



PERSONEL SİBER GÜVENLİK SUNUMU

SİBER GÜVENLİK ÖNLEMLERİ

ile her şey çok net



VERİNİN KORUNACAK NİTELİKLERİ

Gizlilik

Bilginin yetkili olmayan kişiler, varlıklar ve süreçler tarafından erişilemez ve ifşa edilemez niteliğidir.

Bütünlük

Bilginin doğruluk, bütünlük ve kendisine has özelliklerinin korunmasıdır.

Erişilebilirlik

Bilginin yetkili kişiler(görevi gereği) tarafından istenildiğinde ulaşılabilir ve kullanılabilir olma özelliğine denir.

VERİNİN SINIFLANDIRILMASI

Gizli Veri	İç Kullanım	Kişisel	Kuruma Açık
➤ En kritik bilgilerdir. ➤ Sadece yönetim kadrosu erişebilir. ➤ Bu tür bilgilere yetkisiz erişilmesi, ifşa edilmesi veya paylaşılması kurumu zor durumda bırakır. ➤ Gizlilik ön plandadır. ÖRNEK: ➤ Sivil Savunma Planı gibi..	➤ Sadece birimlere özel bilgilerdir. ➤ Departman çalışanları dışında hiçbir 3. taraf kurum veya kişinin görmemesi gereken verilerdir ➤ Gizlilik ön plandadır. ÖRNEK: ➤ Denetim Tutanakları vb.	➤ Birim çalışanlarının kurum işlevleri için yaptığı kişisel çalışmalar ile ilgili verilerdir. ➤ Erişilebilirlik ön plandadır. ÖRNEK: ➤ Haftalık Faaliyet Planı ➤ Haftalık Faaliyet Raporu	➤ Bu bilgiler kurum çalışanlarının kullanımı içindir. ➤ Erişilebilirlik ve bütünlük ön plandadır. ÖRNEK: ➤ Haftalık Yemek Listesi ➤ Dahili Telefon Listesi

VERİNİN BULUNDUĞU ORTAMLAR

Fiziksel Ortamlar

Elektronik Ortamlar

Sosyal Ortamlar

Tanıtım Platformları

Fiziksel Ortamlar

- Kağıt, Tahta
- Pano, Yazı tahtası
- Fax kağıdı
- Çöp/Atık Kağıtlar
- Dosyalar
- Dolaplar



Elektronik Ortamlar

- Bilgisayarlar,
- Mobil iletişim cihazları,
- E-posta,
- USB,CD,Disk
- Disket,
- Manyetik ortamlar...



Sosyal Ortamlar

- Telefon görüşmeleri
- Muhabbetler
- Sosyal Medya Siteleri
- Yemek araları
- Toplu taşıma araçları



Tanıtım Platformları

- İnternet siteleri,
- Broşürler,
- Reklamlar, Sunumlar,
- Eğitimler, Görsel sunumlar.



VERİ GÜVENLİĞİ İÇİN DİKKAT EDİLMESİ GEREKEN TEHDİTLER



KÖTÜ NİYETLİ YAZ/LIMLAR

Kötü niyetli yazılım, bilgisayarınıza ya da ağınıza zarar vermek, bilgilerinizi çalmak amacıyla oluşturulmuş yazılımlardır.



TRUVA ATLARI

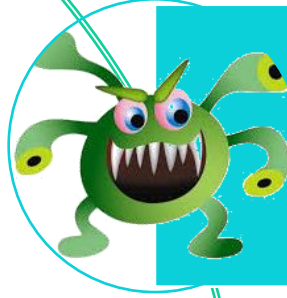
VİRÜSLER

SOLUCANLAR

YIĞIN MESAJ

CASUS YAZILIMLAR

VİRÜSLER



Kullanıcının izni ya da bilgisi dahilinde olmadan bilgisayarın çalışma şeklini değiştiren ve kendini diğer dosyaların içerisinde gizlemeye çalışan aslında bir tür bilgisayar programıdır.

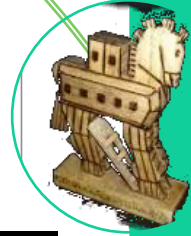


Bağımsız hareket edemezler. Mutlaka bir uygulama dosyasına bağlanarak çoğalır ve yayılırlar.

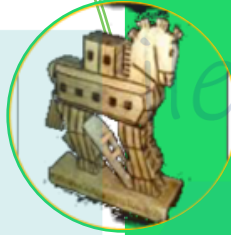


Çoğalmayı ve yayılmayı hedeflerler. Çoğalıp yayılmak için kullanıcıya bağımlıdırlar.

TRUVA ATLARI



Adını Truva Atı Hikayesinden almaktadır.



Kullanıcıya, kullanışlı veya ilginç programlar gibi görünür.



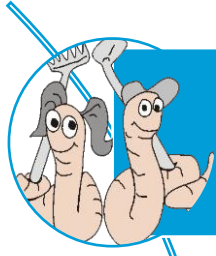
Zararlı program barındıran veya yükleyen programdır.



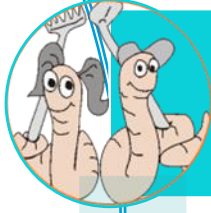
Bilgisayarınızda uzaktan erişim kapısı açmak, internet bağlantınızı pahalı bir tarife yönlendirmek, sizin adınıza istemsiz e-posta göndermek vb işlemler yapabilir.



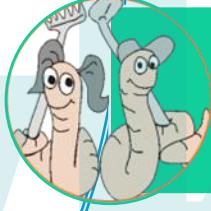
SOLUCANLAR



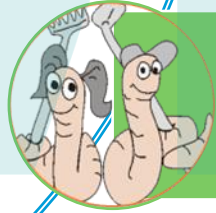
Virüslerle aynı özelliklere sahiptir.



Bağımsız çalışabilir, çoğalıp yayılabilir.



e-posta, kaynağı belirsiz programlar, forum siteleri, korsan oyun dvd ve cd leri gibi yollarla bulaşır.



Kullanım esnasında kendini hissettirmez arka planda efendisine hizmet eder.

- Örnek 1 Sitemize giren 1.000.000. kişisiniz. Bizden hediye şarkı kazandınız. TIKLAYIN gibi
- Örnek 2 Bugün şanslı gününüzdesiniz. Bizden para ödülü kazandınız. TIKLAYIN gibi
- Örnek 3 Tebrikler bizden kol saati kazandınız. TIKLAYIN gibi gelen mailler...

CASUS YAZILIMLAR



Casus yazılım, kullanıcılara ait önemli bilgilerin ve kullanıcının yaptığı işlemlerin, kullanıcının bilgisi olmadan toplanmasını ve bu bilgilerin kötü niyetli kişilere gönderilmesini sağlayan yazılım olarak tanımlanır.

Diğer kötü amaçlı yazılımlar gibi kendilerini çoğaltmaya ihtiyaç duymazlar.



Genellikle bulaştıkları bilgisayarda kendilerini fark ettirecek herhangi bir etki yapmazlar.(Yavaşlama, çökme vb..)

YIĞIN MESAJ



Yığın mesaj (spam) e-posta, telefon, faks gibi elektronik ortamlarda çok sayıda alıcıya aynı anda gönderilen gereksiz veya uygunsuz iletiler.



En yaygın türleri reklamlar ve ilanlardır.



İçerikleri yalan ya da yanıltıcı olur.



Mesajın başlık bilgileri tahrip edilmiş olur.
(Dolayısıyla geriye dönük izleme hayli zor olur)



VERİ GÜVENLİĞİ İÇİN ALINMASI GEREKEN TEDBİRLER

kvnnet



SUNUCU VE SİSTEM GÜVENLİĞİ

Sunucu odalarının fiziksel koruması sağlanmış olmalıdır.

Sunucuların yönetiminden sorumlu personel görevlendirilmelidir.

Sistem yöneticileri 'Admin', 'Root' gibi genel adlar yerine özgün adlar kullanılmalıdır.

Sunucular ve terminallerde lisanslı yazılımlar kullanılmalıdır.

Sunucularda işletim sistemi yedeklemeleri, yamaları ve güncellemeleri yapılmalıdır.

Görevden ayrılan personelin tüm erişim yetkileri ivedilikle iptal edilmelidir.



TEMİZ MASA TEMİZ EKRAN

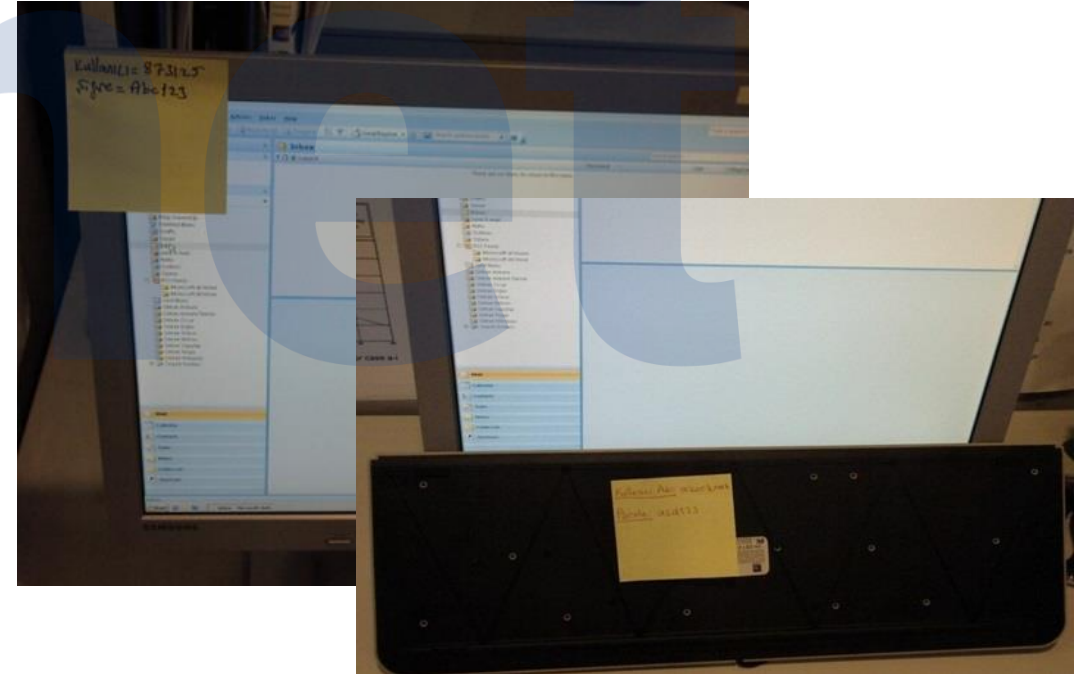
Çalışma masası ve bilgisayar ekranı üzerinde bilgiye yetkisiz ulaşım engellenmelidir.

Çalışma odaları ayrılırken kilitlenerek, anahtarları kontrol altında tutulmalıdır.

Bilgisayar ekran kilidi aktif hale getirilmeli ve süresi çok uzun olmamalıdır.

Bilgisayar başından ayrılırken Windows Logo + L tuşlarıyla bilgisayar kilitlenmelidir.

Kullanıcı adı ve şifre iyi korunmalıdır.



ŞİFRE GÜVENLİĞİ

Sunuculara ve kullanıcı bilgisayarlarına erişim şifre ile korunmalıdır.

Ağa bağlı bilgisayarlarda ağ yöneticisince belirlenen şifreler kullanıcı tarafından ilk kullanımda zorunlu olarak değiştirilmelidir.

Kişisel bilgiler gibi kolay tahmin edilebilecek bilgiler şifre olarak kullanılmamalıdır. (Örneğin doğum tarihiniz, çocuğunuzun adı, soyadınız, gibi)

Sözlükte bulunabilen kelimeler şifre olarak kullanılmamalıdır.

Ardışık sayılar ve alfabetik karakterler kullanılmamalıdır.

Çoğu kişinin kullanabildiği aynı veya çok benzer yöntem ile geliştirilmiş şifreler kullanılmamalıdır.



GÜÇLÜ ŞİFRE BELİRLEME

Belirleyeceğiniz şifreleriniz en az 8 karakterden oluşmalıdır, Bu şifreleriniz içerisinde karakter kullanımına özen gösterilmelidir.

Örneğin
1Env,2Esv.
10Y15mgyhy.



DİKKAT! Güçlü gibi görüldüğü halde zayıf olan parola oluşturmamalı.

Güçlü gibi görünse de çok kullanılan ve çok kolay tahmin edilebilen parolalardan kaçınmak gerekmektedir. Bu parolalar klavyedeki harf sırası, alfabadeki harf sırası gibi popüler kurallardan oluşturulmaktadır.

E POSTA GÜVENLİĞİ

E-posta sizin için ne anlama geliyor?

- Size ve yakınlarınıza erişim.

E-posta kötü niyetli kişiler için ne anlama geliyor?

- Reklam ve Kötü niyetli yazılımları yayma yolu.



İstenmeyen e-postalardan korunma

E-posta adresini **haber grupları, sohbet odaları, internet sayfaları, sosyal paylaşım siteleri** gibi herkese açık yerlerde yayınlamamak.

Birden çok kişiye veya bir gruba e-posta gönderirken kişilerin e-posta adreslerini **gizli karbon kopya (BCC) bölümüne** yazmak.

Bir web sitesinde yapılan işlem gereği e-posta adresi istendiğinde, **sitenin gizlilik politikasını** kontrol etmek.

İstenmeyen e-postalara hiç bir şekilde **cevap yazmamak**.

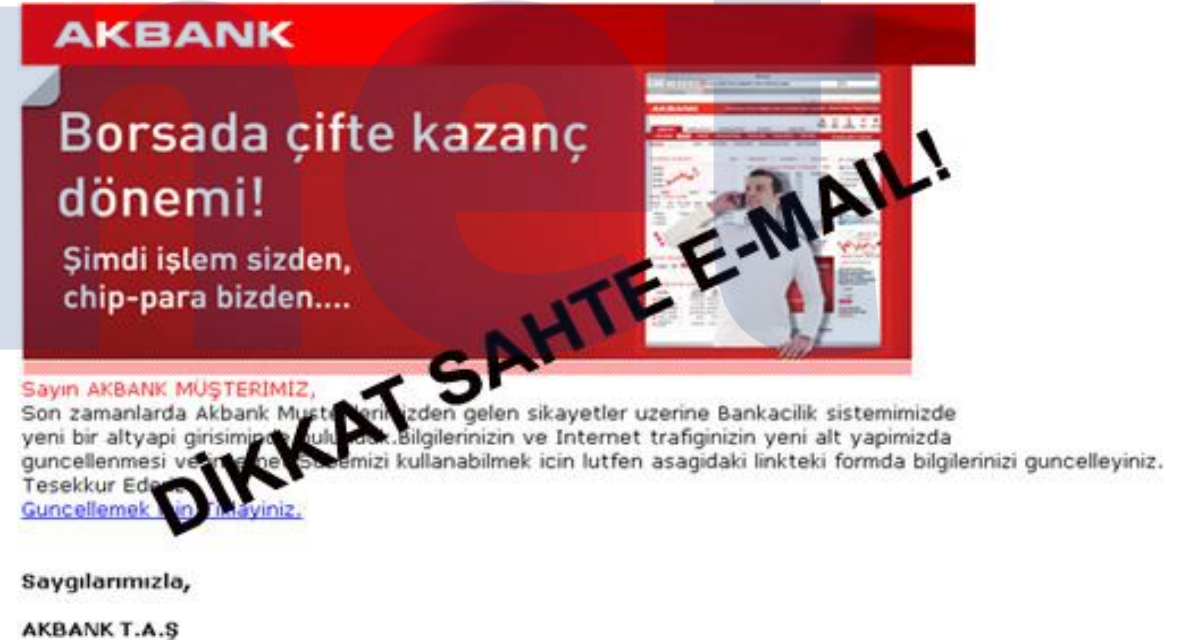
Kullanım amacına göre **farklı e-posta adresleri** kullanmak.

TEDBİRLER

Taklit-Oltalama e-postalardan korunma

Kimlik bilgilerini çalmak amacı ile, istenmeyen e-posta veya açılır pencere yoluyla yapılan bir **aldatma yöntemi**dir.

Saldırgan önceden tasarlanan bir hikâye üzerinden, kullanıcıyı e-postanın güvenilir bir kaynaktan geldiğine inandırıp, özel bilgilerini (kredi kartı, şifre bilgileri vs...) ele geçirmeye çalışır.



Taklit-Ortalama e-postalardan korunma

Kişisel, kurumsal ve mali bilgilerinizi tanıdığınız kişiler dahil hiç kimseye e-posta yoluyla göndermemek.

E-posta mesajlarındaki internet bağlantılarına tıklamamak.

Düzenli olarak kredi kartı hesap özeti, banka bildirimleri gibi bilgilendirme dokümanlarını gözden geçirmek.

Zararlı programlara karşı korunma programları (Anti-virus, anti-spyware,) gibi güvenlik yazılımları kullanmak ve sık sık güncellemek.

SOSYAL MEDYA GÜVENLİĞİ

ile her şey çok net®

İnternet kullanıcılarının aralarında bilgi, görüş ve ilgi alanlarını, yazılı görsel ya da işitsel bir şekilde paylaşarak iletişim kurmalarına olanak sağlayan araçlar ve web sitelerini içermektedir.

SOSYAL MEDYA GÜVENLİĞİ

ZARARLARI



Bağımlılık yapabiliyor.

Sosyal medya, dili yozlaştırıyor.

Zararlı sosyal örgütlenmeler olabilir.

Yorumlarla firmaların marka değeri zarar görebilir.

Birçok zararlı yazılım sosyal medya kanalıyla bulaşabilir.

SOSYAL MÜHENDİSLİK

Normalde insanların tanımadıkları biri için yapmayacakları şeyleri yapmalarını sağlama sanatıdır.

Teknoloji kullanımından çok insanların hile ile kandırılarak bilgi elde edilmesidir.

Sosyal mühendisler: Teknolojiyi kullanarak ya da kullanmadan bilgi edinmek için insanlardan faydalanırlar.

Kullandığı en büyük silahı, **insan zafiyetidir.**

TEŞEKKÜRLER

kvvkn[®]et