GÜVENLİ GÜNLER BÜLTENİ

Bilgisayar kullanıcılarına yönelik hazırlanır. Her ayın 15'i çıkar. Diğer sayılara erişmek ve sonraki mesajların direk posta kutunuza gelmesi için guvenligunler.com adresini ziyaret ediniz.

AĞUSTOS 2019

Eyvah Hack'lendim!

GÜNLÜK HAYATIMIZDAKİ çoğu şeyin dijitalleştiği bu günlerde hack'lenmek de sık karşılaşılan bir risk haline geldi. Hatta haberlere bakılırsa, çoğumuz çoktan bu durumla karşılaştık bile.

"Hack" yasal olmayan yöntemlerle bir bilgisayar sistemine giriş yapmak anlamına gelmektedir. Yaygın anlamda sosyal medya hesaplarının ele geçirilmesi, zararlı yazılımlarla cihazların kullanılamaz hale getirilmesi, kredi kartı bilgilerinin sızdırılması, mesajların yetkisiz kişilerce okunması gibi pek çok kötü niyetli erişim örneği vardır.

HACK'LENDİĞİMİ NASIL ANLARIM?

Şüpheli bir durum ortaya çıktığında çevrimiçi hizmet sağlayıcılar müşterilerini hızlıca bilgilendirmeye çalışırlar. Ancak bu uyarıların size doğru ve zamanında ulaşması için bütün önemli aboneliklerinizde güncel iletişim bilgilerinizi kullanmanız gerekir. En önemli belirtilerden bazıları şunlardır:

- Haberiniz olmayan bir harcamaya dair SMS onayı isteği,
- Kredi kartı hesap özetinizdeki beklenmedik harcama kayıtları,
- Sizin adınıza hesaplarınıza giriş yapıldığına dair bir mesaj,
- Dostlarınızın uyarıları,
- Cihazlarınızda garip hareketler.

Ayrıca https://haveibeenpwned.com sitesinde, e-posta adresinizi yazıp arama yaparak da kişisel bilgilerinizin daha önce hack'lenen bir sitede bulunup bulunmadığını kontrol edebilirsiniz.

Önemli: Gerçekliğinden emin olmadığınız mesajlarda yer alan link'lere tıklamayın ve hiçbir bilginizi paylaşmayın. Oltalama saldırılarında panik yaratıcı sahte mesaj kullanımı çok yaygındır.

HACK'LENDİĞİNİZDEN ŞÜPHELENİYORSANIZ

Sakin olun, panikle harekete geçmeyin. Alacağınız önlemlerin etkili olması için soğukkanlılıkla davranmalı ve gerekli işlemleri sırayla uygulamalısınız.

1. Durum Değerlendirmesi

Öncelikle kötü niyetli kişilerin hangi bilgilere ve kaynaklara erişim sağladıklarını anlamaya çalışın. Örneğin, e-posta hesabınıza erişimi olan kötü niyetli kişi, varsa ilişkilendirilmiş sosyal medya hesaplarınızın şifrelerini sıfırlayabilir; ya da yazdığınız, gördüğünüz ve konuştuğunuz tüm bilgilere erişebilir. Bu aşamada belki de en iyisi bu konuda bilgi sahibi olan bir kişiye danışmaktır.

2. Zararı Durdurma

Durumu anlamanızın ardından ilk işiniz kötü niyetli kişilerin size daha fazla zarar vermesini engellemek olmalıdır. Bu aşamada hızlı davranmalısınız. Ayrıca kullanacağınız bilgisayar ve telefon gibi iletişim araçlarının güvenli olduğundan emin olmanız gerekir.

- Kötü niyetli kişiler finansal varlıklarınıza erişim kazandıysa, ilk olarak bu varlıkları güvenceye almalısınız. Hemen finans kuruluşunuzun çağrı merkezini arayın ve durumu anlatın. Sizi yönlendirdikleri şekilde kartlarınızı ve diğer finansal hizmetlerinizi dondurun.
- Sosyal medya hesaplarınız risk altındaysa, ilk olarak hesabınızın bağlı olduğu e-posta hesaplarınızın şifrelerini değiştirin. Daha sonra sosyal medya hesaplarınızın şifresini değiştirin. Daha sonra sosyal medya

hesaplarınızın şifresini değiştirin. Şifre değiştirirken, tanımlı iletişim bilgilerinizin doğru olup olmadığını tekrar kontrol edin.
- Bazen kötü niyetli kişiler, sosyal medyadaki arkadaşlarınıza sizin adınıza mesajlar göndererek onlardan sizin için taleplerde (borç para vermek, bir link'e tıklamak, vb) bulunabilirler; ya da sosyal medya hesaplarınızdan itibarınızı etkileyecek yayınlar yapabilirler. Bağımsız bir kanaldan arkadaşlarınızı haberdar edin.
- Cihazınızda şüpheli hareketler söz konusuysa, hemen cihazınızı kapatın ve bir uzmandan yardım isteyin.

3. Kurtarma

Kötü niyetli kişiler durdurulduktan sonra kurtarma çalışmalarına başlanılabilir. Kurtarma çoğu kez yavaş işleyen, sizin dışınızdaki faktörlere bağlı olan ve garantisi olmayan bir süreçtir.

- Finansal varlıklarınız izinsiz kullanıldıysa, finans kuruluşunuzdan ilgili işlemlerin iptalini talep etmelisiniz. Bunun için olayın gerçekleşme şekli, zamanı ve etkilenen finansal işlemler konusundaki bilgileri de kapsayan bir dilekçe gönderebilirsiniz.
- Sosyal medya ve diğer çevrimiçi hesaplarınıza erişim sağlayamıyorsanız, hizmet sunucunun iletişim kanallarını kullanarak yardım isteyebilirsiniz. Pek çok hizmet sunucu, kimliğinizi ve iletişim bilgilerinizi

doğrulamanız halinde hesabınıza bağlanabilmenizin yolunu açmaktadır.

» Kötü niyetli kişilerin cihazlarınıza erişim sağladığı durumlarda müdahalenin bir uzman tarafından yapılması önerilir. Özellikle adli süreçlerin sağlıklı yürütülebilmesi için cihaz üzerindeki kanıtların korunması gereklidir. Ayrıca, cihaz üzerinde kötücül bir yazılım çalışıyor olabilir. Önlem olarak verilere izole edilmiş bir ortamda, kötücül yazılım aktif hale getirilmeyecek şekilde erişilmeli ve veriler uygun yöntemlerle kurtarılmalıdır.

» Gizli verilerinize erişilmişse bu verilerin tümüyle yok edilmesini sağlamanız çok zordur. Ancak Kişisel Verileri Koruma Kanunu (KVKK) kapsamındaki haklarınızı kullanarak ya da mahkeme kararıyla bu bilgilerin kamuya açık şekilde yayınlanmasını durdurabilirsiniz. Bunun için ilgili içerik, yer ve erişim sağlayıcı kuruluşlara ulaşmanız gerekmektedir.

4. Yasal Sorumluluklar

Bilgisayar sistemlerine yetkisiz erişim kanunlarımızla tanımlanmış bir suçtur. Böyle bir durumla karşılaştığınızda savcılığa dilekçe vermeniz ve kötü niyetli kişilerden şikâyetçi olmanız gerekmektedir.

Şikâyetçi olarak hem bu tür suçların azalmasına katkı sağlayabilir hem de uğradığınız zararlar için hak talebinde bulunabilirsiniz. Ayrıca, kötü niyetli kişilerin sizin kimliğinizle yapmış olabileceği başka kötü niyetli işlemlere karşı kanun uygulayıcıları önceden bilgilendirmiş olursunuz.

5. Önlem Alma

Aşağıdakileri yaparak, bu tür tatsız durumlarda zararları azaltabilir ve kurtarma başarısını artırabilirsiniz:

» Önemli çevrimiçi hizmetlerde tanımlı iletişim bilgilerinizi güncel tutun,

» Her hesabınız için birbirinden farklı ve güçlü parolalar kullanın. Mümkün olan durumlarda çift faktörlü kimlik doğrulama kullanın,

» Kimlik bilgilerinizi, kimlik belge görüntülerinizi ve arkadaş bilgilerinizi internette paylaşmayın.

» Cihazlarınızda antivirüs yazılımı kullanın.

YAZAR HAKKINDA

İLKER TUTU bilgi teknolojileri ve bilgi güvenliği alanında çalışmaktadır. Şu anda, uluslararası bir finans şirketinde EMEA bölgesi bilgi güvenliği sorumlusu olarak görev almaktadır. CISSP, CCSP, CRISC, CGEIT, CISA, CIA ve ISO27001 profesyonel sertifikalarına sahiptir.