

BİLİŞİM SUÇLARI

ÇALIŞMA KİTABI



Editör

Aybüke Kuruyüz

Orta Doğu Teknik Üniversitesi

Bilgisayar ve Öğretim Teknolojileri Eğitimi

Eğitmen

Zahide Yıldırım

Orta Doğu Teknik Üniversitesi

Bilgisayar ve Öğretim Teknolojileri Eğitimi

İçerik

Bilişim Suçları

KAYNAKÇA

BTK. (2019, Haziran 11). *Türk ye’de Bilişim Hıkkı*
<https://internet.btk.gov.tr/turkiye-de-bilisim-hkkk>

Doğan, B. (n.d.). *B l ş m Sıç Ned r?* <https://barandogan.av.tr/blog/teza-hkkk/bilisim-sllari-nelerdir.html>

Kalan, H. N. (2022, 12 Nisan). *"B l ş m Sıçları Hakkında Bilinmesi Gerekenler - III."* <https://www.gvenliweb.org.tr/blog-detay/bilisim-sllari-hakkında-bilinmesi-gerekenler-iii#:~:text=Bili%C5%9Fim%20Sı%C3%A7lar%C4%B1na%20Kar%C5%9F%C4%B1%20Al%C4%B1na%20Bireysel%20%C3%96nlemler&text=G%C3%BC%C3%A7l%C3%BC%20parola%20kullan%C4%B1mal%C4%B1%20ve%20belirli,b%20parolalar%20kimse%20ile%20payla%C5%9F%C4%B1lmamal%C4%B1d%C4%B1r.&text=Mobil%20ihaz%20ve%20bilgisayarlar%C4%B1n%C4%B1za%20kırak%C4%9F%C4%B1n%C4%B1z%20yglama%20ve%20yaz%C4%B1l%C4%B1mlar%20g%C3%BCvenilir%20web%20sitelerinden%20indirilmelidir>

Kalemci Hukuk. (n.d.). *B l ş m Sıç Ned r? Çeş tler Nelerdir?* <https://kalemci.av.tr/bilisim-sll-nedir-esitleri-nelerdir/>

CEVAP ANAHTARI

1. Bilgisayarlar, bilgi saklayan, bu bilgileri işleyen ve sonuçları kullanıcıya ileten elektronik aygıtlardır. Donanım ve Yazılım bilgisayarın iki ana kısmıdır.
2. İnternet, bilgisayar gibi akıllı cihazlar yoluyla bilgi almayı ve iletmeyi sağlayan iletişim ağıdır.
3. Bilişim suçları, bilgisayar sistemlerini veya bilgi teknolojilerini hedef alan suçları ifade eder.
4. C
5. Kişisel verilerin çalınması, Kredi kartı yoluyla dolandırıcılık yapılması, Tehdit, şantaj ve fidye talepleriyle şirketlerin veya kişilerin tehdit edilmesi, Kötü amaçlı yazılımlar geliştirilmesi ve kullanılması, Yetkisiz dinleme yapılması
6. A
7. A
8. B

ÖNSÖZ

Bu kitapçık;

Orta Doğu Teknik Üniversitesi

Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü

Öğretim Materyali Tasarımı ve Kullanımı Dersi
Kapsamında

Prof. Dr. Zahide YILDIRIM rehberliğinde

Aybüke Kuruyüz tarafından

Kasım 2023 tarihinde hazırlanmıştır.

ÖZET

İnternetin gün geçtikçe yaygınlaşmasıyla suçlar internet ortamına taşındı denilebilir. Bilgisayar, telefon, pos makinesi veya tablet gibi elektronik cihazların kullanımıyla elektronik ortamda işlenen suçlara bilişim suçları (siber suçlar) denir. Bilişim suçlarına, bilgisayar ile dolandırıcılık, kişisel bilgileri çalmak, sosyal medya hesaplarının çalınması, müstehcen veya saldırgan içerikler yoluyla taciz, kanun tarafından korunan bir yazılımın ele geçirilip izinsiz kullanılması gibi örnekler verilebilir. Bunlar gibi birçok bilişim suçuna karşı maddi manevi bir zarar görmemek için önlemler alınmalıdır. Bilişim suçlarına örnekler ve alınabilecek bazı önlemler bu kitapta anlatılmaktadır.

UYGULAMA SORULARI

7. Şifre belirlerken aşağıdakilerden hangisinin yapılması güvenli bir şifre oluşturmamızı sağlar?

- A) Şifrelerimizi en az 7 karakter olacak şekilde belirlemeliyiz.
- B) Şifremizde sadece küçük karakterler kullanmalıyız.
- C) Şifremizde rakam kullanmamalıyız.
- D) Şifremizde ardışık sayılar kullanmalıyız.

8. Ülkemizde bilişim suçlarıyla ilgili olan kanunlara göre aşağıdakilerden hangileri yanlıştır?

- A) Bir bilişim sistemine hukuka aykırı olarak girilmesi suçtur ve cezası vardır.
- B) Başkasına ait bir kredi kartının kullanılmasında bir sakınca yoktur.
- C) Başkasına ait bir kredi kartının kullanılması sonucunda kişi ceza alır.
- D) Bilişim sisteminin işleyişini bozan kişi bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

UYGULAMA SORULARI

1. **Bilgisayar nedir, Bilgisayarın iki ana kısmı nedir ? Açıklayınız.**
2. **İnternet nedir? Açıklayınız.**
3. **Bilişim Suçlarının tanımını yapınız.**
4. **Aşağıdakilerden hangisi siber suçların günümüzde artmasının sebeplerinden değildir?**
 - A) İnternet ve bir elektronik cihazın yeterli olması
 - B) Sahte bilgilerle yapılabilmesi
 - C) Fiziksel bir görüşmenin zorunlu olması
5. **Bilişim suçlarına 5 örnek veriniz.**
6. **Aşağıda verilen bilişim suçlarına karşı alınacak önlemlerden değildir?**
 - A) Şifrelerimizi her yere not etmek
 - B) Farklı hesaplarımızda farklı şifreler kullanmak
 - C) Elektronik cihazlarımızda parmak izi, yüz tanıma gibi giriş yöntemlerini kullanmak
 - D) Şifrelerimizde kişisel bilgilerimizi kullanmamak

SÖZLÜK

1. **Bilişim:** Bilgisayar ve iletişim teknolojilerini kullanarak gerçekleştirilen her türlü suç faaliyetini ifade eden genel bir terimdir.
2. **Suç:** Yasalara aykırı davranışları ifade eder ve bu bağlamda bilişim suçları, bilgisayar sistemlerini hedef alan yasa dışı faaliyetleri içerir.
3. **Müstehcen Veri:** Cinsel içerikli veya uygunsuz materyalleri ifade eder ve bu tür verilerin dağıtımı veya paylaşımı müstehcen veri suçunu oluşturabilir.
4. **Kredi Kartı Dolandırıcılığı:** Kredi kartı bilgilerinin izinsiz kullanımını içeren bir suç türüdür; kişisel finansal bilgilerin hırsızlık amacıyla ele geçirilmesini ve kullanılmasını içerir.
5. **Tehdit:** Bir kişiye zarar verme, itibarını zedeleme veya başka bir zarar tehdidi içeren eylemleri ifade eder.
6. **Şantaj:** Bir kişinin itibarını zedelemek veya ona zarar vermek amacıyla elde edilen tehlikeli bilgilerin kullanılmasıyla gerçekleşen suçtur.
7. **Fidyeye:** Bilgisayar sistemlerini kilitleme veya verileri şifreleme tehdidi ile fidye talep etme eylemlerini ifade eder.
8. **Vaat:** Yasadışı veya etik olmayan eylemleri gerçekleştirmek amacıyla yapılan vaatleri içeren bir suç türüdür.
9. **Korsan İçerik:** Telif haklarına aykırı olarak elde edilen veya dağıtılan içerikleri ifade eder.
10. **Lisanssız Yazılım:** İlgili yazılımın yasal sahipleri tarafından izin verilmeksizin kullanılması veya dağıtılması durumunu ifade eder.
11. **Fuhuş:** Cinsel hizmetleri yasa dışı yollarla ticaret

İÇİNDEKİLER

Bilgisayar ve İnternet	7
Bilgisayar Nedir?	9
İnternet Nedir?	10
Bilişim Suçları	11
Bilişim Suçları Örnekleri	12
Bilişim Suçları ile ilgili Kanunlar	14
Alınabilecek önlemler ve stratejiler	16
Uygulama Soruları	20
Cevap Anahtarı	22
Kaynakça	23

ÖNLEMLER

5651 sayılı yasanın 8. maddesinde yer alan;

- İntihara Yönlendirme,
- Çocukların Cinsel İstismarı,
- Uyuşturucu veya Uyarıcı Madde Kullanılmasını Kolaylaştırma,
- Sağlık için Tehlikeli Madde Temini,
- Müstehcenlik,
- Fuhuş,
- Kumar Oynanması için Yer ve İmkân Sağlama,
- Atatürk Aleyhine İşlenen Suçlar,
- Yasadışı Bahis

ile ilgili yeterli şüpheye sahip olduğu düşünülen içerikler www.ihbarweb.org.tr adresine ihbar edebilmeli. (Kalan, 2022).



ÖNLEMLER

*Şifre dışındaki giriş yöntemleri denenebilir.
(Yüz tanıma, parmak izi gibi)*

Şifre de kişisel bilgilere yer verilmemeli

*Şifrelerde ardışık sayılar, harfler
kullanılmamalı*

Şifreler en az 7 basamaklı olmalı

*Şifreler büyük-küçük harfler, rakam-
noktalama ve özel karakterler içermeli*

KAZANIMLAR

- Bilgisayar ve internet hakkında bilgi sahibi olmak
- Bilişim suçları hakkında bilgi sahibi olmak
- Bilişim suçlarıyla ilgili kanunları özetleyebilmek
- Bilişim suçlarına karşı alınacak önlemleri ve stratejileri geliştirmek

BİLGİSAYAR VE İNTERNET



ÖNLEMLER

Kişisel bilgilerinizi isteyenlere itibar etmemeli

Korsan içerikler indirmemeli

Başkasına ait cihazları ve ağları izinsiz kullanılmamalı ve kopyalamamalı

Farklı hesaplarda aynı şifre kullanılmamalı

Şifreler bir yerlere not edilmemeli

ÖNLEMLER

Kişisel bilgilerimizi korumak ve internetteki kötü insanlardan kendimizi korumak için bazı önlemler almalıyız.

Bilişim suçlarına karşı alınacak bazı bireysel önlemler şu şekilde sıralanabilir.

*Lisanssız yazılımlar ve içerikler
kullanılmamalı.*

Antivirüs programları kullanılmalı



BİLGİSAYAR NEDİR ?

Bilgisayarlar, bilgi depolayan, bu bilgileri işleyen, işlem sonucunu kullanıcıya veren elektronik cihazlardır.

Bilgisayarlar genele bakıldığında iki kısma ayrılır: Donanım ve Yazılım.



Donanım, bilgisayarın fiziksel parçalarıdır.

Yazılım ise bilgisayarda kullanılan programlar bütünüdür.

Donanım bilgisayarın vücudu iken yazılım zihnidir.

İNTERNET NEDİR ?

İnternet, bilgisayar gibi akıllı cihazlar yoluyla bilgi almayı ve iletmeyi sağlayan iletişim ağıdır.

- İnternet sayesinde istenilen web sitesine, uygulamaya ve bilgiye erişilebilir.



İLGİLİ KANUNLAR

2. Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu (TCK 244. Madde):

Bilişim sisteminin işleyişini engelleyen veya bozan, yok eden, değiştiren veya erişilemez kılan kişi bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

3. Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu (TCK 245. Madde):

Başkasına ait banka veya kredi kartının hukuka aykırı şekilde kullanılması durumunda kişi altı aydan üç yıla kadar hapis cezası veya adli para cezası ile cezalandırılır.



Bu düzenlemelerin amacı, bilişim suçlarına karşı hukuki bir çerçeve oluşturmak ve bu suçlarla mücadele etmektir. Ayrıca, bu suçların mağdurlarına yönelik koruma sağlanmaktadır.

İLGİLİ KANUNLAR

Ülkemizde bilişim suçlarına yönelik tek bir kanun yoktur. Mevcut kanunlara bilişim suçlarıyla ilgili hükümler eklenmiştir. Bu hükümler suçu kendi alanına ilişkin düzenlemeler içermektedir. (BTK, 2019).

İlgili maddelere göre, bilişim suçları üç ana kategoride incelenmiştir:

1. Bilişim Sistemine Girme Suçu (TCK 243. Madde):

Bir bilişim sistemine hukuka aykırı olarak girilmesi ve orada kalmaya devam edilmesi halinde kişi bir yıla kadar hapis cezası veya adli para cezası ile cezalandırılır.



BİLİŞİM SUÇLARI

Bilişim Suçu Nedir?

Bilişim suçu bilgisayar, cep telefonu gibi teknolojik cihazların kullanım aracılığıyla işlenen suçlara denir. (Kalemci, n.d.).

Bilişim suçlarına aynı zamanda siber suçlar da denilebilir.



Son dönemlerde bilişim suçlarının artış göstermesinin bazı nedenleri aşağıda sıralanmıştır.

- Sahte bilgilerle yapılabilmesi
- Fiziksel bir görüşmeye gerek olmaması
- İnternet ve bir elektronik cihazın yeterli olması

BİLİŞİM SUÇLARI

ÖRNEKLER

İnternet ortamında işlenen her suç olarak alındığı için bu suçlara geniş yelpazeden örnekler verilebilir.

Kötü amaçlı yazılımlar geliştirilmesi ve kullanılması

İnternet kullanıcılarına hakaret, küfür veya müstehcen içerikli veriler gönderilmesi

Kredi kartı yoluyla dolandırıcılık yapılması

Kişisel verilerin çalınması

BİLİŞİM SUÇLARI

Yetkisiz dinleme yapılması

Bilgi hırsızlığı

Tehdit, şantaj ve fidye talepleriyle şirketlerin veya kişilerin tehdit edilmesi

Sahte ürün veya sahte yatırım vaatleriyle insanların dolandırılması

