BİLGİ GÜVENLİĞİ FARKINDALIĞI

Bilgi güvenliği, bilgilerimizin yetkisiz erişim, değiştirme, kaybolma veya ifşa gibi risklere karşı korunmasını sağlar. Bu, kişisel ve kurumsal verilerin gizliliğini, bütünlüğünü ve erişilebilirliğini korumak için alınan önlemleri kapsar. Güçlü şifreler, iki faktörlü kimlik doğrulama, düzenli yedeklemeler ve siber güvenlik farkındalığı gibi adımlar, bilgi güvenliğini sağlamak için kritik öneme sahiptir. Bilgi güvenliği, hem bireyler hem de kurumlar için vazgeçilmez bir sorumluluktur.

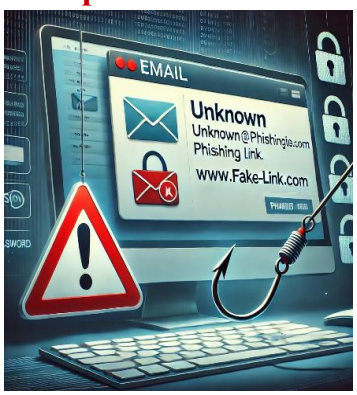
Unutmayın, siz de bu korumanın bir parçasısınız!

1. Güçlü Parola Kullanın: Güçlü şifre kullanımı, kişisel ve kurumsal verilerin güvenliği için kritik öneme sahiptir. En az 12 karakterden oluşan, büyük-küçük harf, rakam ve özel karakterler içeren karmaşık şifreler tercih edilmelidir. Şifrelerde doğum tarihi, isim, telefon numarası veya "123456", "password" gibi kolay tahmin edilebilen bilgiler kullanılmamalıdır. Her hesap için benzersiz şifreler oluşturulmalı ve belirli aralıklarla güncellenmelidir. Ayrıca, şifrelerin düzenli olarak değiştirilmesi ve aynı şifrenin farklı hesaplarda kullanılmaması, güvenlik açıklarını en aza indirmeye yardımcı olur.

Her hesap için farklı ve güçlü parola kullanın.

---

2. E-postalar Üzerinden Gelen Tehditler: E-posta üzerinden gelen tehditler, siber suçluların kişisel ve kurumsal verilere erişmek veya zarar vermek için kullandığı yaygın yöntemlerden biridir. Bu tehditler arasında phishing (oltalama) saldırıları, zararlı yazılım eklentileri, sahte bağlantılar ve kimlik avı gibi yöntemler bulunur. Örneğin, banka veya resmi kurumdan gelmiş gibi görünen sahte e-postalar, kişisel bilgilerinizi çalmaya yönelik olabilir. E-postalarla gelen ekler veya bağlantılar, bilgisayarınıza zararlı yazılım bulaştırabilir. Bu tür tehditlere karşı dikkatli olunmalı; tanımadığınız göndericilerden gelen e-postalar açılmamalı, şüpheli bağlantılara tıklanmamalı ve ekler taramadan geçirilmeden indirilmemelidir.



Bilmediğiniz bağlantılara veya dosyalara tıklamayın.

---

3. Bilinmeyen USB Belleklere Veya Harici Cihazlara Güvenmeyin: USB bellekler veya harici cihazlar, siber güvenlik açısından büyük risk taşır. Bu tür cihazlar, zararlı yazılımları yaymak veya veri hırsızlığı amacıyla kullanılabilir. Örneğin, sokakta bulunan veya tanıdığınız/tanımadığınız birinden gelen USB bellekler, bilgisayarınıza bağlandığında otomatik olarak kötü amaçlı yazılım yükleyebilir veya kişisel verilerinizi çalabilir. Bu nedenle, kaynağını bilmediğiniz USB bellekleri veya harici cihazları asla bilgisayarınıza bağlamayın. Ayrıca, cihazlarınızda otomatik çalıştırma özelliğini devre dışı bırakarak ve güncel antivirüs yazılımları kullanarak bu tür tehditlere karşı ek koruma sağlayabilirsiniz.

Harici cihazlara karşı dikkatli olun, antivirüs taramasından geçirmeden kullanmayın.

---

4. Resmi Uygulama Kanallarını Kullanın: Resmi uygulama kanallarını kullanmak, cihazlarınızın ve kişisel verilerinizin güvenliği için büyük önem taşır. Google Play Store, Apple App Store veya uygulamanın resmi web sitesi gibi güvenilir kaynaklardan uygulama indirerek, kötü amaçlı yazılımlara veya sahte uygulamalara karşı korunabilirsiniz. Üçüncü taraf kaynaklardan indirilen uygulamalar, cihazınıza zararlı yazılım bulaştırabilir, kişisel verilerinizi çalabilir veya cihazınızın güvenliğini tehlikeye atabilir. Bu nedenle, yalnızca resmi kanallardan uygulama indirin, uygulama izinlerini dikkatlice inceleyin ve güncellemeleri düzenli olarak yaparak güvenliğinizi artırın. Güvenliğiniz için resmi kaynaklara sadık kalın!

Kaynağından emin olmadığınız uygulamaları yüklemeyiniz.

---

5. Sosyal Mühendislik Saldırılarına Karşı Dikkatli Olun: Sosyal mühendislik saldırıları, siber suçluların insan psikolojisini kullanarak kişisel bilgilerinizi veya hassas verilerinizi ele geçirmeye yönelik yöntemlerdir. Bu saldırılar, sahte e-postalar, telefon çağrıları, sosyal medya mesajları veya fiziksel erişim yoluyla gerçekleşebilir. Örneğin, sizi acil bir durum veya ödül vaadiyle kandırarak şifrelerinizi, banka bilgilerinizi veya diğer kritik verilerinizi paylaşmanız istenebilir. Sosyal mühendislik saldırılarına karşı dikkatli olun; tanımadığınız kişilerden gelen talep ve mesajlara güvenmeyin, kişisel bilgilerinizi paylaşmadan önce kaynağı doğrulayın ve şüpheli durumlarda yetkililere başvurun.

Unutmayın, güvenlik her zaman önceliğiniz olmalıdır!
