ęretim programlarında sayısal vatandaşlık becerilerinin kazandırılması iin kazanımlara yer vermiřler ve birtakım yeterlilikler belirlemiřlerdir. Uluslararası standartlarda teknolojinin sosyal, etik ve yasal kullanımı zerine pek ok bileřen bulunmaktadır (International Society for Technology in Education/ Uluslararası Eęitimde Teknoloji Topluluęu [ISTE], 2016; Partnership For 21st Century Learning [P 21], 2013).

ISTE 1993 yılından itibaren eęitim teknolojilerini kullanım yeterlilikleriyle ilgili ęretmen, ęrenci ve yneticiler bazında alıřmalar yapmakta ve standartlar (NETS / National Educational Technology Standards / Ulusal Eęitim Teknolojileri Standartları) belirlemektedir. Bu standartlar zaman ierisinde gncellenerek, belirli yeterlilik alanları ve bu alanlara dair performans gstergeleri olarak ifade edilmekte, birçok lke tarafından da ynlendirici bir kaynak olarak kabul edilmektedir. ISTE'nin ęrenciler iin yayımladıęı standartlar (NETS-S / National Educational Technology Standards for Students / ęrenciler iin Ulusal Eęitim Teknolojileri Standartları), sayısal dnyadaki eęitim ortamlarında sahip olunması gereken yeterlilikler erevesinde ęrencilerin bilgi ve becerilerini deęerlendirmek iin gerekli olan standartlardır. Sz konusu standartlar retken ve verimli ęrenmeye ihtiya duyan ęrencilerin bilgi ve becerilerini geliřtirmek iin hazırlanmıřtır. Bu standartlarla, ęrencilerden teknolojiyi kullanarak yaratıcı dřnme becerileri sergilemeleri, bilgiyi yapılandırılmaları ve zgn rnler yaratmaları beklenmektedir. Bu yeterlik alanında ęrencilerden beklenen, var olan bilgileri, yeni fikir, rn ve sreler retmek iin kullanmalarıdır (ISTE, 2016).

ISTE Uluslararası Eęitim Teknolojisi ęrenci Standartları'nda ęrencilerden beklenen eęitim teknolojileri kullanım yeterlikleri řyle sıralanmıřtır.

- Yetkin ęrenen
- Sayısal Vatandaş
- Bilgi İnřa eden
- Yeniliki Tasarımcı

- Bilişimsel Düşünen
- Yaratıcı İletişimci
- Küresel İşbirlikli

Bunların içinde yer alan sayısal vatandaşlık kavramı, öğrencilerin teknolojiyle bağlantılı sayısal dünyada hak, sorumluluk ve fırsatları tanımaları, güvenli, yasal ve etik davranışlarda bulunmaları olarak tanımlanmıştır. ISTE Uluslararası Eğitim Teknolojisi Öğrenci Standartları'nda yer alan sayısal vatandaşlık göstergeleri aşağıda sunulmuştur.

Öğrenciler,

- Sayısal kimliklerini oluştururlar, saygınlıklarını kazanırlar ve sayısal dünyada davranışlarının kalıcılığının farkındadırlar.
- Çevrimiçi ortamda teknolojiyi kullandıklarında güvenli, yasal ve etik davranırlar.
- Bilgiyi kullanırken ya da paylaşıırken telif haklarına saygılıdırlar. Bilginin ve teknolojinin güvenli, yasal ve sorumluluk içinde kullanılmasını savunurlar.
- Kişisel verilerini düzenlerken gizlilik ve güvenliğe dikkat ederler ve çevrimiçi ortamlarda iz bıraktıklarının farkındadırlar.

Teknolojideki hızlı gelişim, bireylerin yaşadığı dünyayı gerçek ve sayısal dünya olmak üzere ikiye bölmüştür. Bu nedenle de okullarda öğrencilere gerçek dünyaya dönük vatandaşlık becerilerinin yanı sıra, sayısal vatandaşlık becerilerinin de kazandırılması zorunlu hale gelmiştir. Okullar sadece gerçek dünya için değil, sayısal dünya için de bireyler yetiştirmek zorundadırlar. Birçok ülke bu konuda çalışmalarını tamamlamıştır. Avrupa Konseyi, Demokratik Vatandaşlık ve İnsan Hakları Eğitimi üzerine ve iş birliği etkinliklerinin yanı sıra Demokratik Kültür Yetkinlikleri Projesi'nin başarıları üzerine Sayısal Vatandaşlık Eğitimi Projesi'ni inşa etmiştir. Bu proje Eğitim Politikası ve Uygulaması Yönlendirme Komitesi tarafından onaylanmış ve Mart 2016'da başlatılmıştır (Council of Europe, 2018). San Francisco, Los Angeles, New York ve Washington'da ofisleri bulunan Common Sense Media birçok ülkeye nitelikli bir sayısal okuryazarlık ve vatandaşlık eğitimi sunmaktadır.

Common Sense Media (2012), 9-12. sınıflar için öğrencilerin eleştirel düşünme, güvenli davranışlar sergileme ve sayısal dünyaya sorumlu olarak katılma gibi davranışlarını geliştirmek amacıyla, “Sayısal Vatandaşlık Programı” hazırlamıştır. Bu programda; özsaygı ve kimliğini belirleme (self-image & identify), arkadaşlık ve iletişim (relationships & communication), sayısal ayak izi ve itibar (digital footprint & reputation), siber zorbalık ve sayısal drama (cyberbullying & digital drama), bilgi okuryazarlığı (information literacy), internet güvenliği (internet safety), gizlilik ve güvenlik (privacy & security) ile itibar oluşturma ve telif hakkı (creative credit & copyright) konuları yer almaktadır. Tamayo (2016) raporunda, sayısal vatandaşlığın ve sayısal vatandaşlık becerilerinin kazandırılmasının bir müfredat hazırlanmasından ve uygulamasından daha fazla olduğunu, teknoloji ile çevrilmiş dünyada gençliği geleceğe hazırlayan bir süreç olması gerektiğinin altını çizmiştir.

Türkiye’de Bilişim Teknolojileri ve Yazılım Derslerinde Sayısal Vatandaşlık ve Sayısal Ayak İzi. Bu bölümde araştırmaya başlanılan tarihte halihazırda uygulanmakta olan Bilişim Teknolojileri ve Yazılım dersi öğretim programındaki eksiklikler tespit edilmiştir. Araştırma sürecinde değişen öğretim programları da incelenerek, sayısal ayak izi ders tasarımı üzerinden eksiklikler belirlenmiş ve hazırlanan dersin kazanımlarının son öğretim programına eklenmiş hali gösterilmiştir. Öğretim programlarında konuyla ilgisi olduğu düşünülen ünite ve konular, 2014’ten beri öğretmenlik yapmakta olan araştırmacının deneyimi, öğretim programında yer alan konuların içeriği hakkındaki bilgisi ve incelemeleri doğrultusunda belirlenmiştir.

Milli Eğitim Bakanlığı Talim ve Terbiye Kurulu Başkanlığının 05.09.2012 tarih ve 150 sayılı kararı ile uygulamaya konan Bilişim Teknolojileri ve Yazılım Dersi (5, 6, 7 ve 8. Sınıflar) Öğretim Programı incelendiğinde programın; gelişen teknolojiler ışığında sorumluluklarını bilen birer sayısal vatandaş yetiştirmek, öğretim teknolojilerinin iş birliği, öğrenme ve bilgi paylaşımı amacıyla kullanımını sağlamak ve yaygınlaştırmak için ulusal düzeyde bilgi ve iletişim teknolojilerinin kullanımı konusunda temel yeterlilikleri belirleyerek oluşturulduğu vurgulanmıştır (Milli Eğitim Bakanlığı Talim ve Terbiye Kurulu Başkanlığı [MEB TTKB], 2012). Programda yer alan konular Tablo 1’de sunulmuştur:

Tablo 1

*2012 Yılı ve Sonrasında Uygulamaya Konan Bilişim Teknolojileri ve Yazılım Dersi
Öğretim Programının Ünite ve Konuları*

Ünite	Konu
Bilişim Okur-Yazarlığı	BİT'in Günlük Yaşamdaki Önemi
	-BİT'in Önemi
	-BİT'in Kullanıldığı Alanlar
	-BİT'i Kullanırken Nelere Dikkat Etmeliyiz?
	-BİT Kullanımı ve Sağlık
	-Ergonomi
	BİT'in Sosyal ve Kültürel Katkıları
	-Bilgi Toplumu
	-Dijital Vatandaşlık
	BİT'in Temel Kavramları
Bilişim Teknolojilerini Kullanarak İletişim Kurma, Bilgi Paylaşma ve Kendini İfade Etme	-BİT'in Ürünleri
	-BİT Çeşitleri
	-Donanım ve Yazılım Teknolojileri
	BİT'ini Kullanma ve Yönetme
	-Teknoloji ile Tanışalım
	-İşletim Sistemleri
	-Dosya Yönetimi
	-Faydalı Programlar
	BİT'in Gizlilik ve Güvenlik Boyutları
	-Bilgi ve Veri Güvenliği
Araştırma, Bilgiyi Yapılandırma ve İşbirlikli Çalışma	-Virüsler ve Diğer Zararlı Yazılımlar
	-Kişisel Mahremiyet ve Taciz
	BİT'ini Kullanırken Etik ve Sosyal Değerler
	-İnternet ve BİT Kullanım Kuralları
	-Telif Hakkı ve Dijital Yazarlık
	-Bilişim Suçları
	İnternet ve İletişim
	-İnternete Bağlanmak İçin Neler Gereklidir?
	-Bilgisayar Ağları
	İletişim Araçları
Problem Çözme, Programlama ve Özgün Ürün Geliştirme	Bilgi Paylaşımı İçin Araçlar
	-İşbirlikli Yazarlık
	-Çokluortam Paylaşımları
	-Web Günceleri
	-Etiketleme ve Sosyal İmlleme
	-Sosyal Medya Kullanımı
	-Dijital Kimlik oluşturma
	Proje Oluşturma ve Yönetimi
	BİT'i Kullanarak Bilgiye Ulaşma ve biçimlendirme
	Metin Tabanlı İçerik Oluşturma Araçları
Yazılım Projesi Geliştirme, Uygulama ve Yaygınlaştırma	Hesaplama, Grafik ve Veri Oluşturma Araçları
	Çokluortam Uygulamaları
	Problem, Analiz ve Çözme Yaklaşımları
	Algoritma ve Strateji Geliştirme
	Programlama
	-Program ve Programlama Dilleri
	-Programlama Araçları
	-Animasyon ve Makrolar
	-Sosyal Kodlama Ortamları
	-Kullanıcı Etkileşimli Program Hazırlama

Tablo 1’de görüldüğü gibi araştırmayla ilgisi olduğu düşünülen konular; Bilişim Okur-Yazarlığı ünitesinde yer alan BİT’in sosyal ve kültürel katkıları, BİT’in gizlilik ve güvenlik boyutları ve BİT’i kullanırken etik ve sosyal değerler konuları ile Araştırma, Bilgiyi Yapılandırma ve İşbirlikli Çalışma ünitesindeki BİT’i kullanarak bilgiye ulaşma ve biçimlendirme konularıdır. Programda yer alan konuların kazanımları sınıflara göre ayrılmamış; Temel I, Temel II, Orta I, Orta II, İleri I ve İleri II şeklinde sınıflandırılmıştır. Bu süreçte belirli bir sınıf için öğretilmesi gereken belirli bir düzey ve konu bulunmamakta, düzey ve konu seçimleri öğretmenin tercihlerine bırakılmaktadır. Bundaki amaç teknoloji kullanımı konusunda bir kültür oluşturmak ve öğrenciyi bulunduğu düzeyden ileriye taşımaktır. Öğretim programında yer alan ve araştırmayla ilgisi olduğu düşünülen konuların farklı düzeyler için kazanımları Tablo 2’de sunulmuştur:

Tablo 2

2012 Yılı ve Sonrasında Uygulamaya Konan Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programının Bilişim Okur-Yazarlığı ile Araştırma, Bilgiyi Yapılandırma ve İşbirlikli Çalışma Ünitesinde Yer Alan Kazanımlar

Ünite	Alt Konu	Temel I Düzey	Temel II Düzey	Orta I Düzey	Orta II Düzey	İleri I Düzey	İleri II Düzey
Ünite 1: Bilişim Okur-Yazarlığı	BIT'in Günlük Yaşamdaki Önemi	-Bilişim Teknolojilerinin bireysel ve toplumsal açıdan sosyal ve kültürel hayata katkılarını açıklar.	-BIT'in sosyal ve kültürel katkılarını bilgiye erişme ve değerlendirme kapsamında yorumlar.	-BIT kullanılarak gerçekleşen bilgi yönetiminin sosyal-kültürel hayata katkılarını açıklar.	-BIT araçları kullanılarak dönüştürülen bilginin sosyal ve kültürel hayata yönelik görüş geliştirir.	-Bireysel ve toplumsal açıdan bilgi oluşturma sürecine ilişkin araştırma yapar.	-Bilgi yönetimi süreçlerine ilişkin araştırma sonuçlarını paylaşır.
	BIT'in Gizlilik ve Güvenlik Boyutları	-BIT'in kullanımında gizlilik ve güvenlik boyutlarını açıklar.	-Gizlilik açısından önemli olan boyutları belirler. -Güvenlik açıklarının oluşması konusunda yorum yapar.	-Gizlilik ve güvenlik ayarlarını kişisel tercihlerine göre düzenler. -Gizli kalması gereken bilgi ile paylaşılması gereken bilgiyi ayırt eder.	-Gizlilik ve güvenlik boyutlarını farklı yazılımları ele alarak karşılaştırır.	-Çeşitli ortamların güvenlik düzeyine ilişkin fikir oluşturur. -Gizlilik ihlallerinden doğabilecek sorunları ortaya koyar.	- Gizlilik ve güvenlik problemlerinin neden olduğu bireysel ve toplumsal etkileri tartışır. -Güvenlik için tehdit oluşturabilecek yapılara alınabilecek önlemleri tartışır.

Tablo 2. devam ediyor.

Ünite	Alt Konu	Temel I Düzey	Temel II Düzey	Orta I Düzey	Orta II Düzey	İleri I Düzey	İleri II Düzey
Ünite 1: Bilişim Okur-Yazarlığı	BIT'i Kullanırken Etik ve Sosyal Değerler	-BIT kullanma ve yönetme sürecinde etik ilkelere uymanın önemini fark eder. -Etik ilkelerin ihlali sonucunda karşılaşılabilecek durumlara örnek verir.	-Sosyal ve kültürel değerler açısından BIT kullanımını sorgular. -Sosyal ortamlarda paylaşılan bilgilere ilişkin olarak dijital ve telif haklarına uygun olmayan davranışlara tepkide bulunur.	-BIT kullanırken etik değerlere uygun davranır.	-İnternet ortamında belirlediği etik ilkelere aykırı davranışları, bu ilkelere uygun davranışlara dönüştürür.	-Farklı sanal ortamlar için etik kuralları belirler.	-İnternet ortamındaki davranışların etik olma durumuna ilişkin sunum yapar.
Ünite 3: Araştırma, Bilgiyi Yapılandırma ve İşbirlikli Çalışma	BIT'i Kullanarak Bilgiye Ulaşma ve Biçimlendirme	-BIT'ini kullanarak bilgiye ulaşma yöntemlerini açıklar. -Arama yaparken kullanılan teknikleri listeler. -Bilgiyi biçimlendirmek için kullanılan araçlara örnek verir. -Bilgiyi biçimlendirmek için yapılacak işlemleri açıklar.	-Bilgiye çeşitli kaynaklardan erişir. -Bilgiye ulaşırken zararlı ve gereksiz içerikleri ayırt eder. -Bilgiyi sunmak için amacına uygun aracı seçer.	-Arama motorlarını etkili biçimde kullanır. -Aranan bilgi yapısı ve dosya biçimine göre sonuçlarını düzenler.	-Belirli bir ölçüte göre izin dosyası hazırlar.	-İhtiyaç duyulan bilgiye ulaşmak için gerekli arama ölçütlerini oluşturur.	-Araştırma yaparken kullandığı yöntemleri paylaşır.

Tablo 2’de görüldüğü gibi önemi büyük olan ve insanların hayatlarında yer alan sayısal ayak izi, siber zorbalık, siber tuzak, siber taciz, sayısal empati gibi konulara 2012 programında yeterince yer verilmemiştir. Sayısal vatandaşlık konusu çok yüzeysel kalmış, sayısal vatandaşlığın önemi, ilkeleri ve kurallarına değinilmemiştir. Güçlü şifrelerin nasıl olması gerektiği konusunda konu ve kazanım eklenmemiştir.

MEB Talim ve Terbiye Kurulu Başkanlığının 17.07.2017 tarih ve 78 sayılı kararı ile uygulamaya konan Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programı (Ortaokul 5. ve 6. Sınıflar) incelendiğinde, hedeflenen temel becerilerin içerisinde yer alan; Türkçeyi doğru ve etkili kullanma becerilerinin desteklenmesi, araştırma yapma, teknolojinin verebileceği zararlara karşı bilinçlendirme, bilgi üretme ve bilgi güvenliği sağlama, teknolojiyi yaşamla ilişkilendirme, teknolojiyi etkili ve verimli bir biçimde kullanma, internetteki kaynaklardan eski ve yeni bilgiyi karşılaştırma, sanal ortamlarda etik kurallara uygun davranma gibi temel beceriler araştırma kapsamında dikkat çekmektedir. Bu bağlamda, 2017-2018 Eğitim - Öğretim yılında 5. Sınıfların Bilişim Teknolojileri ve Yazılım dersi öğretim programında yer alan üniteler ve konular Tablo 3’te sunulmuştur:

Tablo 3

Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programının 5. Sınıf Ünite, Konu ve Ders Süreleri

Ünite	Konu	Ders Saati
1.Bilişim Teknolojileri	1.1. Bilişim Teknolojilerinin Günlük Yaşamdaki Önemi	6
	1.2. Bilgisayar Sistemleri	
	1.3. Dosya Yönetimi	
2.Etik ve Güvenlik	2.1.Etik Değerler	8
	2.2.Sayısal Vatandaşlık	
	2.3. Gizlilik ve Güvenlik	
3.İletişim, Araştırma ve İş Birliği	3.1. Bilgisayar Ağları	8
	3.2. Araştırma	
	3.3. İletişim Teknolojileri ve İş Birliği	
4. Ürün Oluşturma	4.1. Görsel İşleme Programları	14
	4.2.Kelime İşlemci Programları	
	4.3.Sunu Programları	
5.Problem Çözme ve Programlama	5.1.Problem Çözme Kavramları ve Yaklaşımları	36
	5.2.Programlama	
TOPLAM		72

Tablo 3'te görüldüğü gibi araştırmayla ilgisi olduğu düşünülen konular; Etik ve Güvenlik ünitesi ve İletişim, Araştırma ve İş Birliği ünitesinin bir alt başlığı olan Araştırma konularıdır. Etik ve Güvenlik ünitesinde yapılan etkinlikler: bilgisayar laboratuvarı, internet ve bilişim teknolojilerinin kullanım süreçlerinde kurallara uygun davranılması gerektiğinin vurgulanması; etik kurallara uyulmaması durumunda karşılaşılabilecek durumlara yönelik örnekler üzerinde durularak dil kullanım ilkelerinden bahsedilmesi; e-devlet, e-randevu, e-bankacılık, e-okul gibi uygulamaların incelenmesi; çevrimiçi ortamlarda dürüst olma ve sahte kimlikler oluşturulmamasının vurgulanması; şifre güvenliği, kişisel bilgilerin güvenliği, mahremiyet gibi kavramlar üzerinde durulması; öğrencilerin paylaştıkları bilgilerin niteliği konusunda sorumlu davranmaya teşvik edilmesidir. İletişim, İşbirliği ve Araştırma ünitesinin altında yer alan Araştırma konusunda ise: yaygın kullanılan web tarayıcılarının tanıtılması; katalog tarama, kütüphane, sözlük, ansiklopedi gibi farklı örneklerin incelenmesi; bilgilerin bilimsel açıdan güvenilir kaynaklardan alınması gerektiği; bilgiler sunulurken dürüst olmanın ve kişi haklarına saygı duymanın öneminin vurgulanması; bilimsel etik çerçevesinde aşırma ve uydurma gibi etik olmayan durumların açıklanması; ulusal kaynaklarla geliştirilen ortamların ve yazılımların kullanılmasının teşvik edilmesi konusunda etkinlikler yer almaktadır.

Yukarıda sözü geçen ünite ve konunun kazanımları Tablo 4'de verilmiştir:

Tablo 4

Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programının, 5. Sınıf Etik ve Güvenlik Ünitesi ve İletişim, Araştırma ve İşbirliği Ünitesinin Araştırma Alt Başlığında Yer Alan Kazanımlar

Ünite	Konular	Kazanımlar
2. Etik ve Güvenlik	2.1. Etik Değerler	2.1.1. Etik ve bilişim etiği ile ilgili temel kavramları açıklar. 2.1.2. Bilişim teknolojileri ile İnterneti kullanma ve yönetme sürecinde etik ilkelere uymanın önemini açıklar. 2.1.3. Çevrimiçi ortamda başkalarının haklarına saygı duymayı bilir. 2.1.4. Etik ilkelerin ihlali sonucunda karşılaşılabilecek durumları fark eder.
	2.2. Sayısal Vatandaşlık	2.2.1. Dijital vatandaşlık uygulamalarının kullanım amaçlarını ve önemini kavrar. 2.2.2. Dijital kimliklerin gerçeği yansıtmayabileceğini fark eder. 2.2.3. Dijital paylaşımların kalıcı olduğunu ve kendisinden geride izler bıraktığını fark eder.
	2.3. Gizlilik ve Güvenlik	2.3.1. Gizlilik açısından önemli olan bileşenleri belirler. 2.3.2. Gizli kalması gereken bilgi ile paylaşılabilecek bilgiyi ayırt eder.
3. İletişim, Araştırma ve İş Birliği	3.2. Araştırma	3.2.1. İnternet adreslerinin oluşumunu ve yapısını anlar. 3.2.2. Web tarayıcısı kavramını açıklar ve tarayıcıyı kullanır. 3.2.3. Arama motorlarını kullanarak basit düzeyde araştırma yapar. 3.2.4. Ulaştığı bilginin doğruluğunu farklı kaynaklardan sorgular. 3.2.5. Ulaştığı bilgiyi kaynak göstererek düzenler. 3.2.6. EBA kullanılarak yapılabilecekleri açıklar.

MEB Bilişim Teknolojileri ve Yazılım dersi öğretim programı incelendiğinde 2017-2018 Eğitim - Öğretim yılında 6. sınıfların Bilişim Teknolojileri ve Yazılım dersi müfredatında yer alan üniteler ve konular Tablo 5'te sunulmuştur:

Tablo 5

Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programının, 6. Sınıf Ünite Konu ve Süreleri

Ünite	Konu	Ders Saati
1.Bilişim Teknolojileri	1.1.BİT'in Günlük Yaşamdaki Önemi 1.2.Bilgisayar Sistemleri 1.3.Dosya Yönetimi	6
2.Etik ve Güvenlik	2.1.Etik Değerler 2.2.Dijital Vatandaşlık 2.3.Gizlilik ve Güvenlik	6
3.İletişim, Araştırma ve İş Birliği	3.1.Bilgisayar Ağları 3.2.Araştırma 3.3.İletişim Teknolojileri ve İş Birliği	8
4. Ürün Oluşturma	4.1.Tablolama Programları 4.2.Ses ve Video İşleme Programları	16
5. Problem Çözme ve Programlama	5.1.Problem Çözme Kavramları ve Yaklaşımları 5.2.Programlama	36
TOPLAM		72

Tablo 5 incelendiğinde görülebileceği gibi araştırmayla ilgisi olduğu düşünülen konular; Etik ve Güvenlik ünitesi ve İletişim, Araştırma ve İş Birliği ünitesinin bir alt başlığı olan Araştırma konularıdır. Etik ve Güvenlik ünitesinde yapılan etkinlikler: sanal ortamlarda doğru ve dürüst olunması gerektiğinin vurgulanması; sanal ortamda karşılaşılabilecek olumsuz davranışlara karşı duyarlı davranılması gerektiğinin üzerinde durulması; açık erişim felsefesi ve etik kullanım üzerinde durulması; İnternet Bilgi İhbar Merkezi hakkında bilgi verilmesi; sayısal ayak izinin kendisinden geride izler bıraktığının vurgulanması; öğrencinin bilinçli bir kullanıcı olması için öz kontrol becerisini geliştirmesinin sağlanması; gizlilik, bütünlük, erişilebilirlik gibi kavramlara değinilmesi; virüs, spam, truva atı vb. zararlı yazılımlardan bahsedilmesidir. Araştırma konusunda ise: ulaşılan bilgilerin doğruluğu konusunda şüpheli yaklaşımlarla farklı kaynaklardan sorgulama yapmalarının sağlanması, bilgi kirliliği konusunda duyarlı davranmanın gerekliliğinin vurgulanması üzerinde durulmaktadır.

Yukarıda sözü geçen konulara ait kazanımlar Tablo 6'te verilmiştir:

Tablo 6

Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programının, 6. Sınıf Etik ve Güvenlik Ünitesi ve İletişim, Araştırma ve İşbirliği Ünitesinin Araştırma Alt Başlığında Yer Alan Kazanımlar

Ünite	Konular	Kazanımlar
2. Etik ve Güvenlik	2.1. Etik Değerler	2.1.1. İnternet etiğinin önemini ifade eder.
		2.1.2. Etik ilkelerin ihlali sonucunda karşılaşılabilecek durumlara örnekler verir.
		2.1.3. Siber zorbalık kavramını açıklayarak korunma amacıyla alınabilecek önlemleri tartışır.
		2.1.4. Telif hakkı kavramını ve önemini araştırır.
		2.1.5. Kullanım haklarını düzenleyen lisans türlerini açıklar.
		2.1.6. Bilişim suçlarının neler olduğunu tanımlayarak ilgili kanunları özetler.
		2.1.7. Bilişim suçlarına karşı alınabilecek önlemler ve stratejiler geliştirir.
	2.2. Sayısal Vatandaşlık	2.2.1. Dijital paylaşımların kendisi ve başkaları üzerindeki etkilerini fark eder.
		2.2.2. Bilişsel ve ahlaki gelişimine uygun olan dijital oyun ve içerikleri ayırt eder.
	2.3. Gizlilik ve Güvenlik	2.3.1. Bilişim teknolojilerinin kullanımında gizlilik ve güvenlik boyutlarının önemini tartışır.
		2.3.2. Güvenlik açıklarının oluşumu konusunda yorum yapar.
		2.3.3. Bilgi koruma yöntemlerini ifade eder.
		2.3.4. Bilgi paylaşımı sürecinde olası riskleri değerlendirerek alınabilecek önlemleri tartışır.
		2.3.5. Zararlı yazılımları kavrar.
		2.3.6. Güvenlik yazılımlarının kullanım amaçlarını açıklar.
3. İletişim, Araştırma ve İş Birliği	3.2. Araştırma	3.2.1. Arama motorlarını kullanarak ileri düzeyde araştırma yapar.
		3.2.2. Bilgiye ulaşırken zararlı ve gereksiz içerikleri ayırt eder.
		3.2.3. Bilgi yönetimi kavramını ve önemini ifade eder.
		3.2.4. EBA kullanılarak farklı içeriklere erişim sağlar.

Tablo 3 ile Tablo 5'te görülebileceği gibi toplam 72 saatlik öğretim programında 5. sınıflarda 11 saat, 6. sınıflarda 9 saat olmak üzere öğrencileri bilinçlendirme ve iyi birer sayısal vatandaş olmaları konularına değinilmiştir. Bununla birlikte öğretim programında, siber zorbalık, siber taciz, sayısal empati konularının yer almadığı görülmektedir. Sayısal vatandaşlık kurallarına, web kaynaklarının değerlendirilmesine, gizlilik ve güvenlik ayarlarına, güçlü şifreler oluşturulmasına ve sayısal ayak iziyle ilgili konulara yeterince yer verilmediği görülmüştür. Tablo 1 ile karşılaştırıldığında 2012 yılından bu yana Sayısal Vatandaşlık ile Gizlilik ve Güvenlik konularına verilen önemin arttığı değişen öğretim programından da fark edilmektedir. Ancak eklenen kazanımların halen yetersiz kaldığı görülmektedir. Bu konularda Sayısal Vatandaşlık başlığı altında

vatandaşlık uygulamalarının yanı sıra sayısal ayak izinin de vurgulandığı görülmektedir. Ancak bu noktada olumlu ve olumsuz sayısal ayak izi, nasıl olumlu sayısal ayak izi oluşturulabileceği, sayısal itibarın korunması için gizlilik ve güvenlik ayarlarının kontrolünün nasıl sağlanacağı konularına yer verilmemiştir. Bu nedenle “Sayısal Ayak İzi” konulu kazanımlar hazırlanmış (Ek A) ve bu kazanımların Bilişim Teknolojileri ve Yazılım dersi öğretim programına bütünleştirilerek ele alınmasının öğrencilerin sayısal teknolojileri doğru kullanmaları açısından önemli olduğu öngörülmüştür.

MEB Talim ve Terbiye Kurulu Başkanlığının 19.01.2018 tarih ve 10 sayılı kararı ile yeni bir öğretim programı yayınlanmış, ancak bu karar kısa süre içinde 24.01.2018 tarih ve 47 sayılı kararı ile yenilenmiştir. 2018-2019 Eğitim - Öğretim yılından itibaren tüm sınıf düzeylerinde uygulanacak olan en güncel Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programı (Ortaokul 5. ve 6. Sınıflar) incelendiğinde, bir önceki öğretim programına göre çalışmayı etkileyecek herhangi bir değişikliğin olmadığı, 5. sınıflarda Bilişim Teknolojileri ünitesinden 2 kazanımın eksiltildiği, kazanımlardaki ifade hatalarının düzeltilindiği ancak araştırmada incelenmiş olan ünitelerdeki kazanımlarda herhangi bir değişikliğin olmadığı görülmektedir.

Buradan hareketle, hazırlanan kazanımların 5. ve 6. sınıflarda “Etik ve Güvenlik” ile “İletişim, Araştırma ve İş Birliği” ünitelerinin içinde yer alabileceği düşünülmektedir. Belirlenen konu ve kazanımlar Tablo 7’de sunulmuştur.

Tablo 7

Sayısal Ayak İzi Ünitesi Kazanımlarının Öğretim Programına Eklenmesi

Ünite	Konu	Eklenen Kazanımlar
2. Etik ve Güvenlik	2.1. Etik Değerler	2.1.5.Dijital ayak izi, dijital vatandaşlık, dijital zorbalık, internet, siber tuzak, siber taciz, dijital empati, ekran yönetimi gibi kavramları tanımlar. 2.1.6. Dijital ayak izi, dijital vatandaşlık, dijital zorbalık, internet, siber tuzak, siber taciz, siber güvenlik, dijital empati kavramlarının benzer ve farklı yönlerini açıklar.
	2.2. Sayısal Vatandaşlık	2.2.4.Dijital vatandaşlığın önemini açıklar. 2.2.5.Dijital vatandaşlık ilke ve kurallarını açıklar. 2.2.6.Dijital vatandaşlık kurallarının önemini açıklar. 2.2.7.Dijital vatandaşlık kurallarına uyulmadığı takdirde karşılaşılabilecek yaptırımları açıklar.
	2.3. Gizlilik ve Güvenlik	2.3.3.Güvenli internet kullanımının kurallarını açıklar. 2.3.4.Web kaynaklarını değerlendirme ölçütüne göre değerlendirir. 2.3.5.Nasıl güçlü şifreler oluşturacağını açıklar.
	2.4. Dijital Zorbalık	2.4.1.Dijital zorbalık davranışlarının neler olduğunu açıklar. 2.4.2.Çevrimiçi ortamda uygun ve bilinçli davranışların neler olduğunu açıklar. 2.4.3.Dijital zorbalığa maruz kaldığında neler yapması gerektiğini açıklar. 2.4.4.Siber taciz davranışlarının neler olduğunu açıklar. 2.4.5.Siber tacizden korunma yollarını açıklar. 2.4.6.Siber tacize maruz kaldığında kimlere başvuracağını açıklar. 2.4.7.İnternette karşılaşılabileceği siber tuzakların neler olduğunu açıklar. 2.4.8.Dijital empatinin neden gerekli olduğunu açıklar. 2.4.9.Dijital empati davranışını bilinçli olarak sergiler.
2. Etik ve Güvenlik	2.5.Dijital Ayak İzi	2.5.1. Gizlilik ve veri koruma konusunda yapılması gerekenleri açıklar. 2.5.2. Gizlilik ve güvenlik ayarlarını bilinçli bir şekilde uygular. 2.5.3. Çevrimiçi bilginin olası getirilerini açıklar. 2.5.4. Olumlu dijital ayak izinin unsurlarını tanımlar. 2.5.5. Olumsuz dijital ayak izinin unsurlarını tanımlar.
3. İletişim, Araştırma ve İş Birliği	3.2. Araştırma	3.2.7.İnternette etkili arama stratejilerini açıklar. 3.2.8.İnternette etkili arama stratejilerini uygular.

Tablo 7’de görüldüğü gibi Sayısal Ayak İzi ders kazanımlarının bu başlıklar altına eklenmesi gerektiği düşünülmüş ve araştırmanın uygulaması bu kapsamda yapılmıştır. Bu çalışmada “Sayısal Ayak İzi” başlıklı ders tasarımının öğrencilerin sayısal vatandaşlık konusundaki akademik başarılarına etkisi araştırılmaktadır.

Araştırmanın Amacı ve Önemi

İnternet dünyasında yapılan her şey sayısal ayak izini oluşturmaktadır. Fotoğraflar, ses ve görüntüler, blog yazıları, beğeniler, yapılan yorumlar sayısal ayak izinin yapı taşlarıdır. Bu bilgiler internet ortamında sayısal ayak izi olarak sonsuza kadar kalmakta, asla silinmemekte ve bireylerin her an yeniden karşılıklarına çıkabilmektedir (Keşf@ Bilinçli İnternet Hareketi Projesi, 2017). Sosyal medya hesaplarında paylaşılanlar bireylerin güvenliğini zaman zaman tehlikeye sokabilmektedir. Herkese açık olan internet kapıları, bırakılan sayısal ayak izi yoluyla bireylerin bilgilerinin takip edilebilmesini olanaklı kılmaktadır (Akkoyunlu, 2016). Sayısal teknolojilerin kullanımı konusunda evrensel bir kabul bulunmaması, bu teknolojilerin kötüye kullanımı için açık bir kapı oluşturmaktadır. Bu nedenle bu konularda okullarda eğitim verilmesi önemli hale gelmektedir (Livingstone, Bober, & Helsper, 2005). Teknolojinin yaygınlaşmasının getirdiği bir sonuç olarak; teknolojinin yanlış ve kötü amaçlar için kullanıldığını vurgulayan Yang ve Chen (2010) de, bu duruma önlem olarak okullarda erken yaşlarda teknolojinin etkili ve doğru kullanımı üzerine eğitim verilmesi ve öğrencilere sayısal vatandaşlık becerileri kazandırılması gerektiğini belirtmektedir. Özellikle gençler çoğunlukla sosyal medyayı bilinçsiz bir şekilde kullanmakta, paylaşımlarının günlük yaşamda ya da ilerleyen zamanlarda nasıl sorunlar yaratabileceğini kestirememekte ve gizliliklerini korumanın önemini bilmemektedirler. Yapılan araştırmalarda internet okuryazarlıklarının düşük olduğu görülen gençler için, bilinçlendirme ve farkındalık eğitiminin tüm derslerin içine harmanlanması, bu konuda daha yoğun bir eğitimin verilmesi gerekmektedir. Çevrimiçi ortamda birileriyle tanışma, kişisel bilgiler paylaşma, yüz yüze ya da tek başına buluşma gibi tehlikeli davranışların önüne geçmek için öğretmenler ve ailelerin iş birliği içerisinde önleyici çalışmalar yapmaları öngörülmektedir (Odabaşı v.d., 2015).

Alanyazında sayısal ayak izi ile ilgili araştırmaların yetersiz olduğu, okul müfredatlarında ise bu konuya yeterince önem verilmediği ve sayısal vatandaşlık konularının çok yüzeysel olarak ele alındığı görülmektedir. Bu amaçla bu çalışmada sayısal ayak izi ders tasarımı yapılmış ve bu ders tasarımı üzerinden öğrencilerin sayısal vatandaşlık konusundaki akademik başarıları incelenmiştir. Bu çalışmanın, sayısal ayak izi konusunda öğrencileri bilgilendirerek sayısal vatandaşlık konusundaki akademik başarılarının geliştirilmesine, öğrencilerin

doğru ve bilinçli internet kullanımlarının sağlanmasına ve bilinçli birer sayısal vatandaş haline gelmelerine katkı getirebileceği düşünülmektedir. Çalışmanın uygulamaya dönük bu olası katkısının yanı sıra, araştırmaya dönük olarak da verilen sayısal ayak izi ders tasarımının sayısal vatandaşlık konusundaki akademik başarıya etkisi araştırılmıştır.

Ayrıca bu araştırmanın ilköğretim grubunda sayısal ayak izi ile ilgili yapılmış olan ilk çalışma olması alanyazına katkısı açısından da önemlidir.

Araştırma Problemi

Araştırma tek ana problem etrafında toplanmaktadır:

Sayısal ayak izi ders tasarımının öğrencilerin sayısal vatandaşlık konusundaki akademik başarılarına etkisi nedir?

Alt problemler. Araştırmanın tek bir alt problemi bulunmaktadır:

“Sayısal Ayak İzi” ders tasarımı sonunda öğrencilerin sayısal vatandaşlık konusundaki akademik başarılarında istatistiksel olarak anlamlı bir farklılık meydana gelmekte midir?

Sınırlılıklar

Araştırma Özel Reyhanlı Şahika Koleji'nin 5. ve 6. sınıflarında öğrenim gören öğrencilerinden araştırmaya katılan 49'u ile Bilişim Teknolojileri ve Yazılım dersi kapsamında toplam 7 haftalık bir süreçte gerçekleştirilmiştir. Araştırma bulguları sayısal vatandaşlık konusundaki akademik başarıyı ölçmek için hazırlanmış olan 35 maddelik çoktan seçmeli başarı testinden elde edilen sonuçlarla ortaya konmuştur. Bu nedenle ancak benzer nitelikteki gruplar için bir genelleme yapılabilir.

İşlevsel Tanımlar

Sayısal Ayak İzi: Bireylerin internet ortamında bıraktıkları her türlü iz ya da ipucudur (Hewson, 2013). Fotoğraflar, ses ve görüntüler, blog yazıları, beğeniler, yapılan yorumlar, internette yapılan ve görülen şeyler (karşılaşılan reklamlar gibi) sayısal ayak izini oluşturmaktadır (Keşf@ Bilinçli İnternet Hareketi Projesi, 2017).

Sayısal Vatandaşlık: Sayısal ortamda iletişim kurabilme, bilgi üretebilme, bilgiyi kullanabilme ve kullanırken eleştirebilme, sayısal ortamda alışveriş yapabilme, sayısal ortamdan eğitim alabilme ve bu davranışları yaparken etik kurallara uyma, hak ve sorumluluklarının bilincinde olma anlamına gelmektedir (Mossberger, Tolbert, & McNeal, 2007).



Bölüm 2

İlgili Araştırmalar

Bu başlık altında konuyla ilgili araştırmalara yer verilmiştir. Alanyazında sayısal ayak izinin eğitsel bağlamda kullanıldığı sınırlı sayıda araştırma bulunmaktadır. İlgili araştırmalara ISI Web of Knowledge veritabanı ve Google Akademik üzerinden tarama yapılarak ulaşılmıştır. Söz konusu tarama yapılırken sayısal ayak izi, dijital ayak izi ve sayısal vatandaşlık anahtar sözcüklerinden yararlanılmıştır. Tam metnine erişilen ve eğitsel bağlamda sayısal ayak izinin kullanıldığı çalışmalar, aşağıda tarihsel olarak eskiden yeniye doğru özetlenmiştir.

Yang ve Chen (2010) sayısal vatandaşlık akımı ve öğretmenlerin inançları ile alanyazından derlenen çalışmaları inceleyerek, sayısal vatandaşlık ve sorumlulukla ilgili öğretmenlerin düşüncelerini ortaya koyan bir çalışma sunmuşlardır. Alanyazında hizmet öncesi ve hizmet içi eğitim alan öğretmenlerin düşünceleri ve inançları, onların mesleki uygulamaların sayısal vatandaşlığı ve sorumluluğu teşvik etmek ve biçimlendirmek gibi yeni bir öğretim davranışı için istekli oldukları görülmüştür. Yapılan araştırmaya 2009 yılında Birleşik Devletler'in kuzeydoğu bölgesindeki bir üniversitede Multimedya ve İnternet Eğitimi adlı eş zamanlı olmayan çevrimiçi bir kursa kaydolan 87 kişi katılmıştır. Katılımcıların çoğu yüksek lisans eğitimini sürdüren yarı zamanlı hizmet içi öğretmenlerdir. Veri toplamada katılımcılara tartışma bölümünden "İnternetin gücü ve popüleritesi insanları heyecanlandırıyor, sizce sayısal teknolojileri, özellikle de internet tabanlı teknolojileri günümüz eğitime uyguladığımızda düşünmemiz gereken etik / sosyal / insani sorunlar nelerdir?" sorusu yöneltilmiştir. Yanıtlar dersin öğretim üyesi tarafından analiz edilmiştir. Yanıtların çoğu, "telif hakkı, fikri mülkiyet ve kaynakların uygun dökümantasyonuna saygı duymak da dahil olmak üzere sayısal bilgi ve teknolojinin savunması, model olması, güvenli öğretimi, yasal ve etik kullanımı"nı içermiştir. Ayrıca uygun sayısal araçlara ve kaynaklara adil erişime olanak tanıyan öğrenci merkezli stratejilerin gerekliliği, sorumlu sosyal etkileşim ve sayısal etiğin modellenip teşvik edilmesi gerektiği, siber zorbalığın bir sorun olduğu, kültürel anlayış ve kültürel farkındalık geliştirilmesi gerektiği cevapları alınmıştır.

Camacho, Minelli ve Grosseck (2012) bir yüksek öğrenim bağlamındaki öğrencilerin sayısal kimliklerinin algılanmasının altında yatan etkileri keşfetmek için

bir çalışma yapmışlardır. Çalışma İspanya'da bulunan Rovira i Virgili Üniversitesi'nin Pedagoji bölümünde 2011-2012 akademik döneminde gerçekleştirilmiştir. Araştırma lisans mezunu seviyesinde olan, yaşları 18 – 45 arasındaki 135 öğrenci ile gerçekleştirilmiştir. Veriler etkinlik öncesi ve sonrası anket yapılarak toplanmıştır. İlk olarak öğrencilerin sosyal ağlardaki alışkanlıklarıyla, gizlilik yönetimiyle, paylaşımlarıyla ilgili sorular yönelten bir anket uygulanmış; ikinci aşamada bir etkinlik uygulaması yapılarak öğrencilerin sosyal ağ sitelerinde yönettikleri ve ürettikleri bilgilerin kendileri hakkında yanlış ve kesin olmayan bilgiler getirebileceğini düşünmelerini sağlamayı amaçlayan sorular içeren bir anket uygulanmıştır. Katılımcılar, sayısal bir etkileşim sitesinde kimlik oluşturma süreçleri hakkında yüksek seviyede bir farkındalık göstermişlerdir. Çoğu öğrenci, gizlilik ayarlarını kullandıklarını, yükledikleri içeriğe önem verdiklerini ve gerçek kimlikleriyle yakından ilişkili bir kimlik sunduklarını ifade etmişlerdir. Katılımcıların çoğu kişisel ve mesleki hayatlarını korumak için sayısal ayak izlerinin etkisi konusunda endişe duysalar da “çevrimiçi olma” arzusunu ve gerçekte kim olduklarını, canlı ve genç kişilik özelliklerini yansıtmak istediklerini belirtmişlerdir.

Moore ve McElroy (2012) Facebook kullanıcılarının ve gerçek Facebook verilerinin anketlerini kullanarak bazı bireylerin neden diğerlerinden daha karmaşık olduklarını ortaya koymak amacıyla bir araştırma yapmışlardır. Bu çalışmada, kişiliğin, bireylerin sosyal paylaşım ağına bıraktıkları sayısal izlerini yalnızca harcanan zaman açısından değil, aynı zamanda kullanımı ve içeriği açısından da nasıl etkilediğine bakılmıştır. Kişilerin Facebook kullanım oranlarını ve kişiliklerini ölçen anket 219 lisans öğrencisine uygulanmıştır. Öğrencilerin 204 tanesinin Facebook hesabının olduğu bulunmuş, bu öğrencilerden 143 tanesi gönüllü olarak araştırmacıyla Facebook'ta arkadaşlık kurmuş ve böylece araştırmacı katılımcılarla ilgili nesnel bilgilere ulaşabilmiştir. Sonuç olarak katılımcıların Facebook arkadaşlarının sayısının, Facebook deneyimlerinin, cinsiyetlerinin, duvarlarında yaptıkları paylaşımların ve Facebook paylaşımları nedeniyle pişmanlık duyma düzeylerinin onların kişiliklerini anlamlı derecede açıklayabildiği sonucuna ulaşılmıştır.

Çubukçu ve Bayzan (2013) sayısal vatandaşın çevrimiçi ortamda hak ve sorumluluklarını, interneti etkin ve doğru kullanabilmesinin yanında ilgili diğer internet aktörlerinin de atması gereken adımlar çerçevesinde ele alarak sayısal

vatandaşlığın dokuz boyutunu, internet risklerinin üç boyutu ile eşleştirmişler ve mevcut durum ile ortaya konması gerekenleri sunmuşlardır. Araştırma sonuçları aşağıda özetlenmiştir:

- çevrimiçi teknolojileri en doğru şekilde kullanabilme yönteminin çevrimiçi teknolojilerden doğru faydalanabilmeyi bilmek ve fayda esasına dayalı bu platformları kullanmak,
- faydalanılabilecek bilgiye çevrimiçi ortamda erişebilmek için olabildiğince doğru bilgiye ulaşıldığından emin olmak,
- bilgiye kaynağından erişmek,
- farklı web sayfalarından kaynak araştırması yapmak ve arama motorları başta olmak üzere internette bilgi arama yöntemlerini bilmek,
- web 2.0 teknolojilerinin dinamik yapısı ve bu yapı çerçevesinde çevrimiçi platformda aynı zamanda birer internet içerik üreticisi olmak,
- doğru bilgiye ulaşmak kadar birer içerik üreticisi olan sayısal vatandaşların hak ve sorumlulukları çerçevesinde internette doğru ve faydalı bilgiler üretip paylaşmaya özen göstermek olduğunu belirtmişlerdir.

Araştırma sonucunda, çocuklara birer sayısal vatandaş olarak teknolojinin nasıl kullanılacağını öğretmekten ziyade teknolojinin hak ve sorumluluklar çerçevesinde daha etkin ve doğru kullanılabilmesinin öğretilmesi; internetin bilinçli, güvenli ve etkin kullanımının sayısal vatandaşlara kazandırılması; Türkiye’de sayısal vatandaşlık algısının güçlendirilmesi için internetin bilinçli, güvenli ve etkin kullanımı konusunda iş birliği yapılması önerilmiştir. Ayrıca kamuoyu farkındalığını artıracak çalışmalar ile projeler yapılması ve her şeyden önce internette pozitif içerik üretmeleri noktasında sayısal vatandaşların teşvik edilmesi gerektiği vurgulanarak, başta Avrupa’da ağırlıklı olarak sivil toplum kuruluşları bünyesinde yürütülen Güvenli İnternet Merkezleri ve Yardım Hatları yapılanmalarının Türkiye’de olmamasının en büyük eksiklik olduğu belirtilmiştir.

Ferrari (2013) JRC-IPTS2'nin (Joint Research Centre Institute for Prospective Technological Studies) Bilgi Toplumu Birimi tarafından yürütülen sayısal yeterliliğin daha iyi anlaşılmasına ve geliştirilmesine katkıda bulunmak amacıyla sayısal yeterliliğin kapsamlı tanımlayıcılarını belirlemek için yaptıkları DIGCOMP (Digital Competence – Sayısal Yeterlilik) isimli projeyi raporlamıştır. Araştırmanın verileri kavramsal haritalama, durum çalışmaları analizi ve çevrimiçi danışma ile toplanmıştır. Bu projede mevcut sayısal yeterlilik çerçeveleri ve girişimlerini toplamak için vaka çalışmaları toplanmış ve bu çalışmalardan 15 çerçeve analiz edilmiştir. Farklı alanlardan 95 uzmandan çevrimiçi görüşler alınmış ve dışarıdan 17 kişinin katıldığı uzman çalıştay yapılmıştır. Vaka analizlerinden birtakım çerçeveler dikkate alınarak rapor edilmiştir. Yaklaşık 40 paydaş, planların, görüşmelerin, toplantı ve sunumların gözden geçirilmesine katkıda bulunmuştur.

Araştırma sonuçlarına göre sayısal yeterlilik alanları aşağıdaki gibi belirlenmiştir:

1. Bilgi: Bilgiye gözetme, bilgiyi arama ve filtreleme, bilgiyi değerlendirme, bilgiyi alma ve kaydetme.
2. İletişim: Teknoloji ile etkileşim kurma, bilgiyi ve içeriği paylaşma, çevrimiçi vatandaşlığa katılma, sayısal kanallarla iş birliği yapma, internet etiğine uyma, sayısal kimliği yönetme.
3. İçerik oluşturma: İçerik geliştirme, entegre etme ve yeniden düzenleme, telif hakkı ve lisanslar, programlama.
4. Güvenlik: Cihazların korunması, kişisel verilerin korunması, sağlığın korunması, çevrenin korunması.
5. Problem Çözme: Teknik problemlerin çözümü, ihtiyaçların ve teknik yanıtların tanımlanması, teknolojinin yaratıcı ve yenilikçi kullanımı, sayısal yeterlilik boşluklarının belirlenmesi.

Bu alanlardan özellikle iletişim alanının içeriğinde temel seviyede sayısal kimliğe ilişkin fayda ve risklerin farkında olma; orta seviyede sayısal kimliği şekillendirebilme ve sayısal ayak izini takip edebilme; ileri seviyede ise sayısal kimliğini yönetebilme, çevrimiçi üretilen verileri izleyebilme ve sayısal itibarın nasıl korunacağını bilme konuları vurgulanmaktadır.

Kaya ve Kaya (2014) Bilgisayar ve Öğretim Teknolojileri Eğitimi öğretmen adaylarının sayısal vatandaşlık algılarını, sayısal teknolojiyi kullanım amaçlarını ve çevrimiçi alışveriş yapacakları siteleri seçerken nelere dikkat ettiklerini ortaya koymak amacıyla bir çalışma yürütmüşlerdir. 3. ve 4. sınıf Bilgisayar ve Öğretim Teknolojileri Eğitimi öğretmen adaylarından gönüllülük esasına göre seçilmiş olan 5 kadın 5 erkek öğretmen adayı ile yapılandırılmış görüşmeler yapmışlar, verilerin analizinde betimsel analiz yöntemini kullanmışlardır. Öğretmen adaylarının büyük çoğunluğu sayısal vatandaşlık kavramını sayısal teknolojinin bireyin yaşamını kolaylaştırması olarak doğru bir şekilde ele almıştır. Öğretmen adaylarının hepsi teknolojinin bilinçli ve doğru bir şekilde kullanılması için sayısal vatandaşlıkla ilgili okullarda bir eğitimin verilmesinin gerekli olduğunu belirtmişlerdir. Öğretmen adaylarının sayısal teknolojileri en çok sosyal ağlara girmek, alışveriş yapmak ve ödev araştırmak için kullandıkları, sayısal vatandaşlığın dokuz boyutundan biri olan sayısal ticareti ise öğretmen adaylarının hepsinin kullandığı görülmüştür. Öğretmen adaylarının büyük çoğunluğunun çevrimiçi alışveriş yapacakları siteleri seçerken güvenli siteleri seçmeye dikkat etmeleri, onların bu konuda bilinçli olduklarını göstermektedir.

Odabaşı ve arkadaşları (2015) bilinçli internet kullanım düzeylerini belirlemek amacıyla İstanbul'daki çeşitli okullardan %58,9'u kadın, %41,1'i erkek toplam 13.463 katılımcıya bir anket uygulamışlardır.

Araştırmacılar, bilinçli internet kullanım boyutunu;

- internet kullanım profili,
- internet kullanım sıklığı,
- sayısal ayak izi bırakma düzeyi,
- internet okuryazarlığı düzeyi,
- siber tuzaklara yönelik farkındalık,
- güvenli internet kullanım düzeyi,
- siber zorbalığa yönelik farkındalık olmak üzere yedi boyutta ele almış, bu boyutlar arasındaki ilişkilere de bakmışlardır.

Yapılan analizler sonucunda; öğrencilerin bilgisayara ya da bilgisayar özelliği gösteren akıllı telefonlara ve internete yüksek oranda erişime sahip oldukları, bu öğrencilerin her gün internete girdikleri ve sosyal medyayı kullandıkları, interneti en yüksek oranda ders yapmak amacıyla kullandıkları, internetin öğrencilerin eğitimine bir şekilde katkı sağladığı, akıllı cep telefonundan internete bağlanan gençlerin sosyal medyayı oldukça yoğun kullandıkları, sosyal medya kullanımı için internette geçirilen sürenin yaşça büyük gençlerde daha fazla olduğu sonucuna ulaşılmıştır. Ayrıca katılımcıların büyük bir bölümünün interneti araştırma yapmak için 2 saatten daha az kullandığı, interneti daha fazla kullanan ve daha çeşitli kullanım profilleri sergileyen katılımcıların daha büyük sayısal ayak izi bıraktığı, katılımcıların internet okuryazarlıklarının düşük olduğu, internete erişim imkanlarının artması ve internette kullanılan olanakların çeşitlenmesi ile birlikte internet okuryazarlığı oranlarının yükseldiği görülmüştür. Siber tuzaklara ilişkin genel farkındalıklarının orta düzeyde olduğu görülse de katılımcıların kimlik hırsızlığı ile sonuçlanabilecek reklam kampanyaları ve şifre seçimleri konusunda hassasiyet sergilediği, kadınların siber tuzaklara yönelik farkındalıklarının erkek katılımcılara oranla daha yüksek olduğu, evinde bilgisayarı olan katılımcıların farkındalık düzeylerinin bilgisayarı olmayan katılımcılarından daha yüksek olduğu, güvenli internet kullanımı farkındalığı ile internet okuryazarlık düzeyi arasında paralellik bulunduğu ve katılımcıların siber zorbalığa yönelik farkındalıklarının orta düzeyde olduğunu belirtmişlerdir.

Jones ve Mitchell (2016) önerilen sayısal vatandaşlık tanımını daha işlevsel hale getirmek, 11-17 yaş aralığındaki gençler üzerinde bu yapıyı ölçmek ve çevrimiçi taciz mağduriyeti, işkence ve seyirci kalma tecrübelerini açıklamak için bir araştırma yapmışlardır. Sayısal vatandaşlık davranışının tanımını kullanarak kısa bir ölçek geliştirmiş ve İngiltere'den 979 ortaokul ve lise çağındaki gençlerden oluşan bir örnekleme siber zorbalık konusunda yapılan geniş bir çalışmanın parçası olarak psikometrik bulguları incelemişlerdir. Öğrencilere yönetimi okul bilgisayarları tarafından yapılan bir anket gönderilmiştir. Araştırma sonucunda, çevrimiçi saygı ve çevrimiçi yurttaşlıkla ilgili sorumluluk bileşenlerinin ölçümü için güçlü bir psikometrik destek bulunmuştur. Çevrimiçi saygı düzeyi yüksek olan gençlerin, daha az siber taciz mağduriyeti yaşadıkları ve çevrimiçi taciz mağdurlarına yardımcı olma konusunda harekete geçme olasılıklarının daha yüksek

olduğu bulunmuştur. Çevrimiçi yurttaşlık sorumluluğu yüksek olan gençlerin, taciz davranışlarını bildirme olasılıklarının daha düşük olduğu ve bir seyirci olarak yardım etmeye çalışmasının daha olası olduğu bulunmuştur. Sayısal vatandaşlık ölçeğinin sayısal vatandaşlık müfredatının etkililiğini doğrulamak isteyen değerlendirme çabalarını iletmek için kullanılabileceği belirtilmiştir.

Choi, Glassman ve Cristol (2017) genç erişkinlerin internet tabanlı topluluğa katılım yeteneklerini, internet algılarını ve düzeylerini ölçmek için kullanılabilecek; sayısal vatandaşlığın bileşenlerini içeren ve ilişkilendiren kapsamlı bir sayısal vatandaşlık ölçeği oluşturmak amaçlı bir çalışma yapmışlardır. Veriler kağıt üzerinde bulunan bir anket yoluyla toplanmıştır. Sayısal vatandaşlığın alt boyutlarını belirlemek, güvenilirlik ve geçerliliğini değerlendirmek için açımlayıcı faktör analizi, doğrulayıcı faktör analizi ve ilişkisel analizler kullanılmıştır. Katılımcılar büyük bir batı üniversitesinde öğrenim gören 1977-1997 yılları arasında doğmuş olan 436 lisans ve 72 lisansüstü öğrenciden oluşmuştur. Sonuç olarak Sayısal Vatandaşlık Ölçeği; bireylerin yeteneklerini, algılarını, internet tabanlı topluluğa katılım düzeylerini farklı karmaşıklık boyutlarında ölçmüştür. Bu ölçek, öğrencileri bilgilendirmek, eğitmek, aktif sayısal vatandaşlar haline getirmek ve sayısal vatandaşlığın daha üst seviyelerine ulaştırmak için gerekli olan faktör ve koşulları önermek açısından önemli etkilere sahiptir. Çalışmanın sonucunda, öğrencilerin sorumluluk almasının, proje tabanlı çevrimiçi bir topluluğun üretken üyesi olmasının önemi vurgulanmış; geleneksel ve çevrimiçi toplulukları olumsuz yönde etkileyebilecek faaliyetlerden kaçınarak belirli bir çevrimiçi topluluğa özgü yönetim sistemlerini organik olarak geliştirmelerine yardımcı olmalarının öğretilmesi gerektiği belirtilmiştir.

Obschonka, Fisch ve Boyd (2017) süperstar (en etkili liderler) girişimci ve yönetici kişiliklerin iç görülerini anlamak için sayısal ayak izlerini araştırmışlardır. En etkileyici ve güçlü iş dünyası liderlerinden Twitter kullananların örneklemine belirlemek için başka araştırmalarda çok iyi oluşturulmuş ve önceden denenmiş olan listeleri kullanmışlardır. Bireylerin özellikle Twitter mesajlarını temel alan bilgisayarlı bir metin analiz aracı yardımıyla etkili iş liderlerinin 106'sının kişilik özelliklerini karşılaştırmışlardır. Bulgular süperstar yöneticilerin, süperstar girişimcilerden daha girişimci olduklarını göstermiştir.

Azucar, Marengo ve Settanni (2018) yaptıkları çalışmada, Big 5 kişilik özellikleri üzerinde sosyal medyadan toplanan sayısal ayak izinin tahmin edici gücünü ortaya koyabilmek için bir dizi meta analizler gerçekleştirmişlerdir. Scopus, ISI Web of Science, Pubmed, Proquest ve Google Akademik veri tabanlarında birden çok anahtar kelime grubunu kullanarak alanyazın taraması yapmışlardır. Sosyal medya ve Big 5 kişilik özellikleri konusunda yapılmış ve sayısal ayak izine odaklanan 24 araştırmaya ulaşılmıştır. Bununla birlikte sadece Big 5 kişilik özelliklerini ele alan 28 çalışma bulunmuştur. Bu çalışmaların 19 tanesinde Facebook, 5 tanesinde Twitter, 3 tanesinde SinaWebio mikro blog sitesi ve 1 tanesinde Instagram ve Twitter birlikte kullanılmıştır. Yapılan meta analiz sonucunda Big 5 kişilik özelliklerinin sosyal medyaki sayısal ayak izleri kullanılarak ortaya konulabileceği bulunmuştur. Böylece Big 5 kişilik özelliklerinin doğru tahminleri çevrimiçi pazarlama ve reklamcılık, uyarlanabilir ve kişiselleştirilmiş sistemler gibi alanlarda kullanılabileceği sonucuna varılmıştır.

Bölüm 3

Yöntem

Bu bölümde araştırmanın yönteminden, çalışma grubundan, veri toplama araçlarından, veri toplama sürecinden, yapılan istatistiksel analizlerden, geliştirilen ortamın tasarımından ve uygulama sürecinden bahsedilmiştir.

Araştırmanın Yöntemi

Bu çalışma tek gruplu ön test son test ölçümlü deneysel araştırma yöntemi ile desenlenmiştir. Bu yöntem, tekrarlı ölçümlü tek faktörlü deneysel araştırma yöntemi olarak da adlandırılmaktadır. Bu yöntemde tek bir grubun, deneysel işlem öncesi ve deneysel işlem sonrası bağımlı değişkeninde meydana gelen değişiklikler ölçülür ve karşılaştırılır. Söz konusu karşılaştırma sonrasında meydana gelebilecek olası farklılığın deneysel işlemden kaynaklanabileceği kısmen ileri sürülebilir (Creswell, 2012). Yapılan uygulamanın şematik gösterimi Tablo 8’de sunulmuştur.

Tablo 8

Araştırma Deseni

Grup	Ön Test	İşlem / Uygulama	Son Test
5. ve 6. sınıf öğrencileri	Sayısal Vatandaşlığa İlişkin Akademik Başarı Testi	7 Haftalık Sayısal Ayak İzi Ders Tasarımı	Sayısal Vatandaşlığa İlişkin Akademik Başarı Testi

Tablo 8’de de görülebileceği gibi sayısal ayak izi ders tasarımının öğrencilerin sayısal vatandaşlık konusundaki akademik başarılarına olan etkisini incelemek için, öğrencilere öncelikle ön test uygulanmış, 7 haftalık bir ders uygulaması sonrasında da son test uygulanmıştır. Uygulama toplam 9 hafta sürmüştür.

Bu araştırmada seçilen yöntemin zayıf deneysel desen olmasının sebebi, uygulama yapılan okulda 5. ve 6. sınıf öğrencilerinin mevcudunun düşük olması, farklı ve daha güçlü bir deneysel çalışmanın kontrol grubunu oluşturacak kadar yeterli öğrencinin olmamasıdır.

Çalışma Grubu

Araştırmanın çalışma grubunu Hatay'ın Reyhanlı ilçesinde yer alan Özel Reyhanlı Şahika Koleji'nde 2016-2017 Eğitim - Öğretim yılında öğrenim gören 5. ve 6. sınıflardan toplam 49 öğrenci oluşturmuştur. Öğrencilerin yaş ve cinsiyetlerine ilişkin demografik bilgileri Tablo 9'da sunulmaktadır.

Tablo 9

Çalışma grubunun cinsiyetlerine ilişkin demografik bilgiler

Sınıf Seviyesi	Kız Öğrenci Sayısı	Erkek Öğrenci Sayısı	Toplam Öğrenci Sayısı
5. Sınıf	16	20	36
6. Sınıf	9	4	13
Toplam	25	24	49

Tablo 9'da görüldüğü gibi, araştırmaya katılan 5. sınıf öğrencilerinin 16'sının kız, 20'sinin erkek olmak üzere toplam 36 mevcuda sahip oldukları söylenebilir. 16 kız öğrencinin 1 tanesi 10 yaşında, diğer tüm kız öğrencilerle 20 erkek öğrenci ise 11 yaşındadır. 6. sınıf öğrencilerinin ise 9'unun kız, 4'ünün erkek olmak üzere toplam 13 mevcuda sahip oldukları, kız öğrencilerden 1 tanesinin 11, diğer tüm 6. sınıf öğrencilerinin ise 12 yaşında oldukları da bilinmektedir.

Veri Toplama Araçları

Araştırmada problem durumunun sınanması için sayısal vatandaşlık konusundaki akademik başarıyı ölçebilecek bir başarı testinin hazırlanması gerekmiştir. Bu amaçla öğretim programında yer almadığı halde sayısal ayak izi ve sayısal vatandaşlık konularına eklenen kazanımlara ilişkin 48 madde yazılmıştır. Soruların hazırlanması aşamasında Ankara'nın Çankaya ilçesinde yer alan Özel Arı Okullarındaki 2 Bilişim Teknolojileri Öğretmeninden uzman görüşü alınmıştır. Söz konusu öğretmenler hazırlanan başarı testi taslağını incelemişler ve uygun olmadığını düşündükleri 13 maddeyi çıkarmışlardır. 4 öğretim üyesi ve 3 araştırma görevlisinin görüşleri doğrultusunda 35 maddelik 4 seçenekli başarı testi taslağına son şekli verilmiştir. Hazırlanan bu başarı testi ön test ve son test olarak kullanılmıştır (Ek B). Testin konu dağılımı ve soru sayıları Tablo 10'da gösterilmiştir:

Tablo 10

Ön Test- Son Test Konu-Soru Dağılımı

Konu	Soru Sayısı
Temel Kavramlar	7
Güvenli İnternet	7
Etkili İnternet	4
Sayısal Vatandaşlık	5
Siber Zorbalık	4
Siber Taciz	3
Sayısal Ayak İzi	5
Toplam	35

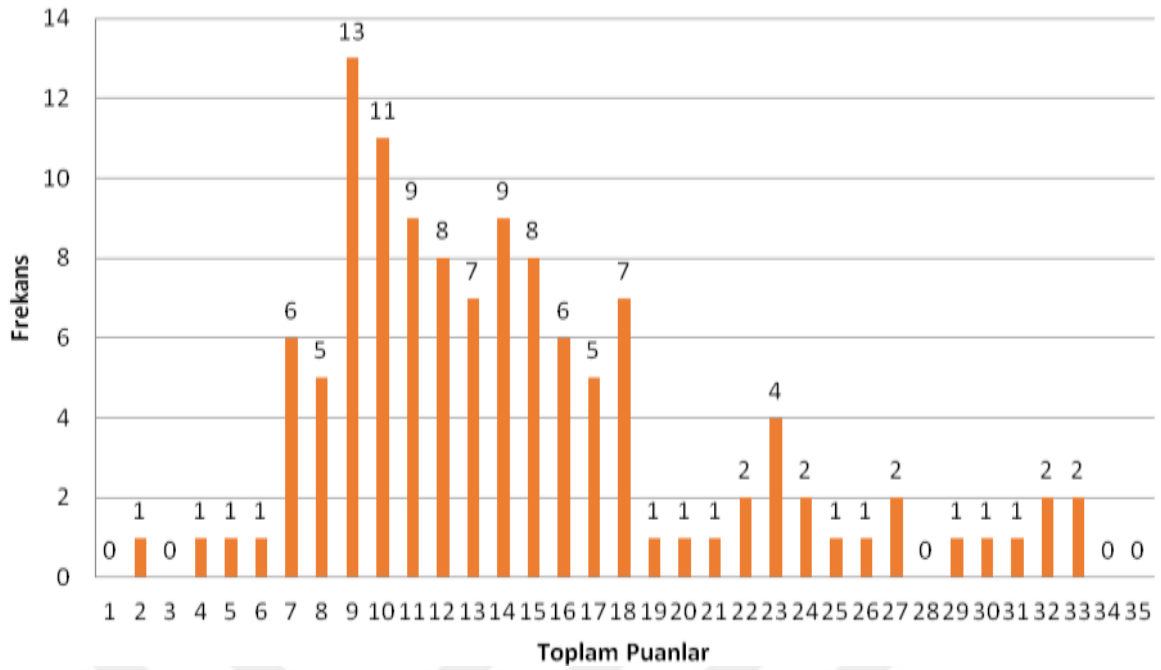
Tablo 10’da görülebileceği gibi test:

- temel kavramlar
- güvenli internet kullanımı
- etkili internet kullanımı
- sayısal vatandaşlık kuralları
- siber zorbalık
- siber taciz
- sayısal ayak izi

konularından oluşmaktadır.

Sayısal ayak izi ders tasarımının etkililiğini ölçmek amaçlı hazırlanmış olan başarı testi, testin geliştirilme sürecinde Özel Arı Okulları’nda 2016-2017 Eğitim - Öğretim yılında 5. ve 6. sınıf öğrencilerine uygulanmıştır. Başarı testi, toplam 141 öğrenciye uygulanmış, ancak başarı testini tamamlamayan 21 öğrencinin sonuçları değerlendirmeye alınmamıştır. Uygulamada toplam 120 öğrencinin verileri değerlendirmeye alınmıştır.

Soruyu yanlış yanıtlayan, boş bırakan ve bir soruda birden fazla seçeneği işaretleyenlere 0 puan verilmiş, doğru cevaplayanlara 1 puan verilmiştir. Öğrencilerin testten alabilecekleri en yüksek puan 35’tir. Test puanlarının dağılım grafiği Şekil 2’de verilmiştir:



Şekil 2. Öğrencilerin başarı testi puanlarının dağılımı

Şekil 2’de verilen grafiğe göre, öğrencilerin aldıkları puanların 7-18 puan aralığında toplandığı görülmektedir. Buna göre puanların sağa çarpık bir dağılım gösterdiği söylenebilir. Yapılan başarı testine ilişkin betimsel istatistikler Tablo 11’de verilmiştir.

Tablo 11

Başarı Testine İlişkin Betimsel İstatistikler

N	Ort	SS	Varyans	Min.	Max.	Çarpıklık	Basıklık
120	14,45	6,580	43,308	2,00	33,00	1,072	,821

Tablo 11’den de görüldüğü gibi testin ortalaması 14,45 bulunmuştur. En düşük puan 2, en yüksek puan 33 olduğundan ranj 31’dir. Standart sapmanın ise, 6,580 olduğu görülmüştür.

Veri toplama araçlarının güvenilir olabilmesi için testin Cronbach Alpha güvenilirlik katsayısının 0,70 değerinin üzerinde olması gerektiği belirlenmiştir. (Büyüköztürk, 2010; Özdamar, 2004). Testin Cronbach Alpha güvenilirlik katsayısı 0,848 olarak hesaplanmıştır. Bu sonuç başarı testinin güvenilir ölçümler yapabileceği sonucunu ortaya koymaktadır.

Testin madde analizi sonuçları Tablo 12’de sunulmaktadır.

Tablo 12

Testin Madde Analizi

	Düzeltilmiş Madde-Toplam Korelasyon Katsayısı	Madde Silindiğinde Cronbach Alpha Değeri
madde1	,102	,850
madde2	,286	,846
madde3	,291	,845
madde4	,283	,846
madde5	,503	,840
madde6	,496	,840
madde7	,286	,846
madde8	,445	,841
madde9	,379	,843
madde10	,354	,844
madde11	,413	,842
madde12	,139	,850
madde13	,382	,843
madde14	,411	,842
madde15	,492	,840
madde16	,058	,851
madde17	,409	,842
madde18	,503	,840
madde19	,511	,840
madde20	,256	,846
madde21	,155	,849
madde22	,192	,848
madde23	,425	,842
madde24	,442	,841
madde25	,492	,840
madde26	,353	,844
madde27	,448	,842
madde28	,433	,842
madde29	,181	,848
madde30	,132	,849
madde31	,337	,844
madde32	,324	,845
madde33	,378	,843
madde34	,215	,848
madde35	,407	,843

Madde-toplam korelasyon katsayısının $+0.25$ 'ten büyük olması ve eksi işaretli olmaması istenir (Alpar, 2014). Bu katsayı, her maddenin toplam puan ile bağıntı gösterip göstermediğini belirlemekte kullanılır. Madde silindiğinde Cronbach Alpha bölümü maddenin ölçekten çıkarılması halinde oluşacak alpha değerini gösterir. Normalde bulunan alpha değerinden oldukça yüksek değerler bulunuyorsa, maddenin çıkarılması iç tutarlılığı artırır (Akbulut, 2010).

Madde-toplam korelasyon katsayısındaki değerler kontrol edildiğinde; madde 1, madde 12, madde 16, madde 21, madde 22, madde 29, madde 30 ve madde 34'ün madde-toplam korelasyon katsayısının 0.25 'ten küçük olduğu görülmüştür. Ancak bu maddelerin, madde silindiğinde Cronbach Alpha

değerlerine bakıldığında oluşacak Alpha değerinde büyük bir değişim olmadığı görüldüğü ve ölçeğin kapsam geçerliğinin de düşmemesi istendiği için maddeler ölçekten çıkarılmamıştır. Tüm maddelerin madde silindiğinde Cronbach Alpha değerinin, testin Cronbach Alpha katsayısı ile çok yakın olduğu görülmüştür. Dolayısıyla herhangi bir maddenin çıkarılmamasına karar verilmiştir.

Uygulama Süreci

Araştırma için öncelikle Hacettepe Üniversitesi Etik Komisyonu'ndan araştırmanın yapılabilmesi amacıyla etik onay alınmıştır (Ek J). Uygulaması yapılacak olan sayısal ayak izi ders tasarımının kazanımları hazırlanmış, kazanımların uygunluğunu kontrol etmek için Bilgisayar ve Öğretim Teknolojileri Ana Bilim Dalındaki 4 öğretim üyesi ve yine bu alandaki 3 Araştırma Görevlisi olmak üzere toplam 7 öğretim elemanından görüş alınmıştır. Farklı görüşler değerlendirilmiş, danışman öğretim üyesi ile birlikte alınan ortak kararlarla kazanımlar düzenlenmiştir. Kazanımlara uygun olarak ders planları 2014'ten beri Bilişim Teknolojileri ve Yazılım dersi öğretmeni olan araştırmacının kendisi tarafından hazırlanmış ve danışman öğretim üyesi ile incelenerek düzenlenmiştir (Ek C). Okul yönetiminden gerekli izinler, velilerden veli onam formu ve öğrencilerden gönüllü katılım onayı alınarak Özel Reyhanlı Şahika Koleji'ndeki 5. ve 6. sınıf öğrencilerine ön test ve son test uygulanmıştır. Uygulama süreci, Bilişim Teknolojileri ve Yazılım dersi kapsamında toplam 9 hafta sürmüştür (1 hafta ön test, 7 hafta uygulama, 1 hafta son test). Uygulamanın tamamı araştırmacı tarafından gerçekleştirilmiş ve öğretmen bu süreçte zaman zaman bilgiyi aktarırken davranışçı yaklaşımı temel alıp aktif anlatıcı olsa da genel olarak bilişsel yaklaşımı temel alarak öğrencilerin yeni bilgileri organize etmelerini ve mevcut bilgiyle ilişkilendirmelerini sağlayarak, öğrencilerin dikkatini, bilgiyi kodlamasını ve hatırlamasını sağlayıcı etkinlikler sunmuştur. Haftalık etkinlikler bu ders planına uygun olarak sırasıyla yürütülmüştür.

Uygulamanın ilk haftasında öğrencilere çalışmanın amacından bahsedilmiş ve çözmeleri için 35 soruluk ön test dağıtılmıştır.

İkinci hafta sayısal ayak izi ile ilgili önce soru cevap, daha sonra önceden hazırlanmış sunu (Ek Ç) ile temel kavramlar tanıtılmıştır. Ders sonunda temel

kavramların tanımları tek tek kartlara yazılarak öğrencilerin kartlardaki tanıma ait kavramı bulmaları istenmiştir.

Üçüncü hafta sayısal vatandaşlık kavramının tanımı öğrencilerden istenmiştir. Ders önceden hazırlanmış olan sunu (Ek D), “Sayısal Yurttaşlık Kuralları” videosu (Keşf@ Bilinçli İnternet Hareketi, 2015) ve sorular eşliğinde işlenmiştir.

Dördüncü hafta güvenli internet kuralları önceden hazırlanmış olan sunu eşliğinde öğrencilere sunulmuştur (Ek E). “Çevrimiçi dünyada güvenli bir şekilde gezmek” videosu (epaydas, 2011) izletilmiş, soru ve cevaplar ile güvenli internet kullanımı güçlendirilmiştir. Güçlü şifreler ile ilgili önceden hazırlanmış sunu öğrencilere verilerek güçlü şifre yazdırma etkinliği yapılmıştır.

Beşinci hafta internette etkili arama yapmayla ilgili sunu eşliğinde öğrencilere uygulamalar yaptırılmıştır (Ek F). İlgili afiş sınıfta asılarak öğrencilerin incelemesi istenmiştir (Ek G). Öğrencilere web sayfası değerlendirme formu (Ek Ğ) dağıtılarak üçerli gruplara ayrılmış, her gruba vikipedi, ekşi sözlük, uludağ sözlük, e-okul seçeneklerinden biri verilerek siteleri incelemeleri ve ölçüte göre değerlendirmeleri istenmiştir.

Altıncı hafta öğrencilere ipuçları verilerek siber zorbalık tanımından yola çıkarak siber zorbalık davranışlarını bulmaları sağlanmıştır. Bu davranışlar tahtaya yazılarak öğrencilere bununla ilgili bir afiş hazırlatılmış ve sınıfa asılmıştır. Öğrencilere, siber zorbalığa maruz kalma durumunda neler yapabilecekleri sorularak, ipuçlarıyla cevap bulmaları sağlanmış ve tahtaya yazılmıştır. “Bir Sanal Zorbalık Hikayesi” isimli video (Dilan, 2014) izletilerek öğrencilerden slogan bulup yazmaları istenmiştir. Siber taciz konusu sunu eşliğinde sunulmuş (Ek H) ve siber tuzakların neler olduğunu anlatan afiş sınıfa asılmıştır (Ek I). “İnternette Siber Tuzaklar” videosu (Tutaysalgır, 2012) öğrencilere izletilmiştir.

Yedinci ve sekizinci hafta gizlilik ve veri korumayla ilgili sorular sorularak derse başlanmıştır. Öğrenciler Facebook, Instagram, Youtube gibi sosyal medya sitelerinde gizlilik politikaları ve ayarları incelemek için 2 ya da 3 gruba ayrılarak, öğrencilerin birtakım gizlilik ve güvenlik sorularına cevap aramaları istenmiştir. Yardımcı olmak açısından öğrencilere bazı site kaynakları verilmiştir. Öğrencilerin ortak karar vererek gizlilik ve çevrimiçi koruma sorumluluğunu sağlamak için en iyi

5 püf noktayı seçmeleri istenmiştir. Childnet International'ın sayfasından alınıp Türkçeye çevrilerek hazırlanmış olan Çevrimiçi İtibar Kontrol Listesi (Online Reputation Checklist) sınıfa asılmıştır (Ek İ). İz bırakan bilgilerle ilgili sorular öğrencilere sorulmuştur. Olumlu sayısal ayak izinin nasıl bırakılabileceğine yönelik soru ile öğrencilerin olumlu izler bırakmaları teşvik edilmiştir.

Dokuzuncu hafta öğrencilere son test uygulanarak uygulama son bulmuştur.

Verilerin Analizi

Araştırma probleminin sınanmasında öğrencilerin ön test ve son test başarı puanları arasındaki farklar, ilişkili örneklem için t testi (paired samples t-test) ile incelenmiştir. İlişkili örneklem için t testi öncesinde istatistiksel varsayımlar sınanmıştır.

Araştırmanın amacına uygun olarak öğrencilerin ön test ve son test başarı puanları arasında anlamlı bir farklılık olması beklenmektedir. Bunun için öğrencilerin ön test ve son testten aldıkları puanların ortalamaları hesaplanmış ve ortalamalar arasındaki fark ele alınmıştır. Araştırma verilerinin çözümlenmesinde 0,05 anlamlılık düzeyi temel alınmıştır. Yapılan analizin etki büyüklüğünü incelemek için ise Cohen's d değeri hesaplanmıştır.

Araştırmanın İç ve Dış Geçerliliği

Bu çalışmada iç geçerliliği ve dış geçerliliği tehdit eden faktörler ve alınan önlemler aşağıda verilmiştir.

Araştırmanın İç Geçerliliği. İç geçerlik, bağımlı değişken üzerindeki değişimin gerçekten bağımsız değişkenden kaynaklı olup olmadığını gösteren geçerlilik türüdür (Fraenkel, Wallen ve Hyun, 2012). İç geçerliliği sağlamak amacıyla:

Katılımcılar aynı sınıftan ve gönüllülük esasına dayalı olarak araştırmaya dahil edilmiş, dolayısıyla öğrencilerin yaşantıları ve önbilgilerinin birbirine benzer olmasına çalışılmıştır.

Araştırmanın uygulaması ders süreci içerisinde yapılmış ve uygulamanın normal bir ders gibi olacağı, sonuçlarının kendilerini dersten farklı olarak

etkilemeyeceđi belirtilmiř, böylece öğrencilerin normalden fazla gayret göstermelerinin önüne geçilmiştir. Ortamın iç geçerliđi etkilememesi için ön test ve son test öğrencilere aynı sınıf ortamında uygulanmıştır.

Ölçme aracının geçerliđini etkilememek için verilerin toplanması ve değerlendirilmesi süreci arařtırmanın kendisi tarafından yapılmıř, bu sürece başkaları müdahale etmemiřtir.

Nicel verilerin toplanmasında kullanılan başarı testi bütün katılımcılara aynı şartlar altında ve eşit süre verilerek uygulanmıştır.

Arařtırmanın Dış Geçerliđi. Dış geçerlik, arařtırma sonuçlarının evrene genellenebilirliđi olarak tanımlanmıştır (Fraenkel, Wallen ve Hyun, 2012). Bu arařtırmanın sonuçları sadece benzer özelliklerdeki katılımcı gruplarına genellenebilir. Bu arařtırmanın sonuçlarını genelleyebilmek için gerekli olan çalışma grubunun özellikleri, veri toplama araçları ve veri analizi arařtırmanın yöntem bölümünde ayrıntılarıyla raporlanmıştır.

Bölüm 4

Bulgular

Bu bölümde sayısal ayak izi ders tasarımının öğrencilerin sayısal vatandaşlık konusundaki akademik başarılarına etkisini incelemek üzere yapılan ön test ve son test verilerinin anlamlı farklılık gösterip göstermediğine ilişkin bulgulara yer verilmiştir.

Araştırmanın Problemine Ait Bulgular

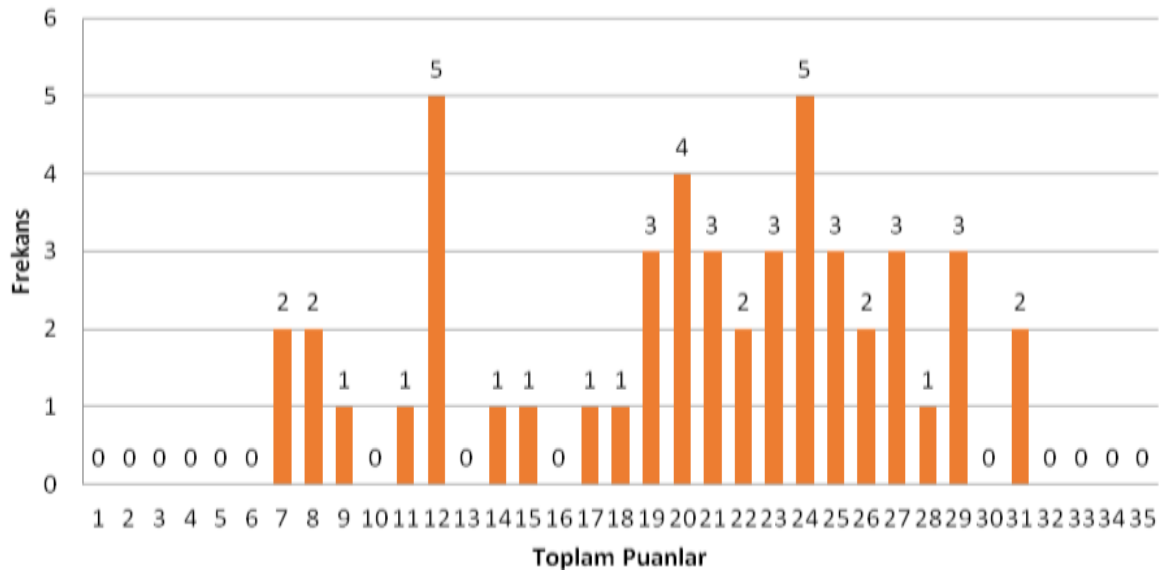
Çalışma grubunun ön test ve son test puanlarına ilişkin betimsel istatistikler Tablo 13'te verilmiştir:

Tablo 13

Çalışma Grubunun Ön Test ve Son Test Puanlarına İlişkin Ortalama ve Standart Sapma Değerleri

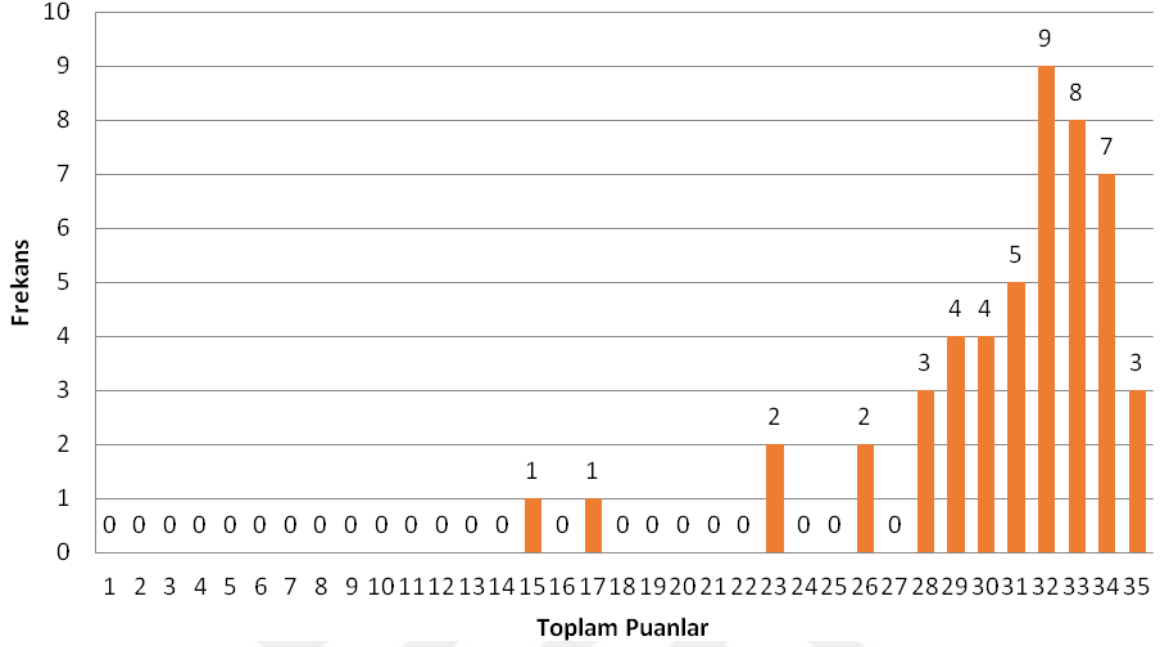
	N	Ort.	SS
Ön Test	49	20,24	6,74
Son Test	49	30,61	4,14

Tablo 13'te çalışma grubunun ön test ve 7 haftalık uygulamadan sonraki hafta yapılan son test puanlarına ait ortalama ve standart sapma bilgileri verilmiştir. Buna göre ön test puanlarının ortalaması 20,24, son test puanlarının ortalaması 30,61'dir. Ön test ve son test puanları arasında 10,37 puanlık bir fark olduğu görülmektedir. Şekil 3'te öğrencilerin ön testten aldıkları puanların dağılım sıklığına ait grafik verilmiştir.



Şekil 3. Ön test puanlarının dağılımı

Şekil 3'te görüldüğü gibi öğrencilerin ön test puanları 7 ile 31 aralığında dağılmaktadır. Şekil 4'te öğrencilerin son testten aldıkları puanların dağılım sıklığına ait grafik verilmiştir.



Şekil 4. Son test puanlarının dağılımı

Şekil 4'te görüldüğü gibi öğrencilerin son test puanları 15 ile 35 aralığında dağılmakta, ancak 28 ile 35 aralığında yığılma göstermektedir.

Öğrencilerin sayısal vatandaşlık konusundaki akademik başarılarını ölçen ön test ve son test puanları arasındaki değişim anlamlı mıdır? sorusunun yanıtlanmasında ilişkili örneklem t-testi yapılmıştır. Bu analiz öncesinde, ilişkili örneklem t-testinin varsayımları sınanmıştır. Öncelikle ön test ve son test sonuçlarının sürekli değişken olduğu bilinmektedir. Ön test ve son test puanları arasındaki fark istatistiğinde herhangi bir aykırı değer olup olmadığı incelenmiş, yapılan analizlerde bir aykırı değer olmadığı görülmüştür. Ayrıca normallik varsayımı da araştırılmıştır. Normal dağılım varsayımının sağlanabilmesi için çarpıklık (skewness) ve basıklık (kurtosis) değerlerinin +1 ve -1 değerlerinin arasında olması gerekmektedir (McKillup, 2012; Tabachnick & Fidell, 2013). Ayrıca, Kolmogorov - Smirnov ve Shapiro - Wilk testlerinin istatistiksel olarak anlamlı olmaması ($p > .05$) gerekmektedir (Field, 2005). Elde edilen bulgulara göre çarpıklık değerinin mutlak değerinin .120 olduğu, basıklık değerinin mutlak değerinin ise .351 olduğu görülmüştür. Ayrıca normallik varsayımı için yapılan

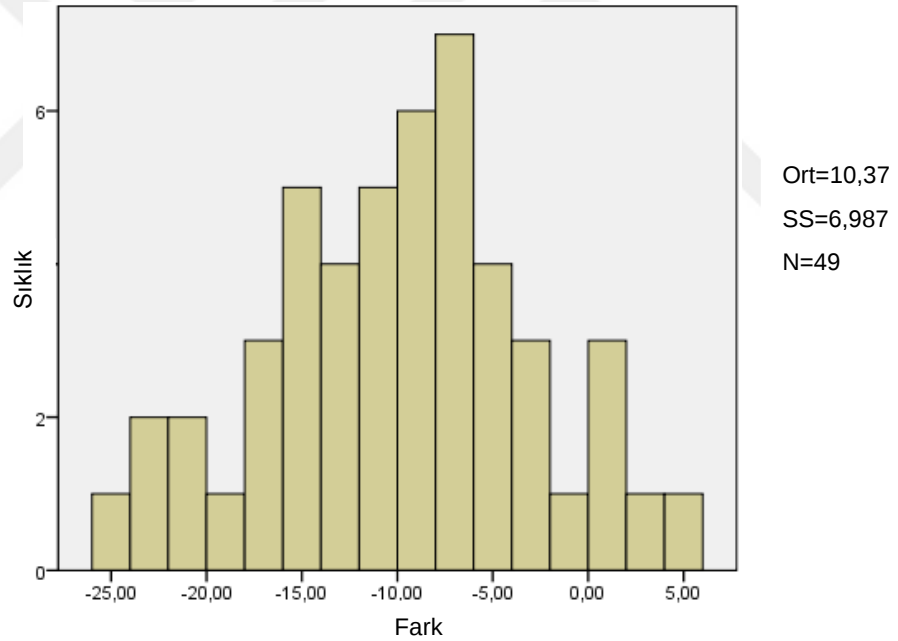
Kolmogorov - Smirnov ve Shapiro - Wilk testlerine ilişkin sonuçlar da Tablo 14'de sunulmuştur.

Tablo 14

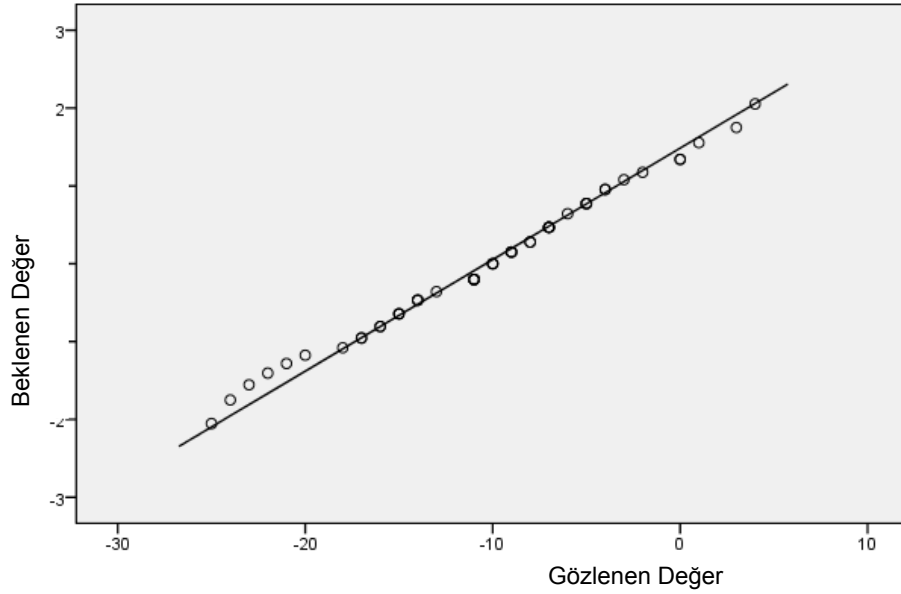
Normallik Testi Sonuçları

	Kolmogorov-Smirnov			Shapiro-Wilk		
	İstatistik	sd	Sig.	İstatistik	sd	Sig.
fark	.097	49	.200	.986	49	.803

Tablo 14 incelendiğinde hem Kolmogorov- Smirnov, hem de Shapiro-Wilk testlerinin istatistiksel olarak anlamsız olduğu ve veride normal dağılım sorunu olmadığı görülmektedir. Kolmogorov- Smirnov ve Shapiro-Wilk testlerinin sonuçları ile çarpıklık ve basıklık değerleri, normal dağılımın bir göstergesi oldukları için ilişkili örneklem t-testinin yapılabileceğine karar verilmiştir. Ayrıca Şekil 5'de fark istatistiğine ilişkin histogram ve Şekil 6'da ise yine fark istatistiğine ilişkin Q-Q grafiği sunulmuştur.



Şekil 5. Fark istatistiğine ilişkin histogram



Şekil 6. Fark istatistiğine ilişkin Q-Q grafiği

Şekil 5’de verilen histograma göre, verilerin normal dağılıma uygun olarak dağıldığı söylenebilir. Ayrıca Şekil 6’ya göre de, beklenen değerlerin gözlenen değerlerle oldukça benzer bir dağılım gösterdiği görülmektedir.

Ön test ve son test puanları arasında anlamlı bir fark olup olmadığını tespit etmek üzere yapılan ilişkili örneklem t-testi sonuçları Tablo 15’te sunulmuştur.

Tablo 15

Çalışma Grubunun Ön Test ve Son Test Puanlarına İlişkin İlişkili Örneklem T-Testi Sonuçları

Grup	Ort.	SS	t	sd	p
Ön test – Son test	-10,36735	6,97822	-10,400	48	,000

Çizelge 14’te görüldüğü gibi t değeri -10,40, serbestlik derecesi (sd) 48, gözlenen alfa düzeyi ise .05’in altında bulunmuştur. Yani t tablosunda belirtilen kritik alfa düzeyinin oldukça altındadır. Bu bağlamda öğrencilerin son test ortalamalarının (30,61) ön test ortalamalarından (20,24) oldukça yüksek olduğu ve aralarındaki farkın istatistiksel olarak anlamlı olduğu [$t_{(48)}=-10,40$, $p<.05$] bulunmuştur. Bu anlamlılığın etkisini inceleyebilmek için, grup ortalama farkına göre hesaplanan etki büyüklüğü değerlerinden Cohen’s d değerinden yararlanılmıştır. Söz konusu değer hesaplanırken aşağıda verilen iki formül temel alınmıştır.

$$d = \frac{\text{Ortalama}}{\text{Standart Sapma}}$$

$$d = \frac{t}{\sqrt{N}}$$

Her iki formüle göre de hesaplandığında Cohen's d deęerinin 1.486 olduęu g r lm şt r. Bu deęer Sawilowsky'e (2009) g re  ok geniř bir etki b y kl ę ne karřılık gelmektedir. Bu sonu  sayısal ayak izi ders tasarımınn  ęrencilerin sayısal vatandaşlık konusundaki akademik başarılarına etkisinin istatistiksel olarak anlamlı olduęunu ve bu etkinin de  ok geniř olduęu ortaya koymaktadır.



Bölüm 5

Sonuç, Tartışma ve Öneriler

Bu çalışmada, sayısal ayak izi ders tasarımının öğrencilerin sayısal vatandaşlık konusundaki akademik başarılarına etkisi incelenmiştir. Bu bölümde, araştırma bulgularına dayalı olarak ortaya konan sonuçlara ve tartışmaya, aynı zamanda bu çalışmayı ileri götürebilecek bazı önerilere yer verilmiştir.

Sonuç ve Tartışma

Dünyanın her yerinde yaygın olarak kullanılan internet teknolojileri hayatın bir parçası haline gelmiştir. Bu teknoloji insanların hayatında bir ihtiyaç olmaktan öteye geçerek yaşamın vazgeçilmez unsurları arasında yer almaya başlamıştır. Birçok faydasının yanında bilinçsiz kullanımından doğan riskleri ve geri dönüşü olmayan hataları da beraberinde getirmiştir. Söz edilen dönüşü olmayan ve geleceği etkileyen hatalar insanların sayısal ayak izlerinin bir parçası olup, onların sayısal vatandaş olarak kimliklerinde yer almaktadır. Sayısal ayak izinin oluşumu ise bir fare tıklaması ya da klavye tuşu ile başlamaktadır. Sayısal kimliği oluşturan bu izler bireylerin gelecekteki yaşantılarını olumlu ya da olumsuz yönde etkilemektedir. Gerek iş gerek sosyal yaşantıda bireylerin izleri takip edilebilmekte ve birtakım kararlar konusunda ön ayak oluşturabilmektedir. Oluşan sayısal ayak izlerinin asla silinememesi ve internet dünyasında sonsuza dek yer alması teknolojinin içine doğan yeni nesil için bir kırmızı ışıktır. Bu nedenle yapılan araştırma ile sayısal ayak izinin bilinçli bir şekilde yönetilmesinin önemli olduğu ayrıntılarıyla açıklanmış ve bu konuyla ilgili kazanımların Bilişim Teknolojileri ve Yazılım dersinin kazanımlarına bütünleştirilmesi önerilmiştir. Bu çalışmada ilköğretim 5. ve 6. sınıf öğrencilerinin sayısal vatandaşlık konusundaki akademik başarılarını ölçmek amacıyla sayısal ayak izi ile ilgili bir ders tasarlanıp uygulanmıştır. Daha sonra, uygulama öncesi ve sonrasında sayısal vatandaşlık konusundaki akademik başarı puanları arasında anlamlı bir fark olup olmadığının belirlenmesi amaçlanmıştır.

Araştırma problemiyle ilgili olarak ön test ve son testten elde edilen veriler incelendiğinde son test puanlarının ön test puanlarına göre artış gösterdiği görülmektedir. Ayrıca, sayısal ayak izi ders tasarımının öğrencilerin sayısal vatandaşlık konusundaki akademik başarıları üzerinde anlamlı bir etkisi olduğu

sonucuna ulařılmıştır. Bu sonular ğrencilerin verilen eēitimden nce sayısal ayak izleri ve bunun gelecekteki yařantılarına etkileri konusunda yeterli bilince sahip olmadıklarını ortaya koymuřtur. Alanyazındaki alıřmalar insanların bu konudaki bilinsizliēini destekler niteliktedir (Camacho, Minelli ve Grosseck, 2012; Moore ve McElroy, 2012; Odabařı ve arkadaşları, 2015). DIGCOMP isimli projenin raporu da sayısal yeterliliēin oluřturulması aısından sayısal kimlik, sayısal ayak izi ve itibar konularının ierikte yer almasının gerekliliēini vurgulamaktadır (Ferrari, 2013).

Her teknolojik ilerleme, teknolojik alanlardaki okuryazarlık becerilerine eklenmesi gereken yeni becerileri beraberinde getirmektedir. Bireylerin kendilerini ve başkalarını evrimii olarak sunma konusunda ise eleřtirel bir tutum sergileyerek sayısal ayak izlerini ve itibarlarını korumayı ğrenmeleri nemli bir noktadır. Bireylere, evrimii olmanın tam olarak ne anlama geldiēinin ve gerek yařamda ortaya ıkarabileceēi etkilerinin kavratılması gerekmektedir (Costa & Torres, 2011). Bu sonu, yapılan bu arařtırmanın temel sonuları ile de rtřmektedir.

Yang ve Chen'in (2010) ğretmenlerin algıları zerine kurguladıkları arařtırmalarında ulařtıkları sonular ile bu arařtırmanın bulguları paralellik gstermektedir. Sz konusu arařtırmada ğretmenler, telif hakkı ve fikri mlkiyet konularının ēretimine dikkat ekilmesi gerektiēini ileri srmřlerdir. Yapılan bu alıřma da sayısal ayak izi farkındalıēına iliřkin yapılan ders tasarımıının amacına ulařtıēını gstermiř ve ğrencilerin sayısal vatandaşlık konusundaki akademik başarılarının arttıēını ortaya koymuřtur.

Kaya ve Kaya'nın (2014) ğretmen adayları zerine yaptıkları alıřma sonularına gre ğretmen adaylarının oēunun okullarda sayısal vatandaşlık eēitiminin verilmesinin gerekliliēi konusundaki grřleri ve sayısal teknolojiyi kullanırken interneti gvenli kullanmayı nemsemeleri, yapılan alıřmanın sonularını desteklemektedir.

Jones ve Mitchell (2016), geliřtirdikleri sayısal vatandaşlık lēēi ile ğrencilerin siber zorbalık, siber taciz ve bu davranıřlara seyirci kalma durumları konularındaki bilgilerini lmek iin yaptıkları arařtırma ile sayısal vatandaşlık eēitiminin gerekliliēinin doēruluēunu kanıtlamıřlardır. Bu sonu da arařtırmanın

öne sürdüğü sayısal vatandaşlık konusunun öğretim programındaki öneminin artırılması yönündeki görüşle örtüşmektedir.

Öneriler

1. Bu araştırmada kullanılan son test, 2016-2017 Eğitim - Öğretim yılı 2. döneminin son haftalarında uygulanmıştır. Dolayısıyla araştırmada akademik başarının ötesinde kalıcılığın sağlanıp sağlanmadığı sınınamamıştır. İleride yapılacak çalışmalarda aynı başarı testi üzerinden kalıcılık da ölçülebilir. Böylece kazanımların uzun süreli olarak öğrencilerde yerleşip yerleşmediğinin de ölçülmesi mümkün olabilir.

2. Uygulamanın yapıldığı okuldaki sınıf sayısı ve öğrenci mevcudu yeterli olmadığından dolayı kontrol gruplu ve daha güçlü bir deneysel çalışma yapılamamıştır. Uygun şartlar sağlanıp daha güçlü bir deneysel desen tasarlanabilir ve elde edilen bulgular kontrol grubu ile sınıanabilir. Böylece deney grubu ile kontrol grubu arasındaki farklılığın gerçekten de deneyden kaynaklı olduğu daha güçlü olarak ileri sürülebilir. Mevcut deneysel desende araştırmacının araştırma sürecini dikkatlice takip etmiş olması, manipülasyon etkisini olabildiğince en aza indirmiştir.

3. Bilişim Teknolojileri ve Yazılım derslerinde sayısal ayak izi ve sayısal vatandaşlık konularına ağırlık verilmeli ve öğrencilerde bu kavramlara ilişkin bilincin yerleşmesi sağlanmalıdır. Öğrencilerin sayısal vatandaşlık konusundaki akademik başarıları, sayısal ayak izi ders tasarımıından etkilendiğine göre, öğrencilere sayısal ayak izi ile ilgili kazanımları kazandırabilecek faaliyetler yaptırılmalı ve konunun önemine dikkat çekilmelidir. Bununla ilgili olarak bu çalışmada eklenen kazanımların, Bilişim Teknolojileri ve Yazılım dersinin öğretim programı ile bütünleştirilmesi gerektiği düşünülmektedir.

4. Öğrencilerin sayısal vatandaşlık konusundaki akademik başarıları üzerinde demografik değişkenlerin etkisi de sınıanabilir.

5. Öğretmenlerin de sayısal ayak izine ilişkin farkındalıklarının araştırılması önerilebilir.

6. Bu araştırmada ortaya konan sonuçların boylamsal bir çalışma ile belirli bir zaman sonra yeniden teyit edilmesine gereksinim duyulduğu söylenebilir.

Kaynaklar

- Akbulut, Y. (2010). Sosyal bilimlerde SPSS uygulamaları: *Sık kullanılan istatistiksel analizler ve açıklanmalı SPSS çözümleri*. İstanbul: İdeal Kültür & Yayıncılık.
- Akca, E. B., Sayımer, İ., Salı, J. B. ve Başak, B. E. (2014). Siber zorbalığın nedenleri, türleri ve medya okuryazarlığı eğitiminin önleyici çalışmalardaki yeri. *Elektronik Mesleki Gelişim ve Araştırma Dergisi (EJOIR)*, 2, 17-30.
- Akkoyunlu, B., ve Yılmaz Soylu, M. (2010). Öğretmenlerin sayısal yetkinlikleri üzerine bir çalışma. *Türk Kütüphaneciliği*, 24(4), 748-768.
- Akkoyunlu, B. (2016). Sayısal ayak izim. Erişim adresi: <http://www.bilimiletisimi.com/show.php?id=2832>
- Alpar, R. (2014). *Spor, sağlık ve eğitim bilimlerinden örneklerle uygulamalı istatistik ve geçerlik-güvenirlik*. Ankara: Detay Yayıncılık.
- Azucar, D., Marengo, D., & Settanni, D. (2018). Predicting the big 5 personality traits from digital footprints on social media: a meta-analysis. *Personality and Individual Differences*, 124, 150-159. doi: 10.1016/j.paid.2017.12.018
- Belsey, B. (2007). Cyberbullying: a real and growing threat. *ATA Magazine*, 88(1), 14-21.
- Bilgi Teknolojileri ve İletişim Kurumu. (2016). *İnternetin riskleri ve zararları*. Erişim adresi: <http://internet.btk.gov.tr/internetin-riskleri-ve-zararlari-detay-61.html>
- Boyle, J. (2017). 11 tips for students to manage their digital footprints. Erişim adresi: <https://www.teachthought.com/technology/11-tips-for-students-tomanage-their-digital-footprints/>
- Büyüköztürk, Ş. (2010). *Sosyal bilimler için veri analizi el kitabı*. Pegem A Yayınları: Ankara.
- Camacho, M., Minelli, J., & Grosseck, G. (2012). Self and identity: raising undergraduate students' awareness on their digital footprints. *Procedia - Social and Behavioral Sciences*, 46, 3176 – 3181. doi: 10.1016/j.sbspro.2012.06.032

- Childnet International. (2013). *Online Reputation Checklist*. Erişim adresi: <http://www.childnet.com/resources/online-reputation-checklist>
- Choi, M, Glassman, M., & Cristol, D. (2017). What it means to be a citizen in the internet age: Development of a reliable and valid digital citizenship scale. *Computers & Education*, 107, 100-112. doi: 10.1016/j.compedu.2017.01.002
- Council of Europe. (2018). What is Digital Citizenship Education? Erişim adresi: <https://www.coe.int/en/web/digital-citizenship-education/what-is-dce>
- Commonwealth of Australia. (2014). *Digital footprint. In cybersmart*. Erişim adresi: <https://esafety.gov.au/esafety-information/esafety-issues/cyberbullying>
- Costa, C., & Torres, R. (2011). To be or not to be, the importance of Digital Identity in the networked society. *Educação, Formação & Tecnologias, (Special issue)*, 47-53.
- Creswell, J. W. (2012). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research*. Boston: Pearson.
- Çubukçu, A., ve Bayzan, Ş. (2013). Türkiye’de sayısal vatandaşlık algısı ve bu algıyı internetin bilinçli, güvenli ve etkin kullanımı ile artırma yöntemleri. *Middle Eastern & African Journal of Educational Research*, 5, 148-174.
- Digital citizenship adventures. (2017). *Managing your digital footprint*. Erişim adresi: <https://sites.google.com/site/digcitizenshipadventures/managing-your-digital-footprint>
- Dilan, T. (2014, 26 Nisan). Bir Sanal Zorbalık Hikayesi [Video]. Erişim adresi: <https://www.youtube.com/watch?v=N87aNk5Uohg>
- Epaydas (2011, 19 Temmuz). Çevrimiçi dünyada güvenli bir şekilde gezmek [Video]. Erişim adresi: <https://www.youtube.com/channel/UC6nhug9-6ln4Jph9HYDFUoQ>
- Ferrari, A. (2013). *DIGCOMP: A framework for developing and understanding digital competence in Europe*. JRC Scientific and Policy Reports. doi:10.2788/52966

- Field, A. (2005). *Discovering statistics using SPSS* (2nd ed.). London: Sage Publications.
- Fletcher, G., Griffiths, M., & Kutar, M. (2011, September). A day in the digital life: A preliminary sousveillance study. *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society*. Oxford Internet Institute, University of Oxford, UK.
- Fraenkel, J. R., Wallen, N. E., & Hyun, H. H. (2012). *How to design and evaluate research in education* (8th ed.). New York: McGraw-Hill Companies.
- Hewson, K. (2013). What size is your digital footprint? *Phi Delta Kappan*, 94(7), 14-22. doi: 10.1177/003172171309400704
- Hollandsworth, R., Dowdy, L., & Donovan, J. (2011). Digital citizenship in K-12: It takes a village. *Tech Trends: Linking Research and Practice to Improve Learning*, 55(4), 37-47. doi: 10.1007/s11528-011-0510-z
- Hengstler, J. (2017). Managing your digital footprint: Ostriches v. eagles. *Education for a Digital World*, 2(1), 89-139.
- International Society for Technology in Education. (2016). *ISTE Uluslararası Eğitim Teknolojisi Öğrenci Standartları*. Erişim adresi: https://www.iste.org/docs/pdfs/iste-standards_one-sheets_students-2016_turkish_v3.pdf
- Jones, L., M., & Mitchell, K., J. (2016). Defining and measuring youth digital citizenship. *New Media & Society*, 18(9), 2063-2079. doi: 10.1177/1461444815577797
- Kaya, A., & Kaya, B. (2014). Öğretmen adaylarının dijital vatandaşlık algısı. *International Journal of Human Sciences*, 11(2), 346-361. doi: 10.14687/ijhs.v11i2.2917
- Keşf@ Bilinçli İnternet Hareketi. (2015, 2 Kasım). Keşf@ Projesi - Dijital Yurttaşlık Kuralları [Video]. Erişim adresi: <https://www.youtube.com/watch?v=5ew2Nxb-b98&t=2s>
- Keşf@ Bilinçli İnternet Hareketi Projesi. (2017). *Bilgi Notları*. Erişim adresi: <http://www.kesfetprojesi.org/kesfet/iceriklist/kesfet-projesi/bilgi-notlari>

- Kim, W., Jeong, O.-R., Kim, C., & So, J. (2011). The dark side of the internet: Attacks, costs and responses. *Information Systems*, 36(3), 675-705. doi: 10.1016/j.is.2010.11.003
- Kuehn, L. (2012). Manage your digital footprint. *Our Schools / Our Selves*, 21(2), 67-69.
- Livingstone, S., Bober, M., & Helsper, E. (2005). Internet literacy among children and young people: Findings from the UK children go online project. London: LSE Research Online.
- Madden, M., Fox, S., Smith, A., & Vitak, J. (2007, Aralık). *Digital footprints: Online identity management and search in the age of transparency*. PEW Research Center Internet & Technology. Erişim adresi: <http://www.pewinternet.org/2007/12/16/digital-footprints/>
- Malhotra, A., Totti, L., Meira, W., Kumaraguru, P., & Almeida, V. (2012). Studying user footprints in different online social networks. *Proceedings of the 2012 International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2012)*, 1065-1070. doi: 10.1109/ASONAM.2012.184
- McKillup, S. (2012). *Statistics explained: An introductory guide for life scientists* (2nd ed.). United States: Cambridge University Press.
- Milli Eğitim Bakanlığı Talim ve Terbiye Kurulu Başkanlığı. (2012). *Ortaokul ve İmam Hatip Ortaokulu Bilişim Teknolojileri ve Yazılım Dersi (5, 6, 7 ve 8. sınıflar) Öğretim Programı*.
- Milli Eğitim Bakanlığı Talim ve Terbiye Kurulu Başkanlığı. (2017). *Bilişim Teknolojileri ve Yazılım dersi (Ortaokul 5. ve 6. sınıflar) Öğretim Programı*.
- Milosevic, T. (2016). Social media companies' cyberbullying policies. *International Journal of Communication*, 10, 5164–5185.
- Moore, K., & McElroy, J.C. (2012). The influence of personality on Facebook usage, wall postings, and regret. *Computers in Human Behavior*, 28(1), 267–274. doi: 10.1016/j.chb.2011.09.009
- Mossberger, K., Tolbert, C., & S. McNeal, R. (2007). *Digital citizenship: The internet, society, and participation*. London, England: The MIT Press.

- Obschanka, M., Fisch, C., & Boyd, R. (2017). Using digital footprints in entrepreneurship research: A Twitter-based personality analysis of superstar entrepreneurs and managers. *Journal of Business Venturing Insights*, 8, 13-23. doi: 10.1016/j.jbvi.2017.05.005
- O'Keeffe, G. S., Clark-Pearson, K., & Council on Communications and Media. (2011). The impact of social media on children, adolescents, and families. *Pediatrics*, 127(4), 800-804. doi: 10.1542/peds.2011-0054
- Odabaşı, F., Varank, İ., Yıldırım, S., Koyuncu, F., Dönmez, O. ve Şumuer, E. (2015). *Bilinçli internet kullanım araştırması*. Erişim adresi: http://www.kesfetprojesi.org/source/Bilincli_internet_Kullanim%20Arastirma_si.pdf
- Özdamar, K. (2004). *Paket programlarda istatistiksel veri analizi*. Eskişehir: Kaan Kitabevi.
- Partnership For 21st Century Learning. (2013). Partnership for 21st Century Skills. Erişim adresi: <http://www.21stcenturyskills.org/>
- Patchin, J. W., & Hinduja, S. (2006). Bullies move beyond the school yard. A preliminary look at cyberbullying. *Youth Violence and Juvenile Justice*, 4(2), 148–69. doi: 10.1177/1541204006286288
- Richardson, W. (2008). Footprints in the digital age. *Educational Leadership*, 66(3), 16-19.
- Ribble, M., & Bailey, G. (2004). Digital citizenship: focus questions for implementation. *Learning & Leading with Technology*, 32(2), 12-15.
- Ribble, M. (2011). *Digital citizenship in schools* (2nd Edition). Washington DC: The International Society for Technology in Education (ISTE).
- Sawilowsky, S. S. (2009). New effect size rules of thumb. *Journal of Modern Applied Statistical Methods*, 8(2), 597-599. doi: 10.22237/jmasm/1257035100
- Tabachnick, B. G., & Fidell, L. S. (2013). *Using multivariate statistics* (6th ed.). United States: Pearson Education.

- Tamayo, P. D. (2016). *Digital citizenship recommendations*. (Report to the legislature). Eriřim adresi: <http://www.k12.wa.us/LegisGov/2016documents/2016-12-DigitalCitizenship-LegislativeReport.pdf>
- Thompson, T. L. (2012). I'm deleting as fast as I can: Negotiating learning practices in cyberspace. *Pedagogy, Culture & Society*, 20(1), 93-112. doi: 10.1080/14681366.2012.649417
- Tutaysalgır, H. (2012, 21 Temmuz). İnternette Siber Tuzaklar [Video]. Eriřim adresi: <https://www.youtube.com/watch?v=8uWQ9nBdaK4>
- Türkiye İstatistik Kurumu (2017). *Hanehalkı Biliřim Teknolojileri Kullanım Arařtırması*, 2017. Eriřim adresi: <http://www.tuik.gov.tr/PreHaberBultenleri.do?id=24862>
- Yang, H., & Chen, P. (2010). Exploring teachers' beliefs about digital citizenship and responsibility. In K. Elleithy, T. Sobh, M. Iskander, V. Kapila, M. A. Karim, & A. Mahmood (Eds.). *Technological Developments in Networking, Education and Automation*. pp. 49-54. doi: 10.1007/978-90-481-9151-2_9

EK-A: Sayısal Ayak İzi Ders Kazanımları

I. Sayısal Ayak İzi ile İlgili Temel Kavramlar
1. Sayısal ayak izi, sayısal vatandaşlık, sayısal zorbalık, internet, siber tuzak, siber taciz, sayısal empati, ekran yönetimi gibi kavramları tanımlar.
2. Sayısal ayak izi, sayısal vatandaşlık, sayısal zorbalık, internet, siber tuzak, siber taciz, siber güvenlik, sayısal empati kavramlarının benzer ve farklı yönlerini açıklar.
II. Sayısal Vatandaşlık
3. Sayısal vatandaşlığın önemini açıklar.
4. Sayısal vatandaşlık ilke ve kurallarını açıklar.
5. Sayısal vatandaşlık kurallarının önemini açıklar.
6. Sayısal vatandaşlık kurallarına uyulmadığı takdirde karşılaşılabilecek yaptırımları açıklar.
III. Güvenli İnternet
7. Güvenli internet kullanımının kurallarını açıklar.
8. Web kaynaklarını değerlendirme ölçütüne göre değerlendirir.
9. Nasıl güçlü şifreler oluşturacağını açıklar.
IV. İnternette Etkili Arama Stratejileri
10. İnternette etkili arama stratejilerini açıklar.
11. İnternette etkili arama stratejilerini uygular.
V. Sayısal Zorbalık
12. Sayısal zorbalık davranışlarının neler olduğunu açıklar.
13. Çevrimiçi ortamda uygun ve bilinçli davranışların neler olduğunu açıklar.
14. Sayısal zorbalığa maruz kaldığında neler yapması gerektiğini açıklar.
15. Siber taciz davranışlarının neler olduğunu açıklar.
16. Siber tacizden korunma yollarını açıklar.
17. Siber tacize maruz kaldığında kimlere başvuracağını açıklar.
18. İnternette karşılaşılabileceği siber tuzakların neler olduğunu açıklar.
19. Sayısal empatinin neden gerekli olduğunu açıklar.
20. Sayısal empati davranışını bilinçli olarak sergiler.
VI. Sayısal Ayak İzi
21. Gizlilik ve veri koruma konusunda yapılması gerekenleri açıklar.
22. Gizlilik ve güvenlik ayarlarını bilinçli bir şekilde uygular.
23. Çevrimiçi bilginin olası getirilerini açıklar.
24. Olumlu sayısal ayak izinin unsurlarını tanımlar.
25. Olumsuz sayısal ayak izinin unsurlarını tanımlar.

EK-B: Ön Test Ve Son Test Olarak Uygulanan Başarı Testi

Sevgili Öğrenciler

Aşağıdaki soruları dikkatlice okuyunuz ve size uygun gelen cevabı işaretleyiniz.

Soru 1: “İnternette gezinirken bıraktığımız her şey” tanımı aşağıdakilerden hangisidir?

- A. Dijital Vatandaşlık
- B. Dijital Zorbalık
- C. Dijital Ayak İzi
- D. İnternet

Soru 2: “Dijital ortamda iletişim kurabilen, dijital ortamda üretip ve tüketebilen, dijital ortamda alışveriş yapabilen ve bu davranışları yaparken etik kurallarına uyan, hak ve sorumluluklarının bilincinde olan kişi” aşağıdakilerden hangisidir?

- A. Dijital Vatandaşlık
- B. Dijital Zorba
- C. Dijital Ayak İzi
- D. Dijital Empati

Soru 3: Aşağıdakilerden hangisi “bilgi ve iletişim araçları vasıtasıyla zararlı ve kırıcı mesajlar yollayarak diğerlerini taciz etme”dir?

- A. Dijital Vatandaşlık
- B. Dijital Zorbalık
- C. Dijital Ayak İzi
- D. İnternet

Soru 4: Siber ne anlama gelmektedir?

- A. İnternet ile ilgili durumlar (kavramlar) için kullanılır.
- B. Virüs programları için kullanılan bir kavramdır.
- C. İnternete bağlanmayı sağlayan bir parçadır.
- D. İnternet kullanıcısı anlamında kullanılan bir terimdir.

Soru 5: Bilgi ve iletişim teknolojileri vasıtasıyla kişisel bilgilerinizi alıp kullanmak amaçlı yapılan hilelere ne denir?

- A. Siber Tuzak
- B. Siber Güvenlik
- C. Dijital Ayak İzi
- D. Siber Taciz

Soru 6: Başkalarına modern iletişim araçları kullanılarak kasıtlı olarak hakaret edilmesi, onların tehdit, teşhir ya da rahatsız edilmesini aşağıdaki kavramlardan hangisini tanımlamaktadır?

- A. Siber Tuzak
- B. Siber Güvenlik
- C. Dijital Empati
- D. Siber Taciz

Soru 7: Sanal ortamda kendimizi başkasının yerine koyarak hareket etmeye, paylaşım yapmaya ne denir?

- A. Siber Tuzak
- B. Siber Güvenlik
- C. Dijital Empati
- D. Dijital Zorbalık

Soru 8: Aşağıdakilerin hangisi bir web sitesinin güvenilir olmadığını gösterir?

- A. İçeriklerin güncel ve doğru olması
- B. Web sitesinin bilinen bir kuruma ait olması
- C. İçeriklerin kimin tarafından yazıldığının açıkça belirtilmiş olması
- D. Web sitesini doğrulayacak telefon, adres ya da e posta adresinin bulunmaması
- E.

Soru 9: İnternette bulduğunuz herhangi bir bilgiyi kullanmadan önce ne yapmalısınız?

- A. Bilginin yazıldığı tarihe bakırım
- B. Bilginin kaynağını yazarını araştırırım
- C. Bilgiyi 3 ayrı siteden doğrulatırım.
- D. Yukarıdakilerin hepsi

Soru 10: Güçlü şifreler oluşturma konusunda aşağıdakilerden hangisi **yanlıştır**?

- A. Parola en az 8 karakter olmalı
- B. Unutmamak için kişisel bilgiler kullanılmalı
- C. Parola oluştururken harflerle birlikte sayılar da kullanılmalı
- D. Parola kimse ile paylaşılmamalı

Soru 11: Aşağıdakilerden hangisi dijital vatandaşlık kuralları içinde yer alır?

- A. Bilinmeyen ya da ücretsiz olduğu söylenen dosyaları bilgisayara indirmemek
- B. Kaba ve başkasını kızdıracak yorumlar yapmamak
- C. Başkasının oluşturduğu içeriği izinsiz kullanmamak
- D. Yukarıdakilerin hepsi

Soru 12: Alan uzantısı .info olan site türü aşağıdakilerden hangisidir?

- A. Bilgi içerikli siteler
- B. Ticari
- C. Üniversiteler
- D. Kar amacı olmayan vakıf veya dernek gibi kuruluşlar

Soru 13: Kullanıcıların internette güvenli bir profil için **hangi kurala uyması gerekir**?

- A. Kişisel bilgilere yer verilmemeli
- B. Profil herkese açık olmamalı
- C. Profili korumak için güçlü bir şifre oluşturmalı
- D. Yukarıdakilerin hepsi

Soru 14: Aşağıdakilerden hangisi dijital vatandaşlık kurallarından biri **değildir**?

- A. Çevrim içi olduğunuzda insanlara çevrim dışında olduğu gibi davranın.
- B. Başkalarına, kendinize davranılmasını istediğiniz şekilde davranın.
- C. Çevrim içi olduğunuzda kimliğinizin bilinmemesinin verdiği gücü kötüye kullanmayın.
- D. Tanıştığınız herkese karşı saygılı ve kibar olmayın, size kötü davrananlara kötü karşılık verin.

Soru 15: Aşağıdakilerden hangisi dijital vatandaşlık kurallarındandır?

- A. Hakaretlere yanıt vermeyin, bu durumda itibarınızı koruyamayabilirsiniz.
- B. Sözlü tacize başvurmayın; insanlara küfretme, hakaret etme, onları taciz etme ya da onlara isim takma yoluyla saygısızlık etmeyin.
- C. Sizi taciz edenleri görmezden gelin ya da engelleyin.
- D. Yukarıdakilerin hepsi

Soru 16: Aşağıda verilen dijital vatandaşlık kurallarından biri **değildir**?

- A. Kişiselliğinizi katmak için yüz ifadesi gibi simgeleri kullanmayın.
- B. Çevrim içi olduğunuzda insanlara çevrim dışında olduğu gibi davranın.
- C. Hakaretlere yanıt vermeyin
- D. Sözcüklerinizi büyük harflerle yazmaktan kaçının.

Soru 17: Dijital vatandaşlık kurallarına uyulmadığı takdirde **aşağıdakilerden hangisi** durumlarla karşılaşabilirsiniz?

- A. Bilişim suçu işlemiş olma
- B. Para cezası
- C. Hapis cezası
- D. Yukarıdakilerin hepsi

Soru 18: İnternetin güvenli kullanımı açısından aşağıdakilerden hangisi doğru **değildir**?

- A. Adınız, okulunuz, adresiniz, telefon numaranız, aile bireylerinizin adı vb. gibi kişisel bilgilerinizi paylaşmayın.
- B. İnternette her bilgi doğru olmayabilir. İnternette elde ettiğiniz bilgiyi en az 3 kaynaktan kontrol edin.
- C. İnternet ortamında resminiz, size ait video gibi paylaşımları düşünmeden paylaşabilirsiniz.
- D. İnternet ortamında tanımadıklarınıza cevap vermeyin, tekliflerini reddedin, size gönderdikleri mesajları açmadan silin.

Soru 19: Aşağıdakilerden hangisi bir web sitesinin güvenilirliğini kontrol etmede kullanılır?

- A. Sitenin kaynağının araştırılması, URL'sinin kontrol edilmesi.
- B. Sitedeki iletişim bilgilerinin doğrulanabilir olması.
- C. Web sitesinde doğru dilbilgisi, yazım , cümle yapısı ve içeriğin güncelliğinin kontrol edilmesi.
- D. Yukarıdakilerin hepsi

Soru 20: Aşağıda şifrelerle ilgili verilenlerden hangisi **yanlıştır**?

- A. Şifreleriniz sadece sayılardan veya sadece harflerden oluşuyorsa zayıf bir şifredir.
- B. Şifre belirlerken unutmayacağınız bir şifre bulmalısınız.
- C. Şifreniz, klavyede yan yana bulunan tuşlardan oluşuyorsa zayıf bir şifredir.
- D. Şifreleriniz en fazla 10 basamaklı olmalıdır.

Soru 21: İnternette etkili arama yapmak için verilenlerden hangisi **yanlıştır**?

- A. Aradığınız kelimeleri çoğul yazmalısınız. (kediler gibi)
- B. Yazdığınız tüm kelimelerin arama sonuçlarında yer almasını istiyorsanız tırnak işareti (") kullanmalısınız.
- C. Arama yaparken içerisinde mutlaka geçmesini istediğiniz kelimeleri yazarken başına '+' koymalısınız.
- D. Arama motorları büyük harf- küçük harf ayrımı yapmaz. Kelimeleri istediğiniz gibi yazabilirsiniz.

Soru 22: Alan uzantısı .com olan site türü aşağıdakilerden hangisidir?

- A. Üniversiteler
- B. Ticari şirketler
- C. Kar amacı olmayan vakıf veya dernek gibi kuruluşlar
- D. İlkokul, ortaokul ve liseler

Soru 23: Aşağıdakilerden hangisi dijital zorbalık davranışı **değildir**?

- A. Küçük düşürücü sözler içeren mesaj göndermek
- B. Yalan bilgiler yayınlamak
- C. Başkasına ait olan bir içerik ya da fotoğrafı izin alıp kullanmak
- D. Başkalarının şifre ve kişisel bilgilerinin gizliliğine saygı duymayıp bunları öğrenmeye çalışmak

Soru 24: Aşağıda verilenlerden hangisi bir dijital zorbalık davranışdır?

- A. İnternette yalan bilgiler yayınlamak
- B. Başkasına ait olan bir içerik ya da fotoğrafı izin alıp kullanmak
- C. Arkadaşına sohbet amaçlı mesaj yazmak
- D. Kendi bilgilerimizle, gerçek bir profil oluşturup, paylaşım yapmak

Soru 25: Dijital zorbalığa maruz kalındığında aşağıdaki davranışlardan hangisinin yapılması doğru olmaz?

- A. Engelleme seçeneğini kullanmak için gizlilik ayarlarını değiştirmek
- B. Dijital zorbaya onun üslubuyla karşılık vermek
- C. Şikayet olarak kullanmak amaçlı, kanıtları saklamak
- D. Eğer sohbet ortamında zorbalık yapılırsa, o ortamdan uzaklaşmak

Soru 26: Aşağıdakilerden hangisi bir siber taciz davranışıdır?

- A. Birini sosyal medyadan takip etmek.
- B. Birine sosyal medyadan “merhaba” mesajı yollamak.
- C. Birine “merhaba, tanışabilir miyiz?” şeklinde mesaj atmak.
- D. Birini telefonla yanlışlıkla aramak.

Soru 27: Aşağıdakilerden hangisi siber tacizden korunma yollarından biri değildir?

- A. Parolalarınızı hiçbir zaman başkalarıyla paylaşmayın, parolalarınızı sık sık değiştirin.
- B. Katılmayı planladığınız etkinlikleri gösteren çevrimiçi takvimleri ve seyahat programlarını sosyal ağınızda olsa bile silin veya özel hale getirin.
- C. Adınızı ve aile bireylerinizin adını aratarak internette sizinle ve çocuklarınızla ilgili ne tür bilgiler bulunduğu bakın.
- D. Bilgisayar programlarındaki oturumunuzu her zaman açık tutun.

Soru 28: Siber tacize maruz kaldığında aşağıdakilerden hangisinin yapılması uygun değildir?

- A. Okuldaki bir öğretmenine söylemek
- B. Anne ya da babaya söylemek
- C. Kimseye söylememek
- D. Polise söylemek

Soru 29: Aşağıdaki hangisi bir eğitim kurumuna ait sitenin alan adıdır?

- A. .gov
- B. .edu
- C. .org
- D. .com

Soru 30: Dijital ayak iziyle ilgili aşağıdakilerden hangisi yanlıştır?

- A. Dijital ayak izlerimiz bizi olumlu veya olumsuz olarak tanımlayabilir.
- B. Dijital ayak izimiz sonsuza kadar kalır, silinemez.
- C. Dijital ayak izimiz silinebilir.
- D. Dijital ayak izlerimiz herkes tarafından aranabilir, görülebilir.

Soru 31: Gizlilik ve veri koruma konusunda aşağıdakilerden hangisi yanlış bir davranıştır?

- A. Kişisel bilgileri internette paylaşmamak
- B. Siyasi görüş bildiren paylaşımlar yapmamak
- C. Paylaştığımız video ve ya görsellere sadece kendi arkadaşlarınız ile paylaşmak
- D. Okul bilgilerini sosyal medyada paylaşmak.

Soru32: Gizlilik ve güvenlik ayarlarıyla ilgili hangisi yanlış bir uygulamadır?

- A. Profilimi herkesin görmesine izin veririm.
- B. Paylaştıklarımı sadece arkadaşlarımla görmesine izin veririm.
- C. Hesabıma giriş bilgilerimi hiç kimseye paylaşmam.
- D. Güçlü bir parola kullanırım.

Soru 33: Aşağıdakilerden hangisi internet ortamında iz bırakabilir?

- A. Ziyaret edilen web siteleri
- B. Sosyal medyada beğendiğin, paylaştığın şeyler
- C. E-postanda, sosyal medyada söylediklerin
- D. Yukarıdakilerin hepsi

Soru 34: Dijital zorbalığa maruz kalındığında aşağıdaki davranışlardan hangisi yapılmalıdır?

- A. Zorbalık yapan kişiyle konuşmak
- B. Zorbalık sohbet ortamında yapılıyorsa sohbete devam etmek
- C. Zorba kişiyi sosyal medyada, buton yardımıyla şikayet etmek.
- D. Zorbanın isteklerini yerine getirmek.

Soru 35: Aşağıdakilerden hangisi olumsuz dijital ayak izine örnek oluşturur?

- A. Kişisel bilgisayarın dışındaki bilgisayarlarda “Beni hatırla” seçeneğini kullanmamak.
- B. Sosyal medya sitesinde kişisel paylaşımlarınızı sadece arkadaşlarınıza özel yapmak.
- C. Sosyal medyada fikirlerinizi herkesle açıkça paylaşmak.
- D. Başkalarına yeni bir şeyler öğretmek için youtube’da kanal açıp video paylaşmak.

EK-C: Ders Planları

ETKİNLİK 1

Dijital Ayak İzi – Temel Kavramlar (80 dk)

Öğrencilerinize aşağıdaki soruları sorarak derse başlayınız? Farklı öğrencilere söz veriniz.

- İnterneti hangi amaçlarla kullanıyorsunuz?
- İnternette bir şey paylaşıırken nelere dikkat ediyorsunuz?
- Kendinizle ilgili hangi (fotoğraf, adres, e – posta vb) bilgileri paylaşıyorsunuz?
- İnternetteki paylaşımlarınızdan ailenize bilgi veriyor musunuz?
- İnternetteki paylaşımlarımızda neden dikkatli olmalıyız?

Gelen cevaplardan sonra aşağıdaki açıklamayı yapınız.

“İnternetteki diğer tüm bilgiler gibi, internette paylaştığımız her bilgi de internette sürekli kalabilir. İnternet herkese açıktır ve dünyadaki herkes bu bilgileri takip edebilir. Paylaştığımız her şey bir gün karşımıza yeniden çıkabilir. İnternette bizimle ilgili her şey iz bırakır.”

Buna dijital ayak izi diyoruz. Dijital ayak izimizin daha sonra bizi üzmemesi ya da istenmeyen durumlarla karşılaşmamak için internette bilgi paylaşıırken çok dikkat etmeliyiz.

Dijital Ayak İzi Nedir?

Klavyeden, fareden ya da ekrandan, tuşlayarak, tıklayarak ya da dokunarak elektronik ortama aktardığımız bizimle ilgili her türlü iz. İnternette bizlerin nerede olduğunu takip eden bir pasaport gibidir. Ne aldığımızı, neyi araştırdığımızı, hangi reklamları gördüğümüzün kaydedilmesidir. Facebook, Twitter vb. hesaplarımızda paylaştıklarımız, bloglarımız, bizimle ilgili çıkmış her türlü haber, yazılmış her yazı internette uzun zaman saklanır ve olmadık yerde karşınıza çıkarak bizi şaşırtabilir. İnternette paylaştıklarımız güvenliğimiz için riskleri de beraberinde getirir. İnternet üzerinde ne kadar az iz bırakırsak bizim için o kadar iyi olur. Özel bilgilerimizi paylaşıırken, elektronik posta alıp verirken ya da sosyal medya paylaşımlarında bulunurken çok dikkatli davranmalı, kendimize zarar verecek davranışlardan uzak durmalıyız. Bu nedenle, ileriki yaşamımıza, iş bulmamıza zarar verecek paylaşımlardan kaçınmalı, başka bir deyişle itibarımızı korumak için daha dikkatli olmalıyız.

Paylaştığımız resim ya da videoları, yazdığımız yorumları paylaşmadan önce bir kez daha düşünmeli, ileride karşımıza çıkarsa rahatsız olup olmayacağımıza karar vermeliyiz.

ETKİNLİK 1

Dijital Ayak İzi – Temel Kavramlar (45 dk)

Dijital vatandaşlık, teknolojiyi kullanırken etik ve uygun davranışlarda bulunma ve bu konuda bilgilenmeyi içermektedir. İyi birer dijital vatandaş olmak için çok dikkatli olmalı, çok çalışmalıyız.

Dijital vatandaş bilgi ve iletişim kaynaklarını kullanırken eleştirebilen, çevrimiçi davranışlarının etik sonuçlarını bilen, ahlaki çevrimiçi kararlar alabilen, teknolojiyi kötüye kullanmayan, dijital dünyada iletişim kurarken ve iş birliği yaparken doğru davranışı teşvik eden vatandaşdır

İyi birer dijital vatandaş olmak için dijital zorbalıktan uzak durmalı, dijital empati kurmalıyız.

Dijital Zorbalık, bilgi ve iletişim araçları vasıtasıyla zararlı ve kırıcı mesajlar yollayarak diğerlerini taciz etmektir. Başkalarına yalnız mesajlar yollamak, onları üzmeektir.

Dijital Empati, sanal ortamda kendimizi başkasının yerine koyarak hareket etmek, paylaşım yapmak vb.

Değerlendirme

- *Kavramlar (Dijital ayak izi, dijital vatandaşlık, dijital zorbalık, dijital empati) tek tek kartlara yazılır.*
- *Tanımları tek tek kartlara yazılır.*
- *Tanımlar öğrencilere okutulur. Kavramlar gösterilir ve doğru kavram sorulur.*

ETKİNLİK 2

Dijital Vatandaşlık (80 dk)

Dijital vatandaşlık tanımı hatırlatılır.

Dijital vatandaş;

- Dijital iletişim kurabilen ,
- E devlet uygulamalarını kullanabilen,
- Dijital alışveriş yapabilen,
- Dijital ortamda üretim yapabilen,
- Dijital ortamdan eğitim alabilen ve bu davranışları yaparken etik kurallarına uyan hak ve sorumluluklarının bilincinde olan kişidir.

“Günlük yaşamımızda iyi birer vatandaş olarak uymamız gereken kurallara örnekler verir misiniz?” sorusu yöneltilir.

“Gerçek hayatta uymamız gereken kurallar olduğu gibi dijital dünyada da herkesin uyması gereken toplumsal ve yasal kuralları vardır.” Hatırlatması yapılarak, bir video izletilir.

Video izletilerek öğrencilere sorular yöneltilir?

- “Videoda anlatılan dijital vatandaşlık kuralları nelerdi?”
- “Eklemek istediğiniz dijital vatandaşlık kuralları var mı?”

(öğrencilere ipuçları verilerek dijital vatandaşlık kurallarını bulmaları ve tahtaya yazmaları sağlanır.

- Çevrim içi olduğunuzda insanlara çevrim dışında olduğu gibi davranın.
- Başkalarına, kendinize davranılmasını istediğiniz şekilde davranın.
- Bulduğunuz bilgiyi olduğu gibi almayın, hırsızlık yapmayın.
- Sahtekârlık yapmayın.
- Tanıştığınız herkese karşı saygılı, kibar ve duyarlı olun.
- Çevrim içi olduğunuzda kimliğinizin bilinmemesinin verdiği gücü kötüye kullanmayın.
- Bir şey yayınlamadan önce düşünün. İtibarınızı koruyun.
- Hakaretlere yanıt vermeyin, bu durumda itibarınızı koruyamayabilirsiniz.
- Zorbalık yapmayın. Sözlü tacize başvurmeyin; insanlara küfretme, hakaret etme, onları taciz etme ya da onlara isim takma yoluyla saygısızlık etmeyin.
- Zorbalara katlanmak zorunda değilsiniz. Sizi taciz edenleri görmezden gelin ya da engelleyin.

ETKİNLİK 2

Dijital Vatandaşlık (80 dk)

- Ses tonunuzu, duygu durumunuzu iletmek, mizah ve kişiselliğinizi katmak için yüz ifadesi gibi simgeleri kullanın.
- Sözcüklerinizi büyük harflerle yazmaktan kaçının. Bağırıyormuşsunuz gibi olur ve zor okunur.
- Çevrimiçi ortamda rahatsız edici bir durumla karşı karşıya kaldığınızda, bunu güvendiğiniz bir yetiştikine söyleyin.)

Değerlendirme

Aşağıdaki soruları öğrencilere yönelterek dersi bitiriniz.

- Siz dijital ortamda bu kurallara uyuyor musunuz? Bundan sonraki davranışlarınız nasıl olacak?
- Dijital vatandaşlık kurallarına uyulmazsa ne gibi sonuçları olur?
- Dijital vatandaşlık kuralları neden önemli?

ETKİNLİK 3

Güvenli İnternet (80 dk)

Etkinlikler

İnterneti kullanmak hepimizin hakkıdır. İnternet işimizi kolaylaştırıyor mu? Zorlaştırıyor mu? Neden? Sorusu ile ders başlanır.

İnternetin işimizi kolaylaştırmasına örnekler istenir.

İnternetin işimizi zorlaştırmasına örnekler istenir.

Öğrencilerden gelen cevaplar tamamlanarak aşağıdaki riskler tahtaya yazılır:

- Yanlış veya zararlı bilgiye erişim
- Sanal dolandırıcılık
- Kişisel bilgilerin paylaşımı
- Zararlı yazılımlar
- Oyun ve internet bağımlılığı
- Dijital zorbalık

Bu risklerden kaçınmak için interneti kullanırken çok dikkatli olmalı ve kurallara uymalıyız” açıklaması yapılır.

Bu kurallar “güvenli internet” sunusu ile açıklama yapılır.

1. İnternet hayatınızın tamamı değil, sadece bir parçası olsun. Çok fazla zamanınızı çalmasına izin vermeyin.
2. İnterneti ailelerinize ve arkadaşlarınıza değişmeyin. Aileleriniz ön koltukta, internet ise arka koltukta otursun.
3. İnternette her bilgi doğru olmayabilir. İnternette elde ettiğiniz bilgiyi en az 3 kaynaktan kontrol edin. Ödevinizde kullanıyorsanız kaynağını belirtin.
4. İnternet ortamındaki bedava teklifler büyük ihtimalle gerçek değildir. Tanımadığınız kişi size neden bedava bir şey teklif etsin ki.
5. Adınız, okulunuz, adresiniz, telefon numaranız, aile bireylerinizin adı vb. gibi kişisel bilgilerinizi paylaşmayın. Paylaşılan küçük gibi görünen bilgiler, büyük zararlara sebep olabilir.
6. İnternet ortamında paylaşacağınız resminiz, size ait video gibi paylaşımları önce düşünün, sonra paylaşın. Paylaştıklarınız sizin veya sevdiklerinizin üzülmesine sebep olmasın.

ETKİNLİK 3

Güvenli İnternet (80 dk)

7. Şifreleriniz güçlü olsun. Adınızı ve doğum tarihinizi, ard arda gelen kelimeleri ve sayıları şifre olarak belirlemeyin. Anlamlı bir cümle kurun ve o cümlenin kelimelerinden seçtiğiniz en az 8 karakterden oluşan şifreler oluşturun.

8. İyi ve nazik bir kullanıcı olmaya çalışın. Gerçek hayatta Merhaba dediğiniz arkadaşınıza internet ortamında "mrB" değil, yine merhaba deyin. Tamam derken "Ok." veya "Tmm" yerine yine tamam deyin.

9. Gerçek hayatta yüzüne söylemeyeceğiniz ifadeleri internet ortamında da söylemeyin.

10. Gerçek hayatta olduğu gibi, internet ortamında da tanımadıklarını arkadaş edinmeyin.

11. İnternet ortamında tanımadıklarınıza cevap vermeyin, tekliflerini reddedin, size gönderdikleri mesajları açmadan silin.

12. İnternet ortamında sizi rahatsız edenleri, sizi taciz edenleri ailelerinize söyleyin. Ailelerinle birlikte emniyete veya savcılığa suç duyurusunda bulunun.

13. İnternetin zararlı içeriklerinden korunmak için tamamıyla ücretsiz olan "Güvenli İnternet Hizmeti"nden ailelerinizi haberdar edin.

Çevrimiçi dünyada güvenli bir şekilde gezmek" videosu öğrencilere izletilir.
<https://www.youtube.com/watch?v=KP3pHv8Zfyo>

Güçlü şifreler sunusu öğrencilere sunulur.

Öğrencilerden her birinin birer güçlü şifre yazmaları istenir. Her bir şifre güçlü şifrelerin özellikleri doğrultusunda değerlendirilir ve yazılan şifrenin güçlü mü, orta mı, zayıf mı olduğu karşısına yazılır.

Değerlendirme

- Öğrencilere 10 tane şifre örneği verilir. Bunlardan hangilerinin güçlü bir şifre olduğu, zayıf olanların neden zayıf şifre olduğunu bulmaları istenir.

ETKİNLİK 4

İnternette Etkili Arama Stratejileri (80 dk)

“Sorumlu bir dijital vatandaş olabilmek, interneti güvenli kullanabilmek ve internetten gelebilecek tehlikelerden kendimizi koruyabilmek için internette nasıl arama yapacağımızı bilmemiz gerekir.” diyerek derse başlanır.

İnternette etkili arama yapmayla ilgili sunum yapılır.

Web sayfaları birçok konuda güzel ve çekici gelebilecek kaynaklar sunabilir. Ancak, bu kaynaklarda yer alan bilgi her zaman güvenilir olmayabilir. Çünkü birçok yanlış ve değerlendirilmemiş bilgi de web üzerinde bulunabilir. Bu nedenle de internet üzerinden ulaşılan bilginin **doğruluğu**, **güvenirliği** ve **güncelliği** konusunda şüpheli olunmalıdır.

Web sitelerini değerlendirme ölçütleri öğrencilere gösterilir. (Ek Ğ)

İlgili afiş sınıfa asılarak öğrencilerin incelemesi ve kullanması istenir. (Ek G)

Değerlendirme

1. Aşağıdaki alan uzantıları ile ilgili eşleştirmeleri yapınız.

1. .com	a) devlet kurumları
2. .org	b) okullar
3. .net	c) kar amacı gütmeyen kuruluşlar
4. .gov	d) üniversiteler
5. .edu	e) bilgi içerikli siteler
6. .info	f) özel şirketler
7. .k12	g) internet hizmeti sağlayan şirketler

2. Ülkelerin kullandığı alan kodları ile ülke eşleştirmelerini yapınız.

1. .au	Kanada
2. .be	Fransa
3. .ca	Türkiye
4. .tr	Meksika
5. .br	Belçika
6. .fr	Avustralya
7. .mx	Brezilya

3. Öğrencilere ödevleri ile ilgili web siteleri verilerek, değerlendirme ölçütlerine göre incelemeleri istenir.

Değerlendirme

- Web siteleri değerlendirme ölçütü öğrencilere dağıtılır ve öğrenciler 4 ya da 5 gruba ayrılır. Her gruba ayrı bir web sitesi verilerek siteyi değerlendirmeleri istenir.

1. grup: Vikipedi
2. grup: Ekşi sözlük
3. grup: Uludağ sözlük
4. grup: e-okul

ETKİNLİK 5

Konu:Dijital Zorbalık (80 dk)

Etkinlikler

Dijital vatandaşlık kurallarına uyulmadığı takdirde dijital zorbalık yapılmış olduğunu söylemiştik.

“Tanımından ve dijital vatandaşlık kurallarından yola çıkarak dijital zorbalık davranışlarının neler olduğunu söyleyebilir misiniz?” İpuçları verilir, birlikte bir afiş hazırlanır.

- Aşağılamak
- Şantaj yapmak
- Küfür etmek
- İstedığı şeyi yapmamanız halinde ihbar etmekle tehdit etmek
- Hırsızlık yapmak (başkasına ait olan bir içerik veya fotoğrafı izin almadan kullanmak)
- Küçük düşürücü sözler içeren mesaj göndermek, isim ya da lakap takmak
- Sahtekarlık yapmak. Yanlış bilgiler ile profil oluşturup, paylaşım yapmak
- Yalan bilgiler yayınlamak
- Hakınızdaki özel bilgileri yayınlamak ya da yayınlamakla tehdit etmek
- Başkalarının şifre ve kişisel bilgilerinin gizliliğine saygı duymayıp bunları öğrenmeye çalışmak
- Almak istemediğiniz mesajlar göndererek taciz etmek)

Hazırlanan afiş sınıfa asılır.

Öğrencilere dijital zorbalık davranışları ile karşılaşılırsa neler yapacakları sorulur? Tahtaya yazmaları istenir.

- Yanıt vermeyin, çünkü o kişinin asıl amacı bu zaten.
- Engelleme seçeneğini kullanmak için gizlilik ayarlarını değiştir.
- Eğer sohbet ortamında zorbalık yapılırsa, o ortamdan uzaklaş.
- Dijital zorbaya onun üslubuyla karşılık verme, yoksa sen de dijital zorba olursun. Misilleme yapma.
- Dijital zorbaları tahrik etme, başkaları hakkında dedikodu yapmak ve tahrik edici söz söylemek seni zorbalığa maruz bırakabilir.
- Şikayet olarak kullanmak amaçlı, kanıtları sakla.
- Bir arkadaşın, bir yetişkin veya bir ebeveyninden yardım iste. Okuldaysan bu rehber öğretmen de olabilir.
- Sosyal medya sitesindeysen, “şikayet et” butonunu kullan. Zorbalık ileri seviyede, fiziksel şiddet içeriyorsa polise şikayet et.
- Dijital zorbalığa karşı seyirci kalma, göz yumma, maruz kalan kişilere destek ve yardımcı ol.

ETKİNLİK 5

Konu:Dijital Zorbalık (80 dk)

Öğrencilere “bir sanal zorbalık hikayesi” videosu (<https://www.youtube.com/watch?v=N87aNk5Uohg>) izletilerek yanıtlara ipucu bulmaları sağlanır ve yanıtlar tahtaya yazılır. Her bir davranış öğrencilere bölüştürülerek fon kağıtlarına slogan yazmaları istenir. Yazılan sloganlar okul duvarlarına veya panolara asılır.

Siber tacizin tanımı hatırlatılır. “Siber taciz” sunusu öğrencilere sunulur. Sunulan bilgiler sonucunda siber tacize maruz kaldığında kimlere başvuracağı sorulur. “Siber tacize ya da dijital zorbalığa maruz kaldığında başvurman gereken yerler aynı. Bunları aklından çıkarmamalı ve arkadaşın buna maruz kalıyorsa sessiz kalmamalısn”

“Siber tuzak neydi?”

<http://www.kesfetprojesi.org/kesfet/imagesbuyuk/1b345-50x70-SIBER-TUZAKLAR-Afisi.pdf> afişi öğrencilere gösterilir ve buradan öğrencilerin siber tuzakların neler olduğunu bulmaları istenir. (Ek 1) Siber tuzakların neler olduğu tahtaya yazılır.

ETKİNLİK 5

Konu:Dijital Zorbalık (80 dk)

Siber tuzaklardan korunma videosu öğrencilere izletilir.

(<https://www.youtube.com/watch?v=8uWQ9nBdaK4>)

“Dijital empati kavramı hatırlatılarak, dijital empatinin neden gerekli olduğu öğrencilere sorulur.

Değerlendirme

Öğrencilere sanal zorbalıkla ilgili hazırladıkları ve fon kağıtlarına yazdıkları sloganlardan bir sınıf afişi hazırlamaları istenir.



ETKİNLİK 6

Konu: Gizlilik ve Veri Koruma (80 + 80 dk)

Etkinlikler

Dijital ayak izimizin olumsuz etkilerinden korunmak için neler yapabiliriz? Sorusu ile derse başlanır.

Gizlilik ve kişisel bilgi kelimeleri tahtaya yazılır. Öğrencilere bu kelimeler konusunda beyin fırtınası yaptırılır, internetten kelimeleri araştırmak için serbest bırakılır.

“Gerçek dünyada özel bilgileri nasıl gizli tutarsınız? Dijital dünyada bilgilerinizi nasıl gizli tutarsınız?” sorusu yöneltilir.

“Tarayıcımız haftalar içinde hangi siteleri ziyaret ettiğimizi ve bizim için şifrelerimizi hatırlayabilir. Arama motorumuz bizim araştırdığımız ve son girdiğimiz anahtar kelimeler temelinde bize öneriler sağlar. Web sitelerinde tıklamış olduğumuz reklamlar bu sitelerin dışında da karşımıza çıkar.” Açıklamasından sonra, “bunların nasıl olduğunu hiç düşündünüz mü?” sorusu yöneltilir, öğrenci cevapları alınır.

“Birisi kişisel bilgilerinizi tüm dünya çapında paylaşırsa, neler olabilir?” sorusu sorularak, bu konuda öğrencilere bir video izletilir.

“Şirketler kişileri işe alırken sizin dijital ayak izinizi kullanır. Resimlerin, paylaşımların, yazıların seni işe almalarında önemli bir rol oynar. Ayrıca daha sık ziyaret edilen, Facebook, Instagram gibi sosyal medya sitelerinde fazlaca kişisel bilgi yer aldığı için siber zorbalık meydana gelir. Kişisel verilerin korunması siber zorbalığı önlemeye yardımcı olur”

Öğrenciler Facebook, Instagram, Youtube gibi sosyal medya sitelerinde gizlilik politikaları ve ayarları incelemek için 2 ya da 3 gruba ayrılır. Öğrencilerin aşağıdaki sorulara cevap araması istenir:

- Hangi özellikler insanların gizliliklerini korumalarına yardımcı olmayı sağlar?
- Profil/Gizlilik ayarlarımı nasıl güncellerim?
- İznim olmadan yayınlanan içerikleri nasıl kaldırabilirim?
- Paylaşımlarımı ve fotoğraflarımı kimlerin görebileceğini nasıl seçerim?
- Paylaştığım şeyleri nasıl silebilirim?

Yardımcı olması açısından öğrencilere aşağıdaki kaynaklar verilir:

<https://www.facebook.com/help/>

<https://www.facebook.com/about/basics>

<https://help.instagram.com/>

<http://goo.gl/iBHDeZ>

<https://www.youtube.com/yt/policyandsafety/tr/policy.html>

ETKİNLİK 6

Konu: Gizlilik ve Veri Koruma (80 + 80 dk)

Önerilen web sitelerini inceledikten sonra, her takım gizlilik ve çevrimiçi sorumluluğunu korumak için 5 en iyi püf noktaı sınıfta sunar.

Öğrencilerin bulgularından en iyileri seçilerek slogan oluşturmaları istenir ve en iyi 5 tanesi okulun duvarlarına asılır.

“Çevrimiçi İtibar Kontrol Listesi” öğrencilere sunulur ve sınıfta asılır. (Ek İ)



ETKİNLİK 6

Konu: Gizlilik ve Veri Koruma (80 + 80 dk)

“Hangi bilgilerin iz bırakabilir?” sorusu öğrencilere sorulur ve aşağıdaki cevaplar aranır:

- Ziyaret edilen web siteleri
- Aramaların ve kullandığın anahtar kelimeler
- IP adresleri
- İletişime girdiğin kişiler
- Hakkında söylenenler
- Sosyal medyada ya da çevrimiçi olarak beğendiğin, paylaştığın şeyler
- Yaşın
- Günün kaç saati bilgisayardasın
- Bir haber veya blog sitesinden bahsettiysen veya aıntıladıysan
- Tarama yaparkenki konumun
- Ne için arama yaptığın
- E-postanda, sosyal medyada, yazılarda neler söylediğin
- Ne kadar para harcadığın
- Nerede yaşadığın

“Peki bu bilgiler nasıl toplanır?” sorusu sorulur ve aşağıdaki cevaplar aranır:

- Arama kelimelerinden
- Websitelerindeki çerezlerden
- Sosyal medyada paylaştığın bilgileinden
- Satın alma işlemlerinden
- Tarayıcılardan
- Doldurduğun form ve anketlerden
- Yorumlarından
- Siteye giriş işleminden
- Telefonundaki GPS’den
- Ve daha bir sürü şey...

“Peki bu bilgiler niçin, nerelerde kullanılır?” sorusu sorulur ve aşağıdaki cevaplar aranır:

- Pazarlamada
- Dijital itibarın için
- Gelecekte göreceğiniz reklamlar için önerilerde
- Gizliliğine yapılan saldırılar için: korsanlık (hacking), siber tutak, casus yazılım, kötü amaçlı yazılımlar
- Toplum baskısı (sosyal etki)
- Davanışsal ekonomi
- E-postalar ve diğer pazarlama hedefleri için

ETKİNLİK 6

Konu: Gizlilik ve Veri Koruma (80 + 80 dk)

- “Peki bu durumları nasıl denetim altına alabilir ve olumlu dijital ayak izi bırakırız?” sorusu sorularak aşağıdaki cevaplar aranır:
- Göndermeden önce, hangi bilgileri paylaşacağını, nerede paylaşılacağını ve nasıl paylaşılacağını düşün.
- Kimliğini korumak için avatarları(fotoğraf) ve kimliğini gösterilmeyen kullanıcı adlarını kullanmayı düşün
- Güçlü şifreler kullan ve farklı sitelerde şifreni değiştir. Şifrelerini sık sık değiştir.
- Cep telefonlarını, tabletleri ve bilgisayarları parola korumalı yap.
- "Katılıyorum" u tıklamadan önce ince yazıları (gizlilik politikaları, terimler) oku.
- Çevrimiçi hesaplarının gizlilik ayarlarını düzenli olarak kontrol et (Facebook ve Instagram gibi sosyal medya siteleri gizlilik ayarları sıkça değişir)
- Çekildiğiniz fotoğraflardan ve diğer kişilerin "etiketlediği" fotoğraflardan haberdar ol.
- Parolaları paylaşma (ebeveynler hariç)
- İletişim bilgilerini kiminle paylaşacağınızı düşün.
- İşlemleri yalnızca bir şifre gerektiren güvenli bir wi-fi bağlantısı üzerinden gerçekleştir.
- Başkalarının mahremiyetine, mülklerine, mekanlarına saygı göster.
- Çevrimiçi ve çevrimdışı insanlara hoş görülü ol.
- Güvenlik / virüs koruma yazılımını kullan.
- Verilerini yedekle.
- Çevrimiçi gördüğün, okuduğun veya duyduğun her şey doğru değil. İnsanlar ve web siteleri, olmayan bir şeyi olmuş gibi yapabilir.

Değerlendirme

“Dijital ayak izinin senin hakkında neler söylemesini istiyorsun?

Olumlu dijital itibar senin için neden önemli?” sorularına cevap verecek kompozisyon yazmaları istenir.

EK-Ç: Sayısal Ayak İzi Sunusu Ekran Görüntüleri



Dijital Ayak İzi Hazırlık Soruları

- ❑ İnternette hangi amaçlarla kullanıyorsunuz?
- ❑ İnternette bir şey paylaşıpken nelere dikkat ediyorsunuz?
- ❑ Kendinizle ilgili hangi (fotoğraf, adres, e – posta vb) bilgileri paylaşıyorsunuz?
- ❑ İnternetteki paylaşımlarınızdan ailenize bilgi veriyor musunuz?
- ❑ İnternetteki paylaşımlarınızda neden dikkatli olmuyuz?



Dijital Ayak İzi

- ❑ İnternetteki diğer tüm bilgiler gibi, internette paylaştığımız her bilgi de internette sürekli kalabilir.
- ❑ İnternette herkes okur ve dünyadaki herkes bu bilgileri takip edebilir.
- ❑ Paylaştığımız her şey bir gün karşımıza yeniden çıkabilir.
- ❑ İnternette bizimle ilgili her şey iz bırakır.



Dijital Ayak İzi

- ❑ Dijital ayak izimizin daha sonra bizi üzmemesi ya da istemeyen durumlarla karşılaşmamak için internette bilgi paylaşıpken çok dikkat etmeliyiz.



Dijital Ayak İzi Nedir?

- ❑ Klavyeden, fareden ya da ekrandan, tırlayarak, tıklayarak ya da dokunarak elektronik ortama aktardığımız bizimle ilgili her türlü iz.



- ❑ İnternette bizlerin nerede olduğunu takip eden bir pasaport gibidir.
- ❑ Ne aldığımızı, neyi araştırdığımızı, hangi reklamları gördüğümüzün kaydedilmesidir.



- Facebook, Twitter vb. hesaplarımızda paylaştıklarımız, bloglarımız, bizimle ilgili çıkmış her türlü haber, yazılmış her yazı internette uzun zaman saklanır, ve olmadık yerde karşımıza çıkarak bizi şaşırtabilir.

- İnternette paylaştıklarımız güvenliğimiz için riskleri de beraberinde getirir.



- İnternet üzerinde ne kadar az iz bırakırsak bizim için o kadar iyi olur.



- Özel bilgilerimizi paylaşırken, elektronik posta alıp verirken ya da sosyal medya paylaşımlarında bulunurken çok dikkatli davranmalı, kendimize zarar verecek davranışlardan uzak durmalıyız.

- İleriki yaşamımıza, iş bulmamıza zarar verecek paylaşımlardan kaçınmalı, başka bir deyişle itibarımızı korumak için daha dikkatli olmalıyız.



- Paylaştığımız resim ya da videoları, yazdığımız yorumları paylaşmadan önce bir kez daha düşünmeli, ileride karşımıza çıkarsa rahatsız olup olmayacağımıza karar vermeliyiz.

Temel Kavramlar

- Dijital vatandaşlık**, teknolojiyi kullanırken etik ve uygun davranışlarda bulunma ve bu konuda bilgilenebilmeyi içermektedir. İyi birer dijital vatandaş olmak için çok dikkatli olmalı, çok çalışmalıyız.



Temel Kavramlar

- Dijital vatandaş bilgi ve iletişim kaynaklarını kullanırken eleştirebilen, çevrimiçi davranışlarının etik sonuçlarının bilen, ahlaki online kararlar alabilen, teknolojiyi kötüye kullanmayan, dijital dünyada iletişim kurarken ve işbirliği yaparken doğru davranışı teşvik eden vatandaşdır.
- İyi birer dijital vatandaş olmak için dijital zorbalıktan uzak durmalı, dijital empati kurmalıyız.

Temel Kavramlar

- Dijital Zorbalık**, bilgi ve iletişim araçları vasıtasıyla zararlı ve küfür mesajlar yayarak diğerlerini taciz etmektir. Başkalarına yalnız mesajlar yollamak, onları üzmeştir.



- Dijital Empati**, sanal ortamda kendinizi başkasının yerine koyarak hareket etmek, paylaşım yapmak vb.

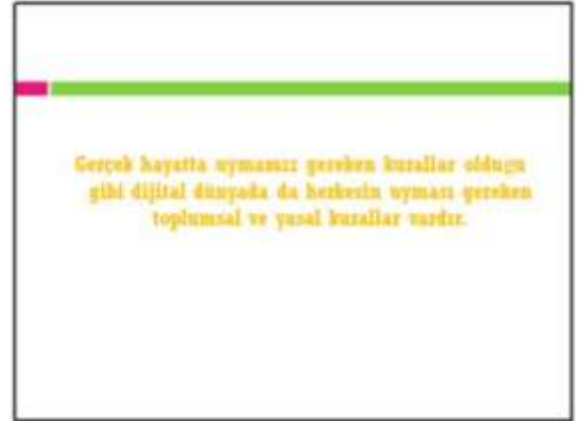
Temel Kavramlar

- ❑ **İnternet** bilgisayar sistemlerini birbirine bağlayan elektronik iletişim ağıdır.
- ❑ **Siber Tuzak**, bilgi ve iletişim teknolojileri vasıtasıyla kişisel bilgilerinizi alıp kullanmak amaçlı yapılan hilelerdir.
- ❑ **Siber Taciz**, başkalarına modern iletişim araçları kullanılarak kasıtlı olarak hakaret edilmesi, onların tehdit, teşhir ya da rahatsız edilmesidir.

TEŞEKKÜRLER



EK-D: Sayısal Vatandaşlık Sunusu Ekran Görüntüleri



"Videoda anlatılan dijital vatandaşlık kuralları nelerdi?"

?

"Eklemek istediğiniz dijital vatandaşlık kuralları var mı?"



Dijital Vatandaşlık Kuralları

- ❑ Zorbalık yapmayın. Sözlü tacize başvurmayın; insanlara küfretme, hakaret etme, onları taciz etme ya da onlara isim takma yoluyla saygısızlık etmeyin.
- ❑ Zorbalara katlanmak zorunda değilsiniz. Sizi taciz edenleri görmezden gelin ya da engelleyin.



Dijital Vatandaşlık Kuralları

- ❑ Çevrim içi olduğunuzda insanlara çevrim dışında olduğu gibi davranın.
- ❑ Başkalarına, kendinize davranılmasını istediğiniz şekilde davranın.
- ❑ Bulduğunuz bilgiyi olduğu gibi almayın, hırsızlık yapmayın.
- ❑ Sahtekârlık yapmayın.

Dijital Vatandaşlık Kuralları

- ❑ Ses tonunuzu, duygu durumunuzu iletme, mizah ve kişiselliğinizi katmak için yüz ifadesi gibi sembelleri kullanın.
- ❑ Sozcuklerinizi büyük harflerle yazmaktan kaçının. Bağırıyor gibisinden olur ve zor okunur.
- ❑ Çevrimiçi ortamda rahatsız edici bir durumla karşı karşıya kaldığınızda, bunu güvendiğiniz bir yetişkine söyleyin.



Dijital Vatandaşlık Kuralları

- ❑ Tanıştığınız herkese karşı saygılı, kibar ve duyarlı olun.
- ❑ Çevrim içi olduğunuzda kimliğinizin bilinmemesinin verdiği gücü kötüye kullanmayın.
- ❑ Bir şey yayınlamadan önce düşünün. İtibarınızı koruyun.
- ❑ Hakaretlere yanıt vermeyin, bu durumda itibarınızı koruyamayabilirsiniz.

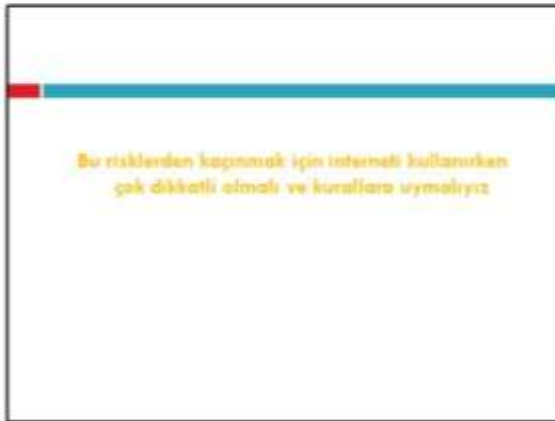
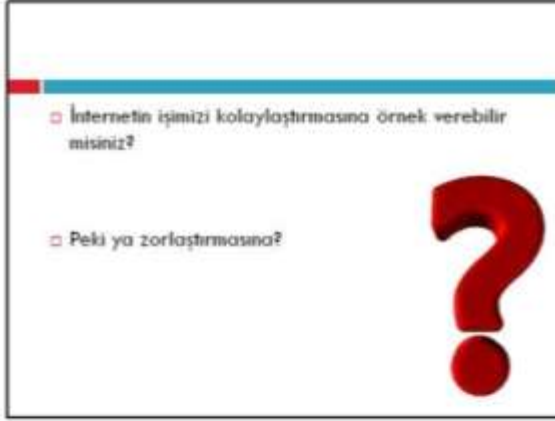


Dijital Vatandaşlık Kuralları

- ❑ Siz dijital ortamda bu kurallara uyuyor musunuz? Bundan sonraki davranışlarınız nasıl olacak?
- ❑ Dijital vatandaşlık kurallarına uyulmazsa ne gibi sonuçları olur?
- ❑ Dijital vatandaşlık kuralları neden önemlidir?



EK-E: Güvenli İnternet Sunusu Ekran Görüntüleri



Güvenli İnternet Kuralları

2. İnterneti ailelerinize ve arkadaşlarınıza değişmeyin.

Aileleriniz ön koltukta, internet ise arka koltukta otursun.



Güvenli İnternet Kuralları

3. İnternette her bilgi doğru olmayabilir. İnternette elde ettiğiniz bilgiyi en az 3 kaynaktan kontrol edin.

3

Ödevinizde kullanıyorsanız kaynağını belirtin.



Güvenli İnternet Kuralları

4. İnternet ortamındaki bedava teklifler büyük ihtimalle gerçek değildir.

Tanımadığınız kişi size neden bedava bir şey teklif etsin ki.



Güvenli İnternet Kuralları

5. Adınız, okulunuz, adresiniz, telefon numaranız, aile bireylerinizin adı vb. gibi kişisel bilgilerinizi paylaşmayın.

Paylaşılan küçük gibi görünen bilgiler, büyük zararlara sebep olabilir.



Güvenli İnternet Kuralları

6. İnternet ortamında paylaşacağınız resminizi, size ait video gibi paylaşımları önce düşünün, sonra paylaşın.

Paylaşıtlarınız sizin veya sevdiklerinizin üzülmesine sebep olmasın.



Güvenli İnternet Kuralları

7. Şifreleriniz güçlü olsun.

Adınızı ve doğum tarihinizi, ard arda gelen kelimeleri ve sayıları şifre olarak belirlemeyin.

Anılamlı bir cümle kurun ve o cümledeki kelimelerden seçtiğiniz en az 8 karakterden oluşan şifreler oluşturun.



Güvenli İnternet Kuralları

8. İyi ve nazık bir kullanıcı olmaya çalışın.

Gerçek hayatta Merhaba dediğiniz arkadaşınıza internet ortamında "mrh" değil, yine merhaba deyin.

Tamamı derken "Ok," veya "İttm" yerine yine tamam deyin.



Güvenli İnternet Kuralları

9. Gerçek hayatta yüzüne söylemeyeceğiniz ifadeleri internet ortamında da söylemeyin.



Güvenli İnternet Kuralları

10. Gerçek hayatta olduğu gibi, internet ortamında da tanımadıklarınızı arkadaş edinmeyin.



Güvenli İnternet Kuralları

11. İnternet ortamında tanımadıklarınıza cevap vermeyin, tekliflerini reddedin, size gönderdikleri mesajları açmadan silin.



Güvenli İnternet Kuralları

12. İnternet ortamında sizi rahatsız edenleri, sizi taciz edenleri ailelerinize söyleyin.

Ailelerinle birlikte emniyete veya savcılığa suç duyurusunda bulunun.

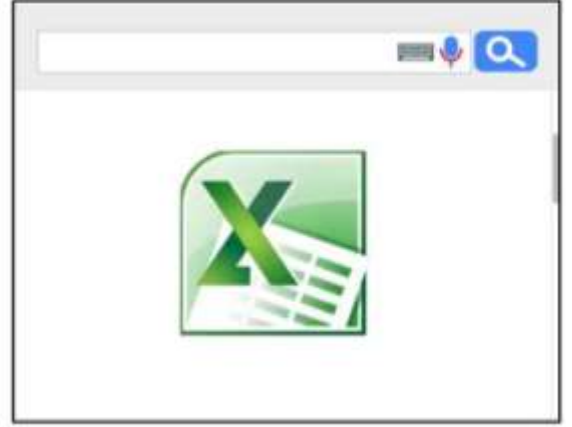


Güvenli İnternet Kuralları

13. İnternetin zararlı içeriklerinden korunmak için tamamıyla ücretsiz olan "Güvenli İnternet Hizmeti"nden ailelerinizi haberdar edin.



EK-F:İnternette Etkili Arama Yapma Sunusu Ekran Görüntüleri







Web sayfaları birçok konuda güzel ve çekici gelebilecek kaynaklar sunabilir. Ancak, bu kaynaklarda yer alan bilgi her zaman güvenilir olmayabilir.

Çünkü birçok yanlış ve değerlendirilmemiş bilgi de web üzerinde bulunabilir.

Bu nedenle de internet üzerinden ulaşılan bilginin **doğruluğu**, **güvenirliği** ve **güncelliği** konusunda şüpheli olmalıdır.

Sınıfa asılan afişe göre eşleştirilim:

1. .com	a) devlet kurumları
2. .org	a) okullar
3. .net	a) kar amacı gütmeyen kuruluşlar
4. .gov	a) üniversiteler
5. .edu	a) bilgi içerikli siteler
6. .info	a) özel şirketler
7. .k12	a) internet hizmeti sağlayan şirketler

Ülkelerin kullandığı alan kodları ile ülkeleri eşleştirilim:

1. .au	Kanada
2. .be	Fransa
3. .ca	Türkiye
4. .tr	Meksika
5. .br	Belçika
6. .fr	Avustralya
7. .mx	Brezilya

Aşağıdaki siteleri web siteleri değerlendirme ölçütüne göre değerlendirelim:

1. grup: Vikipedi
2. grup: Ekşi sözlük
3. grup: Uludağ sözlük
4. grup: E-okul

TEŞEKKÜRLER

EK-G: İnternette Etkili Arama Yapma Afişİ

İNTERNET

İNTERNETTE DAHA HIZLI ARAMA YAPABİLİRSİN. İŞTE SANA KÜÇÜK İP UÇLARI:



Birkaç kelime ile arama yap.
Basit anahtar kelimeler kullan.
Kelimelerin arasına **'+' işareti** koy.
Kısaltma kullanma. (Örn. : İst. yerine İstanbul)
Kelimeleri **'tekil'** olarak yaz.
(Örn. : Kitaplar yerine kitap)
Kalıp halinde bir şey arıyorsan, **tırnak işareti** ("...") içine al.

İNTERNETTE ÜLKELERİN KULLANDIĞI ALAN KODLARI:



.au	AVUSTRALYA
.be	BELÇİKA
.br	BREZİLYA
.ca	KANADA
.ch	İSVİÇRE
.cn	ÇİN
.fr	FRANSA
.in	HİNDİSTAN
.jp	JAPONYA
.mx	MEKSİKA
.nz	YENİ ZELANDA
.uk	BİRLEŞİK KRALLIK
.tr	TÜRKİYE

HANGİ ALAN UZANTILARINI KİMLER KULLANIR?



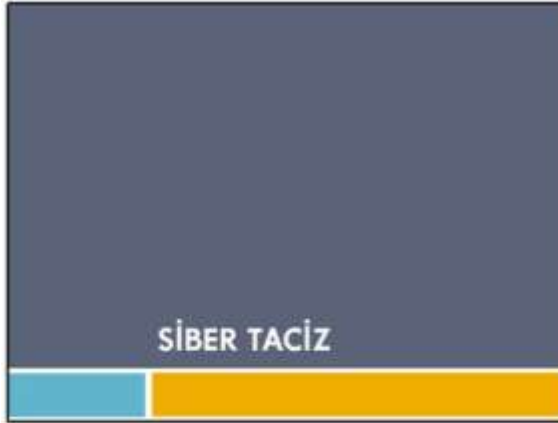
.com: Özel şirketler
.net: İnternet hizmeti sağlayan firmalar
.org: Kâr amacı olmayan vakıf veya dernek gibi kuruluşlar
.gov: Devlet kurumları
.edu: Üniversiteler
.info: Bilgi içerikli siteler
.meb.k12.tr: İlkokul, ortaokul ve liseler

EK-Ğ: Web Sayfası Değerlendirme Formu

Web sayfaları aşağıdaki ölçütlere göre değerlendirilir.

Bilginin Kaynağı Belli mi?	Evet	Hayır
Hazırlayanla ilgili bilgi var mı?	☐	☐
Hazırlayan bir kurum ya da kuruluş mu?	☐	☐
Hazırlayan bir kişi mi?	☐	☐
Bir kişiyse, onunla ilgili yeterince bilgi var mı?	☐	☐
Kişi o konuda uzman mı?	☐	☐
Bilgi Güvenilir mi?		
Sayfada yer alan bilginin, hangi kaynaklardan yararlanarak hazırlandığı belirtilmiş mi?	☐	☐
Bilgi, dilbilgisi ve yazım hataları içeriyor mu?	☐	☐
Bilgi Objektif mi?		
Sunulan bilgi kamu yararı için mi hazırlanmış?	☐	☐
Sunulan bilgi reklam amaçlı mı hazırlanmış?	☐	☐
Sunulan bilgi, okuyucunun görüşünü değiştirmeye uğraşıyor mu?	☐	☐
Sunulan bilgi, doğruluğu kanıtlanmış bilgilere mi kişisel görüşlere mi dayanıyor?	☐	☐
Bilgi Güncel mi?		
Sayfanın ne zaman hazırlandığı belli mi?	☐	☐
Sayfanın ne zaman güncelleştiği belli mi?	☐	☐
Yer alan bilginin ne zaman hazırlandığı belli mi?	☐	☐
Sayfa Kapsamlı mı?		
Sayfa tamamlanmış mı yoksa hazırlanmaya devam ediyor mu?	☐	☐
Sayfa, ihtiyacın olan bilgiyi içeriyor mu?	☐	☐

EK-H: Siber Taciz Sunusu Ekran Görüntüleri



SİBER TACİZ

- ❑ Başkalarına modern iletişim araçları kullanılarak kasıtlı olarak hakaret edilmesi, onların tehdit, teşhir ya da rahatsız edilmesine **siber taciz** denmiştir.
- ❑ Basit kelimelerle ifade edecek olursak siber taciz, çevrimiçi tacizdir.
- ❑ Genel özellikler arasında suç uydurma, izleme, tehdit, kimlik hırsızlığı, veri tahriri ya da manipülasyon yer alır.



SİBER TACİZ

- ❑ Siber takipçiler cinsel taciz, uygunsuz iletişime geçme veya sadece hayatınız ve ailenizin faaliyetleri ile ilgili rahatsız edici tacizde bulunmak için e-posta, anlık mesajlar, telefon aramaları ve başka iletişim araçları kullanır.



- ❑ Tacizciniz çoğu zaman yabancı değil, tanıdığınız birisidir. Eski bir sevgili, eski bir arkadaş veya sadece sizi ve ailenizi uygunsuz bir şekilde rahatsız etmek isteyen biri olabilir.

SİBER TACİZ

- ❑ Aile içi şiddet kurbanları çoğu zaman siber taciz kurbanlarıdır.
- ❑ Bilgisayar ve cep telefonunuzda olup biten her şeyi takip etmek için [casus yazılımlar](#) kullanılabilir ve bu da siber takipçilere inanılmaz bir güç ve bilgi sağlar.



Siber Tacizden Korunma Yolları

- ❑ Siber takipçiler, kurbanlarını izlemek için yazılım ve donanım araçları kullanır (bazen siz farkında bile olmadan bilgisayarınız arkasına takılıdır).
- ❑ Bilgisayardan uzaklaştığınızda her zaman bilgisayar programlarındaki oturumunuzu kapatın ve parola ile ekran koruyucu kullanın.



Siber Tacizden Korunma Yolları

- ❑ [İyi parola yönetimi](#) ve güvenliği konusunda alıştırmalar yapın.

Parolalarınızı hiçbir zaman başkalarıyla paylaşmayın.

Ayrıca parolalarınızı sık sık değiştirmeyi unutmayın!



Siber Tacizden Korunma Yolları

- Adınızı ve aile bireylerinizin adını aratarak internette ne tür bilgiler bulunduğuna bakın. Özel ya da uygunsuz olan her şeyi kaldırın.
- Katılmayı planladığınız etkinlikleri gösteren takvimleri ve seyahat programlarını sosyal ağınızda olursanız veya özel hale getirin. Bu bilgi bir takipçinin ne zaman nerede olabileceğini öğrenmesine neden olabilir.



Siber Tacizden Korunma Yolları

- Güvendiğiniz kişilerin dışındaki kişilerle paylaşımınızı sınırlamak için tüm çevrimiçi hesaplarınızda gizlilik ayarlarını kullanın.
- Bu ayarları kullanarak birisi sizin adınıza aradığında profilinizin görünmemesini sağlayabilirsiniz.
- İnsanlara yayınladıklarınızı ve fotoğraflarınızı görmemesi için onları engelleyebilirsiniz de.



Siber Tacizden Korunma Yolları

- Birisinin günlük etkinliklerinizi takip etmek için casus yazılım kullandığından şüpheleniyorsanız ve tehlikeye olduğunuzu düşünüyorsanız, yardım almak için kamuya açık bilgisayarlar veya telefonlar kullanın.

Aksi takdirde, siber takipçi yardım almaya çalıştığınız öğrenir ve bu da sizin için daha da büyük bir tehlike oluşturabilir.



Siber Tacizden Korunma Yolları

- Her zaman olduğu gibi birisinin bir [bilgisayar](#) soldurması veya virüs bulaşması olan bir Web sitesi aracılığıyla bilgisayarınıza casus yazılım yüklemesini önlemek için iyi, güncellenmiş [güvenlik yazılımı](#) kullanın.



Hangi güvenlik yazılımının mevcut olduğunu görmek için cep telefonunuzun uygulama mağazasına gidin.

Güvenlik yazılımları, uygulamanızda casus yazılımları tespit etmenizi sağlayabilir ve takip edene riski azaltabilir.

Bir kaç öneri...

- Ne kadar güvenli olduğunu düşünseniz de internette kendinizle ilgili kişisel bilgiler vermeyin.
- Hiçbir zaman gerçek adınızı, okullarınızın adını, adreslerinizi veya yaşadığınız şehri belirtmeyin.
- İnternette telefon numaranızı kesinlikle vermeyin

Siber tacize maruz kalırsanız

- "Siber tacizciyi" engelle. İşe yaramazsa, itirmeyen irtibatları önlemek için son çare olarak da, kendi anında mesaj ya da cep telefonu numaranı gibi irtibat bilgilerini değiştirebilirsiniz.
- Cevap verme. Onur kırıya ya da hasusa gitmeyen mesajlara, sana zor gelebilecek, asla karşılık verme. Senin karşılık vermen, "siber tacizcinin" tam da istediği şey – böylece kendini onaylanmış hissedecektir. Mesajlar bir kılıf kesilmiyor, yeni bir e-posta hesabı aç.



Siber tacize maruz kalırsanız

- Delilleri sakla
Hoş olmayan mesajların, resimlerin ya da online sohbetlerin kopyalarını çıkar (kayıt ederek, ekran resimleri çekerek vs.).



Bunlar, ne olduğunu başkalarına gösterebilme veya kanıtlayabilme yardımcı olacaktır ve tacizciyi tespit etmekte de işe yarayabilir (örn. okulunda, cep telefonu şirketinde, internet servis sağlayıcısında ve hatta poliste).

Siber tacize maruz kalırsanız

- Bundan söz et

Sen ya da senin tanıdığın birisi internette ya da cep telefonu yoluyla tehdit ya da rahatsız ediliyorsa, bununla tek başına başa çıkmak zorunda değilsin.

- Bu durumu ailene, güvendiğin bir yetişkine ya da okuldaki bir öğretmenine anlatmalısın.

- Durum daha



Se bildirmelisin.

NELER HİSSEDER?

Şişsinin taciz edildiğini fark edersen seyirci kalma



Tacize uğrayan kişiye destek ol ve siber taciz olayını bildir.

Bu tür bir olay senin başına geldiğinde hiç kimse sana yardım etmezse kendini nasıl hissedersen?

SİBER TUZAKLARI NASIL ANLARIM?

- 1 İnternette **kimlik bilgilerini** isteyen web sitelerine karşı **dikkatli ol.**
- 2 **Bedava** hediyelerden, programlardan ve **kazanacağını söyleyen yarışmalardan uzak dur.**
- 3 Eğlenceli gibi görünen testler, **senin hakkında bilgi toplamak için** hazırlanmış olabilir. **Bir kez daha düşün.**
- 4 Unutma! Bilinen markalar veya kurumlar e-posta yoluyla senden **parola, kimlik bilgileri gibi kişisel bilgiler istemez.**
- 5 Açılır pencerelerle (**pop-up**) gelen yarışma ve anketlere **katılma.**
- 6 Şüpheli bulduğun **e-postaların** içindeki bağlantıya (linke) tıklama ve gönderilen dosyayı **açma.**
- 7 Tanımadığın kişilerden gelen e-postaları açmadan önce, **tekrar düşün.**
- 8 İçeriği arkadaşlarına da göndermeni isteyen **e-postalar**, seni ve arkadaşlarını riske atabilir. E-postayı sil ve arkadaşlarını **uyar.**
- 9 İsteğin dışında bilgisayar kameranın açılmaması için, kameranı **kontrol et.**
- 10 Oyun oynamak için, **üye olmanı isteyen siteleri önce dikkatlice incele.**

POP-UP
KATIL! BEDAVİ HEDİYELER KAZAN!
KİMLİK BİLGİLERİ
SİPİRELER

EK-İ: Çevrimiçi İtibar Kontrol Listesi Afışı



Çevrimiçi İtibar Kontrol Listesi

Dijital ayak iziniz, internet'i kullanırken geride bıraktığınız izdettir ve çevrimiçi itibarınızı şekillendirebilir. Dijital ayak izleriniz olumlu veya olumsuz olabilir ve insanların sizi şimdi nasıl gördüğünü veya gelecekte nasıl göreceğini şekillendirebilir. Çevrimiçi itibarınızı yönetmek ve korumak için basit kontrol listesini kullanın.

	Kendinizi çevrimiçi olarak arayın: sizin hakkınızda çevrimiçi ne olduğunu biliyor musunuz? Adınız ile basit bir web araması yapın ve neler bulabileceğinizi görün. Mutlu olmadığınız bir şeyi bulursanız, bu içeriği kaldırmak için gerekli adımları izleyin. Unutmayın, Facebook veya Twitter sayfalarınız görünüyorsa, gizlilik ayarlarınızı değiştirerek bunu değiştirebilirsiniz.
	Gizlilik ayarlarını kontrol edin: Kullandığınız web sitelerinde, özellikle sosyal paylaşım sitelerinde hangi bilgileri paylaştığınızdan emin olun. Çoğu sosyal paylaşım sitesinde, paylaştığınız içeriği ve onu paylaştığınız içeriği yönetmenize yardımcı olacak gizlilik ayarları bulunur; yayınlarınız yalnızca çevrimiçi arkadaşlarınızla ve takipçilerinizle ya da herkes tarafından paylaşılmasını isteyip istemediğinize karar verebilirsiniz. Arkadaşlarınız içeriğinizin ve ayarlarınızın da dijital ayak izinizi etkileyebileceğini unutmayın.
	Gönderi yapmadan önce düşünün: arkadaşınızın o komik resmini yüklemeyen veya Twitter'da birisiyle ilgili şaka yapmadan önce, herkesin görmesini ister misiniz diye kendinize sorun; arkadaşlar, aile, gelecekteki işverenler? Başkalarının sizinle ilgili bu tür bir içeriği yayınlarsa mutlu olur musunuz? Çevrimiçi gönderdiğiniz her şeyden gurur duymalısınız, çevrimiçi gönderinizin potansiyel olarak sonsuza kadar orada kalacağını unutmayın!
	Devre dışı bırakın ve silin: Bir sosyal paylaşım profili veya web sitesini kullanmayı bıraktığınızda, hesabınızı devre dışı bırakmak veya silmek iyi bir fikirdir. Bu, içeriğin artık canlı olmadığı ve çevrimiçi olarak aranabilir olmaması gerektiği anlamına gelir; ayrıca, bu hesapların siz bilmeden saldırıya uğramasının riskini de ortadan kaldıracaktır.
	Olumlu bir ayak izi bırak: çevrimiçinde kalan olumsuz ayak izleri hakkında çok şey duyuyoruz. Çevrimiçi itibarınızı kontrol altında tutmanın en iyi yolu, yaratıcı olmak ve çevrimiçi zamanınızı olumlu bir ayak izi oluşturmak için kullanmaktır. Örneğin, neden yaptığınız tüm harika şeyleri tanıtmak için bir blog yazmayasınız. Bir çevrimiçi sponsorluk sayfasını kullanarak hayır kurumu için bağış yapabilir veya başkalarına yeni şeyler öğretmek için bir video oluşturabilirsiniz.

EK-J: Etik Komisyonu Onay Bildirimi*



T.C.
HACETTEPE ÜNİVERSİTESİ
Rektörlük

Sayı : 35853172/

433-2319

29 Haziran 2017

EĞİTİM BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜNE

İlgi: 05.06.2017 tarih ve 1275 sayılı yazınız.

Enstitünüz Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı tezli yüksek lisans programı öğrencisi **Gizem KUH**'un **Prof. Dr. Buket AKKOYUNLU** sorumluluğunda yürüttüğü "**Sayısal Ayak İzi**" Ders Tasarımının Öğrencinin Sayısal Vatandaşlık Becerilerine Etkisi" başlıklı tez çalışması, Üniversitemiz Senatosu Etik Komisyonunun 20 Haziran 2017 tarihinde yapmış olduğu toplantıda incelenmiş olup, etik açıdan uygun bulunmuştur.

Bilgilerinizi ve gereğini rica ederim.

Prof. Dr. Rahime M. NOHUTCU
Rektör a.
Rektör Yardımcısı

Hacettepe Üniversitesi Rektörlük 06100 Sıhhiye-Ankara
Telefon: 0 (312) 305 3001 - 3002 • Faks: 0 (312) 311 9992
E-posta: yazimd@hacettepe.edu.tr • www.hacettepe.edu.tr

Ayrıntılı Bilgi için:
Yazı İşleri Müdürlüğü
0 (312) 305 1008

* Etik Kurul onayı alındıktan sonra, Eğitim Bilimleri Enstitüsü Yönetim Kurulunun 05.12.2017 tarih ve 50 sayılı oturumunda aldığı 2017-50/02 sayılı karara istinaden danışman değişikliği yapılmıştır. Ayrıca bu tezin başlığı ile alınan etik kurul onayındaki başlığın farklılığı, 05.03.2018 tarihinde yapılan Yüksek Lisans Tez Savunma Sınavı jürisinin önerisi ve Eğitim Bilimleri Enstitüsü Yönetim Kurulu'nun 13.03.2018 tarih ve 11 sayılı oturumunda almış olduğu 2018-11/05 sayılı tez başlığı değişikliği onayından kaynaklanmaktadır.

EK-K: Etik Beyanı

Hacettepe Üniversitesi Eğitim Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmada,

- tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- görsel, işitsel ve yazılı bütün bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- atıfta bulunduğum eserlerin bütününe kaynak olarak gösterdiğimi,
- kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- bu tezin herhangi bir bölümünü bu üniversitede ya da başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

19/03/2018



Gizem KUH

EK-L: Yüksek Lisans Tez Çalışması Orijinallik Raporu

19/03/2018

HACETTEPE ÜNİVERSİTESİ

Eğitim Bilimleri Enstitüsü

Bilgisayar ve Öğretim Teknolojileri Eğitimi Ana Bilim Dalı Başkanlığına,

Tez Başlığı : Sayısal Ayak İzi Ders Tasarımının Öğrencilerin Sayısal Vatandaşlık Konusundaki Akademik Başarılarına Etkisi

Yukarıda başlığı verilen tez çalışmamın tamamı (kapak sayfası, özetler, ana bölümler, kaynakça) aşağıdaki filtreler kullanılarak **Turnitin** adlı intihal programı aracılığı ile kontrol edilmiştir. Kontrol sonucunda aşağıdaki veriler elde edilmiştir:

Rapor Tarihi	Sayfa Sayısı	Karakter Sayısı	Savunma Tarihi	Benzerlik Oranı	Gönderim Numarası
19/03/2018	114	141022	05/03/2018	% 22	932513168

Uygulanan filtreler:

1. Kaynaklar hariç
2. Alıntılar dâhil
3. 5 kelimeden daha az örtüşme içeren metin kısımları hariç

Hacettepe Üniversitesi Eğitim Bilimleri Enstitüsü Tez Çalışması Orijinallik Raporu Alınması ve Kullanılması Uygulama Esasları'nı inceledim ve çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan eder, gereğini saygılarımla arz ederim.

Ad Soyadı: Gizem KUH
Öğrenci No.: N13227170
Ana Bilim Dalı: Bilgisayar ve Öğretim Teknolojileri Eğitimi
Programı: Bilgisayar ve Öğretim Teknolojileri Eğitimi
Statüsü: ☒ Y.Lisans ☐ Doktora ☐ Bütünleşik Dr.



DANIŞMAN ONAYI



UYGUNDUR.

Yrd. Doç. Dr. Gökhan DAĞHAN

EK-M: Thesis Originality Report

19/03/2018

HACETTEPE UNIVERSITY
Graduate School Of Educational Sciences
To The Department Of Computer Education and Instructional Technology

Thesis Title : The Effect of Digital Footprint Course Design on Students' Academic Achievement About Digital Citizenship

The whole thesis that includes the *title page, introduction, main chapters, conclusions and bibliography section* is checked by using **Turnitin** plagiarism detection software take into the consideration requested filtering options. According to the originality report obtained data are as below.

Time Submitted	Page Count	Character Count	Date of Thesis Defense	Similarity Index	Submission ID
19/03/2018	114	141022	05/03/2018	% 22	932513168

Filtering options applied:

1. Bibliography excluded
2. Quotes included
3. Match size up to 5 words excluded

I declare that I have carefully read Hacettepe University Graduate School of Educational Sciences Guidelines for Obtaining and Using Thesis Originality Reports; that according to the maximum similarity index values specified in the Guidelines, my thesis does not include any form of plagiarism; that in any future detection of possible infringement of the regulations I accept all legal responsibility; and that all the information I have provided is correct to the best of my knowledge.

I respectfully submit this for approval.

Name Lastname: Gizem KUH
Student No.: N13227170
Department: Computer Education and Instructional Technology
Program: Computer Education and Instructional Technology
Status: ☒ Masters ☐ Ph.D. ☐ Integrated Ph.D.



ADVISOR APPROVAL



APPROVED
Assist. Prof. Dr. Gökhan DAĞHAN

EK-N: Yayımlama ve Fikrî Mülkiyet Hakları Beyanı

Enstitü tarafından onaylanan lisansüstü tezimin/raporumun tamamını veya herhangi bir kısmını, basılı (kâğıt) ve elektronik formatta arşivleme ve aşağıda verilen koşullarla kullanıma açma iznini Hacettepe Üniversitesine verdiğimi bildiririm. Bu izinle Üniversite'ye verilen kullanım hakları dışındaki bütün fikrî mülkiyet haklarım bende kalacak, tezimin tamamının veya bir bölümünün gelecekteki çalışmalarda (makale, kitap, lisans ve patent vb.) kullanım hakları bana ait olacaktır.

Tezin kendi orijinal çalışmam olduğunu, başkalarının haklarını ihlal etmediğimi ve tezimin tek yetkili sahibi olduğumu beyan ve taahhüt ederim. Tezimde yer alan telif hakkı bulunan ve sahiplerinden yazılı izin alınarak kullanılması zorunlu metinleri yazılı izin alarak kullandığımı ve istenildiğinde suretlerini Üniversite'ye teslim etmeyi taahhüt ederim.

☐ Tezimin/Raporumun tamamı dünya çapında erişime açılabilir ve bir kısmı veya tamamının fotokopisi alınabilir.

(Bu seçenekle teziniz arama motorlarında indekslenebilecek, daha sonra tezinizin erişim statüsünün değiştirilmesini talep etmeniz ve kütüphane bu talebinizi yerine getirirse bile, teziniz arama motorlarının ön belleklerinde kalmaya devam edebilecektir)

☒ Tezimin/Raporumun 19.03.2021 tarihine kadar erişime açılmasını ve fotokopi alınmasını (İç Kapak, Özet, İçindekiler ve Kaynakça hariç) istemiyorum.

(Bu sürenin sonunda uzatma için başvuruda bulunmadığım takdirde, tezimin/raporumun tamamı her yerden erişime açılabilir, kaynak gösterilmek şartıyla bir kısmı veya tamamının fotokopisi alınabilir).

☐ Tezimin/Raporumun tarihine kadar erişime açılmasını istemiyorum ancak kaynak gösterilmek şartıyla bir kısmı veya tamamının fotokopisinin alınmasını onaylıyorum.

☐ Serbest Seçenek/Yazarın Seçimi:

.....
.....
.....

19/03/2018


Gizem KUH

