ESKİŞEHİR OSMANGAZİ ÜNİVERSİTESİ

BİLGİ İŞLEM DAİRE BAŞKANLIĞI

SİBER GÜVENLİK FARKINDALIK EĞİTİMİ

Siber Güvenlik Uzmanı Aytaç YILMAZ

SİBER OLAYLARA MÜDAHALE EKİBİ (SOME)

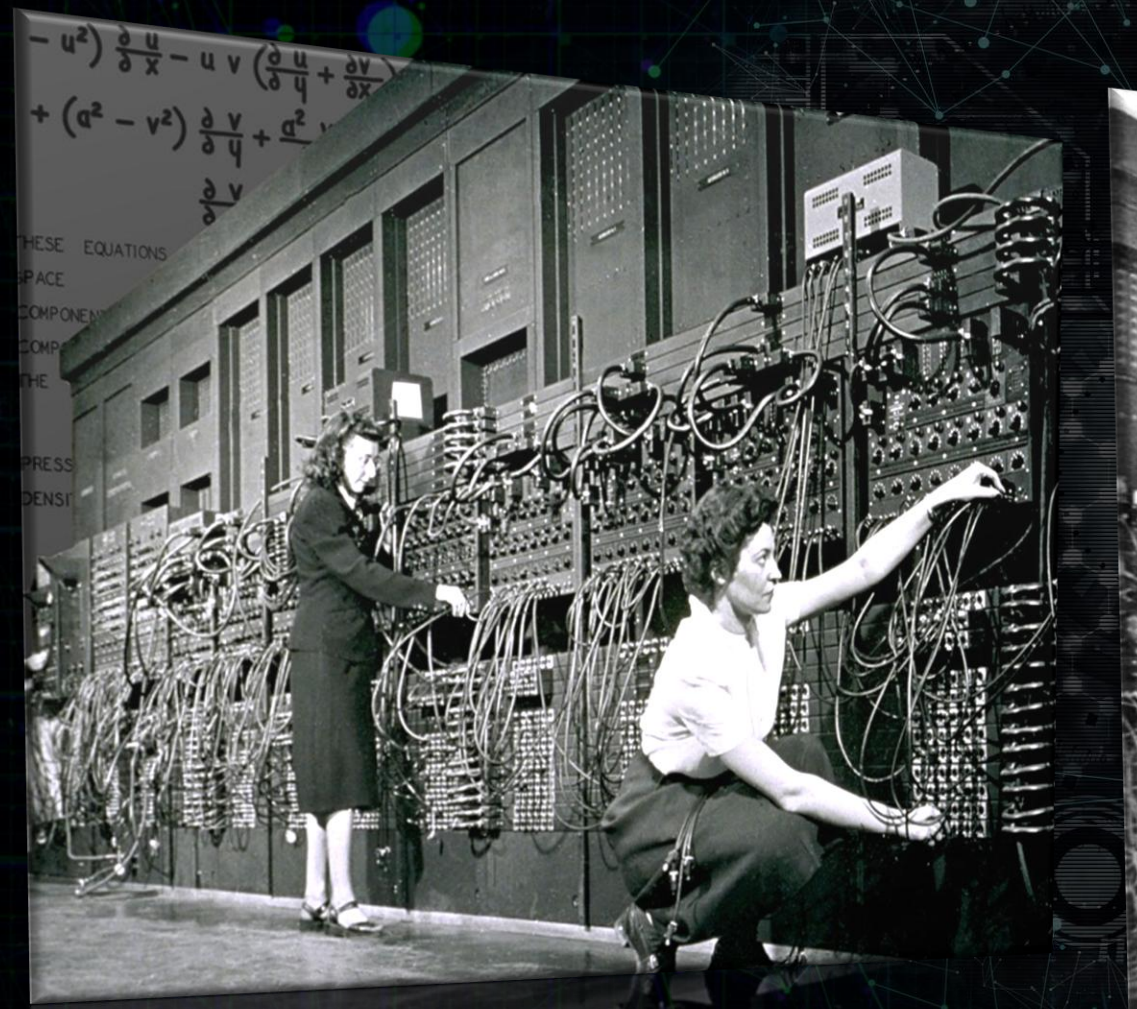
https://some.ogu.edu.tr

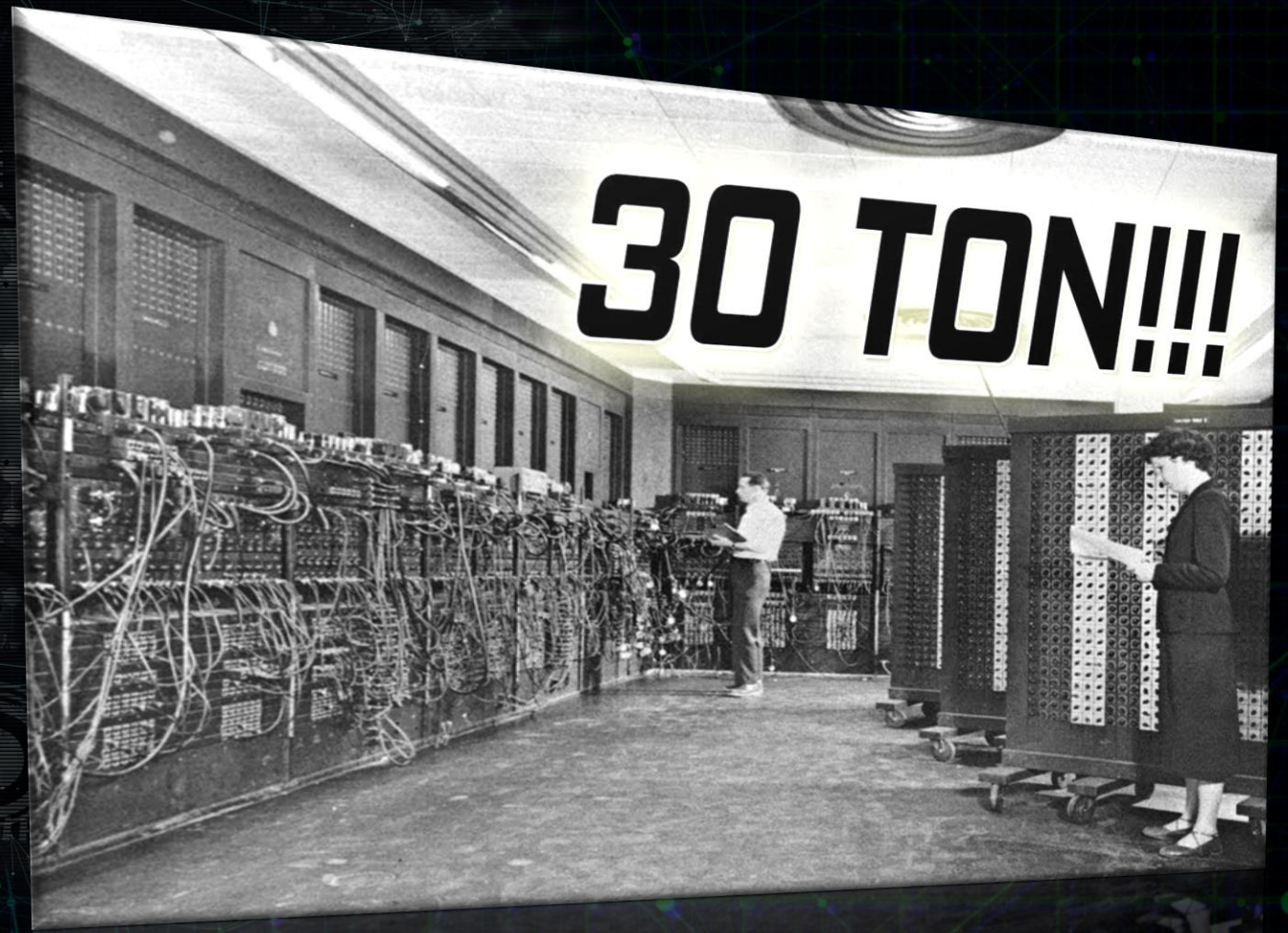
- SİBER GÜVENLİK NEDİR?
- ÜLKEMİZDE SİBER GÜVENLİK ÇALIŞMALARI
- SIKÇA KARŞILAŞILAN TEHDİTLERDEN ÖRNEKLER
- BİREYSEL SİBER GÜVENLİK ÖNLEMLERİ

SİBER GÜVENLİK NEDİR?

Dijital ortamdaki sistemleri, ağları ve verileri; izinsiz erişim, saldırı, bozulma veya çalınmaya karşı koruma sürecidir.

SİBER DÜNYAYA DOĞRU >> İLK BİLGİSAYAR ENIAC





WEB 0.0 ‘dan WEB 4.0 ’a >>

1980’ler

1990’lar

2000 ’ler

SİBER GÜVENLİK NEDİR?

Dijital ortamdaki sistemleri, ağları ve verileri; izinsiz erişim, saldırı, bozulma veya çalınmaya karşı koruma sürecidir.

SİBER GÜVENLİK NEDEN ÖNEMLİ?

- 🌐 Dünya çapında her gün milyonlarca siber saldırı gerçekleşiyor.
- 🔓 Zayıf bir parola, tüm hesabınızı ele geçirtebilir.
- 👤 Kimlik bilgileriniz kötü niyetli kişilerin eline geçebilir.
- 🏦 Kurumlar için veri sızıntısı milyarlarca TL zarara yol açabilir.
- 📱 Telefonunuzdaki bir uygulama bile sizi izliyor olabilir.

TÜRKİYE'DE SİBER GÜVENLİK

2008

İlk Siber Güvenlik Tatbikatı

2010

MGK Bildirisinde Siber Güvenlik vurgusu

2012

TÜBİTAK Siber Güvenlik Enstitüsü

2013

USOM

2013

Siber Savunma Komutanlığı

2013

Emniyet Siber Suçlarla Mücadele Daire Başkanlığı

2018

Dijital Dönüşüm Ofisi

2023

MİT Siber İstihbarat Başkanlığı

2023

Siber Güvenlik Meslek Yüksekokulları

2024

Siber Güvenlik Mühendisliği

2025

Siber Güvenlik Başkanlığı

USOM TARAFINDAN GELİŞTİRİLEN UYGULAMALARDAN BAZILARI

AVCI

Zararlı yazılım bulaşmış sistemlerin ve komuta kontrol merkezlerinin tespiti

AZAD

Makine öğrenmesi ve yapay zeka ile BotNET'lere dahil olan köle bilgisayarların belirlenmesi

KULE

Tespit edilen siber güvenlik eksikliklerine ilişkin bilgilerin ilgili taraflara iletilmesi

KASIRGA

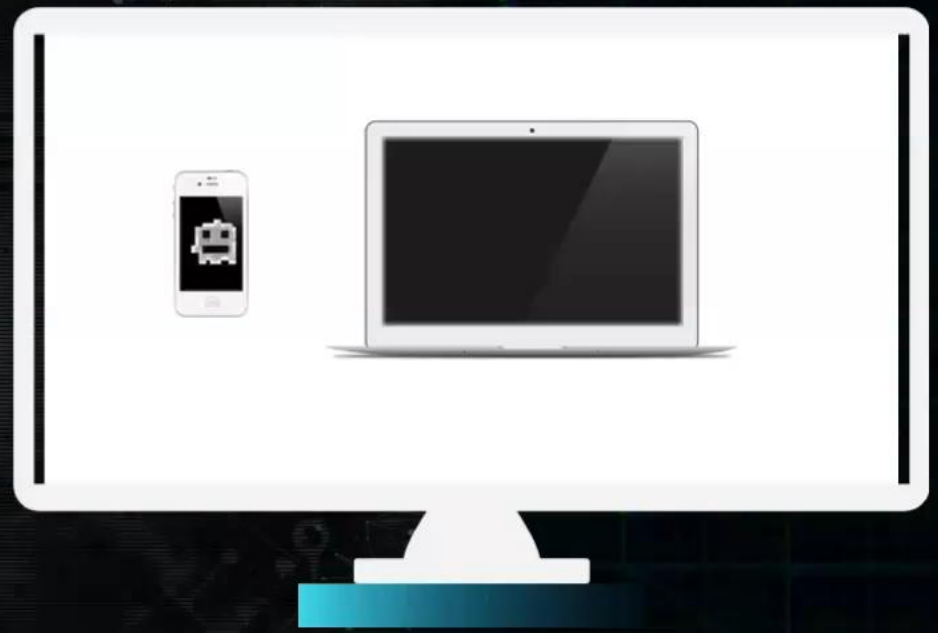
Ülkemizin internete açık kaynaklarına ilişkin zafiyet taraması ve hizmet sürekliliğinin sağlanması

ATMACA

Zafiyete ait risklerin proaktif şekilde engellenmesi

USOM
ULUSAL SİBER OLAYLARA MÜDAHALE MERKEZİ

SIKÇA KARŞILAŞILAN SİBER TEHDİTLER



KİMLİK AVI (PHISHING)
SALDIRILARI

KÖTÜ AMAÇLI YAZILIMLAR
(MALWARE)

ŞİFRE SALDIRILARI

SOSYAL
MÜHENDİSLİK

KİMLİK AVI (PHISHING) SALDIRILARI

- E-POSTA PHISHING
- SPEAR PHISHING
- SMISHING PHISHING
- VISHING

KİMLİK AVI (PHISHING) SALDIRILARI

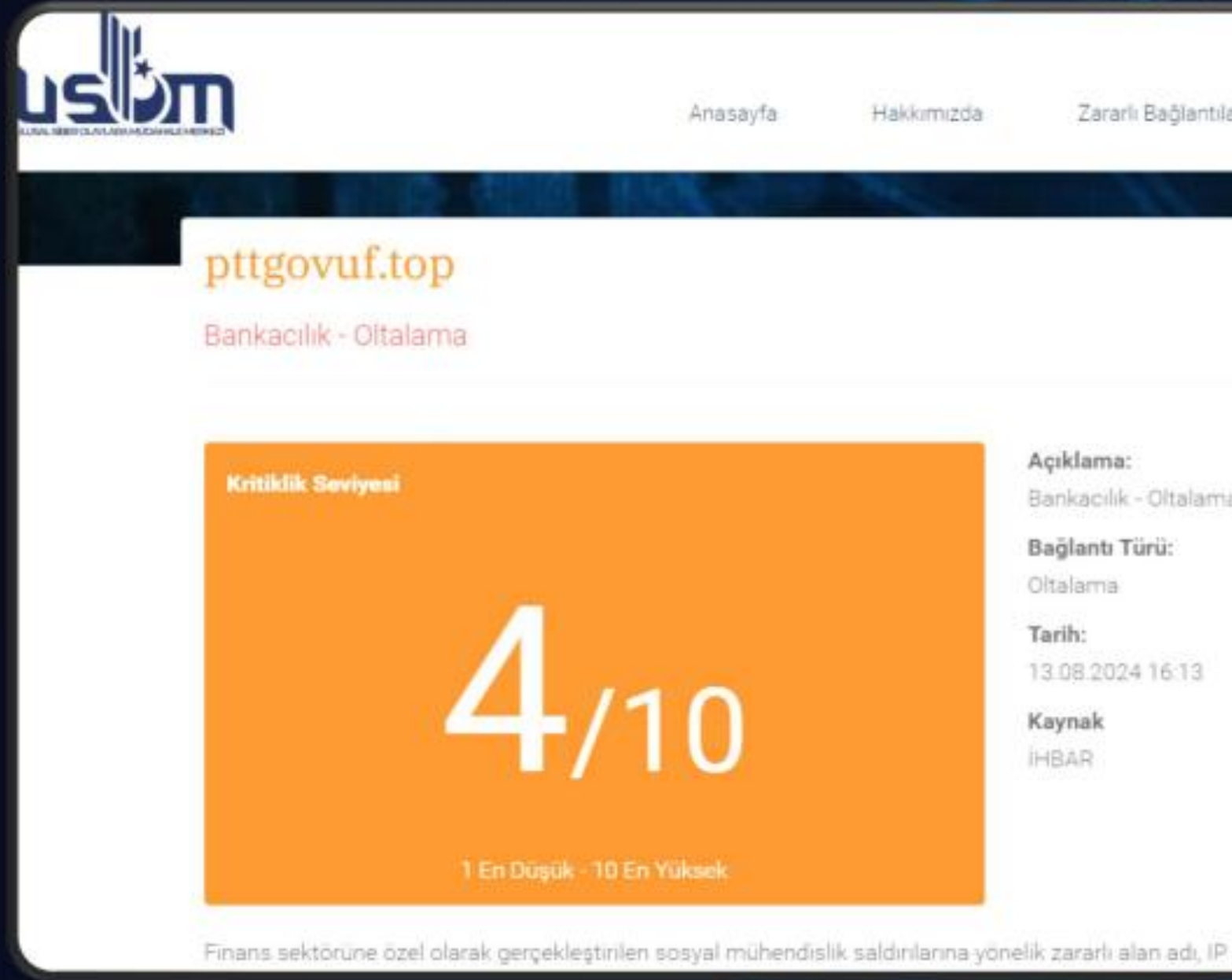
E-POSTA PHISHING>> SAHTE E-POSTALAR YOLUYLA KİŞİLERİ KANDIRARAK PAROLA, KREDİ KARTI BİLGİSİ VB. HASSAS VERİLERİ ELE GEÇİRMEYE ÇALIŞIR.

SPEAR PHISHING>> BELİRLİ BİR KİŞİYE VEYA KURUMA ÖZEL OLARAK HAZIRLANMIŞ PHISHING SALDIRISIDIR.

SMISHING PHISHING>> SMS YOLUYLA GERÇEKLEŞTİRİLEN OLTALAMA SALDIRISIDIR.

VISHING>> TELEFON ARAMALARI ÜZERİNDEN YAPILAN PHISHING SALDIRISIDIR.


13:00
4G
+855 99 829 377
[Adsız]
Mesaj - SMS
13 Ağu Sal 15:15
PTT Kargo: Paketiniz, adres nedeniyle iade edildi. Yeniden gvnderilebilmesi icin lötfen adresinizi göncelleyin. https://is.gd/pttgovuf2


Anasayfa
Hakkımızda
pttgovuf.top
Bankacılık - Oltalama
Kritiklik Seviyesi
4/10
1 En Düşük - 10 En Yüksek
Açıklama:
Bankacılık - Oltalama
Bağlantı Türü:
Oltalama
Tarih:
13.08.2024 16:13
Kaynak
İHBAR
Finans sektörüne özel olarak gerçekleştirilen sosyal mühendislik saldırılarına yönelik zararlı alan adı, IP

KÖTÜ AMAÇLI YAZILIMLAR (MALWARE)

- VIRÜSLER
- SOLUCANLAR
- TRUVA ATI (TROJAN)
- CASUS YAZILIM (SPYWARE)
- FIDYE YAZILIMI (RANSOMWARE)

KÖTÜ AMAÇLI YAZILIMLAR (MALWARE)

VIRÜSLER>> SİSTEMLERDE KENDİ KENDİNİ KOPYALAYABİLEN VE DİĞER DOSYALARA BULAŞAN ZARARLI YAZILIMLARDIR.

SOLUCANLAR>> AĞLAR ÜZERİNDEN YAYILAN, KENDİ KENDİNİ ÇOĞALTABİLEN ZARARLI YAZILIMLARDIR.

TRUVA ATI (TROJAN)>> ZARARSIZ GİBİ GÖRÜNEN AMA ARKA PLANDA KÖTÜ AMAÇLI İŞLEVLER GERÇEKLEŞTİREN YAZILIMLARDIR.

CASUS YAZILIM (SPYWARE)>> KULLANICININ HABERİ OLMADAN BİLGİLERİNİ TOPLAYAN YAZILIMLARDIR.

FIDYE YAZILIMI (RANSOMWARE)>> SİSTEM DOSYALARINI ŞİFRELEYEREK ERİŞİMİ ENGELLEYEN VE ŞİFREYI ÇÖZMEK İÇİN FİDYE İSTEYEN YAZILIMLARDIR.

ŞİFRE SALDIRILARI

- BRUTE FORCE SALDIRILARI
- CREDENTIAL STUFFING SALDIRILARI

ŞİFRE SALDIRILARI

CREDENTIAL STUFFING VS. BRUTE FORCE KARŞILAŞTIRMASI

GERÇEK KULLANICI ADI + PAROLA
(DAHA ÖNCE SIZDIRILMIŞ)

BİRÇOK HESABI HEDEFLER

BAŞARI ORANI YÜKSEKTİR
(ŞİFRE TEKRARINDAN DOLAYI)

OTOMATİZE EDİLEBİLİR
(TOPLU DENEME)

RASTGELE PAROLA TAHMİNLERİ

GENELLİKLE TEK BİR HESAP

BAŞARI ORANI DÜŞÜKTÜR

ŞİFRELERİ TAHMİN ETME

SOSYAL MÜHENDİSLİK

- MANIPÜLASYON TAKTIKLERI
- YÖNETICIYI TAKLIT ETME (CEO FRAUD)
- ACILIYET HISSI YARATMA

SOSYAL MÜHENDİSLİK MANİPÜLASYON TEKNİKLERİNDEN ÖRNEKLER

YÖNETİCİYİ TAKLİT ETME (CEO FRAUD)>> SALDIRGANIN, ŞİRKET YÖNETİCİSİ VEYA ÜST DÜZEY BİR YETKİLİ GİBİ DAVRANARAK ÇALIŞANLARI KANDIRMASI.

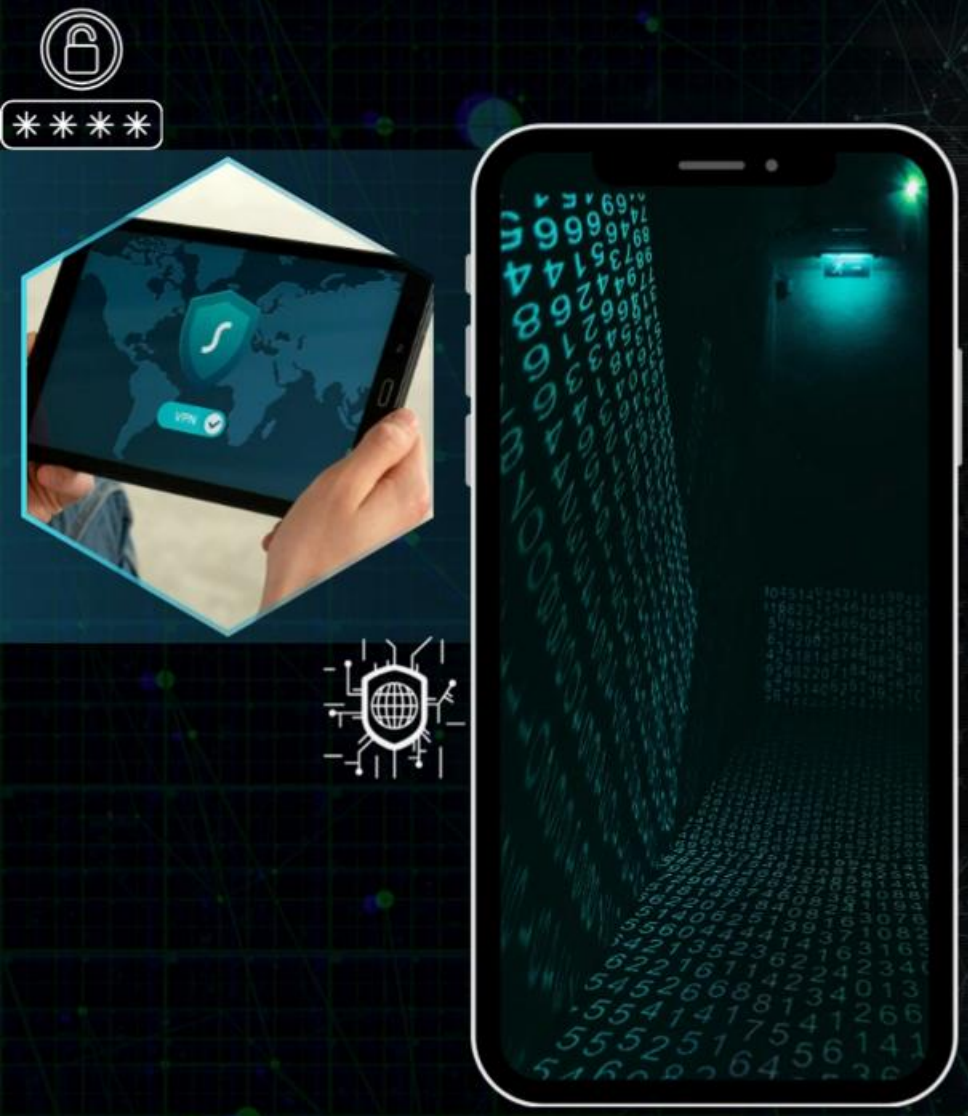
ACİLİYET HİSSİ YARATMA>> KURBANIN DÜŞÜNMEDEN HIZLI KARAR VERMESİ İÇİN BASKI KURMAK.

ÖRNEK VAKA

AVUSTURYALI BİR HAVACILIK ŞIRKETİ, CEO'SUNUN E-POSTA HESABININ TAKLİT EDİLMESİ SONUCU 50 MİLYON EURO'YU DOLANDIRICILARA GÖNDERDİ.

NASIL OLDU? DOLANDIRICILAR CEO'NUN E-POSTA ADRESİNİ TAKLİT EDİP FINANS DEPARTMANINA ACİL BİR PARA TRANSFERİ TALIMATI GÖNDERDİ. ŞİRKET, BU SAHTE TALIMATA İTİBAR ETTİ.

BİREYSEL SİBER GÜVENLİK ÖNLEMLERİ



- İKİ FAKTÖRLÜ KİMLİK DOĞRULAMA KULLANIN
- GÜÇLÜ PAROLA KULLANIN
- İŞLETİM SİSTEMLERİNİZİ VE UYGULAMALARINIZI GÜNCEL TUTUN
- GÜVENLİ BİR WI-FI AĞI KULLANIN
- BİLİNMEYEN E-POSTALARA DİKKAT EDİN VE EKLERİNİ AÇMAYIN
- SAHTE İNTERNET SİTELERİNDEN KAÇININ
- SOSYAL MÜHENDİSLİK SALDIRILARINA KARŞI DİKKATLİ OLUN
- SOSYAL MEDYA HESAPLARINIZI KORUYUN

Hesaplarınızda güvenliği sağlamanın ilk adımı güçlü bir parola oluşturmaktır.

Güçlü Parolaların Özellikleri

Uzunluk

Parolalar en az 12-16 karakter uzunluğunda olmalıdır. Uzun parolalar, tahmin edilmesi zor olduğu için daha güvenlidir.

Karmaşıklık

Büyük harf, küçük harf, rakam ve özel karakterler (örn. !, @, #, $, %) içermelidir. Bu, parolanın gücünü artırır.

Tekrarlanmaması

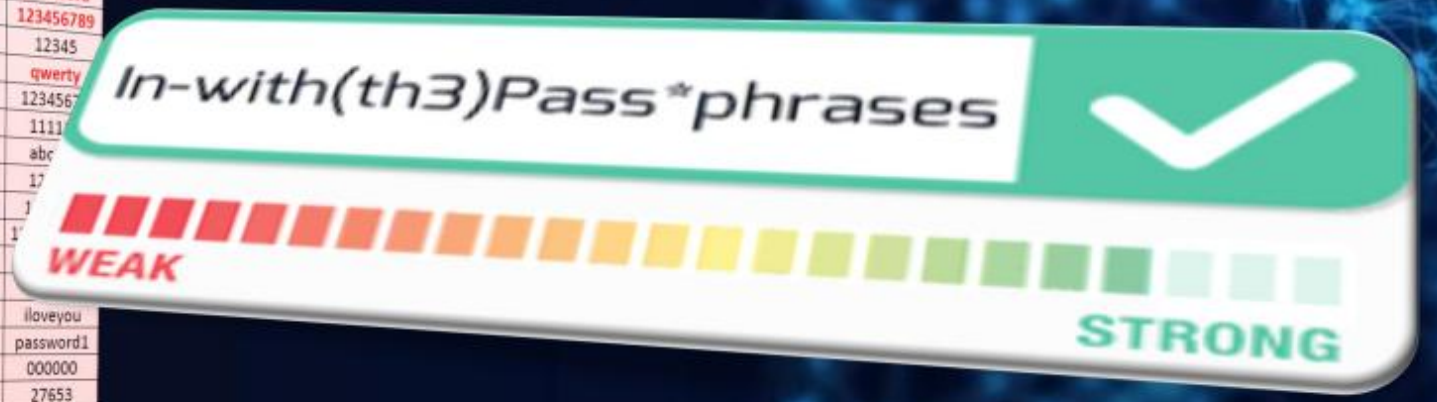
Aynı parolayı birden fazla hesapta kullanmaktan kaçınılmalıdır. Bir hesapta meydana gelen bir ihlal, diğer hesapların da tehlikeye girmesine yol açabilir.

Tahmin Edilemezlik

Kişisel bilgiler (doğum tarihi, ad vb.) içermemelidir. Saldırganlar bu bilgileri kolayca tahmin edebilir.

Sızdırılan 15 milyon parola arasında en çok kullanılanlar

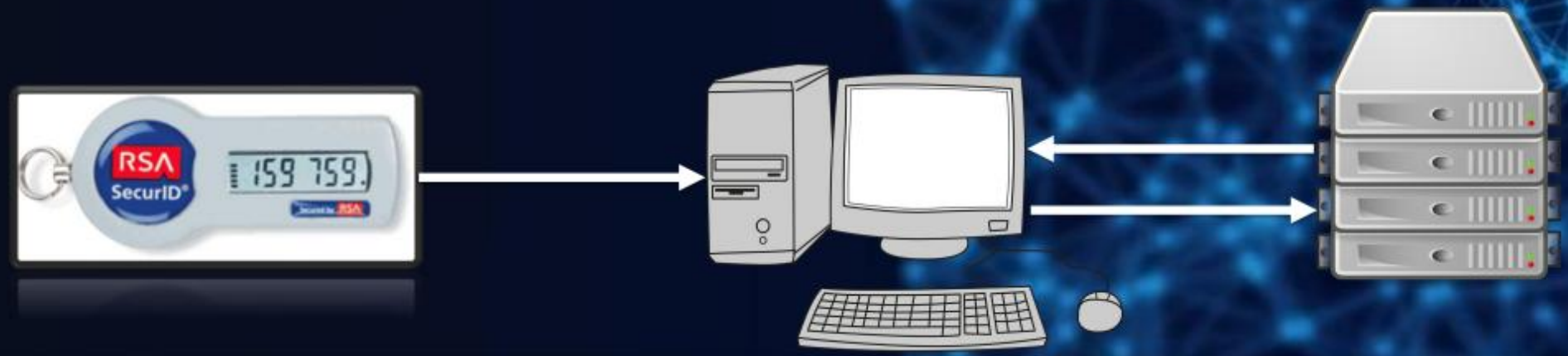
No	Sayısı (gmail?)	Parola	No	Sayısı (yandex,mail.ru?)	Parola
1	112951	qwerty	1	47779	123456
2	47986	123456	2	11524	password
3	37672	qwertyuiop	3	11145	123456789
4	29197	qwe123	4	8083	12345
5	9132	klaster	5	5908	qwerty
6	7893	qweqwe	6	5241	123456
7	7393	1qaz2wsx	7	3515	1111
8	6940	1q2w3e4r	8	3008	abc
9	6893	qazwsx	9	2968	1
10	4223	123qwe	10	2904	1
11	4166	1q2w3e	11	2706	1
12	4029	123456789	12	2411	
13	3991	1q2w3e4r5t	13	1983	
14	3489	zxcvbnm	14	1973	iloveyou
15	3098	qwer1234	15	1852	password1
16	3000	111111	16	1742	000000
17	2741	1234qwer	17	1722	27653
18	2120	asdfgh	18	1538	zaq12wsx
19	1739	marina	19	1534	tinkle
20	1731	q1w2e3r4t5	20	1514	qwerty123



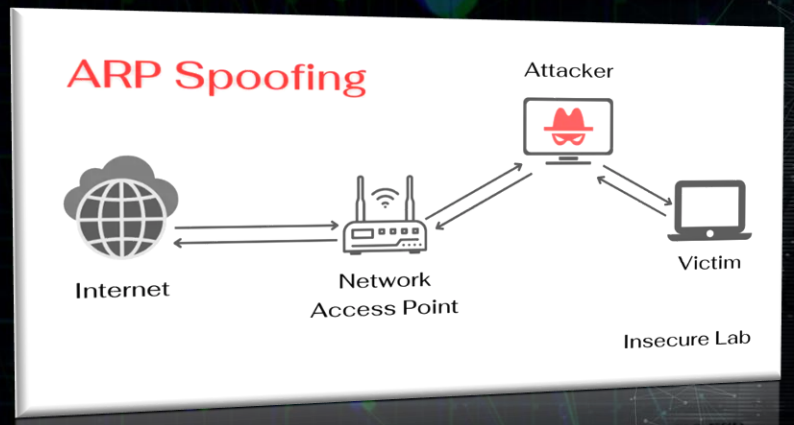
İki Faktörlü Kimlik Doğrulama (2FA)

İki faktörlü kimlik doğrulama, bir hesaba giriş yaparken yalnızca parolanızı kullanmak yerine, ikinci bir kimlik doğrulama katmanı ekleyen bir güvenlik yöntemidir. Bu, genellikle telefonunuza gönderilen bir kod veya bir uygulama üzerinden oluşturulan bir kod ile gerçekleştirilir.

SMS, e-posta veya kimlik doğrulama uygulamaları (örn. Google ve Microsoft Authenticator, Authy) gibi farklı yöntemler ile iki faktörlü kimlik doğrulama uygulanabilir.
(2FA'nın en büyük avantajı; parolalar çalınsa bile, ikinci faktör olmadan hesaba erişim mümkün olmaz.)



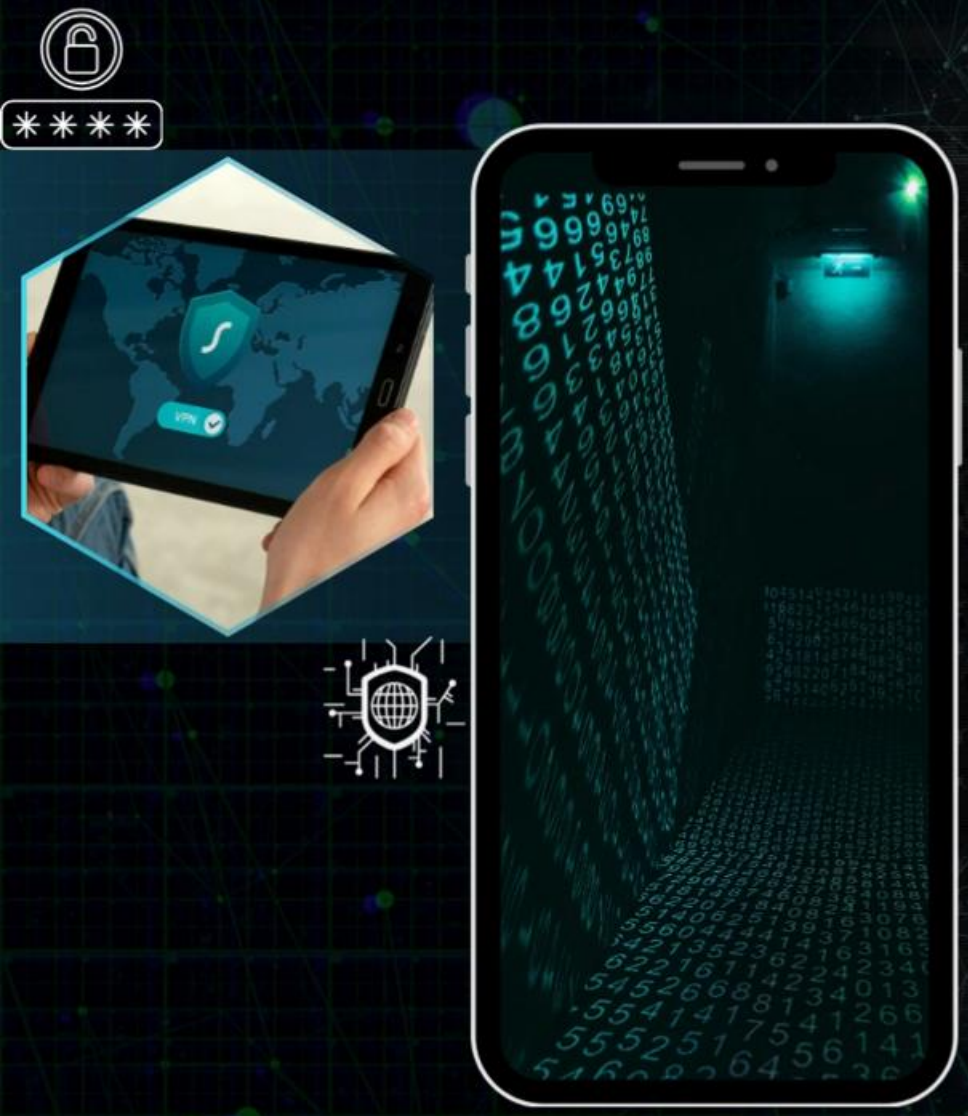
NEDEN GÜVENLİ OLMAYAN Wi-Fi AĞLARINDAN UZAK DURMALIYIZ!!!



MitM saldırıları, saldırganın iletişimdeki iki taraf arasında gizlice veri alışverişini dinlemesidir. Bu sayede saldırgan, bilgileri çalabilir veya manipüle edebilir.

```
Interface: 192.168.43.65 --- 0x16
  Internet Address      Physical Address      Type
  192.168.43.1          08-00-27-89-03-db     dynamic
  192.168.43.220        08-00-27-89-03-db     dynamic
  192.168.43.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Halka açık ve güvenli olmayan bir Wi-Fi ağı üzerinden gerçekleştirilen bir saldırıda, bir kullanıcı bu ağda oturum açtığında, saldırgan kullanıcı ile sunucu arasındaki veriyi dinleyebilmektedir.



- İKİ FAKTÖRLÜ KİMLİK DOĞRULAMA KULLANIN
- GÜÇLÜ PAROLA KULLANIN
- İŞLETİM SİSTEMLERİNİZİ VE UYGULAMALARINIZI GÜNCEL TUTUN
- GÜVENLİ BİR WI-FI AĞI KULLANIN
- BİLİNMEYEN E-POSTALARA DİKKAT EDİN VE EKLERİNİ AÇMAYIN
- SAHTE İNTERNET SİTELERİNDEN KAÇININ
- SOSYAL MÜHENDİSLİK SALDIRILARINA KARŞI DİKKATLİ OLUN
- SOSYAL MEDYA HESAPLARINIZI KORUYUN

UNUTMAYIN! EN ZAYIF HALKA ÇOĞU ZAMAN "İNSAN" DIR.

BİLİNÇLİ KULLANICI OLUN, DİJİTAL DÜNYADA KENDİNİZİ KORUYUN. 🛡️

TEŞEKKÜRLER...

https://some.ogu.edu.tr