Kimlik Hırsızlığı & Dolandırıcılık

Herhangi bir siber suç olayı ele alınırken, alınacak en ufak bir önlem bile ileride karşılaşabileceğiniz sorunlar konusunda size çok yardımcı olacaktır. Siber suçlar pek çok farklı şekilde karşınıza çıkabilir. Çevrimiçi kimlik hırsızlığı, finansal dolandırıcılık, takip etme (röntgencilik), zorbalık, hackleme, e-posta sızdırma, bilgi korsanlığı ve sahtekârlık, entelektüel mülk suçu vb. pek çok suç siber suçlara örnek olabilir. Kişinin finansal anlamda çökertilmesi ve itibarının tehdit edilmesini en kötü senaryolar olarak sayabiliriz.

Herhangi bir siber suç olayı ele alınırken, alınacak en ufak bir önlem bile karşılaşılabilecek sorunlar konusunda çok yardımcı olacaktır. Siber suçlarla çok farklı şekillerde karşılaşılabilmektedir. Çevrimiçi kimlik hırsızlığı, finansal dolandırıcılık, takip etme (röntgencilik), zorbalık, hackleme, e-posta sızdırma, bilgi korsanlığı, sahtekârlık, entelektüel mülk suçu gibi pek çok suç siber suçlara örnek olabilir.

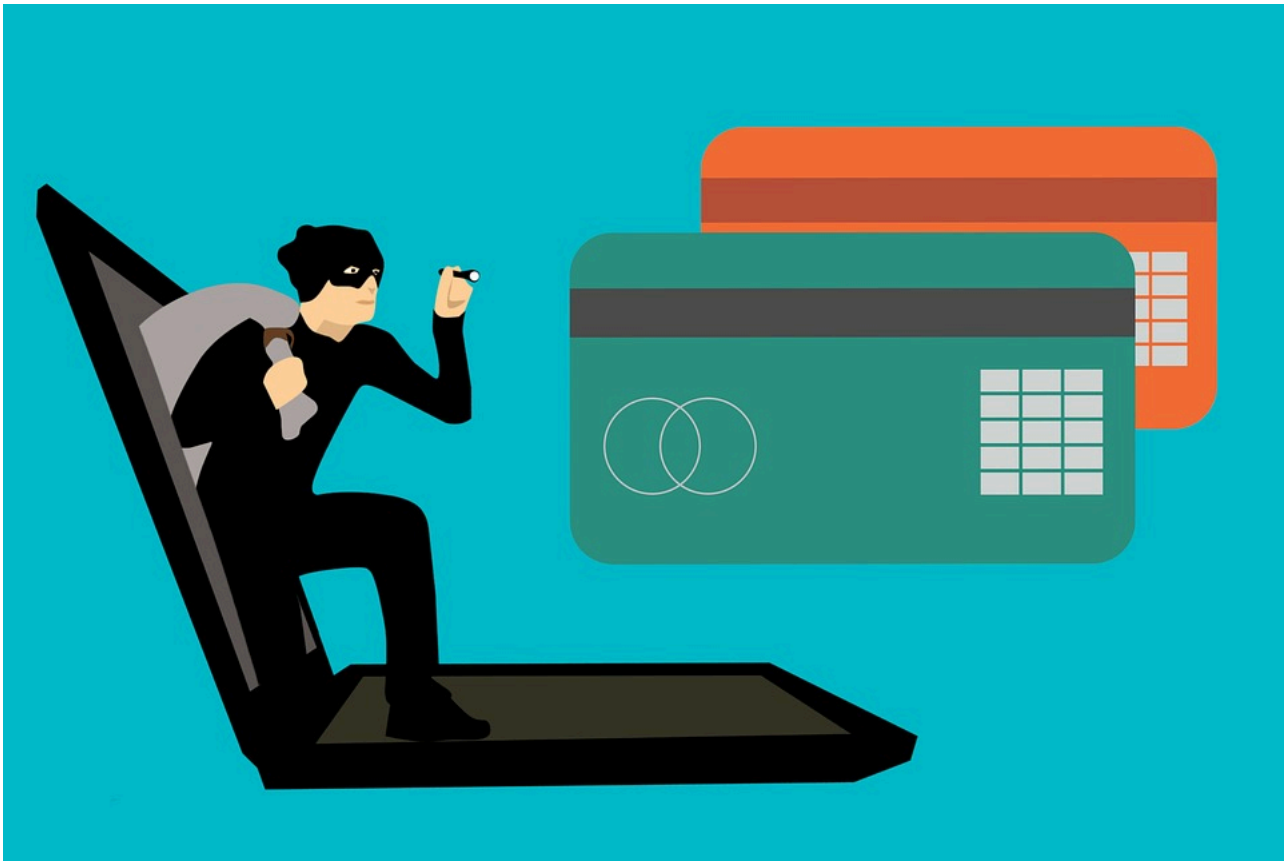
Bütün çabalara rağmen, dijital ortamda geçirilen zamanın artması ve dijital teknolojinin hızla ilerlemesi, kullanıcıları, onun zararlı taraflarına maruz kalmaya itebilir. Çünkü siber suçlarla uğraşan suçlular, çalmak, taciz etmek ve başka pek çok suça teşebbüs etmek için her zaman yeni yollar aramaktadır. Bu nedenle, eğer herhangi bir siber suç olayı ile karşı karşıya kalınırsa ne yapılması gerektiği bilinmeli ve çabuk davranılmalıdır.

Siber suç olayı ihbar edilmeli mi?

Siber suç olayını ayrıntılı bir biçimde incelemek ve takip etmek biraz zor olabilir. Çünkü çoğu siber suçlu, olay, yetkili kişinin kulağına gitmeden yaptığı çevrimiçi suçu terhis eder.
İyi haber şu ki, devletin pek çok kurumu ve yerel kolluk kuvvetleri siber suçlar ve bu sorunların ele alınma yöntemleri konularında her geçen gün daha tecrübeli hale gelmektedir. Ancak kolluk kuvvetleri, siber suçluları adalete teslim etmek için mağdurların da yardımına ihtiyaç duyabilir.
Siber suç olayı ihbar edildiği anda, şikâyete bağlı olarak ufak da olsa bir delilin olması, olayın çözülmesine ciddi yardımda bulunacaktır. Dolayısıyla, inceleme ve soruşturma için gerekli kanıtlar güvenli bir ortamda saklanmalıdır.
Aşağıdaki listede kanıt niteliği taşıyabilecek bazı hususlar bulunmaktadır:

- İptal edilen çekler,
- Sertifikalı veya diğer e-postalar,
- Sohbet odaları veya haber metinleri,
- Kredi kartı makbuzları,
- Fakslar,
- Log dosyaları,
- Sosyal paylaşım sitelerinden gelen mesajlar,
- Havale makbuzları,
- El ilanları veya broşürler,
- Telefon faturaları,
- E-postaların baskıları veya mümkünse elektronik kopyaları,

- Web sayfalarının baskıları veya mümkünse elektronik kopyaları
- Organizasyon makbuzları.
  Siber suç mağduru olunduğu anlaşıldığı anda verilmesi gereken tepki, suçun tipine ve belirli koşulların derecesine bağlı olarak değişkenlik gösterecektir.



Örneğin;

Kimlik hırsızlığı durumunda:

- Kullanılan bütün çevrimiçi hesapların şifreleri değiştirilmelidir. Şifreler değiştirildiğinde, yeni şifrenin şifre güvenliği kurallarına uygun olmasına özen gösterilmelidir. Suçlunun kullanıcı finansal hesaplarına ulaşamaması için banka hesapları dondurulmalıdır.
- Tehlikede olduğu düşünülen kredi kartları iptal edilerek, yeni hesap numaraları olan yeni kartlar edinmelidir. İlgili şirketler, sahip olunan kartların başkaları tarafından kullanılıyor olma ihtimaline karşı uyarılmalı ve kredi kartı ile herhangi bir harcama yapılıp yapılmadığı öğrenilmelidir.
- Başka hangi bilgilerin tehlikede olabileceği düşünülmelidir. Hırsızlığın türüne göre başka ilgili şirketlerle görüşmek durumunda kalınabilir.
- Bu tarz olaylar savcılığa ihbar edilmeli ve durumla alakalı rapor hazırlanması talep edilmelidir.

Çevrimiçi takip (röntgencilik) durumunda:

- Takip eden kişinin adının bilinmesi durumdan, rahatsız olunduğu ve devam ederse yasal işlem başlatılacağını bildiren açık bir uyarı mesajı gönderilmelidir. Bunu sadece bir kere yapılmalı, kişiyle tekrar muhatap olunmamalıdır. Çünkü tekrarlayan iletişimler suçluyu tekrar irtibata geçmesi konusunda cesaretlendirir.
- Suçlu ile her türlü iletişim türü saklanmalı (mektup, e-posta, tehdit mesajları vs.) ve uygun olan en uygun fırsatta olayların yaşanmış olduğu tarihi, saati ve içeriği belgelenmelidir.
- Çevrimiçi kimliğe sahip çıkılmalıdır. Sosyal ağlarda ve diğer hizmetlerde güvenlik ve gizlilik ayarlarının tam yapıldığından emin olunmalıdır.
  Kimlik hırsızlığı ve dolandırıcılık aktivitelerinde sıklıkla başvurulan bir yöntem olan oltalama (phishing) amaçlı iletiler, istenmeyen veya kötü amaçlı yazılımlar (malware ve casus yazılımlar) içerebilir. Eğer kullanılan bilgisayarda böyle bir yazılımın varlığından şüphe ediliyorsa, çevrimiçi koruma sağlayan güvenlik yazılımlarından biri kullanılabilir. Bunların bir örneğini safety.live.com adresinden edinebilir ve zararlı yazılımların bulunması ve kaldırılması için kullanılan bilgisayar taranabilir.
  İnternette daha güvende olmak için Google tarafından hazırlanan şu ipuçlarına göz atılabilir:
  https://safety.google/security/security-tips/

ETİKETLER

#Dolandırıcılık #KimlikHırsızlığı