GÜVENLİ İNTERNET İÇİN DİKKAT EDİLMESİ GEREKENLER

HAZIRLAYAN=Hatice Filiz CAMADAN

1. KİŞİSEL BİLGİLERİNİZİ PROFESYONEL VE SINIRLI TUTUN

- **Potansiyel işverenlerin veya müşterilerin kişisel ilişki durumunuzu veya evinizin adresini bilmeleri gerekmez. Uzmanlık alanınızı, profesyonel geçmişinizi ve sizinle nasıl iletişim kurabileceklerini bilmeleri gerekir. Son derece kişisel bilgilerinizi yabancılarla paylaşmaz, internette milyonlarca insanla paylaşmazsınız.**

eSafety Label
for a safer school

2. GİZLİLİK AYARLARINIZI AÇIK TUTUN

- **Pazarlamacılar sizinle ilgili her şeyi bilmek ister. Korsanlar da öyle... İkisi de göz atma geçmişinizden ve sosyal medya kullanımınızdan çok şey öğrenir. Ancak bilgilerinizin sorumluluğunu üstlenebilirsiniz. Hem web tarayıcılarının hem de mobil işletim sistemlerinin internette gizliliğinizi koruyabilecek ayarları vardır. Facebook, instagram gibi önemli web sitelerinin de gizliliği iyileştiren ayarları vardır. Şirketler pazarlama değeri nedeniyle kişisel bilgilerinizi istediği için bu ayarların bulunması bazen (kasten) zordur. Bu gizlilik korumalarını etkinleştirdiğinizden emin olun ve bunları etkin tutun.**

3. İNTERNETTE GÜVENLİ ŞEKİLDE GEZİNİN

- Tehlikeli bir mahalleden geçmeyi tercih etmediğiniz gibi internette de tehlikeli yerleri ziyaret etmeyin. Siber suçlular heyecan verici içerikleri yem olarak kullanır. Şüpheli içerikler bazen insanları cezbeder ve bunları ararken gardlarını düşürebilirler. İnternet dünyası görülmesi zor tuzaklarla doludur. Dikkatsizce tek bir tıklama, kişisel verilerinizi ifşa edebilir veya cihazınıza kötü amaçlı yazılımlarla virüs bulaştırabilir. Dürtülerinize direnerek korsanlara şans bile vermezsiniz.

4. İNTERNET BAĞLANTİNİZİN GÜVENLİ OLDUĞUNDAN EMİN OLUN

- **Kamusal bir alanda internete girerken, örneğin herkese açık bir Wi-Fi bağlantısı kullanırken güvenlik konusunda kontrolünüz sıfırdır. Kurumsal siber güvenlik uzmanları, özel bir ağın dış dünyaya bağlandığı "uç noktalar" konusunda şüphe duyarlar. Sizin savunmasız uç noktanız ise yerel internet bağlantınızdır. Cihazınızın güvenli olduğundan emin olun ve şüphe duyduğunuzda banka hesabı numaranız gibi bilgileri paylaşmadan önce daha iyi bir zamanı bekleyin (ör. güvenli bir Wi-Fi ağına bağlanana kadar).**

5. Ne İndirdiğinize Dikkat Edin

- **Siber suçluların temel hedeflerinden biri, sizi kandırarak kötü amaçlı yazılım taşıyan programları veya uygulamaları indirmenizi sağlamak veya bilgilerinizi çalmaktır. Bu kötü amaçlı yazılımlar bir uygulama kılığına girebilir. Popüler bir oyundan trafiği veya hava durumunu kontrol eden başka uygulamaya kadar her şey olabilir, şüpheli görünen veya güvenmediğiniz bir siteden uygulamaları indirmeyin.**

6. GÜÇLÜ PAROLALAR SEÇİN

- **Parolalar tüm internet güvenliği yapısındaki en büyük zayıf noktalardan biridir. Ancak şu anda bunlardan kaçınmanın bir yolu yoktur. Parolalarla ilgili sorun, insanların hatırlaması kolay, dolayısıyla siber hırsızların da tahmin etmesi kolay parolaları ("parola" ve "123456" gibi) tercih etmeye meyilli olmalarıdır. Siber suçluların çözmeleri daha zor olan güçlü parolaları seçin. Parola yöneticisi yazılımı, unutmamanız için birden fazla parolayı yönetmenize yardımcı olabilir. Güçlü bir parola, benzersiz ve karmaşıktır. En az 15 karakter uzunluğundadır, harfler, sayılar ve özel karakterlerin karışımını içerir.**

7. ÇEVRİMİÇİ SATIN ALMA İŞLEMLERİNİ GÜVENLİ SİTELERDEN YAPIN

- **İnternette satın alma işlemi yaptığınız her defasında kredi kartı veya banka hesap bilgilerinizi paylaşmanız gerekir. Siber suçluların ele geçirmeyi en çok istedikleri bilgiler bunlardır. Bu bilgileri yalnızca güvenli ve şifreli bağlantısı olan sitelerle paylaşın.**
- ***http:* yerine *https:***
- **(S harfi *secure* (güvenli) anlamına gelir) ile başlayan adreslere bakarak güvenli siteleri tespit edebilirsiniz. Adres çubuğunun yanındaki asma kilit simgesi de bunu gösterir.**

8. NE PAYLAŞTIĞINIZA DİKKAT EDİN

- **New Hampshire'daki genç adayın da öğrendiği gibi, internette sil tuşu yoktur. İnternette paylaştığınız her yorum veya fotoğraf sonsuza kadar internette kalabilir. Çünkü orijinali (mesela Twitter'dan) kaldırmak, diğer insanların aldıkları kopyaları kaldırmaz. Keşke yapmasaydım dediğiniz bir yorumu "geri almanızın" veya bir partide çektiğiniz utanç verici selfie'den kurtulmanın bir yolu yoktur. Annenizin veya gelecekteki işvereninizin görmesini istemediğiniz hiçbir şeyi internette yayınlamayın.**

9. İNTERNETTE KİMLE TANIŞTIĞINIZA DİKKAT EDİN

- İnternette tanıştığınız kişiler her zaman söyledikleri kişiler değildir. Hatta gerçek bile olmayabilirler.Sahte sosyal medya profilleri, korsanların tedbirsiz web kullanıcılarıyla samimi olup siber ceplerini seçmek için kullandıkları popüler bir yoldur. İnternetteki sosyal yaşamınızda, kişisel sosyal yaşamınızda olduğu gibi dikkatli ve mantıklı olun.

10. ANTİVİRÜS PROGRAMINIZI GÜNCEL TUTUN

- İnternet güvenliği yazılımı her tehdide karşı koruma sağlayamaz ancak çoğu kötü amaçlı yazılımı algılayıp kaldırır. Tabii güncelliğinden emin olursanız. İşletim sisteminizi ve kullandığınız uygulamaları güncel tuttuğunuzdan emin olun. Bunlar önemli bir güvenlik katmanı sunar.
- Bu 10 temel internet güvenliği kuralını aklınızda tutun ve internette tedbirsizleri pusuda bekleyen kötü sürprizlerin çoğundan kaçının.

FENERBAHÇE ANADOLU LİSESİ 5 ŞUBAT'TA GÜVENLİ İNTERNET KULLANIMI İLE İLGİLİ ÖĞRENCİLERİ BİLGİLENDİRDİ.