BEYAS 2019 SEMPOZYUMU
10-11 EKİM

‘EKİM’ SİBER GÜVENLİK FARKINDALIK AYI

Her yıl Ekim ayı **‘Siber Güvenlik Farkındalık Ayı’** olarak çeşitli etkinlikler düzenlenerek değerlendirilmektedir.

Siber güvenlik tümüyle tek bir kişinin veya bir birimin sorumluluğunda değildir. 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.”

“Çevrimiçi Güvenlik için Basit Adımlar”

1. **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. **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.
3. **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.
4. **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.
5. **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.
6. **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.
7. **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.
8. **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.
9. **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.
10. **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.

Ankara Üniversitesi
Bilgi İşlem Daire Başkalığı

Ankara Üniversitesi
Bilgi Yönetim Sistemleri Belgelendirme ve Bilgi Güvenliği Merkezi (BİL-BEM)