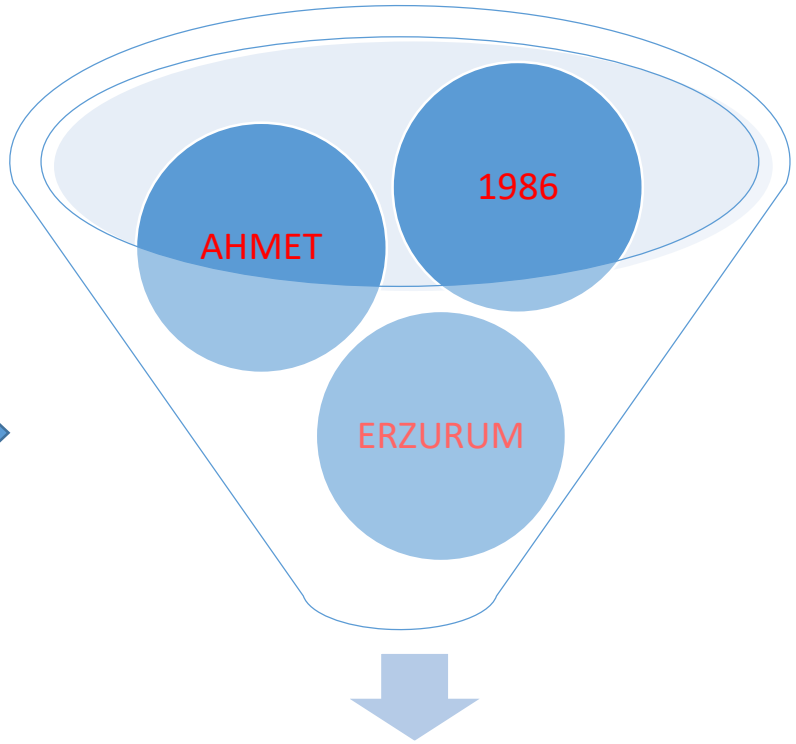
BİLGİ GÜVENLİĞİ FARKINDALIK EĞİTİMİ

Niğde Ömer Halisdemir Üniversitesi
Ağız Diş sağlığı Uygulama ve Araştırma Merkezi

Veri Nedir ? Bilgi Nedir ?

VERİ

Sayısal ve mantıksal her bir değer.
İşlenmemiş ham bilgi.
(Harf , rakam, sembol, kelime vb..)



Bilgi =

AHMET 1986 DA ERZURUM'DA DOĞDU

BİLGİ

Verinin işlenmiş hali.

BİLGİ GÜVENLİĞİ NEDİR?

Bilgi güvenliği, “bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önleme olarak” tanımlanır.

SORUMLU KİM ?

HEPİMİZ

Güvenliğin sadece
küçük bir kısmı **% 20** teknik,
güvenlik önlemleri ile sağlanıyor.
Büyük kısım ise **% 80** kullanıcı

Amaç;

Bilgisayar teknolojilerinde güvenliğin amacı ise “kişi ve kurumların bu teknolojilerini kullanırken karşılaşabilecekleri tehdit ve tehlikelerin analizlerinin yapılarak gerekli önlemlerin önceden alınmasıdır. Bilgi güvenliği; kurumdaki işlerin sürekliliğinin sağlanması, işlerde meydana gelebilecek aksaklıkların azaltılması ve yatırımlardan gelecek faydanın artırılması için bilginin geniş çaplı tehditlerden korunmasını sağlar.

Bilgi güvenliğinin sağlanabilmesi bilginin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin yeterli düzeylerde sağlanabilmesi ile mümkündür.

Bilginin Korunacak Nitelikleri

Gizlilik

- Bilginin yetkili olmayan kişiler, varlıklar ve süreçler tarafından erişilemez ve ifşa edilemez niteliği

Bütünlük

- Bilginin doğruluk, bütünlük ve kendisine has özelliklerinin korunması,

Erişilebilirlik

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

Bilginin Sınıflandırılması

Gizli Bilgi

- En kritik bilgilerdir.
- Sadece yönetim kadrosu erişebilir.
- Bu tür bilgilere yetkisiz erişilmesi, ifşa edilmesi veya paylaşılması kurumu zor durumda bırakır.
- Gizlilik ön plandadır.

ÖRNEK:

- Disiplin Soruşturması

İç Kullanım

- Sadece birimlere özel bilgilerdir.
- Departman çalışanları dışında hiçbir 3. taraf kurum veya kişinin görmemesi gereken bilgilerdir.
- Gizlilik ön plandadır.

ÖRNEK:

- Hastane Denetim Tutanağı

Kişisel

- Birim çalışanlarının kurum işlevleri için yaptığı kişisel çalışmalar ile ilgili bilgilerdir.
- Erişilebilirlik ön plandadır.

ÖRNEK:

- Haftalık Faaliyet Planı
- Haftalık Faaliyet Raporu

Kuruma Açık

- Bu bilgiler kurum çalışanlarının kullanımı içindir.
- Erişilebilirlik ve bütünlük ön plandadır.

ÖRNEK:

- Haftalık Yemek Listesi
- Dahili Telefon Listesi

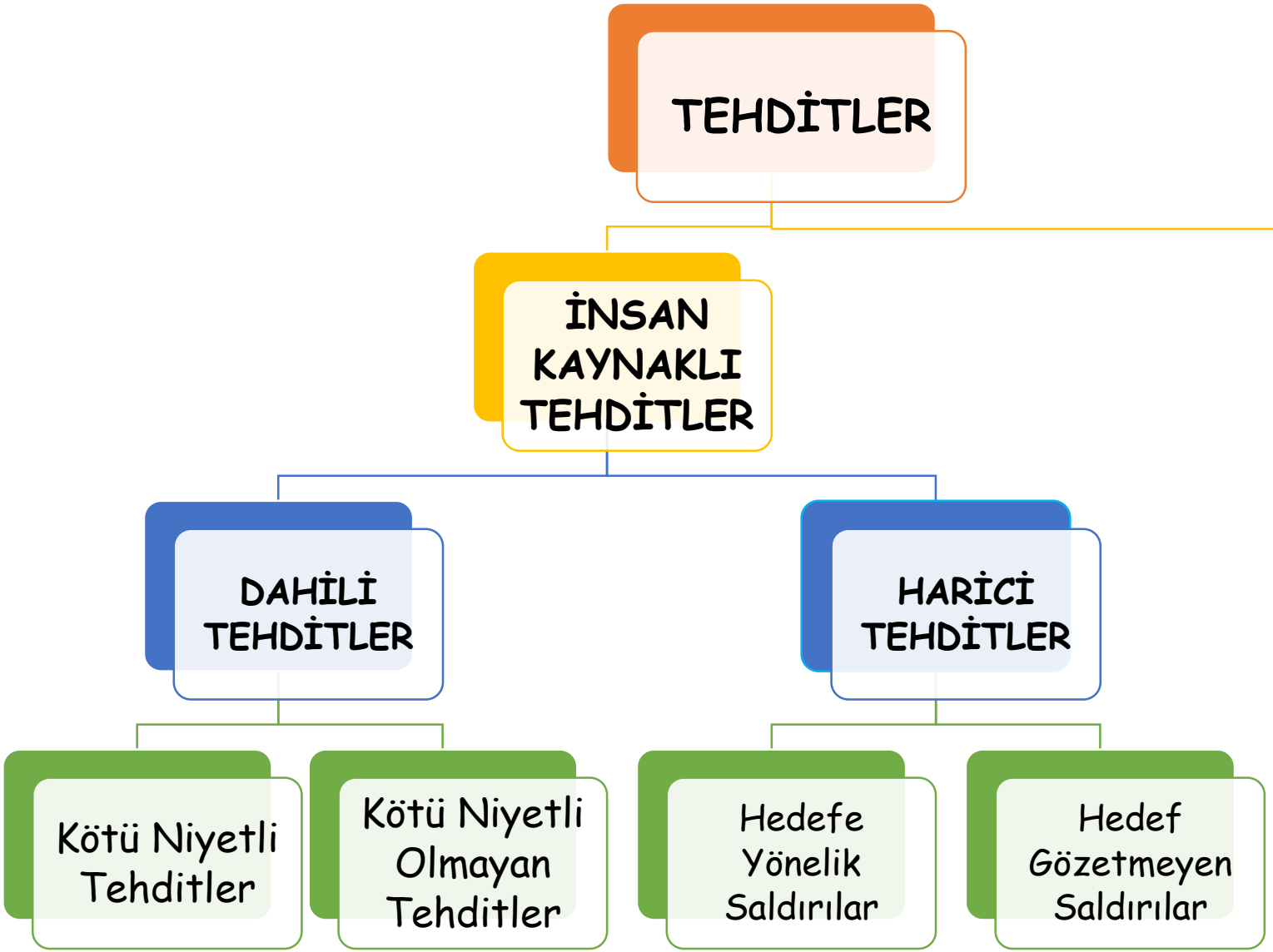
BİLGİNİN KORUNMASINA YÖNELİK MEVZUAT

- Anayasa,
- 5237 sayılı Türk Ceza Kanunu,
- 4721 sayılı Türk Medeni Kanun,
- 3359 sayılı Sağlık Hizmetleri Temel Kanunu,
- 1219 sayılı Tababet ve Şuabatı San'atlarının Tarzı İcrasına Dair Kanun,
- 5258 sayılı Aile Hekimliği Pilot Uygulaması Hakkında Kanun,
- 663 sayılı Kanun Hükmünde Kararname,
- 5070 sayılı Elektronik İmza Kanunu,
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
- 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun",

Bilgi Güvenliğinin Sağlanması

- Fiziksel ve Çevresel Güvenlik
- Ekipman Güvenliği
- İşletim Sistemleri ve Son Kullanıcı Güvenliği
- Parola Güvenliği
- Sunucu ve Sistem Güvenliği

TEHDİTLER



- ✓ Deprem,
- ✓ Sel,
- ✓ Yangın vb.

TEHDİTLER VE TEDBİRLER

DAHİLİ TEHDİTLER

Kötü Niyetli Tehditler

- İşten Çıkarılan Çalışanın, Kuruma Ait Web Sitesini Değiştirmesi,
- Bir Çalışanının, Ağda "Sniffer" Çalıştırarak E-postaları Okuması,
- Bir Yöneticinin, Geliştirilen Ürünün Planını Rakip Kurumlara Satması.

Kötü Niyetli Olmayan Tehditler

- Bilgisiz ve Bilinçsiz Kullanım,
- Temizlik Görevlisinin Sunucunun Fişini Çekmesi,
- Eğitilmemiş Çalışanın Veri tabanını Silmesi.

TEHDİTLER VE TEDBİRLER

HARİCİ TEHDİTLER

Hedefe Yönelik Saldırılar

- Bir Saldırganın Kurum Web Sitesini Değiştirmesi,
- Bir Saldırganın Kurum Muhasebe Kayıtlarını Değiştirmesi,
- Birçok Saldırganın Kurum Sunucusuna Hizmet Aksatma Saldırısı Yapması.

Hedef Gözetmeyen Saldırılar

- Virüs Saldırıları (Melissa, CIH – Çernobil, Vote),
- solucan Saldırıları (Code Red, Nimda),
- Trojan Arka Kapıları (Netbus, Subseven, Black Orifice).

TEHDİTLER

FİZİKSEL VE ÇEVRESEL TEHDİTLER

- Yiyecek-İçecek
- Yangın,
- Hırsızlık,
- Deprem,
- Su Baskını,
- Elektriksel etki,

- Donanımların yanında yiyecek içecek tüketilmemeli, bulundurulmamalıdır.
- Yangın önleme ve söndürülmesine yönelik tedbirler alınmalıdır.
- Kuruma giriş ve çıkışlar kontrol altına alınmalıdır.
- Ofisler ve çalışma odalarına yetkisiz girişler engellenmelidir.
- Depremin etkilerini azaltmaya yönelik önlemler alınmalıdır.
- Sunucuların ve verilerin bulunduğu ortamlarda su baskını tehditlerine karşı önlemler alınmalıdır.
- Paratoner kullanılmalıdır.
- Elektrik teçhizatı periyodik bakımları yapılmalıdır.
- Sistem elektrik kesintilerine karşı kesintisiz güç kaynakları ile desteklenmelidir.

TEHDİTLER

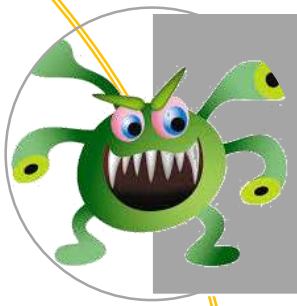
KÖTÜ NİYETLİ YAZILIMLAR

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

- VİRÜSLER
- TRUVA ATLARI
- SOLUCANLAR
- CASUS YAZILIMLAR
- YIĞIN MESAJ

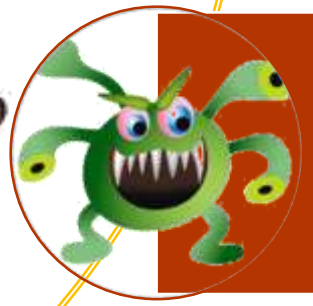
TEHDİTLER

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.

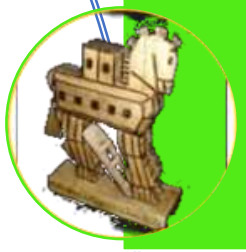


Çoğalmayı ve yayılmayı hedeflerler. Çoğalıp yayılmak için kullanıcıya bağımlıdırlar.

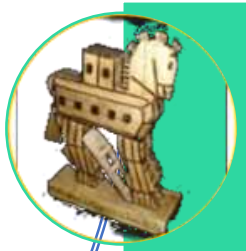
TEHDİTLER

TRUVA ATLARI

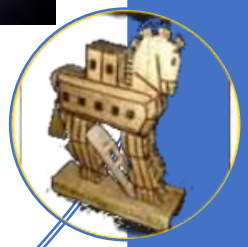
Adını Truva Atı Hikayesinden almaktadır.



Kullanıcıya, kullanışlı veya ilginç programlar gibi görünür.



Zararlı program barındıran veya yükleyen programdır.

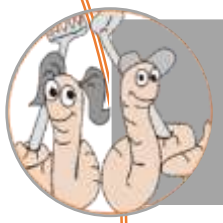


Bilgisayarınızda uzaktan erişim kapısı açmak, internet bağlantınızı pahalı bir tarifeye yönlendirmek, sizin adınıza istemsiz e-posta göndermek vb işlemler yapabilir.

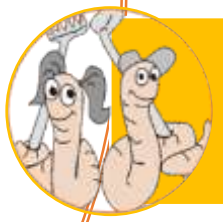
TEHDİTLER

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.

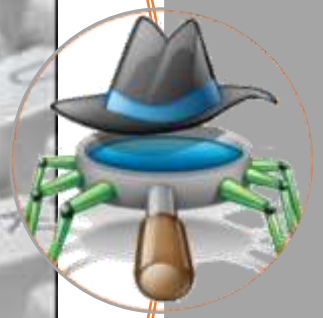
Kullanım esnasında kendini hissettirmez arka planda efendisine hizmet eder.

- *Sitemize giren 1.000.000. kişisiniz. Bizden hediye şarkı kazandınız.* TIKLAYIN
- *Bugün şanslı gününüzdesiniz. Bizden para ödülü kazandınız.* TIKLAYIN
- *Tebrikler bizden kol saati kazandınız.* TIKLAYIN

TEHDİTLER

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..)

TEHDİTLER

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)

TEDBİRLER

TEMİZ MASA TEMİZ EKRAN

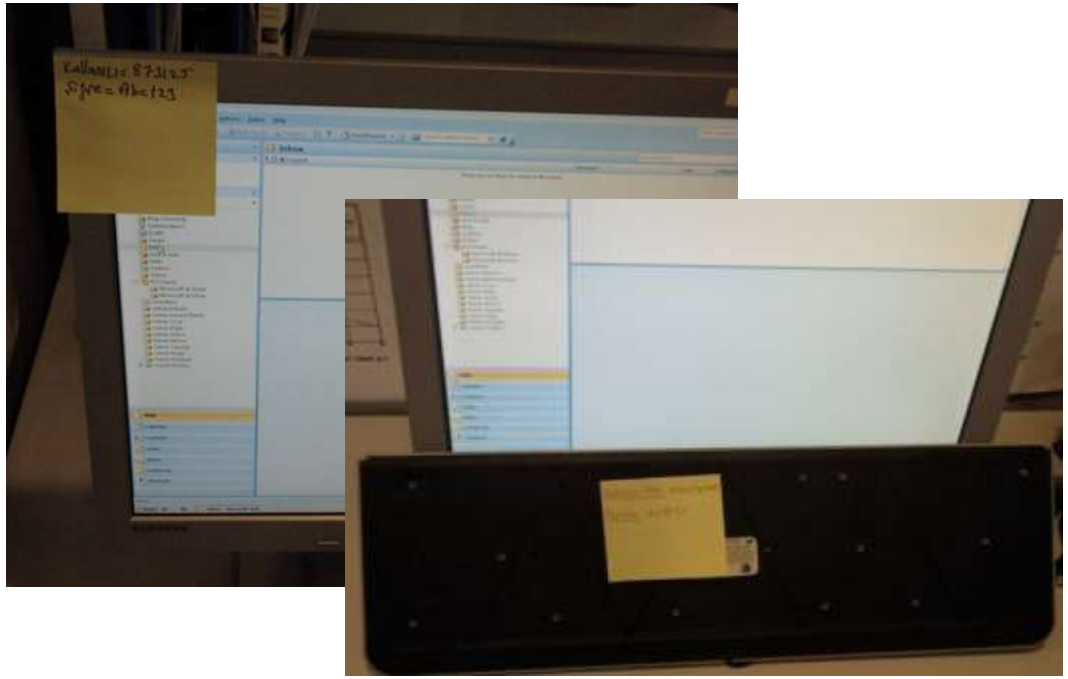
Çalışma masası ve bilgisayar ekranı üzerinde bilgiye yetkisiz ulaşım engellenmelidir.

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.



TEDBİRLER

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)
- Ardışık sayılar ve alfabetik karakterler kullanılmamalıdır.
- Çoğu kişinin kullanabildiği aynı veya çok benzer yöntem ile geliştirilmiş şifreler kullanılmamalıdır.

TEDBİRLER

TAŞINABİLİR AYGIT GÜVENLİĞİ

Taşınacak veri eğer usb disk ile taşınacaksa bu usb diskin tehdit unsuru olan bir yazılım içermediğine emin olunmalıdır.

Taşınacak verinin de tehdit unsuru içeren herhangi bir yazılım içermediğine emin olunmalıdır.

Veriyi ister usb disk isterse de cd, dvd ortamında taşınsın kesinlikle şifrelemelidir.

Veriyi usb disk ile taşıyorsak; bunları bilgisayara takarken usblerin sağlıklı çalıştığından emin olmalıyız

TEDBİRLER

GÜÇLÜ ŞİFRE BELİRLEME

Cümlelerin baş harflerini birleştirebilirsiniz.
Günlük hayatınızdan kolay hatırlayacağınız herhangi bir cümle kullanabilirsiniz.
Benzer şekilde
•Atasözlerinden
•Şarkı sözlerinden
•Şiirlerden
•...
seçeceğiniz cümlelerin aralarında rakamlar ve özel karakterler kullanarak çok daha güçlü bir parola oluşturmanız mümkün.
Örneğin

•Bir elin nesi var, iki elin sesi var. --> 1Env,2Esv.

•Ben 1996 yılının 7. ayında mezun oldum --> B1996y7.amo

TEDBİRLER

GÜÇLÜ ŞİFRE BELİRLEME

Cümleleri olduğu gibi parola yapabilirsiniz.
Özellikle rakam ve karakter içeren cümleler hoş olacaktır.Tabiki klişe ve kolay tahmin edilen, basit bir ifade ya da cümle ("My Pass", "benim şifrem" gibi) olmamak şartı ile.

Örneğin

- Ali'ninAyşe'ye20TLBorcuVar.
- Ankara'ya10SaattemiGeldin?
- Dikkat!Yolda3KişiVar.
- OtobüsümKızılay'dan17:30'daKalkar.

TEDBİRLER

GÜÇLÜ ŞİFRE BELİRLEME

DİKKAT! Güçlü gibi göründüğü halde zayıf olan parola oluşturmamalı.

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

Örneğin:

- "123qwe", "qwe123", "123qweasd", "qwer1234", ...
- "qweasd", "123QweAsd", "asd12345", "Asd123", ...
- "qwerty", "qwerty123", "qazwsx123", ...
- "abc123", "123abc", "1234abcd", ...
- "123456", "987654321", "1234qqqQ", ...

TEDBİRLER

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.

TEDBİRLER

E POSTA GÜVENLİĞİ

İstenmeyen e-postalardan korunma

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

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

E POSTA GÜVENLİĞİ

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

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-Oltalama e-postalardan korunma

“Eğer bir şey bedavaysa oradaki ürün sensindir”

TEDBİRLER

E POSTA GÜVENLİĞİ

Taklit-Oltalama 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 kart 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.

TEDBİRLER

SOSYAL MEDYA GÜVENLİĞİ

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.

TEDBİRLER

SOSYAL MEDYA GÜVENLİĞİ

TEDBİRLER

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 medyada, açıkça verilmiş bir izin olmadıkça kurum adına açıklama yapılamaz.

- Kurumumuzun saygınlığı göz önünde bulundurularak kuruma ait fiziki alanlarda yapılan işe ait paylaşım yapılamaz.

- Bilgi Güvenliği kapsamında hassas ve gizlilik içeren bilgiler sosyal mecrada yayınlanamaz.

- Sosyal medya kullanımında; “İtibar Kaybına”, “Mali Kayıplara”, “Gizlilik İhlallerine”, “Mevzuat İhlallerine” imkân verecek, “Etik İlkelere” uygun olmayan paylaşımların yapılmaması gerekir.

TEDBİRLER

SOSYAL MEDYA GÜVENLİĞİ

SONUÇ

Bizler internet üzerinde bir karakter yaratma çabasındayken aslında birileri için birer **istatistikten** ve **dolandırılacak bir hesaptan** başka bir şey değiliz.

TEDBİRLER

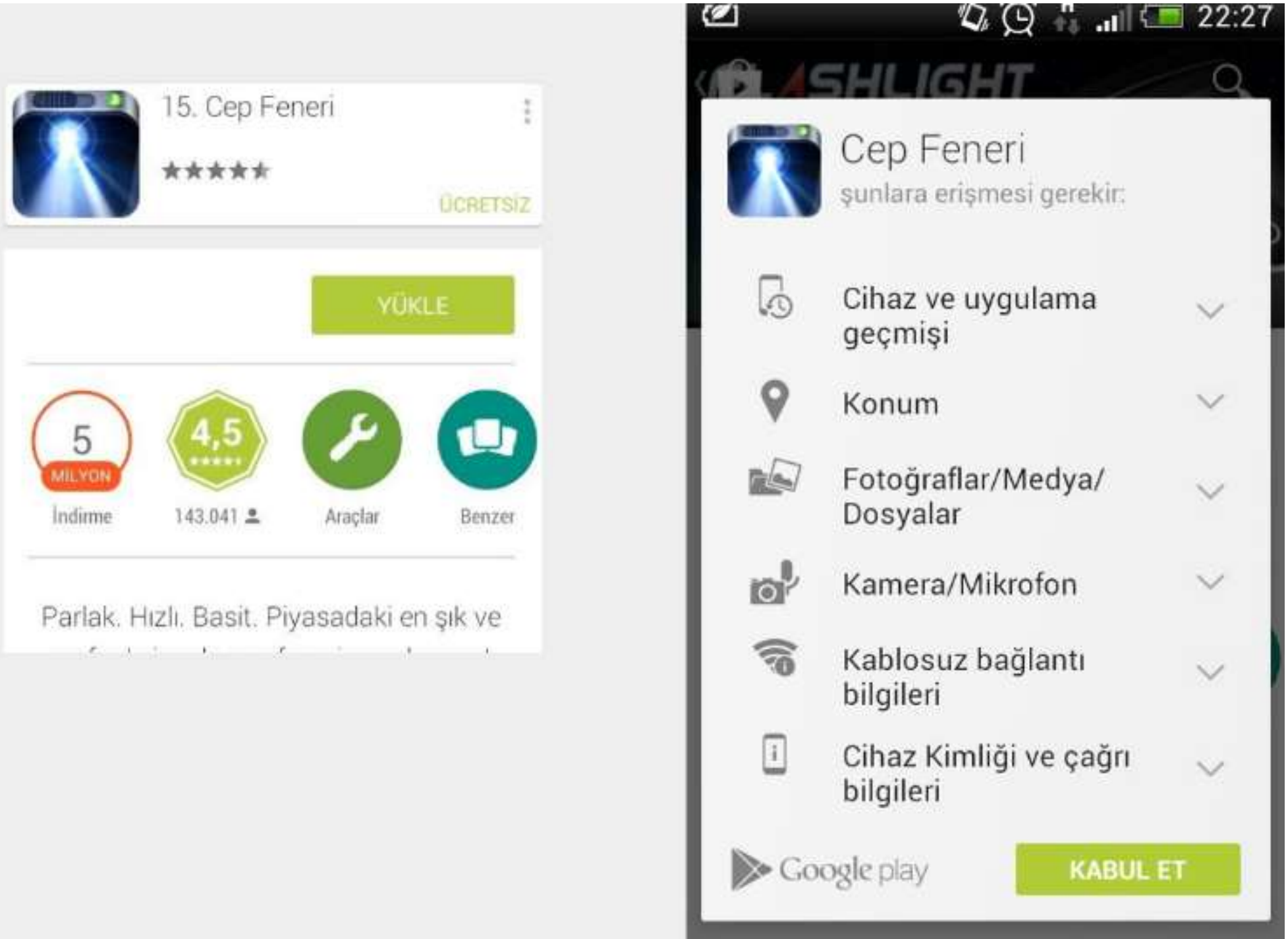
SOSYAL MÜHENDİSLİK

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.**


15. Cep Feneri
ÜCRETSİZ
YÜKLE
5
MİLYON
İndirme
4,5
143.041
Araçlar
Benzer
Parlak. Hızlı. Basit. Piyasadaki en şık ve
22:27
Cep Feneri
şunlara erişmesi gerekir:
Cihaz ve uygulama geçmişi
Konum
Fotoğraflar/Medya/ Dosyalar
Kamera/Mikrofon
Kablosuz bağlantı bilgileri
Cihaz Kimliği ve çağrı bilgileri
Google play
KABUL ET

TEDBİRLER

SOSYAL MEDYA GÜVENLİĞİ

ZARARLARI

En çok kullandığımız Sosyal Medya Uygulamaları cep telefonumuzun hangi verilerini alıyor.

Sosyal Medya Adı	Cihaz ve Uygulama Geçmişi	Kimlik (Hesaplar, Profil)	Konum	Takvim	Kişiler	SMS	Telefon	Fotoğraflar Medya Dosyalar	Kamera	Mikrofon	Kablosuz Bağlantı Bilgileri	Cihaz Kimliği ve Çağrı Bilgileri	Diğer
Facebook													
Instagram													
Twitter													
Foursquare													
WhatsApp													
LinkedIn													

İHLAL BİLDİRİM YÖNETİMİ

TANIM:

Bilginin gizlilik, bütünlük ve kullanılabilirlik açısından zarar görmesi,

Kurumun bilgi güvenliği yetkilisine bildirilmeli

Bilgi güvenlik olayı raporlarının bildirilmesini, işlem yapılmasını ve işlemin sonlandırılmasını sağlayan uygun bir geri besleme süreci oluşturulmalıdır.

Güvenlik olayının oluşması durumunda olay anında raporlanmalıdır.

İHLAL BİLDİRİM YÖNETİMİ

İhlali yapan kullanıcı tespit edilmeli ve ihlalin suç unsuru içerip içermediği belirlenmelidir.

Güvenlik ihlaline neden olan çalışanlar, üçüncü taraflarla ilgili resmi bir disiplin sürecine başvurulur.

Tüm çalışanlar, üçüncü taraf kullanıcıları ve sözleşme tarafları bilgi güvenliği olayını önlemek maksadıyla harekete geçer ve resmi süreç başlatılır.

Bilgi sistemi arızaları ve hizmet kayıpları, zararlı kodlar, dos atakları, tamamlanmamış veya yanlış iş verisinden kaynaklanan hatalar ihlal bildirimi gerektirir.

Disiplin

Personel Yönetmeliği gereğince aşağıdaki yaptırımlardan bir ya da birden fazla maddesini uygulayabilir

Uyarma

Kınama

Para cezası

Sözleşme feshi

BİLGİ GÜVENLİĞİNİN İHLALİ !

Bilgi güvenliğinin ihlali ile;

- Maddi Kayıplar
- Manevi Zararlar
- İtibar Kaybı gibi olumsuz durumlar oluşur.