BATMAN ÜNİVERSİTESİ
BİLGİ İŞLEM DAİRE BAŞKANLIĞI

Siber Tehditlerin Farkında mısınız?

Bilginiz, paranız, itibarınız ve her türlü veriniz tehdit altında..

Farkında olun, korumak için tedbir alın!

Batman Üniversitesi Son Kullanıcı Siber Güvenlik Rehberi için TIKLAYINIZ!

Batman Üniversitesi Kurumsal Siber Güvenlik Rehberi için TIKLAYINIZ!

Bilgi İşlem Daire Başkanlığı Siber Güvenlik Videoları için TIKLAYINIZ!

Basit Önlemlerle Korunabilirsiniz:

1. Kendinizi ve bilgilerinizi koruyun. “Benim başıma gelmez” düşüncesinden uzaklaşın. Kendinizi ve bilgilerinizi koruyun. Siber suçluların saldırılarına karşı siz savunmasızsanız; ailenizi, arkadaşlarınızı ve kurumunuzu da riske atmış olabilirsiniz.

2. Parolalarınızı denetleyin. Parolalarınızın güçlü olduğundan ve karakter çeşitliliği içerdiğinden emin olun. Parolalarınızı belirli aralıklarla değiştirin. Farklı site üyelikleri için aynı parolayı kullanmayın. Parolalarınızı kimseyle paylaşmayın.

3. E-posta eklerine dikkat edin. Almayı beklemediğiniz e-posta eklerini hemen açmayın. Eğer doğruluğundan şüpheniz varsa, emin olmak için o e-postayı gönderen kişiyi arayın. E-posta ekleri aracılığıyla gelecek saldırılara karşı her zaman uyanık olun.

4. Kamuya açık ortak Wi-Fi’den uzak durun. İnternetten alışveriş, tıbbi randevu ve kayıt işlemleri veya bankacılık gibi kişisel işlerinizi yürütmek için güvenli olmayan veya herkese açık ortak Wi-Fi ağlarını kullanmayın.

5. Web kameranızı koruyun. Özellikle kullanmadığınız zamanlarda web kameranızı kapatmak için bir parça opak bant veya web kamerası kapağı kullanın. Siber suçlular, kişilerle ilgili her türlü bilgiyi almak için web kameralarını kullanabilirler, bu yüzden onların işini daha kolay hâle getirmeyin.

6. Tarayıcılarınızı düzenli olarak güncelleyin. İnternet tarayıcılarınızı ve ilgili eklentileri güncel tutun. En son sürümlerini kullandığınızdan emin olun.

7. Ağınızı güvenli tutun. Kurumda bunu biz sizler için yapıyoruz ama evde de atabileceğiniz adımlar var. Ev Wi-Fi ağınızda güçlü bir parola kullandığınızdan emin olun. Ağa bağlı tüm cihazları güncelleyin ve parolaları belirli aralıklarla yenileyin.

8. Oltalama e-postalarına karşı uyanık olun. Siber suçlular her geçen gün daha da yaratıcı oluyorlar. Oltalama e-postalarına karşı her an uyanık olun. E-posta içeriklerine her zaman şüphe ile yaklaşın ve yanıt vermek veya bir linki tıklamak için çok aceleci davranmayın.

9. Sosyal medyada kimseye güvenmeyin. Kişisel bilgilerinizi toplamaya çalışanlara karşı şüphe ile yaklaşın. Sosyal ağlarda tanımadığınız kişilerden gelen davetleri kabul etmeyin, talep ettikleri kişisel bilgilerinizi paylaşmayın.

10. Cihazlarınızı kilitleyin. Telefonunuzu, bilgisayarınızı ve benzer diğer cihazlarınızı bir güvenlik giriş kodu ile kilitleyin. Cihazlarınızı kullanmadığınız zamanlarda başkalarının erişebileceği şekilde açık bırakmayın.

11. Sistemlerinizi koruyun. Antivirüs, güvenlik duvarı ve reklam engelleyici çözümlerinin düzenli olarak yamalandığından ve güncellendiğinden emin olun. Kurumda bu çözümleri iş cihazlarınızda bizler sizin için sağlıyoruz ama evde kullandığınız cihazlarda da bu önlemleri almayı düşünün.

12. 2FA'yı ayarlayın. 2FA; iki faktörlü kimlik doğrulamasıdır. Oturum açtığınızda kimliğinizi doğrulamak için hesaplarınızı cep telefonunuza veya e-posta adresinize bağlamanızı gerektirir. Sosyal medya hesaplarınızın, siber saldırganlar tarafından çalınıp kötü amaçlarla kullanılmasını zorlaştırır.

13. Banka hesaplarınızı kontrol edin ve sahtekârlık uyarıları oluşturun. Siber suçlular banka hesap bilgilerinizi çaldığında, büyük miktarda parasal hareketler yapmadan önce genellikle deneme amaçlı küçük miktarlı işlemler yaparlar. Sizden habersiz yapılabilecek harcama ve benzeri işlemlerin takibine yönelik banka hesaplarınız ve kartlarınız için işlem uyarıları oluşturduğunuzdan emin olun.

14. Uygulamalarınızı temizleyin. Telefonunuza ve bilgisayarınıza hangi uygulamaları yüklediniz? Hâlâ bunları kullanıyor musunuz? Kullanmakta olduğunuz her şeyi gözden geçirin ve güncelleyin! Kullanmadığınız uygulamaları kaldırın. Ayrıca, uygulama izinlerini kontrol ettiğinizden, uygulamalarınızın hangi bilgileri okuyabileceğini ve değiştirebileceğini bildiğinizden emin olun.

15. Uygulama erişimlerini kontrol edin. İlginizi çekebilecek yeni uygulamalar her yerde! Resmi uygulama mağazasından gelmedikçe hiçbir uygulamayı yüklememe alışkanlığı edinin. Bu sırada, uygulamanın şüpheli veya müdahaleci izinler istemediğinden emin olmak için yüklemeden önce her uygulamayı kontrol edin. İçiniz uygulamayı yükleme konusunda hâlâ rahat değilse, farklı bir seçenek bulun.

16. Otomatik bağlantıyı devre dışı bırakın. Telefonunuzun evinizdeki Wi-Fi ağına veya arabanızın Bluetooth'una otomatik olarak bağlanması sizin için çok kullanışlı olabilir; ancak seyahat ederken veya halka açık yerlerde yabancı ağlara veya cihazlara bağlanabiliyor olması çok da iyi bir şey değildir. Kablosuz ağ otomatik keşif işlevinizin ve Bluetooth'un kapalı olduğundan emin olun.

17. Araştırın ve paylaşın. Sizin için yararlı olabilecek bazı güvenlik ipuçlarını bir araya getirin ve bunları kullanabilecek kişiler (İnternette yeni olan çocuğunuz, havaalanında beklerken oradaki Wi-Fi ile internet alışverişi yapmayı seven arkadaşınız, hangi e-postaları açmaktan veya içindeki linki tıklamaktan kaçınması gerektiğini bilmeyen teyzeniz, banka hesabını kafede Wi-Fi'ye bağlanarak kontrol eden iş arkadaşınız) ile paylaşın. Güvenlik bilginizi başkalarıyla paylaşarak onların da güvende kalmasını sağlayın.

18. Dikkatli olun. İş yerinizin girişinde size bedava dağıtılan bir USB cihazı veya banka hesabınızın ele geçirildiğini iddia eden bir telefon araması veya bilgisayarınızın ekranında "hemen tıkla ve güncelle" diye çıkan bir uyarı. Kabul etme yolunu izlemeden önce iki kez düşünün. Sorular sorun, kendi bağımsız araştırmanızı yapın ve size doğru gelmiyorsa, sizin için şüpheli bir durumsa hayır demekten korkmayın.

19. Yazılımınızı güncelleyin. Kurumda bizler kurum bilgisayarlarınızdaki işletim sistemlerinin güncelliğini takip ediyoruz, ancak evde de atabileceğiniz bazı adımlar var. Kişisel bilgisayarınızda kullandığınız tüm yazılımların düzenli olarak güncellendiğinden emin olun. Otomatik güncellemeleriniz etkin olsa bile, her şeyin düzgün bir şekilde çalıştığından emin olmak için kontrol edin. IP kameralar, akıllı tv ve akıllı ev teknolojisine yönelik cihazlar gibi İnternet cihazlarının güncellemelerini kontrol ettiğinizden emin olun. İşlerin nasıl yürüdüğünden ne kadar çok anlarsanız o kadar güvende olursunuz.

20. Verilerinizi yedekleyin. Değerli fotoğraflarınızı, önemli belgelerinizi ve hassas bilgilerinizi kaybetmek veya siber suçluların bunları ele geçirmesini istemezsiniz. Verilerinizi sık sık ve birden fazla farklı ortamda yedekleyin. Kritik bilgileri veya fotoğraf gibi yeri doldurulamaz dosyaları cihazınızdan ayrı taşınabilir ortamlarda depolamak, fidye yazılım saldırısına kurban gittiğinizde bu verilerinizi kaybetmemenizi ve zarar görmemenizi sağlar.

21. E-posta hesaplarınızı kontrol edin. Çok eskiden açtığınız Yahoo e-posta hesabını uzun süredir kullanmıyor ve de varlığını unutmuş olabilirsiniz; ancak bir siber saldırgan bu hesabınızı ele geçirip ailenizden, arkadaşlarınızdan ve diğer kişilerinizden bilgi almaya çalışmak için e-posta hesabınızı ve sizin adınızı kullanabilir. E-posta hesaplarınızı gözden geçirin, artık kullanmadığınız hesapları silin ve tutmak istediğiniz hesaplar için sıkı güvenlik önlemlerini ayarlayın.

22. Hesap aktivitelerini izleyin. Sosyal medya ve bankacılık gibi hesaplarınızın hareket kayıtlarını düzenli olarak kontrol edin. Sizin bilginiz dışında gerçekleşen bir hareket tespit ettiğinizde işlemin sonlandırılması veya iptali için gerekli işlemleri hızlıca yapın.

23. Şüpheli kaynaklardan gelen bağlantılara tıklamayın. Kısa e-postaları, kısa telefon görüşmelerini ve kısa videoları seviyoruz; ancak bilinmeyen veya şüpheli kaynaklardan gelen kısa isimli bağlantıları tıklamıyoruz. Siber saldırganlar bunları bir bağlantının gerçek adını maskelemek için kullanabilir ve sizin o linke tıklamanız cihazınızda bir zararlı yazılım enfeksiyonu ile sonuçlanabilir.

24. Bir can yeleğiniz olsun. E-posta adresinizi, telefon numaranızı değiştirdiyseniz, e-posta ve hesap kurtarma seçenekleriniz güncel olmayabilir. Bu, kendi hesaplarınıza erişememe olasılığınızı ve siber suçluların erişemediğiniz hesaplara girme olasılığını artırır. Hesaplarınızla ilişkili ikincil e-posta adreslerini, telefon numaralarını ve fiziksel adresleri kontrol edip güncelleyin.

25. Akıllı kart siz olun. İnternetten veya uygulamadan satın alma yaptığınızda "Ödeme bilgilerimi kaydet" seçeneğini tıklamanın sonraki işlemlerinizi ne kadar kolaylaştırdığını biliyoruz; ancak bunu yaparken çok dikkatli olun. Site https kullanıyor mu? Şirket kredi kartı bilgilerinizi nasıl koruduğunu açıklıyor mu? Uygulama düzenli olarak güvenlik güncellemeleri sağlıyor mu? Size güven vermiyorsa ve sürekli olarak kötüye kullanım olup olmadığını kontrol edemiyorsanız, kredi kartı bilgilerinizi kesinlikle kaydetmeyin.

26. Alternatif e-posta hesabı oluşturun. Haber bülteni abonelikleri, çekilişler, internetten alışveriş! İnternetten yapmak istediğiniz çoğu şey bir e-posta adresi gerektirir. Bunlar için kurumsal e-posta adresinizi kullanmak yerine, bültenlere abone olmak veya alışveriş sitesine kaydolmak için kişisel bir e-posta adresi oluşturun ve kesinlikle kurum e-posta adresinizi kullanmayın.

27. Şüpheci olun. Doğru olamayacak kadar çok iyi, çok ucuz, çok sansasyonel bir teklif geliyorsa ve çok acil sizden yanıt vermeniz bekleniyorsa muhtemelen şüpheci olmakta haklısınız. Siber suçlular her zaman hemen tıklamanıza, açmanıza, izin vermenize veya paylaşmanıza yardımcı olacak yollar arar. Ne

türden dolandırıcılıkların olduğunu bildiğinizden emin olun ve bilgilerinizi karşılığında size bir şey sunan biriyle paylaşmadan önce durun ve düşünün.

28. Yönetici haklarını vermeyin. Yeni bir yazılım veya yeni bir uygulama sisteminizde yönetici hakları edinmek istiyorsa, istediği erişim yetkileri hakkında bilgi edinin. Nedenleri için dokümanlara bakın ve eğer mümkünse uygulama/yazılım destek ekibiyle iletişim kurun. Her zaman hayır diyebileceğinizi unutmayın.

29. Konum servislerini her zaman açık tutmayın. Çoğu telefon ve bilgisayar, konum servisleri ile donatılmıştır. Her şeyde olduğu gibi bu hizmetlerin de ne sunduğunun farkında olun. İhtiyacınız yokken konum servislerini kapatın. Konum bilgilerinizin siber suçlular tarafından farklı amaçlar için kullanılabileceğini unutmayın.

30. Bağlantıyı kesin. Telefonunuzun, dizüstü bilgisayarınızın, evdeki modeminizin ihtiyacınız olmadığı zamanlarda İnternet bağlantısını kesin.

31. Bir güvenlik planı oluşturun. Siber güvenlik farkındalık ayı kapsamında öğrendiklerinizi düşünün ve yapılacaklar, yapılmaması gerekenler için bir kontrol listesi hazırlayın. Düzenli yedeklemeler ve güncellemeler için hatırlatıcılar oluşturun. Parolalar ile genel siber güvenlik için dikkat etmeniz gereken ipuçlarını not edin.

Siber güvenlik tümüyle tek bir kişinin veya bir birimin sorumluluğunda değildir. Herkes, kullandığımız internete bağlanabilen cihazların da dâhil olduğu siber uzayın bir parçası olarak siber güvenlikte sorumluluk sahibidir. Bireysel eylemlerimiz ortak bir etki oluşturur. Her birimiz birey olarak daha güçlü güvenlik alışkanlıkları edinir, kurum olarak farkındalığımızı artırırsak, hep birlikte siber saldırılara karşı daha dirençli ve daha güvenli bir kurum hâline geliriz.

KAYNAK