Bilgisayar güvenliği 2

Geçtiğimiz sayıda bilgisayar virüsleri ve güvenlik önlemlerine değinilmişti. Bu sayımızda da bilgisayar güvenliğine ilişkin bilgiler verilecektir. Her geçen gün bilgisayar teknolojilerinin daha fazla hayatımıza girdiği şu günlerde bilişim alanında ihmal edilen en önemli konuların başında bilgisayar güvenliği ve internet güvenliği gelmektedir.

Bilgisayar güvenliği, bilgisayar kullanımıyla ortaya çıkabilecek risklerin kontrol edilmesiyle ilgilenen bilgisayar bilimi alanıdır. Ne yazık ki bilgisayarların bilinçsiz ve dikkatsiz kullanımı maddi ve manevi zararlarla sonuçlanabilir. Bu zararlardan kaçınmak için bazı temel konuları bilmek ve bazı güvenlik önlemlerini almak gerekir.

Bilgisayar kullanımından kaynaklanabilecek riskler, çeşitli şekillerde ortaya çıkar. Çalıştırdığımız programlarda bulunması muhtemel açık/hatalar, bunlara yerleştirilmiş olabilecek arka kapılar, zarar verme amacıyla yazılmış virüs ve benzeri programlar, kötü niyetli kişilerin yapabileceği direk ve dolaylı saldırılar, aldatmaca girişimleri ve kullanıcı hataları bunlara örnektir.

Bilgisayarınızı Koruyun

En kolay yol bir dosyanın içine virüs programı saklamaktır. İçinde virüs bulunan dosya bilgisayara kopyalandığında (veya e-mail ekinden açıldığında) ve çalıştırıldığında, virüs kullanılan bilgisayara bulaşmış olur. Virüsler genellikle uygulama (.exe) dosyalarında saklanabilmektedir. Ancak, macro virüsü ofis programlarının içinde de saklanabilir. (.doc, .xls ve .ppt dosyaları). İki virüs tipi de kullanılan sisteme zarar verebilir veya bilgisayardaki ya da ofis ağındaki gizli bilgilerin kopyalanmasına neden olabilir. Bilgisayarınızı korumak için;

- Antivirüs programı kullanın.
- %100 güvenilmeyen sitelerden program indirmeyin.,
- Tanınmayan kişi veya kurumlardan gelen elektronik postalarda ekli olan dosyaları açmayın.
- Bilgisayarda kullanılacak CD ve disketleri virüs taramasından geçirin.
- İnternetten gelebilecek saldırılara ve güvenlik açıklarına karşı güvenlik duvarı kullanın.
- İşletim sisteminin açıkları ile ilgili yamaları yükleyin.
- İşletim sistemi güncellemelerini düzenli yapın.
- Casus yazılımları tespit eden yazılımlar kullanın.

Kişisel Bilgilerinizin Korunması

Günümüzde internet kullanıcılarının %80 gibi bir kısmının artık olmazsa olmazlarından olan e-posta, anlık ileti v.b. internet bankacılığı, e-alışveriş gibi birçok kullanım alanları kötü niyetli internet kullanıcıları tarafından istismar edilmektedir. Kişisel bilgilerinizi korumak için;

- Kişisel bilgilerinizi hiçbir zaman e-posta, anlık ileti (MSN Messenger, ICQ v.b.) veya pop up içinde yazmayın.
- Bir ileti veya pop up içindeki bir linki, butonu tıklarken doğruluğundan emin olun.
- İşlemlerinizi online yaparken internet tarayıcınızın üst kısmında bulunan adres bölümünde bulunan adresin https:// olduğundan emin olun. **s** harfi bu sayfanın güvenli ve çeşitli şifreleme metotları ile işlem yaptığını belirtir.
- İnternet tarayıcınızın sağ alt kısmında kapalı kilit işareti olduğundan emin olun.
- İnternet adresi olarak sayısal rakamlar içeren adresler ile karşılaşırsanız kullanmadan önce mutlaka kontrol edin.
- E-posta ile gelen bildirimleri düzenli olarak gözden geçirin.
- İnternet şubesinden tam anlamıyla çıkış yapmadan bilgisayarın başından kalkmayın.
- Sanal alışveriş ortamları hariç, internet üzerinden kredi kartı numarası, şifre veya özlük bilgileri isteyen e-postalara kesinlikle bilgi vermeyin.
- Şifre ve parola işlemlerinde tıksız sanal klavye kullanın.
- Müşteri numarası, kullanıcı adı, şifre ve parolanızı hiç kimseye söylemeyin.
- Güvenlik tedbiri olarak belirli aralıklarla kullanılmakta olan kullanıcı adınızı, şifrenizi ve parolanızı değiştirin.
- İsim, doğum tarihi gibi kolay tahmin edilebilir kullanıcı adı veya parola kullanmayın.
- E-postalar ile yapılan yönlendirmeler yoluyla işlem yapılan sayfaya giriş yapmayın.
- PC güvenliği olmayan ortamlarda (özellikle internet cafe gibi yerlerde), şifre, kullanıcı adı gerektiren siteleri (internet bankacılığını) kullanmayın.
- Şifre ve kullanıcı adı ile giriş yapılan sitelerden belirtilen "Güvenli Çıkış" butonu ile çıkış yapın.

İstenmeyen e-postalardan (Spam Mail) Korunun

Kullanıcının isteği dışında gönderilen e-postalara spam adı verilmektedir. İstenmeyen e-postalardan

korunmak için;
• Outlook gibi daha güvenli bir elektronik mektup programı kullanın.
• Mektup gönderilecek kişi ve kişilerin adreslerini BCC(Gizli) kısmına yazın.
• Size gelen bir iletiyi bir başka kişiye iletirken (Forward) mektubun içersindeki **----orginal message---** başlığıyla başlayan satırları silin.
• Spam mailleri başkalarına göndermeyin.

Spyware ve Adware yazılımlardan Korunma

Bilgisayarınıza kurulan spyware yazılımı size ait bilgileri karşı tarafa aktarır ve her an karşınıza çıkan reklamları bilgisayarınıza indirir. Siz internet tarayıcınızı açtığınızda varsayılan sayfa olarak gelmesini istediğiniz sayfa ayarlarını değiştirir ve internet tarayıcınızı her açtığınızda istemediğiniz sayfa gelir. Spyware yazılımlardan korunmak için;
• Kuracağınız programların Adware taşımadığından emin olun.
• Adware ve spyware pop-up pencelerinden korunmak için sisteminize pop-up durdurucu program kurun.
• Zararsız gibi görünen bir linke tıkladığınızda açılan sayfaya güvenmiyorsanız "Yes" butonuna tıklamayın.
• Casus programları tespit eden program kullanın.

Ailenizi Koruyun

İnternette çocuklarınızı korumanın basit bir yolu yoktur! Gerçek dünyada olduğu gibi, çocukların tehlikeli veya uygunsuz içeriklerle karşılaşma olasılığını azaltmak için ebeveynlerin internet ortamında da önlem alması gerekmektedir. Çocuklarınızı korumak için;
• Ebeveyn denetimi olan bir güvenlik programı kullanın. Bu programla sayfa içeriklerini kontrol edebilir, web sayfalarını fitreleyebilir, silah, kumar, bahis, uyuşturucu içerikli sayfaların görüntülenmesini engelleyebilirsiniz.
• Bilgisayarı açık bir oda da monitörü dışarıdan görünecek şekilde yerleştirin. Bu durum da çocuğunuz bilgisayar başında iken internette olup biteni görmenizi ve kontrol etmenizi sağlayacaktır.
• Çocuklarınızı internetin artı ve eksileri hakkında eğitin.
• İnternet tarayıcısında bulunan bookmarklar çocukların dostu sitelerdir. Daha önceden kullanılmış bu sitelerin kullanımı ile ilgili çocuklarınıza izin verebilirsiniz.
• Çocuklarınızı kişisel bilgilerini asla internet üzerinden paylaşmamalarını öğretin.
• Çocuklarınıza sohbet odalarından sakınmalarını öğretin.
• Çocuklarınıza konuşmayı ve tartışmayı öğretin. Eğer çocuklarınız kötü bir deneyimle karşı karşıya kalırlarsa hemen bilgisayarlarını kapatacak ve sizinle bu durum hakkında konuşacaklardır.
• Çocuklarınızın online oturumlardan birileri ile görüşmelerine ve buluşmalarına izin vermeyin.
• Çocuklarınızın arkadaşlarını tanıyın.
• Çocuklara tanımadıkları kişilerden gelen e-mailleri asla açmamaları gerektiğini öğretin.
• Tanınmayan birinden gelen pornografik bir e-maile asla cevap vermemesi gerektiğini öğretin.

Bilgisayar Güvenliği ile İlgili Yararlı Tavsiyeler

1- "worm"ların birçoğu Microsoft Outlook ya da Outlook Express ile e-mail transferi yapan kullanıcılarıyla yayılmaktadır. Eğer Outlook kullanmanız gerekiyorsa, Microsoft'un sitesinden Outlook güvenlik güncellemesini yükleyip kurmalısınız. Ana satıcısından direkt güncelleme yaptığınız sürece sisteminizi koruyacağından emin olabilirsiniz.
2- E-mail alırken ve gönderirken e-mail eklentilerinden olabildiğince sakının.
3- Windows içeriği her zaman dosya uzantılarını gösterir. Windows 2000'de, tarayıcıdaki araçlar menüsünde; araçlar / klasör seçenekleri / görünüm bölümünde "bilinen dosya tipleri için dosya uzantılarının gizlenmesi" kısmı işaretlenmemelidir. Zararlı dosyaların (.exe ve .vbs) uzantıları çoğu zaman ".txt veya .jpg" olarak değiştirilmektedir.
4- Asla e-mail eklentileriyle gelen ve uzantıları ".VBS, .SHS, ya da .PIF" olan dosyaları açmayın. Bu uzantılar çoğunlukla normal eklentilerde kullanılmazlar ama sıklıkla virüslerde kullanılırlar.
5- Asla çift uzantılı eklentileri açmayın (NAME.BMP.EXE ya da NAME.TXT.VBS)
6- Gerekli olmadıkça diğer kullanıcılarla dosyalarınızı paylaşmayın. Eğer bunu yapmanız gerekiyorsa, paylaşımın sürücünüzün tamamı ya da Windows bileşenlerinizle olmamasından emin olun.
7- Bilgisayarınızı kullanmıyorsanız ve bir internet bağlantınız varsa ya bağlantıyı kesmeli ve modem kablonuzu çıkartmalı ya da bilgisayarınızı kapatmalısınız.
8- Eğer tanıdığınız bir arkadaşınızdan bir e-mail aldıysanız ve bu e-mail farklı bir dil ile yazılmışsa herhangi bir eklentiyi açmadan önce arkadaşınızın isminin yazdığı kısmı çift tıklayarak inceleyin.
9- Bir reklam e-maili ya da davetsiz bir e-mail alırsanız eklentilerini açmayın ve web linklerini kullanmayın.
10- Seks içerikli dosya isimleri olan eklentilerden sakının. E-mail wormları sık sık Porno.Exe ya da Pamela_Nude.Vbs ismine benzer eklentilerle karşınıza çıkarlar.
11- Ekli dosyaların ikonlarına güvenmeyin. Wormlar sık sık bilindik ikonların resimleri kullanılarak görünürler.
12- IRC, ICQ ya da AOL mesajlaşma sistemlerini kullanırken yabancılardan gelen eklentileri asla kabul etmeyin.
13- Haber gruplarından gelen dosyaları indirmekten ve yüklemekten sakının. Bu gruplar virüs oluşturanlar ve yeni virüslerini dağıtmak isteyenler tarafından sık sık kullanılırlar.

Kaynak

https://abonenet.e-kolay.net/fsecure/bilgisayar_guvenlik.asp