Günümüzde internette; iletişim kurma, bilgiye ulaşma, eğlence, bankacılık, alışveriş yapma ve diğer pek çok şeyi yapabilme şansına sahibiz. Hayatımızı bir çok yönüyle kolaylaştıran bir konumda artık internet dünyası. Özellikle içinde bulunduğumuz şu zor dönemde sanal dünyada çok vakit geçirir olduk. Fakat suçlar, suçlular, dolandırıcılar, istismarcılar, **siber zorbalar**, tacizciler, teşhirciler v.s gibi karanlık bir tarafı da var malesef bu dünyanın....

Teknoloji hızla gelişirken, sanal alemin bu karanlık tarafında olanların sayısı da her geçen gün katlanarak artıyor. İnternetin insanlığa sunduğu kolaylıklar ve fırsatlar inkâr edilemez elbette ama, bizden alıp götürdükleri de yadsınamayacak kadar çok. (yıkılan aileler, kaybolan hayatlar, kültürel yozlaşma, boşa harcanan zaman, sağlığın elden gitmesi, bağımlı olmak, v.s) Dolayısıyla bu noktada "**İnternet Güvenliği**", "**İnternetin Bilinçli Kullanımı**", "**İnternetin Etik Kullanımı**", "**İnternet Hak-Hukuk ve Sorumlulukları**" konusunun ne kadar önemli olduğu da ortaya çıkmış oluyor.

Gerekli tedbirler alınmadığı takdirde internetin güvenli olduğunu söylemek doğru değildir! Hiç kimse internet ortamında %100 güvenlik garantisi veremez. İnternet kullanıcısı; kendi üzerine düşen sorumlulukları yerine getirirse, interneti belli bir düzeyde güvenli hale getirebilir.

İnternet Neden Güvenli Bir Yer Olmak Zorunda?

Çünkü sanal dünya aynı zamanda; çocuk istismarcılarının, uyuşturucu ve kumar bataklığının, sözde sağlık ürünleri simsarlarının, sapkın inanışların, terör propagandalarının, müstehcenliğin ve gençlerimizi kötü yola sürükleyen fuhuş tehlikesinin yuvalandığı bir çukurdur ve tedbir alınmazsa bu tehlikeler bütün bir toplumu tehdit etmeye ve çoğalmaya devam edecektir.

Bu sebeple öncelikle çocukların ve gençlerin; sonra da bütün bir toplumun internetten gelebilecek zararlardan korunması için internetin bilinçli kullanılması şarttır. Ayrıca bilinçli kullanım güvenliği de otomatik olarak beraberinde getirecektir.

İNTERNET ORTAMINDA KİŞİSEL VERİLERİN KORUNMASI

Dünyada ve ülkemizde giderek artan internet kullanımı, birçok kolaylığı beraberinde getirirken kişisel verilerin korunması konusunu da daha önemli hale getirmiştir. İnternet kullanan bireylerin %82,4'ünün sosyal medya kullanıcısı olduğu günümüzde, yapılan her paylaşım, internet ortamına girilen her veri; size ve bilgilerinize ulaşmak isteyen kötü niyetli kişiler tarafından kullanılabilmektedir.

Kişisel veriler, kişinin kimlik yapısını ortaya koyan ve kişiye özel bilgiler olarak tanımlanabilir. Kişisel veri kavramının sadece ad, soyad, doğum yeri, doğum tarihi gibi bilgilerden oluşmadığı ayrıca kişilerin fiziksel, sosyal, kültürel, ekonomik, psikolojik tüm bilgileri kapsadığı ifade edilmiştir. Bu kapsamda kişinin kimlik bilgilerine ek olarak, vatandaşlık numarası, vergi numarası, pasaport numarası, sosyal güvenlik numarası, sürücü belgesi numarası, taşıt plakası, ev adresi, iş adresi, e-posta adresi, telefon numarası, faks numarası, özgeçmişi, fotoğrafı, videosu, genetik bilgileri, kan grubu, kriminal geçmişi ve adli sicil bilgileri gibi kişinin belirli veya belirlenebilir olmasını sağlayan tüm bilgiler de kişisel veri sayılabilmektedir.

Bugün sosyal ağlarda birçok kullanıcı kendini tanımlayıcı ve tasvir edici resim, video ve çeşitli diğer görsel ve işitsel araçları çok rahatlıkla paylaşabilmektedir. Bu bilgilerden çok rahatlıkla diğer kişisel veriler de üçüncü şahıslar tarafından oluşturulabilmektedir. Kişisel verilerin korunmasında yasaların ve uluslararası sözleşmelerin getirmiş olduğu birtakım uygulama ve yaptırımlar olsa da **temel gizlilik ve güvenlik kişinin kendisinde başlamaktadır.** Bu güvenlik ve gizliliğe de özellikle internet alanında daha çok dikkat edilmesi gerekmektedir. Özellikle sosyal paylaşım ağları kötü niyetli kişilerin bilgilerinize ulaşabileceği en kestirme yoldur. Paylaşım yapmadan önce, yapacağınız paylaşımın ne gibi sonuçlar ve riskler doğurabileceğini detaylı bir şekilde düşünmeniz gerekir.

BİLİNÇLİ İNTERNET KULLANIMI VE KİŞİSEL VERİLERİN KORUNMASI İÇİN İNTERNET KULLANICILARININ YAPMASI GEREKENLER NELERDİR?

- İnternette ve sosyal ağlarda kendinizi tasvir edici, betimleyici bilgiler paylaşmayınız. Çok fazla konum bilgisi, adres ve diğer iletişim bilgilerinizi vermeyiniz. Kiminle tanıştığınıza ve ne yazdığınıza dikkat ediniz.

- Bilinen ve güvenli sitelerden işlem (alışveriş, iletişim, ticaret, dosya indirme vs.) yapınız.
- Gördüğünüz her linke tıklamayınız. Başka bir internet sayfası üzerinden, arama motoru ya da e-posta ile gelen linklerden değil, doğrudan internet adresi yazılarak işlem yapmak istediğiniz sitelere bağlanınız. Bunun için web tarayıcınızda sık kullanılanlar oluşturunuz. İnternetten ne indirdiğinize de dikkat ediniz.
- İnternet kafe ve alışveriş merkezleri gibi internetin ortak kullanıldığı alanlar yerine kendi bilgisayarlarınızdan işlemler yapınız. Bu gibi yerlerdeki interneti sadece bilgi alma ve eğlence gibi temel amaçlar için kullanınız.
- İşlem yaptığınız (alışveriş, iletişim, ticaret, dosya indirme vs.) web sitelerin https bağlantısına sahip olduğunu ve geçerli bir sertifikasının olduğunu kontrol ediniz.
- İnternetten yaptığınız ödemeleri mutlaka kredi kartı ekstrenizden kontrol ediniz. Bunun için sanal kredi kartı veya sanal limit oluşturunuz. Bilgisayarınızda da sanal klavye kullanınız.
- Gerek internette işlem yaptığınız sayfalarda gerek bilgisayarınızda tahmin edilmesi güç şifreler belirleyiniz ve bu şifreleri belirli periyotlarla değiştiriniz.
- Lisanssız yazılımlar kullanmayınız, işletim sisteminizi güncel tutunuz ve anti-virüs yazılımlar kullanınız.
- Dışarıdan (harici bellekler) veya internetten bilgisayarınıza yüklediğiniz dosyaları virüs ve casus yazılım taramalarından geçiriniz.
- Telefon veya internetten sosyal ağlar aracılığı telefon numarası isteği, hediye çeki arzı, para isteği gibi tuzaklara düşmeyiniz. Hatta bu istek arkadaşınızdan veya polisten gelmiş olsa bile arkadaşınızın hesabı büyük bir ihtimalle ele geçirilmiş veya kendini polis gibi göstermeye çalışan kişilerin tuzağına düşürülmeye çalışıyorsunuz demektir. Böylesi bir durumda savcılık ve polis kanallarını kullanınız.
- Akıllı cep telefonlarınıza işinize çok yaramayan ve birçok bilginize kolayla erişebilen uygulamaları yüklemeyiniz. Uygulama marketlerinin izin vermediği uygulamaları kullanmayınız ve telefonunuza bir ekran kilidi belirleyiniz.

Aşağıdaki linklere tıklayarak da bilgi edinebilirsiniz.

http://www.resmigazete.gov.tr/eskiler/2016/04/20160407-8.pdf

meb_iys_dosyalar/39/05/965162/dosyalar/2020_11/20101853_Guvenli_Ynternet_KullanYmY.pdf

meb_iys_dosyalar/39/05/965162/dosyalar/2020_11/20101853_Lise_OYrenci_Ynterneti_NasYl_KullanmalYyYm.pdf

meb_iys_dosyalar/39/05/965162/dosyalar/2020_11/20101853_CocuklarYmYz_icin_Bilincli_Ynternet_KullanYmY.pdf

meb_iys_dosyalar/39/05/965162/dosyalar/2020_11/20101853_Siber_ZorbalYk.pdf