TEMEL GÜVENLİK PRENSİPLERİ

1- Bilgisayara Giriş Güvenliği Aşamaları

Bilgisayara giriş güvenliği, bilgisayarın içinde sakladığınız bilgilerin de güvenliği anlamına gelmektedir. Bu nedenle son derece önemlidir.

Bu konuda ilk adım fiziksel güvenliktir. Öncelikle bilgisayarınızın bulunduğu yerin güvenliği sağlanmalıdır. En çok karşılaşılan problemlerden birisinin dizüstü bilgisayarların çalınması olduğunu utmamak gerekir.

Bilgisayarınız açılırken kullanıcı adı ve parola sormuyorsa bilgisayarınızı bilgisayarınıza fiziksel olarak ulaşabilen herkes açabilir ve kişisel bilgilerinize erişebilir.

Fiziksel güvenliği sağladıktan sonra bilgisayarını "kullanıcı adı" ve "parola" ile açılmasını sağlamak gerekir.

Bu işlemi iki şekilde yapabilirsiniz:

- **Bilgisayarınızın her açılışta(BIOS) parola sormasını sağlayarak;**
- **Bilgisayarınızda kurulu olan işletim sisteminin açılışında parola sormasını sağlayarak.** Farklı işletim sistemlerinde farklı adımlar izlemek gerekebilir.

2- Parola Güvenliği Aşamaları

En önemli kişisel bilgilerden olan parola çok farklı yöntemlerle ele geçirilebilmekte ve zararımıza kullanılabilmektedir. Bu yüzden parola güvenliği son derece önemlidir.

Bu sebeple;

- Kolay tahmin edilemeyen (güçlü) parolalar kullanılmalı,
- Kullanılan parolalar korunmalı ve paylaşılmamalı,
- Ara sıra değiştirilmeli,
- Herhangi bir yerde yazılı bulundurulmamalı
- Anti-virüs programı güncel tutulmalıdır.

Parolalar genel olarak iki şekilde ele geçirilebilir.

a- Tahmin ederek ya da deneme yanılma yolu ile ele geçirilebilir.
b- Parolanızın çalınması ile yani hırsızlık yaparak ele geçirilebilir.

Parolamız başkası tarafından ele geçirilirse veya böyle bir şüphemiz varsa;

İlk işi olarak parolamızı değiştirilmeli sonrasında ise aynı parola ya da çok benzerleri başka sistemlerde de kullanılıyorsa, onları da değiştirilmelidir.

Bu durumdan etkilenebilecek diğer kişilere haber vermemiz olası başka problemleri önüne geçmemize yardımcı olacaktır.

Benzer problemleri tekrar yaşamamak için, yeni oluşturacağın parolalar, tahmin edilmesi zor, yani güçlü parolalar olmalıdır.

Oluşturulan bir parolanın "güçlü" kabul edilebilmesi için aşağıdaki özellikleri göstermelidir.

- **En az 8 karakterden oluşur.**
- **Harflerin yanı sıra, rakam ve "?, @, !, #, %, +, -, *, %" gibi özel karakterler içerir.**
- **Büyük ve küçük harfler bir arada kullanılır.**

Bu kurallara uygun parola oluştururken genelde yapılan hatalardan dolayı saldırganların ilk olarak denedikleri parolalar vardır. Bu nedenle parola oluştururken aşağıdaki önerileri de dikkate almak gerekir.

- Kişisel bilgiler gibi kolay tahmin edilebilecek bilgiler parola olarak kullanılmamalıdır. (Örneğin doğum tarihiniz, çocuğunuzun adı, soyadınız, ... gibi)
- Sözlükte bulunabilen kelimeler parola olarak kullanılmamalıdır.
- Çoğu kişinin kullanabildiği aynı veya çok benzer yöntem ile geliştirilmiş parolalar kullanılmamalıdır.

Parolanızı korumak için:

- Kağıt ya da elektronik, herhangi bir ortamda açıkça yazılmış olarak bulundurulmamalıdır. Yazılı bulundurulması gerektiğinde saklanan ortamın güvenliği sağlanmalı ve parolalar kilit altında saklanmalıdır.
- Farklı sistemlerde farklı parola kullanılması olası riskleri azaltacaktır.
- Parolalar belirli aralıklarla değiştirilmelidir.

Parolalar kişiye özeldir,

- Başkalarıyla paylaşılmaz. Herkesin parolası farklıdır.
- Ara sıra yenilemek gerekir.

3- E posta Güvenliği Aşamaları

Günlük hayatımızda haberleşme ve dosya transferi için çok sık kullandığımız e-postalar, dikkatli davranılmadığında kolayca insanlara zarar vermek, aldatmak ve bu yolla ekonomik çıkar elde etmek için kullanılıyor olabilirler.

Bu sebeple;

- E-posta adresleri herkese açık web sitelerinde paylaşılmamalı,
- Tanımadığınız kişilerden gelen her türlü e-postaya cevap verilmemeli,
- Kişisel ve mali bilgiler e-posta üzerinden hiç kimseyle paylaşılmamalı,
- E-posta içinde bulunabilecek bağlantılara tıklanılmamalı,
- İçeriği ne olursa olsun, başkalarına göndermeni isteyen e-postaları kimseye gönderilmemeli
- Güncel anti-virüs ve güvenlik duvarı yazılımları kullanılmalı.

4- İnternet Erişimi Güvenliği Aşamaları

İnternet yaşamımızı bir çok açıdan kolaylaştırsa da dikkatsiz kullanıldığı taktirde sorunlar yaşanmasına neden olabilir. Internet'te var olan tuzakları fark edebilmek ve hangi web sitesine güvenilebileceği, nasıl güvenli hareket edilebileceğine dikkat etmek önemlidir. Ayrıca;

- Özellikle internet ortamında, hassas bilgilerin paylaşımı güvenli iletişim yolları ile gerçekleştirilmelidir.
- Tuzak web sitelerine dikkat etmek ve güvenilmeyen web sitelerini ziyaret etmemek.
- E-posta mesajları ile gönderilen bağlantılara dikkat etmek
- Web sitelerinde gezerken yayılabilen zararlı programlardan korunmak için açılır pencere engelleyicisi kullanmak gereklidir.
- Bunların yanı sıra çocukların güvenliğini sağlamak anne babanın görevidir ve bu konuda alınabilecek tedbirler konusunda aileler hem kendilerini hem de çocuklarının bilinçli birer kullanıcı olmaları için özen göstermelidir.

5- Sosyal Medya Güvenliği Aşamaları

Bireylerin internet aracılığıyla bilişim teknolojilerini kullanarak birbirleriyle etkileşim sağlayan araç, hizmet ve sanal uygulamalara "Sosyal Medya denir".

Sosyal medya güvenliği için dikkat etmemiz gerekenler şunlardır:

- Hangi sosyal paylaşım sitesinde olursa olsun, resmi olmayan hiçbir sayfa ve profillere itibar edilmemesi gerekir.
- Kişisel bilgilerin herkese açık görünür şekilde yer almasına izin verilmemesi gerekir.
- Yapılan paylaşımların ne olduğuna, suç unsuru taşıyıp taşımamasına mutlaka dikkat edilmesi gerekir.

- Aynı şekilde gelen paylaşımların da suç unsuru taşıyıp taşımamasına, küfür, hakaret, sövme, aşağılayıcı sözler içerip içermemesine dikkat edilmelidir. Bu durumlar da size yönelen söz ve davranışlar hakkında suç duyurusunda bulunma hakkınız mevcuttur.
- Hiçbir yerde özel bilgilerinizin paylaşılmaması ve tanımadığınız kişilerin listenizde yer almasına izin vermemeniz gerekir.
- Fotoğraf veya videolar paylaşılmadan önce fotoğrafta yer alanlardan mutlaka izin alınmalıdır.
- Yer bildiriminde bulunurken aslında bulunduğunuz adresi ve konumunuzu da paylaştığınızı unutmayınız...
- Ekranlarda görülen her bilginin doğruluğu mutlaka sorgulanmalı ona göre hareket edilmelidir.
- Twitter ve Facebook gibi sosyal ağlarda gezinirken kaynağı belirtilmeyen aldatıcı linkler tıklanmamalı.
- Sosyal ağ sitelerinde etiketlenme gibi durumların yaşanmaması için mutlaka kişisel profil ayarlarından bu ayarların özenle onaylı olması gerektiğinden emin olunmalıdır.

6- Sosyal Mühendislikten Korunma Yöntemleri

Sosyal mühendislik, internet ortamında, insanların zafiyetlerinden faydalanarak çeşitli ikna ve kandırma yöntemleriyle istenilen bilgileri elde etmeye çalışmaktır. İnsanların karar verme süreçlerini değiştirmeye yönelik teknikler içerir.

Sosyal mühendislik yöntemleri çok çeşitli olmak ile birlikte en çok kullanılan yöntemler şunlardır.

a- **Telefon yolu ile: En etkili sosyal mühendislik ataklarından biridir. Hedef kişi, bir dolandırıcı tarafından aranır ve arayan kişi yetkili biri gibi davranarak yavaş yavaş kişisel belgilere ulaşır veya istediği eylemleri yaptırır.**

b- **Çöpleri Boşaltma (Dumpster Diving): Önemli ve kötü niyetli kişilerin kullanıma uygun birçok bilgileri, kurumun veya şirketin çöplerinden derlenerek elde edilmesidir.**

c- **İkna Etme: Taklit etme, kendini sevdirme, riayet etme, sorumluluk yayma ve sade bir arkadaş olarak görünme yöntemlerini denerler**

d- **On-Line Sosyal Mühendislik Sosyal ağları(Twitter, Instagram, Facebook vb.) : çok etkin kullanarak sizi arkadaşınız kadar iyi tanıyabilirler. Facebook aracılığıyla anne kızlık soyadını öğrenmek dakikalar almakta ve bu basit bilgi ile birçok işlem yapılabilmektedir.**

Sosyal Mühendislikten korunmak için aşağıdakilere dikkat etmek gerekir.

- Kullanıcılar eğitilmelidir.
- Telefonda arayan hiç kimseye şifreler ve önemli bilgiler verilmemelidir.
- Büyük şirketlerde veya kurumlarda "yardım masası" denilen bölümler vardır. Bu bölümleri arayıp kimlik doğrulaması tam olarak yapılmalıdır.
- Uygun olmayan yöntem ve kanallardan kurumsal bilgiler paylaşılmamalıdır.
- Parola gizliliği prensibi, kurum genelinde uygulanmalıdır.
- Gerektiğinde, “Ben kurumsal hattan sizi arayayım” denilmelidir.
- Kurumsal gizlilik taşıyan evraklar, uygun yöntemlerle imha edilmelidir.
- E-Posta, posta ile gelen CD, yardımcı yazılımlar vs. kullanımında dikkatli olunmalıdır.

7- Dosya Erişim ve Paylaşım Güvenliği Aşamaları

Bilgisayarda bilgilerin kaydedildiği birimlere dosya adı verilir. Dosya içerisindeki bilgi; resim, yazı, çizim, ses gibi her şey olabilir.

Herhangi bir şekilde, ister paylaşıma açarak ister dosya paylaşım yazılımları kullanarak başkalarının erişimine imkan verdiğiniz zaman bilgisayarınızı korumak için güvenlik önlemleri almanız gerekir. Bunun için

- Paylaşıma açtığınız dosya veya klasörler, kimlerin hangi haklarla erişmesi gerektiği göz önünde bulundurularak yapılandırabilir.
- Kişisel veya önemli bilgilerin olduğu dosyalar şifrelenerek saklanabilir.
- Paylaştığınız dosya veya klasörlerin zaman zaman denetimini yapmak ve önceden verilmiş hakları güncellemek gerekir.

- Dosya paylaşım yazılımları kullanırken telif haklarını göz önünde bulundurarak paylaşımda bulunmak yasal açıdan önemlidir.

8- Sistem ve Verilerin Yedeklenmesi Aşamaları

Yazılım veya donanım hataları yaşandığında veri kaybı yaşanabilir. Yedekleme, bilgi kaybını azaltmak için önlem almaktır. Yedeklemenin önemi, değerli bir bilginin yitirilmesinden sonra daha iyi anlaşılır. Ancak yitirilen bilginin arkasından üzülmektense, akıllı davranıp yedek almak hem zaman kazandırır hem de iş gücü tasarrufu sağlar.

Verilerimizi:

- **Dosyalarınızı veya verilerinizi farklı ortamlara (CD, DVD, USB gibi) kopyalayarak**
- **Yedekleme yazılımları ile yedeğini alarak sağlayabilirsiniz.**

Neleri ne zaman yedekleyeceğiniz sorusuna cevap vermek ve bir yedekleme planı oluşturmak etkin yedekleme süreçleri için önemlidir.

9- Zararlı Yazılımlardan Korunma Aşamaları

Zararlı programlar bilgisayarımız üzerinde başka şahısların kontrol sahibi olmasını sağlarlar. Programlarımız bozulabilir, istediğimiz gibi çalışmamaya başlarlar. Dosyalarımız silinebilir. Kişisel bilgilerimiz başkalarının eline geçebilir.

Bu sebeple;

- Antivirüs (virüsten korunma) ve antispyware (casus yazılımdan korunma) programları kullanmalıyız
- Antivirüs ve antispyware programlarını güncel tutmalıyız
- İşletim sistemini güncel tutmalıyız (işletim sistemi yamalarını yapmalıyız)
- Güvenlik duvarı kullanmalıyız
- İnternette girdiğimiz sitelere ve indirdiğimiz dosyalara dikkat etmeliyiz
- Lisanslı programlar kullanmalıyız.
- E-postaları açmadan önce içeriğinin güvenilirliğini kontrol etmeliyiz.

10- Mobil cihaz güvenlik aşamaları

Haberleşmeden bankacılığa, alışverişten elektronik cüzdana günlük hayatımızda her türlü iş için kullanmakta olduğumuz mobil haberleşme araçları olan cep telefonları, en önemli araç olarak hemen hemen her kişinin cebindeki yerini alırken hem akıllanıp kapasite ve yetenekleri artmakta hem de çok çeşitli siber tehditlerin hedefi haline gelmiş bulunmaktadır.

Bu konuda dikkat edilmesi gereken en önemli konuları şöyle sıralamak mümkündür;

- Bilmediğiniz kaynaklardan gelen ya da şüphe uyandıran elektronik postaları açmayınız,
- Bilmediğiniz kaynaklardan gelen ya da şüphe uyandıran elektronik postaların eklentileri üzerine tıklamayınız, bu ekleri cihazınıza indirmeyiniz,
- Cihazınıza kaynağından emin olmadığınız ve/veya işlevini bilmediğiniz yazlım yüklemeyiniz,
- Uygulama dükkanlarından indireceğiniz uygulama yazılımlarını dikkatlice seçiniz, özellikle ücretsiz olanları mümkün olduğunca indirmeyiniz,
- Cihazının içinde sakladığınız kritik bilgilerinizi (örneğin şifre dosyanız, kimlik belgeleriniz vs.) şifreleyiniz,
- Cihazınızın ayarlarını yaparken özellikle dışarıya gidecek ya da dışarıdan gelecek verileri (konum bilgisi vb.) otomatik hale getirmeyiniz, sizin onayınızı isteyiniz,
- Cihazınızı tanımadığınız kişilere vermeyiniz,
- Cihazınızı üreticilerin resmi tamir-bakım merkezleri dışında tamir ettirmeyiniz,
- Şüpheli kaynaklardan hediye telefon kabul etmeyiniz,
- Cihazınızda mutlaka virüs koruma programı bulundurunuz,
- Cihazınızdaki yazılımları sık sık güncelleyiniz,
- Cihazınızı zaman zaman fabrika ayarlarına döndürünüz ve/veya formatlayıp yeniden kurunuz.