Bilinçli ve Güvenli internet Kullanımı

Web güvenliğine öncelikle web tarayıcınızın güvenliğiyle başlamak doğru olacaktır. Bunun için hangi web tarayıcısını kullanıyorsanız kullanın tarayıcı gizlilik ve güvenlik ayarlarını yapmakla başlamalısınız.

İzleme seçeneği, web sitelerinin sizin web platformunda dolaştığınız mecraların tarayıcı aracılığıyla takibinin yapılmasına olanak tanıyan bir seçenektir. Geçmişi hatırlama seçeneklerinde ise geçmişinizin asla hatırlanmamasını veya özel ayarların kullanılmasını tavsiye ederiz.

Özel ayarları yaptığınız takdirde çerez yönetimi karşınıza çıkacaktır. Çerez, herhangi bir internet sitesi tarafından bilgisayarınıza bırakılan bir hatırlama dosyasıdır. Çerez dosyalarında oturum bilgileri ve benzeri veriler saklanır. Burada; güvendiğiniz sitelere, örneğin otomatik olarak oturum açmasına olanak sağlamak üzere, sürekli çerez bırakma yetkisi verebilirsiniz. Hiçbir sitenin bilgisayarınıza çerez bırakmasını istemiyorsanız bu seçeneği işaretlemeyin. Yalnız, kimi sitelerin çerezler devre dışıyken düzgün işlemeyeceğini de unutmayın. Bununla birlikte, bir siteyi ziyaret ederken başka bir site tarafından bırakılan "üçüncü kişilere ait çerezler" ya da "yabancı çerezler"i kapalı tutmanızı öneririz.

Ayarlara Internet Explorer'da Araçlar-İnternet Seçenekleri'nden ve Google Chrome için Chrome menüsü (sağ üstte yer alan 3 noktadan ulaşılıyor) - Ayarlar - (Gelişmiş) Gizlilik bölümünden ulaşabilirsiniz.

Tarayıcı ayarlarını kendi bilgisayarınızdan ve/veya tanımadığınız bir bilgisayardan internete bağlanırken yaptıktan sonra internette gezinmeye başlayabiliriz.
İnternet sitelerinde gezinti yaparken bilgisayarımıza virüs ve tehlikeli yazılım bulaştırma ihtimali yüksek olan siteler genellikle şunlardır:

1. Çok fazla bilinmeyen siteler,
2. Bahis siteleri,
3. Pornografik siteler,
4. Korsan yazılım indirilen siteler.

Birçok web sitesi çeşitli tuzaklar barındırıyor olabilir. Bu yüzden güvendiğiniz, bildiğiniz web sayfalarını tercih etmeniz, bilmediğiniz web sayfalarının hakkında/iletişim gibi bölümlerinden web sayfaları hakkında bilgi edinmemiz gerekmektedir.

Ayrıca sık kullandığımız web siteleri için tarayıcımızda sık kullanılanlar listesi oluşturmanız, tuzak sitelerden korunmak adına önem teşkil etmektedir. Bunun için web güvenliğinde öncelikli olarak:

- Tuzak web sitelerine dikkat etmek ve güvenilmeyen web sitelerini ziyaret etmemek,
- E-posta mesajları ile gönderilen bağlantılara dikkat etmek,
- Sık kullanılanlar listesi oluşturmak,

Web sitelerinde gezerken yayılabilen zararlı programlardan korunmak için açılır pencere engelleyicisi kullanmak.
Arama motorlarını kullanırken özellikle çocuklu ailelerin yüksek düzeyli filtreleme araçları sayesinde özellikle müstehcen sitelerin arama sonuçlarında engellenmesini ve bu sayede güvenli arama sağlamaları gerekmektedir.

GAZİANTEP LİSESİ REHBERLİK VE PSİKOLOJİK DANIŞMANLIK SERVİSİ ÖĞRENCİ BİLGİLENDİRME BROŞÜRÜ

İnternet Güvenli mi?

İnternet kullanıcısı kendi üzerine düşen sorumlulukları yerine getirirse, interneti belli bir düzeyde güvenli hale getirebilir. Peki, nedir bu sorumluluklar:

- Antivirüs ve firewall programı kullanmak, İşletim Sistemimizi güncel tutmak,
- Neyi nerede aradığımıza dikkat etmek,
- Kablosuz ağımızın şifresini paylaşmamak ve herkese açık şekilde bırakmamak, şifre güvenliğine dikkat etmek,
- İnternet üzerinden alışveriş yapıyorsak sanal kredi kartı kullanmayı tercih etmek,
- Şüpheli linkleri ve e-mailleri açmamak, tıklamamak, Phishing tuzağına düşmemek

- Çok kişinin kullandığı bilgisayarda, bankacılık işlemlerini zorunlu olmadıkça yapmamak, İnternet Bankacılığı ve çevrimiçi alışverişte dikkatli olmak
- Üyelik istenen sitelerde kişisel bilgilerin tamamını vermemek, Kimlik Hırsızlığı ve Dolandırıcılığa maruz kalmamak
- Sosyal paylaşım sitelerinde kişisel gizlilik, mahremiyet ve paylaşım konularında ölçüler ve sınırlar belirlemek, Sosyal Ağ Güvenliğine dikkate etmek

"Bilinçli İnternet Kullanımı" Nedir?

Çoğu kez dillere pelesenk olan söylemler derinlemesine düşünülmez. İnternette bilmeden, başını-sonunu hesap etmeden yapılan şeylerden genellikle zarar görülür. Denilebilir ki bilince giden yol; öğrenmekten, düşünmekten, sorgulamaktan ve farkında olmaktan geçer.

- İnternet teknolojilerini kullanırken aynı zamanda kendimizi ve içinde bulunduğumuz durumları sorgulayabiliyor muyuz?
- İnternette sergilediğimiz davranışların kendimize, ailemize ve diğer kullanıcılara yansımalarının ne olacağını biliyor muyuz?
- İnterneti doğru ve ahlaki davranışlar çerçevesinde mi yoksa kötüye mi kullanıyoruz?

Bilinçli bir internet kullanımı noktasında bütün bu soruların cevaplarını düşünmek yol gösterici olacaktır.

Akıllı telefonunuza indirdiğiniz ve oynamak için sabırsızlandığınız bir oyun bile küçük bir pop-up ile sizin rızanızı basit bir onaylama yöntemi ile aldıktan sonra siz oyunu oynarken rehberinizdeki kontakları kendi veri tabanına aktarabilmekte ve sonrasında da bunları ne iş yaptığını bilmediğiniz şirketlerle paylaşabilmektedir. Bu bağlamda, uzun zamandır devletler ve ilgili sektör paydaşları veri paylaşımında kullanıcının kontrolünü arttıracak teknik çözümler üretmeye çalışırlarken öte yandan internet kullanıcılarının da dikkat etmesi gereken birtakım noktalar bulunmaktadır.

Bunun için;

1. İnternet web tarayıcınızın 'do not track (izlememe)' seçeneğini aktif hale getirmenizi öneririz. Konu ile ilgili daha detaylı bilgiye web güvenliği bölümünden ulaşabilirsiniz.
2. İşlem yapmak istediğiniz web sayfalarının kullanım politikası ve gizlilik sözleşmelerini okuyunuz. Ayrıca ilgili sayfanın iletişim, hakkımızda bölümlerinden sayfa hakkında bilgi alınız.
3. Mobil platformlardan indirdiğiniz uygulamaların sizlerden ne gibi bilgiler toplandığını hususunu iyi analiz ediniz. Gerekirse çok fazla kullanmayacağınız uygulamaları telefonunuza indirmeyiniz.
4. İndirdiğiniz mobil uygulamaların nelerle senkronize olduğuna dikkat edin. Senkronize olmasını istemediğiniz bilgileri devre dışı bırakın. Bunun için telefon ayarlarınızdan hesaplarınızı, uygulama yönetiminizi, konum servislerinizi ve güvenliğinizi tekrar gözden geçirmenizi tavsiye ederiz.
5. Sosyal ağlarda gizlilik ve güvenlik ayarlarınızı tekrar gözden geçirin. Bunun için sosyal ağlarda güvenlik bölümünü okumanızı tavsiye ederiz.

Ayrıca, Trend Micro Güvenlik Araştırmalarından Sorumlu Başkan Yardımcısı Rik Ferguson, kullanıcıların Facebook'ta dikkat etmesi gereken 5 maddeyi şu şekilde sıralamaktadır:

Facebook'ta Dikkat Etmeniz Gereken 5 Husus

1. Eğer bir arkadaşınızın duvarında paylaştığınız mesajın gizlilik ayarlarını kontrol etmezseniz, otomatik olarak "arkadaşınızın arkadaşları" mesajınızı görebilecek şekilde ayarlanır.
2. Paylaştıklarınızın istemediğiniz kişiler tarafından görülmesinin önüne geçmek için gizlilik ayarlarını yapmanız da yeterli olmuyor. Eğer sizin paylaştığınız şeyin altına herhangi bir Facebook kullanıcısı etiketlenirse, bu kişi tüm konuşmaları ve paylaşımınızı görüyor.
3. Kamuya açık bir etkinlik ya da sayfada bir paylaşımda bulunduğunuzda, bu paylaşımın gizlilik ayarlarını değiştiremezsiniz. Sadece o paylaşımı kendi profilinizden kaldırabilirsiniz.
4. Gizlilik ayarları "Arkadaşlarımın arkadaşı" olarak belirlenmiş bir paylaşımı arkadaşınızın duvarına yerleştirdiğinizde, "İstemediğiniz" kişiler de o paylaşımı görecektir. Çünkü onlar sizin arkadaşınız.
5. Paylaştıklarınız herkese açık olsun ya da sadece arkadaşlarınızın arkadaşları görebilsin. Tanımadığınız birçok insanın sizi gördüğünü ve arkadaşlıktan çıkardığınız kişilerin dahi sizi takip edebildiğini unutmayın. Bu sebeple paylaşımlarınıza her zaman dikkat edin.