

**T.C.**

**ATATÜRK ÜNİVERSİTESİ**

TOPLUMSAL DUYARLILIK PROJELERİ UYGULAMA VE ARAŞTIRMA MERKEZİ

**“Güvenli İnternet Kullanımı ve Siber Zorbalık Eğitimi”**

**Proje Kodu**: **621F7088C1BAA**

**SONUÇ RAPORU**

**Proje Yürütücüsü:**

Doç. Dr. Ülhak ÇİMEN

**Araştırmacılar:**

Nurşah YİĞİT

Mayıs, 2022  
ERZURUM

**İÇİNDEKİLER**

Önsöz2

Özet 3

Abstract (İSTEĞE BAĞLIDIR. DİLERSENİZ DOLDURUNUZ.)………………………………4

Materyal ve Yöntem 5

Proje Uygulamasına Ait Görseller7

Sonuçlar20

# ÖNSÖZ

Hayatın neredeyse her alanında evimizde, cebimizde, kafelerde, restoranlarda, AVM’lerde ve aklınıza gelebilecek her türlü ortamda interneti özgürce kullanabiliyoruz. Bu denli büyüyen ve gün geçtikçe gelişmeyi sürdüren internetin gerek sosyal gerekse iş hayatındaki olumlu katkıları yadsınamaz ancak kimi zaman da pek çok olumsuz durumla da bizi yüz yüze bırakabiliyor. İşte bu noktada olumsuz durumları yaşamamak ya da en azından minimuma indirmek adına birtakım önlemler almak gerekiyor. Güvenli internet kullanımı için yapılması gerekenler fazlasıyla önem arz etmektedir.

# ÖZET

Siber zorbalık, dijital teknolojiler kullanılarak gerçekleştirilen zorbalıktır. Bu tür zorbalıklar sosyal medyada, mesajlaşma platformlarında, oyun platformlarında ve cep telefonlarında görülebilir.  Hedef seçilen kişileri korkutmaya, kızdırmaya ya da utandırmaya yönelik olarak tekrarlanan bir davranıştır. Buna örnek olarak şu eylemler gösterilebilir:

* Sosyal medyada bir kişi hakkında yalanlar yaymak ya da utandırıcı fotoğraflar yayınlamak
* Mesajlaşma platformlarından incitici mesajlar ya da tehditler yollamak
* Başka birinin kimliğiyle başkalarına kötü mesajlar göndermek.

Yüz yüze zorbalık ve siber zorbalık çoğu kez birlikte gerçekleşir. Ancak siber zorbalık geride dijital iz bırakır; bu da aslında istismarın durdurulmasını sağlayacak yararlı ip uçları temin edebilir. Bu projede Atatürk Üniversitesi İletişim Fakültesi öğrencilerine güvenli internet kullanımı ve siber zorbalıkla ilgili eğitim verilmiştir. Ayrıca fakülte ile sınırlı kalmaması düşüncesiyle 102.00 frekansından yayın yapan Radyo Üniversiteden tüm şehrimize bu eğitim aktarılmıştır.

Bu proje Atatürk Üniversitesi Toplumsal Duyarlılık Projeleri tarafından desteklenmiştir.

**Anahtar Kelimeler:** Güvenli internet, siber zorbalık, sosyal medya

# 

# MATERYAL VE YÖNTEM

# Araştırmanın Türü

Bu çalışma bir Toplumsal Duyarlılık Projesi’dir.

# Araştırmanın Yapıldığı Yer ve Zaman

Proje ekibi tarafından 29.01.2022-16.04.2022 tarihleri arasında Atatürk Üniversitesi İletişim Fakültesinde gerçekleştirilmiştir.

# Projenin Uygulanışı

Proje uygulayıcısı İl Emniyet Müdürlüğü Siber Suçlarla Mücadele Şube Müdürlüğü personeliyle bir toplantı yapılmıştır. Projenin İletişim Fakültesi öğrencilerine gerçekleştirilmesi kararlaştırılmıştır. Eğitim slaytlarında projenin Atatürk Üniversitesi Toplumsal Duyarlılık Projeleri tarafından desteklendiğini gösteren ibareler yer almıştır.

Siber Suçlarla Mücadele Şube Müdürlüğünde görev yapan Komiser Ali Özoğluöz ile Radyo programı Polis Memuru Mücahit Albayrak ile de eğitim programı gerçekleştirilmiştir. Verilen eğitimin metin özeti aşağıda gösterilmiştir:

DİJİTAL OKURYAZARLIK VE SİBER GÜVENLİK

Okuryazarlık denilince aklımıza ilk okuma, yazma, konuşma ve dinleme  gelmektedir.

Okuryazarlık, bir toplumdaki gelişmişlik düzeyini tanımlayan önemli göstergelerden bir tanesidir.

Dijital okuryazarlık; telefon, tablet ve bilgisayar gibi ağ cihazları aracılığıyla bilgiyi bulma, anlama, analiz etme, üretme ve paylaşma becerilerini ifade eder.

# Dijital Okuryazarlık Türleri Nelerdir?

# Teknoloji Okuryazarlığı

# İnternet Okuryazarlığı

# Sosyal Medya Okuryazarlığı

# İletişim Okuryazarlığı

# Bilgisayar Okuryazarlığı

# Bilgisayar Okuryazarlığı

# Bir bilgisayarı ve diğer ilgili teknolojileri kullanma bilgi ve becerisine sahip bireyleri tanımlamak için kullanılan bir terimdir.

# Teknoloji Okuryazarlığı

# Kişilerin bilgi ve iletişim teknolojilerini, hayatlarının farklı alanlarında ve başkalarıyla kurdukları iletişimde kullanması için sahip olması gereken becerilerdir.

# İnternet Okuryazarlığı

# İnternet ortamında bilgiyi okumak, bilgi paylaşmak, yorumlar yapmak gibi eylemleri gerçekleştirebilmeyi kapsayan bir terimdir.

# Sosyal Medya Okuryazarlığı

# Sosyal medya mecralarındaki bilgi, mesaj, gönderi ve haberleri yorumlayabilme, kullanabilme ve sorgulayabilme becerileridir.

# Dijital Okuryazarlığın 3 Ana İlkesi

# • Bilgisayar programlarını kullanmak, arama motorları gibi bilgi kaynaklarına erişim için daha gelişmiş daha etkili yeteneklere kadar uzanmaktadır.

# KULLANMAK

# •Dijital medyayı anlamamıza ve eleştirel olarak değerlendirmemize yardımcı olmaktadır.

# ANLAMAK

# Çeşitli dijital medya araçları ile içerik üretme ve etkili bir şekilde iletişim kurma becerisidir.

# OLUŞTURMAK

# Dijital Okuryazarlığın 3 Ana İlkesi

# Dijitalleşen dünya ile hayatımıza giren dijital okuryazarlık kavramı, dijital mecradaki içerik ve eylemleri doğru anlamak ve yorumlamak açısından önemlidir.

# NELER ÖĞRENECEĞİZ?

# Kişisel Veri Nedir?

# Bilgi Kirliliği Nedir ve Nasıl Önlenir?

# Bilişim Etiği Nedir ve Nelere Dikkat Edilmeli?

# Dijital Ayak İzi Nedir?

# DİJİTAL VATANDAŞ

# İnterneti doğru, etkin ve etik kullanma becerisi sizin iyi bir “dijital vatandaş” olduğunuzun bir göstergesidir.

# DİJİTAL AYAK İZİ

# ‘‘İnternet kullanımı sırasında arkanızda bıraktığınız izlerdir.’’

# Sosyal medya kullanımından ziyaret ettiğiniz sitelere, yaptığınız alışverişlerden aklınıza gelen bütün işlemler dijital ayak izleri olarak adlandırılır.

# BİLİŞİM ETİĞİ

# Bilişim teknolojileri kullanıcılarının ve bu kullanıma aracılık yapan kuruluşların uyması gereken kuralları ifade eder. Bilişim etiği amacı; kullanıcıların dijital ortamı daha güvenli kullanmasını sağlamak ve ortaya çıkabilecek riskleri en aza indirmektir.

# ETİK KURALLARA SAHİP KULLANICI;

# Teknolojik cihazları insanlara zarar vermek için kullanmaz.

# Dijital ortamda başka kullanıcıların kişisel verilerini paylaşmaz.

# Doğruluğundan emin olunmayan bilgileri paylaşmaz.

# Başkalarının ürünü olan eserleri alıntılamaz.

# Lisanssız yazılım kullanmaz.

# Diğer kullanıcı haklarına saygı gösterir.

KİŞİSEL VERİ NEDİR?

Kişiyi doğrudan ya da dolaylı olarak belirlenebilir kılan tüm bilgiler kişisel veri olarak kabul edilmektedir.

1. telefon numarası
2. araç plakası
3. pasaport numarası
4. özgeçmiş
5. fotoğraf
6. ses kayıtları
7. parmak izleri
8. e-posta adresi
9. hobiler
10. grup üyelikleri
11. aile bilgileri

# sağlık bilgileri

# Kişisel Verilerimizi Korumak İçin;

# Hesaplarınız için güçlü parolalar oluşturun.

# Kişisel bilgilerinizi kimseyle paylaşmayın.

# Kullandığınız uygulamaların gizlilik ayarlarını kontrol edin.

# Tanımadığınız kullanıcılardan gelen arkadaşlık isteklerini kabul etmeyin.

# Yüklediğiniz uygulamalara verdiğiniz izinleri kontrol edin.

# Bilgi Kirliliği

# Doğru bilgilerin yanında veya dışında; yalan, yanlış ya da asılsız bilgilerin listelenmesi, yayılmasıdır.

# TÜİK

# 16-74 yaş grubundaki bireylerde Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması kapsamında yapılan araştırmaya göre;

# İnternete erişim imkanı olan hane oranı %92,0 oldu.

# İnternet kullanan bireylerin oranı %82,6 oldu.

# İnternet üzerinden mal veya hizmet siparişi verme ya da satın alma oranı %44,3 oldu.

# İnternetten en fazla %70,7 ile giyim, ayakkabı ve aksesuar satın alındı.

# En çok satın alınan veya abone olunan dijital içerik %30,6 ile film veya dizi izleme hizmeti oldu.

# GÜVENLİ DİJİTAL OKURYAZARLIK

# E-posta adresinizde güçlü parolalar kullanın ve parolanızı sık sık değiştirin.

# İki faktörlü kimlik doğrulaması kullanın.

# Hesabınızı kısmen veya tamamen gizleyin.

# Rahatsızlık duyduğunuz hesapları engelleyin veya kısıtlayın.

# Konumunuzu paylaşmaktan kaçının.

# Fotoğraf etiketleme seçeneğini kapatın.

# Herkesten gelebilecek mesaj isteklerine izin vermeyin.

# Ortak alanlardaki bilgisayarlardan çıkış yapın.

# Güvenli web sayfaları tercih edin.

# Tanımadığınız kullanıcılardan e-posta alırsanız veya bilmediğiniz bir e-posta eki alırsanız kesinlikle açmayın.

# Bilgisayarınızda mutlaka anti-virüs programınız ve güvenlik duvarınız olsun.

# Açık kablosuz ağları mecbur olmadıkça kullanmayın.

# Önemli verilerinizi yedekleyin.

# Güncellemeleri ihmal etmeyin.

# Tüm dijital dünyanızı tek bir parola ile yönetmeyin.

# ÇEVRİM İÇİ ALIŞVERİŞLERDE;

# Ürün hakkındaki kullanıcı yorumlarını okuyun.

# Site hakkında araştırma yapın.

# Ortak bilgisayarları kullanmayın.

# Bağlantı ve adresin doğruluğunu teyit edin.

# Sitenin ticari unvanını ve iletişim bilgilerini e-devlet üzerinden kontrol edin.

# İnternet sitesi satış sözleşmesi ve formları okuyun.

# MAĞDURİYETLE KARŞILAŞILMASI DURUMUNDA YAPILABİLECEKLER VE BAŞVURU YOLLARI

# Anne-babanız, ailenizden yakın bir kişi, okulda iseniz rehber öğretmeninize yada okul idaresinden bu konuda yardım isteyin.

# Siber zorbayı engelleyin.

# Misilleme yapmayın.

# Siber zorbayı platforma şikayet edin.

# Mağduriyetinize ait delilleri saklayın.

# Mağduriyet yaşadığınız konuya ilişkin delilleri toplayarak,

# 18 yaşından büyükseniz ŞAHSEN; Cumhuriyet savcılığına, polise ve jandarmaya başvurabilirsiniz.

# 18 yaşından küçükseniz ANNE VEYA BABANIZLA birlikte; Cumhuriyet savcılığına, polise ve jandarmaya başvurabilirsiniz.

# ARAYABİLECEĞİNİZ ACİL TELEFON HATLARI

# Acil bir konu / durum olması halinde 112 ihbar hattını aramalısınız.

# ÇEVRİMİÇİ İHBAR ADRESİ

# Çevrim içi olarak

# PROJE UYGULAMASINA AİT GÖRSELLER

**Radyo Fotoğrafları**



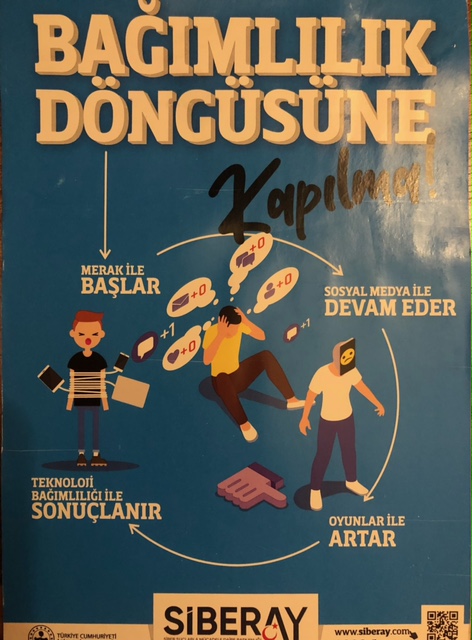
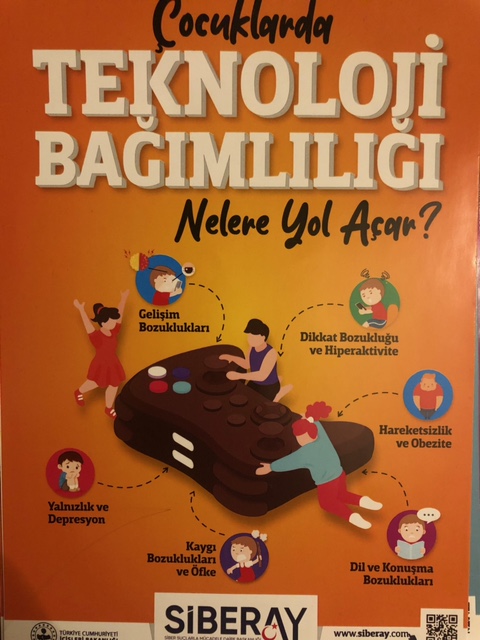
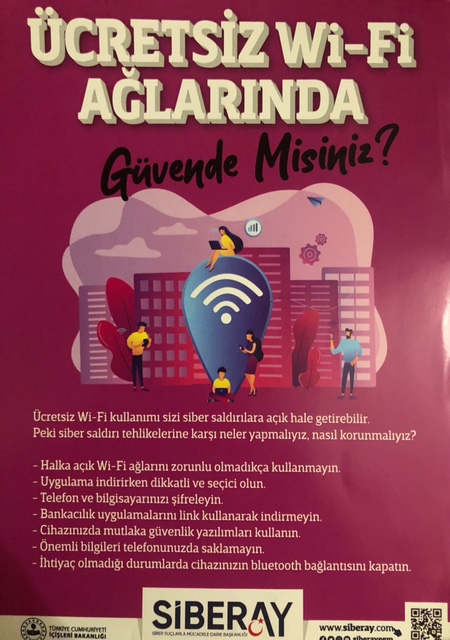
# Eğitim Fotoğrafları

# 



# Afiş Fotoğrafları

# s



# SONUÇLAR

# Her geçen gün teknolojinin ve bu teknolojilere erişilebilirliğin artmasına paralel olarak bilişim sistemlerine yönelik işlenen suçlar da artmaktadır. Siber Suç, bir bilişim sisteminin güvenliğini ve/veya buna bağlı verileri ve/veya kullanıcısını hedef alan ve bilişim sistemi kullanılarak işlenen suçlardır. Siber Suçu diğer suçlardan ayıran özelliği bir bilişim sistemi olmadan işlenememesidir. Bu suç türü bilgisayar ve internete özgü suçlar olarak da adlandırılabilir. Tüm suçların bilişim sistemleri kullanılarak işlenebileceği de bir gerçektir. Ancak böyle olması o eylemi siber suç yapmayacaktır. Siber Suçlar Sözleşmesi ve dairemiz görev alanı perspektifinde bakıldığında, siber suç bir bilişim sistemine izinsiz olarak ve hukuka aykırı olacak şekilde girilmesi ve sonrasında yapılan eylemdir. Bu suçta hedef bir kişi olabileceği gibi kişinin malvarlığı veya bir sistemin kendisi de olabilir. Örneğin, bir sisteme girerek, zarar verme, verileri silme, şifreleme, ele geçirme, veri ekleme, sistemin kullanımını engelleme, özel hayatın gizliliğine müdahale etme, iletişimi engelleme, iletişimi izinsiz izleme ve kayıt etme gibi eylemler siber suç kategorisinde değerlendirilir.