BİLİŞİM SUÇLARI

Bilişim Suçu Ne Demektir?

- ✓ Bilişim teknolojinin yardımı ile (genellikle sanal ortamda) kişi veya kurumlara maddi veya manevi zarar vermek, suç işlemek.
- ✓ Bilgisayar, çevre birimleri, pos makinesi, cep telefonu gibi her türlü teknolojinin kullanılması ile işlenen suçlardır.

HANGİ SUÇLAR BİLİŞİM SUÇUDUR?

1. E-POSTA ELE GEÇİRME

- ✓ Bir kişiye ait e-posta veya kullanıcı bilgilerini ele geçirmek, değiştirmek veya silmek.

2. KULLANICI HESAPLARI İLE İLGİLİ SUÇLAR

- ✓ Bir kişi veya kurum adına sahte e-posta / profil / hesap oluşturmak.
- ✓ Bu sahte hesapları kullanarak çeşitli paylaşımlar yapmak.

3. WEB SAYFALARI KULLANILARAK İŞLENEN SUÇLAR

- ✓ Başkalarının adına web sayfası hazırlamak ve bu web sayfasının tanıtımı amacıyla başkalarına e-mail ve mesaj göndermek ve bu mesajlarda da mağdur olan şahsın telefon numaralarını vermek.
- ✓ Sahte alışveriş siteleri kurarak kullanıcıları dolandırmak.
- ✓ Satışı yapılan ürünlere ait yanlış bilgiler verme.
- ✓ Müşteriye vaat edilen ürün yerine farklı ürün göndermek.
- ✓ Sosyal ağlar, forum ve video sitelerinde başkasına ait fotoğraf, video veya eserleri izinsiz paylaşmak.
- ✓ Devlet karşıtı gruplara ait içerikleri yayınlamak / paylaşmak.
- ✓ İnternetten alışverişte kullanıcıların kredi kartı bilgilerini ele geçirmek.

4. BİLGİSAYARI VEYA BİLGİLERİ ELE GEÇİREREK İŞLENEN SUÇLAR

- ✓ Başkasına ait bilgisayara, ağa veya sisteme izinsiz girmek, bilgileri kopyalamak, silmek veya değiştirmek.

5. LİSANSIZ YAZILIM VE İÇERİKLERİN KULLANIMI İLE İLGİLİ SUÇLAR

- ✓ Telif hakkı ile korunan yazılım, dosya, resim, fotoğraf, müzik, video klip ve film dosyalarını izinsiz indirmek, paylaşmak, tamamını veya bir kısmını kullanmak.

6. ÇEVRİMİÇİ İLETİŞİM SIRASINDA İŞLENEN SUÇLAR

- ✓ Sosyal ağlar, sohbet siteleri, forumlar gibi kullanıcıların birbirleriyle iletişim kurdukları sitelerde kişi ya da kuruluşa hakaret, küfür etmek veya aşağılayıcı ifadeler kullanmak.

7. KREDİ KARTI, KONTÖR/TL DOLANDIRICILIĞI

- ✓ Telefon, e-posta ve çeşitli iletişim araçları kullanarak kişilerden kredi kartı bilgileri istemek.
- ✓ Tehdit veya şantaj yoluyla çeşitli hesaplara TL veya kontör yüklenmesini istemek.

BİLİŞİM SUÇLARINA KARŞI ALINABİLECEK TEDBİRLER

Bilişim suçlarına karşı alınabilecek tedbirler nelerdir?

- ⦿ Lisanssız yazılımlar ve içerikler (müzik, resim, fotoğraf video vs.) kullanmayın.
- ⦿ Çeşitli yollarla kırılmış, içeriği değiştirilmiş veya güvenilir olmayan yazılımlar yüklemeyin.
- ⦿ Bilgisayar sistemini korumaya yönelik anti-virüs, güvenlik duvarı gibi yazılımlar kullanın ve mümkün olduğunca güncellemelerini yapın.
- ⦿ Kullanılan yazılımların en güncel ve sorunsuz sürümlerini temin etmeye çalışın.
- ⦿ Telefon, e-posta vs. gibi yollarla sizden kişisel bilgilerinizi (ad, soyad, adres, telefon gibi), parolanızı ya da kredi kartı şifrenizi isteyenlere itibar etmeyin.
- ⦿ Unutmayın hiçbir banka görevlisi size banka veya kredi kartı bilginizi sormaz!
- ⦿ İnternet ortamında tanımadığınız veya şüphelendiğiniz kişilere kişisel ve özel bilgilerinizi vermeyin!
- ⦿ Telif haklarıyla korunmuş içerikleri (müzik, film, oyun vs.) kesinlikle korsan olarak temin etmeyin, indirmeyin ve paylaşmayın!
- ⦿ Sosyal ağlarda, forum ve sohbet yazılımlarında kişi veya kurumlara karşı küfür, hakaret veya aşağılayıcı sözler kullanmayın.
- ⦿ Türkçe'mizi en güzel şekilde kullanmaya çalışın.
- ⦿ Kimsenin e-posta ve çeşitli hesaplarına (facebook, twitter vs.) giriş yapmaya, şifresini tahmin etme yoluyla ele geçirmeye çalışmayın!
- ⦿ Sahte hesaplar oluşturmayın ve bu hesapları kullanarak paylaşımlar yapmayın!
- ⦿ Başkasına ait bilgisayarı, interneti ve ağları izinsiz olarak kullanmayın, bilgileri silmeyin, değiştirmeyin veya kopyalamayın!

Kişisel Şifreler İle İlgili Öneriler

- Kişisel şifrelerini kesinlikle en yakınınız olsa dahi kimse ile paylaşmayın!
- Tüm hesaplarınızda aynı şifreyi kullanmayın!
- Şifrelerinizi hiçbir yere not etmeyin!
- Şifrelerinizi belirli aralıklar mutlaka değiştirin.
- Şifrenizi sosyal ağlar, sohbet yazılımları, siteler vs. aracılığı ile kimseye göndermeyin!
- Şifreler dışında daha güçlü giriş yöntemleri destekleyen bir sisteminiz varsa kullanın. Örneğin, parmak izi, yüz veya ses tanıma özellikleri.

Güvenli Şifre Oluşturma

- Şifrelerinizde kişisel bilgilerinize yer vermeyin. Örneğin, adınız, doğum tarihiniz veya kimlik numaranız.
- ali1999, 32423526655, 1986 gibi
- Şifrenizde ardışık sayılar, harfler kullanmayın. Örneğin, 123456, 1234, abcd gibi.
- Tahmin edilmesi kolay yanyana bulunan tuşları kullanmayın. Örneğin, qwerty, asdf gibi.
- Şifreniz en az 7 basamaklı olsun.
- Mümkün olduğunda aşağıdaki karakterlerden içersin.
- Büyük/küçük harf (A,a…Z,z)
- Rakam (0-9)
- Noktalama (.,; gibi)
- Özel karakter (-!+ gibi)

Bunları Unutmayın!

- İnternet ortamında işlediğiniz suçlardan dolayı evinize kadar takip yapılabilir.
- Bilişim suçları hakkında yakınlarınızı mutlaka uyarın.
- Bir bilişim suçundan dolayı mağdur olursanız mutlaka 155 Polis İmdat Hattına veya 155@iem.gov.tr adresine ihbarda bulunun!

BİLİŞİM SUÇLARINDAN MAĞDUR OLMAMAK İÇİN YAPILACAKLAR

1. İnternet ortamında %100 güvenliğin hiçbir zaman sağlanamayacağını unutmayın!
2. Şirketinize veya şahsınıza ait önemli bilgilerinizin yer aldığı bilgisayarınız ile özel güvenlik önlemleri almadan internete bağlanmamalı,
3. Özellikle chat (messenger) ortamında bilgisayarınıza sanal âlemden saldırılabileceğini;
4. Chat de tanıştığınız kişilere şahsınız, aileniz, adres, telefon, iş gibi konularda şahsi bilgilerinizi vermemeniz gerektiğini unutulmamalı
5. İnternet ortamında tanıştığınız kişilere kredi kartı bilgilerinizi verilmemeli,
6. İnternet üzerinden yapılan yazışmalarınızda karşınızdaki kurumlarla özel bir yöntemle yazışmanızda fayda olacaktır.
7. Kimliğini verdiği, kendini tanıttığı kişi olmayacağı düşüncesiyle tedbirli olmalıdır.