MARMARA ÜNİVERSİTESİ

BİLGİ İŞLEM DAİRE BAŞKANLIĞI

Bilgi Güvenliği Farkındalık Eğitimi

ÖZNUR ÖZÇELİK

2023

Bilgi Güvenliği

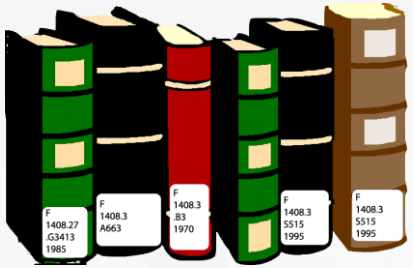
Bilgi Nedir?

* **Bilgi**, verinin (Kişisel Veri de dahil) işlenmiş şeklidir.
* **Bilgi**, kopyalanabilir ve taşınabilirdir.

Bilgi Gizlilik Sınıfları		
Gizli	**Hizmete Özel**	**Genel**
Yetkisiz kişi, kurum ya da kuruluşlarla paylaşılması ya da kaybolması durumunda Kurum'un operasyonları, saygınlığı, imajı etkilenir, finansal kayıp yaşanır, yasal soruşturma ya da incelemeye neden olabilir, başkalarına geniş yararlar sağlayabilir. 24.Mart.2016 tarih ve 6698 numaralı Kişisel Verilerin Korunması Kanunu kapsamında tanımlanan kişisel veriler gizli sınıfındadır.	Kurum içinde ve tedarikçilerle, belirli bir sürecin yürütülebilmesi kapsamında paylaşılabilen, izinsiz paylaşılması ya da kaybolması durumunda kuruluş için önemli etki ya da zarara neden olmayacak verilerdir. Varlık sahibinin yazılı onayı olmadan alt gizlilik sınıflarına indirilemez.	Geneli ilgilendiren, en düşük güvenlik seviyesindeki bilgilerdir. İşlenmesi sırasında risk oluşmaz. İzinsiz açıklanmasında ya da dağıtılmasında, Kurum içine ya da dışına paylaşılmasında herhangi bir kısıtlama yoktur.

Hangi Bilgi Bu Kapsamda?

- Sunucularda,
- Kablosuz ağlarda,
- Bilgisayarlarda,
- Veritabanlarında,
- Telefon konuşmalarında,
- Yazıcılarda,
- Basılı dokümanlarda,
- Masalarda / dolaplarda,
- Kurum çalışanlarının zihinlerinde bulunur.



Bilgi Güvenliği

* Bilgi Güvenliği, bilgi varlıklarının, gizliliğini, bütünlüğünü ve erişilebilirliğini korumayı amaçlayan çalışma alanıdır.

Bilginin Gizliliği

Bilgiye, yalnızca yetkisi olan kişiler erişmelidir.
Bilgiye, yetkisi olan kişiler yetkisi süresince erişmelidir.

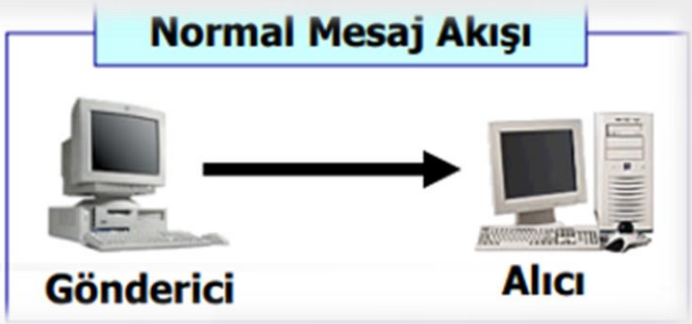
Bilginin Bütünlüğü

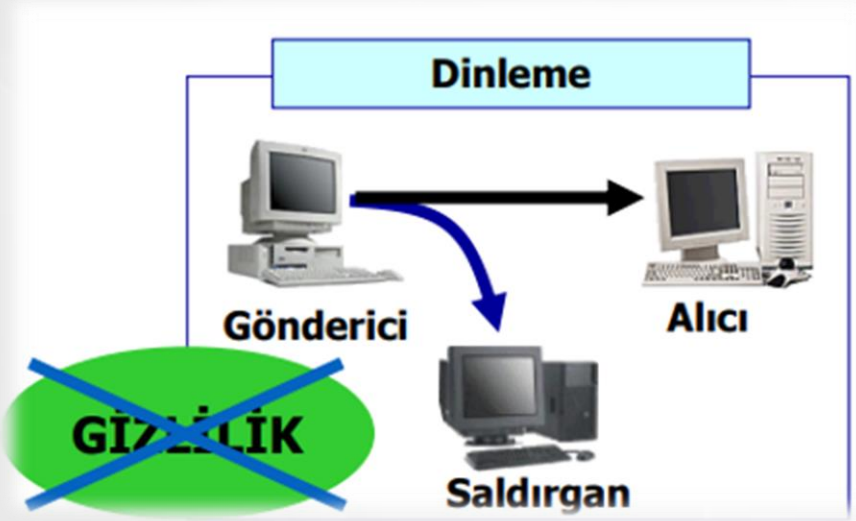
Bilgi yalnızca yetkisi olan kişiler tarafından değiştirilebilmelidir. Bilgi her zaman kullanılabilir ve doğru olmalıdır.

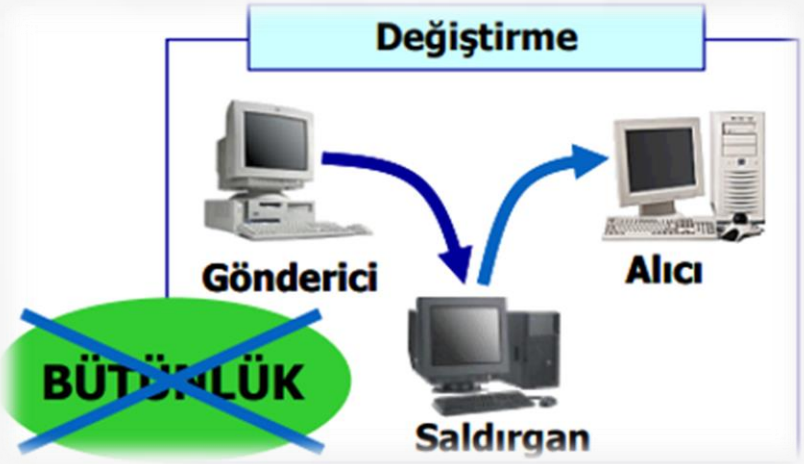
Bilginin Erişilebilirliği

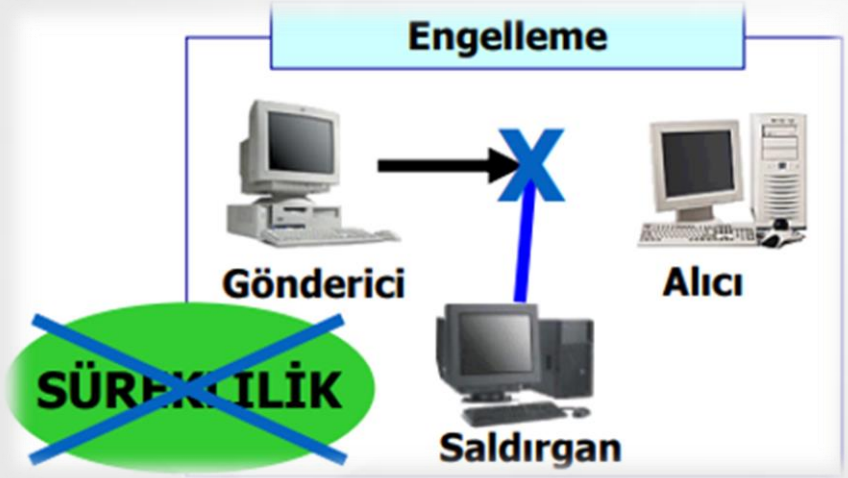
Erişilmesi gereken bilgi her zaman erişilebilir olmalıdır.

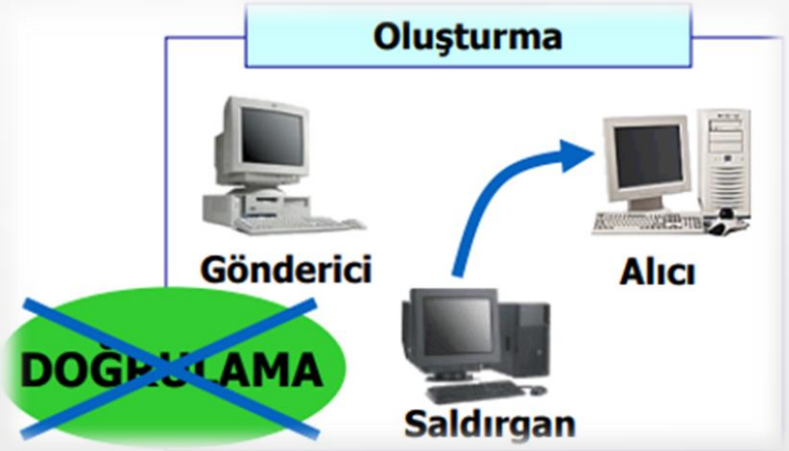
Bilgi Güvenliği











Bilgi Güvenliği

- BG sadece Bilgi Teknolojilerini ilgilendirmez!
- Kendi kendini uygulayamaz ve zaman geçtikçe güncellenmesi gerekir!
- Sadece İdari yada Teknik bir politika değildir!
- Başta yönetim kurulunun, ardından personelin katkısı gerekir.
- Personele, yaptıkları iş kadar, iş yapış yöntemlerinin ve işledikleri bilginin değerini fark ettirir.
- Kurumu, bilgi kaybı nedeni ile uğrayacağı zarardan korur.
- Riskleri sıfıra indirmez, yönetilebilir kılar.
- Toplam kalitenin artmasına neden olur.

Bilgi Güvenliği Tehdit Kaynakları

İç Tehditler

- Bilgisiz ve bilinçsiz kullanıcılar
- Kötü niyetli çalışanlar

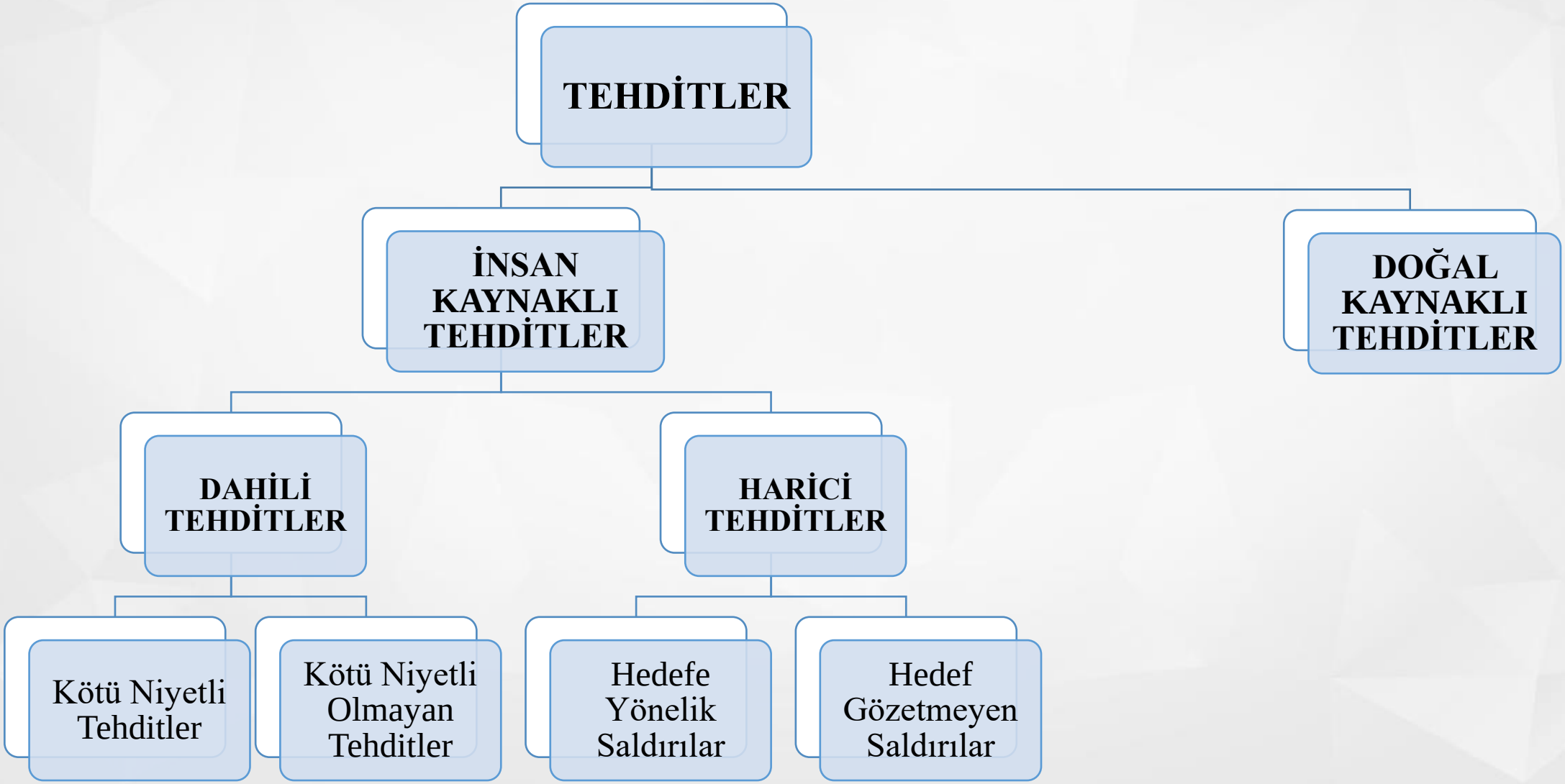
% 80

% 20

Dış Tehditler

- Meraklılar, genç kuşak saldırganlar
- Profesyonel suçlular
- Endüstri ve teknoloji casusları
- Dış ülke yönetimleri

Bilgi Güvenliği Tehdit Kaynakları



Bilgi Güvenliği Tehdit Kaynakları

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.

Bilgi Güvenliği Tehdit Kaynakları

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),
- Worm Saldırıları (Code Red, Nimda),
- Trojan Arka Kapıları (Netbus, Subseven, Black Orifice).

!

Güvenliğin sadece küçük bir kısmı teknik güvenlik önlemleri ile sağlanır.

Büyük kısım ise kullanıcıya bağlıdır.

‘Ve zincir en zayıf halkası kadar güçlüdür.’

Bilgi Güvenliği Adına Alınacak Tedbirler

Personel Farkındalığının Önemi

- Bilgi güvenliğinin en önemli parçası kullanıcı güvenlik bilincidir.
- Oluşan güvenlik açıklıklarının büyük kısmı kullanıcı hatasından kaynaklanmaktadır.
- Saldırganlar (Hacker) çoğunlukla kullanıcı hatalarını kullanmaktadır.
- Bir kullanıcının güvenlik ihlali tüm sistemi etkileyebilir. KVKK için bütün üniversiteyi sorumlu kılabilir.
- Teknik önlemler kullanıcı hatalarını önlemede yetersiz kalmaktadır.
- Kullanıcılar tarafından dikkat edilmesi gereken kurallar sistemlerin güvenliğinin sağlanmasında kritik bir öneme sahiptir.

!

Kurum personeli Bilgi Güvenliğini bilmelidir!

Kurum personeli KVKK’yı bilmelidir!

Personelden Beklenen

Fiziksel Güvenlik

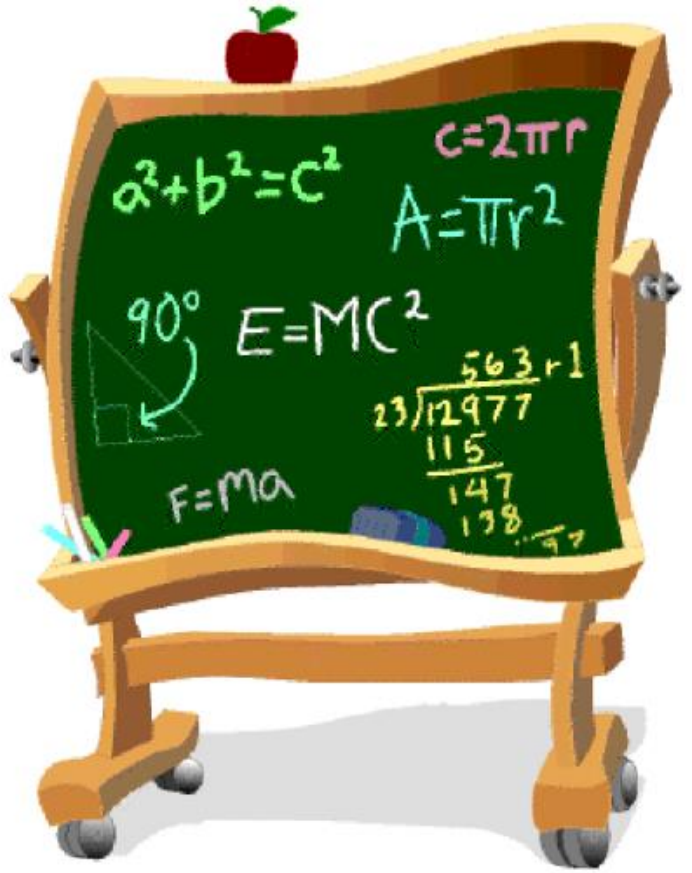
- Bina/ofislerin korunması
- Kilitler
- BT bileşenlerinin korunması
- Güvenlik görevlisi
- Kapı giriş sistemleri

Personelden Beklenen - Fiziksel Güvenlik

Çalışma ortamı temizliği (Temiz Masa İlkesi)

Personelden Beklenen - Fiziksel Güvenlik

Toplantı odalarında döküman bırakılmamalı, tahta silinmelidir.



Çalışma ortamı temizliği (Temiz Masa İlkesi)

Personelden Beklenen - Fiziksel Güvenlik

- Çalışma saatleri dışında bilgisayarlar kapalı ya da otomatik parola koruma ekranı (5dk) şekilde bırakılmalıdır. Çalışma saatleri içerisinde başından ayrıldığında mutlaka bilgisayar kilitli bırakılmalıdır. (WİNDOWS+L)
- Kuruma ait gizli dokümanlar etiketli ve kilitli ortamda tutulmalıdır.
- Gizlilik dereceli evraklar, işlevini tamamladıktan sonra imha edilmelidir.
- Gelen ve giden mesaj notları ve yazıcılar başıboş olarak bırakılmamalıdır.

Personelden Beklenen - Fiziksel Güvenlik

- Kuruma ait antetli kağıtlar kilitli dolaplarda tutulmalıdır.
- Bilgisayarların masaüstlerinde kuruma ait özel bilgiler içeren dokümanlar bulundurulmamalıdır.
- Bilgisayarlara ait olan şifreler kesinlikle kağıt ortamlara yazılı bir şekilde bırakılmamalıdır.
- Ofis ve çalışma ortamlarında bulunan başı boş USB/CD gibi medyalar, bilgisayarlara takılmamalıdır. Gerekli yerlere teslim edilmelidir.

Personelden Beklenen - Fiziksel Güvenlik

Donanım ve Yazılım Kurulması

- İlgili ekipman güvenlik açığına sebep olabilir.
- İlgili ekipman mevcut sistemin çalışmamasına sebep olabilir.
- Kopya ve lisanssız ise hukuki problem oluşturabilir.
- İnternetten indirilmiş ise virüs taşıyor olabilir.
- Mevcut sistemle uyuşmuyor olabilir.

Personelden Beklenen - Fiziksel Güvenlik

Parola belirleme

- En az 8 karakterden oluşmalı.
- Büyük harf, küçük harf, rakam ve özel karakterler içermeli.
- Harflerle oluşmuş kısmı anlamlı sözcükler içermemeli.
- Düzenli olarak değişmeli.
- Başkaları ile paylaşılmamalı.
- Rahat erişebilir yerde saklanmamalı.
- Kolay tahmin edilir olmamalı.

Kelimeler üzerinde bariz olan değişikliklerden kaçının: Eğer parolanız **m3r7c4n** tarzı bir parolaysa, hemen değiştirin. Bir kelime üzerinde yapılan bu şekilde bariz değişiklikleri emin olun size saldıranlar da düşünüyorlar.

!

Personelden Beklenen - Fiziksel Güvenlik

Parola belirleme

123qwe	123QweAsd
qwe123	asd12345
123qweasd	Asd123
qwer1234	Qwerty123
qweasd	qazwsx123

!

Kelimeler üzerinde bariz olan değişikliklerden kaçının: Eğer parolanız **m3r7c4n** tarzı bir parolaysa, hemen değiştirin. Bir kelime üzerinde yapılan bu şekilde bariz değişiklikleri emin olun size saldıranlar da düşünüyorlar.

!

Personelden Beklenen - Fiziksel Güvenlik

* Günlük hayatınızdan kolay hatırlayacağınız herhangi bir cümle kullanabilirsiniz (atasözlerinden, şarkı sözlerinden, şiirlerden vb.)

* 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
* Mezuniyet tarihim 1998 yılının 4. ayıdır. --> Mt98y4.a

!

Zararlı Yazılımlar

- Zararlı yazılımlar, trojan, virüs, malware, spyware ve wormler için kullanılan genel bir terim olmakla beraber bir bilgisayara üzerinde bulunan verileri çalmak ya da yok etmek gibi amaçları olan yazılım türleridir.
- Zararlı yazılımlardan uzak durmak adına kaynağı bilinmeyen linklere tıklamamak, ekleri açmamak, güncel bir firewall kullanmak ve işletim sistemini her daim güncel tutmak gerekir.
- Bilgi Güvenliği için gerçek ve kesin bir tehdit oluştururlar.
- Nasıl bulaşır ?
  - İnternet yada ağ üzerinden,
  - USB bellek yada harici disklerden,
  - Korsan \ Lisanssız yazılım CD lerinden,
  - E-Posta yoluyla.

E-Posta Kullanımında Güvenlik

- Virüslerin en fazla yayıldığı ortam e-postalardır.
- Kaynağı tanınmayan e-postalar kesinlikle açılmamalıdır.
- Güvenilmeyen eklentiler açılmamalıdır.
- Gizli bilgi şifrelenmedikçe e-postalarla gönderilmemelidir.
- Spam e-postalara cevap verilmemelidir.
- E-posta adres bilgisi güvenilir kaynaklara verilmelidir.
- E-posta kötü niyetli kişiler için '**reklam ve kötü niyetli yazılımları yayma yolu**'dur.

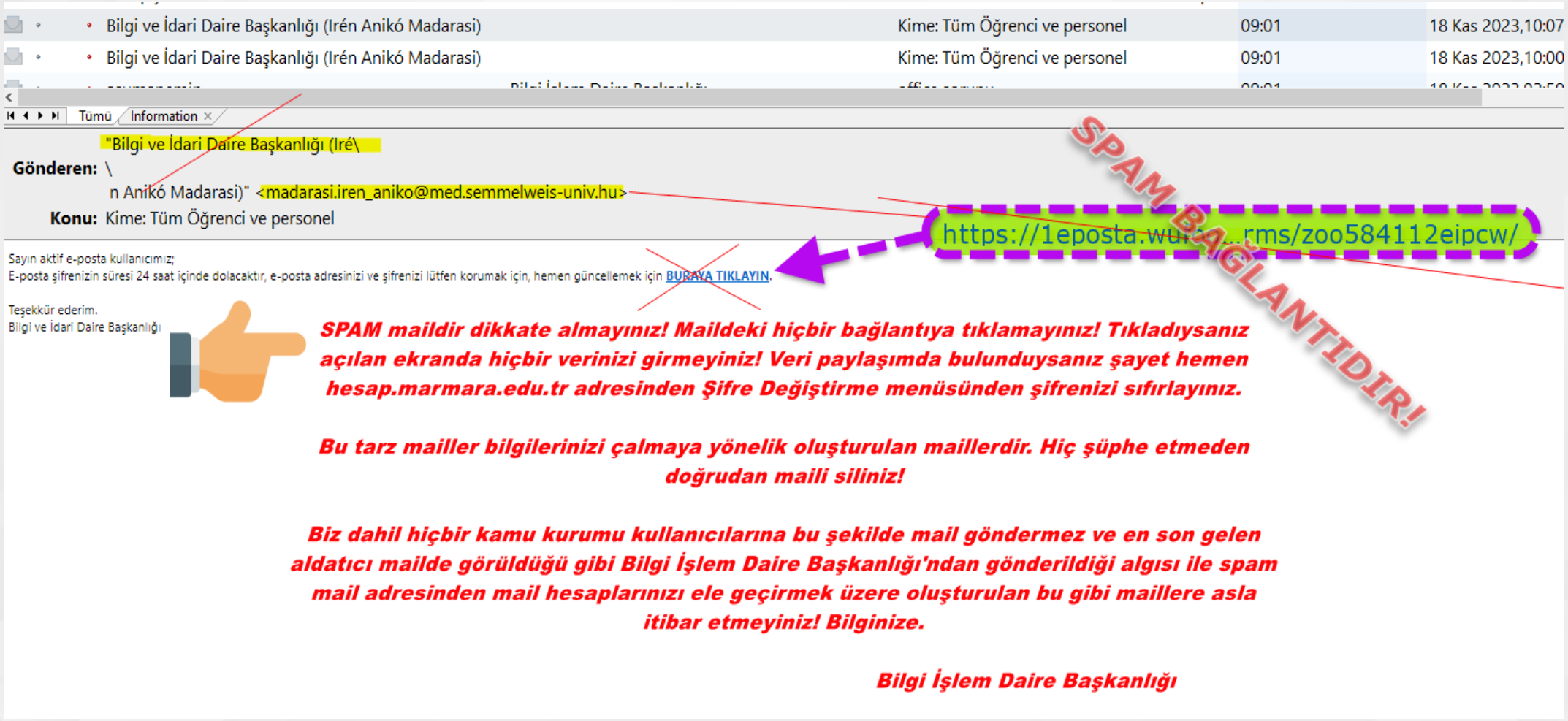
E-Posta Kullanımında Güvenlik

- 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.

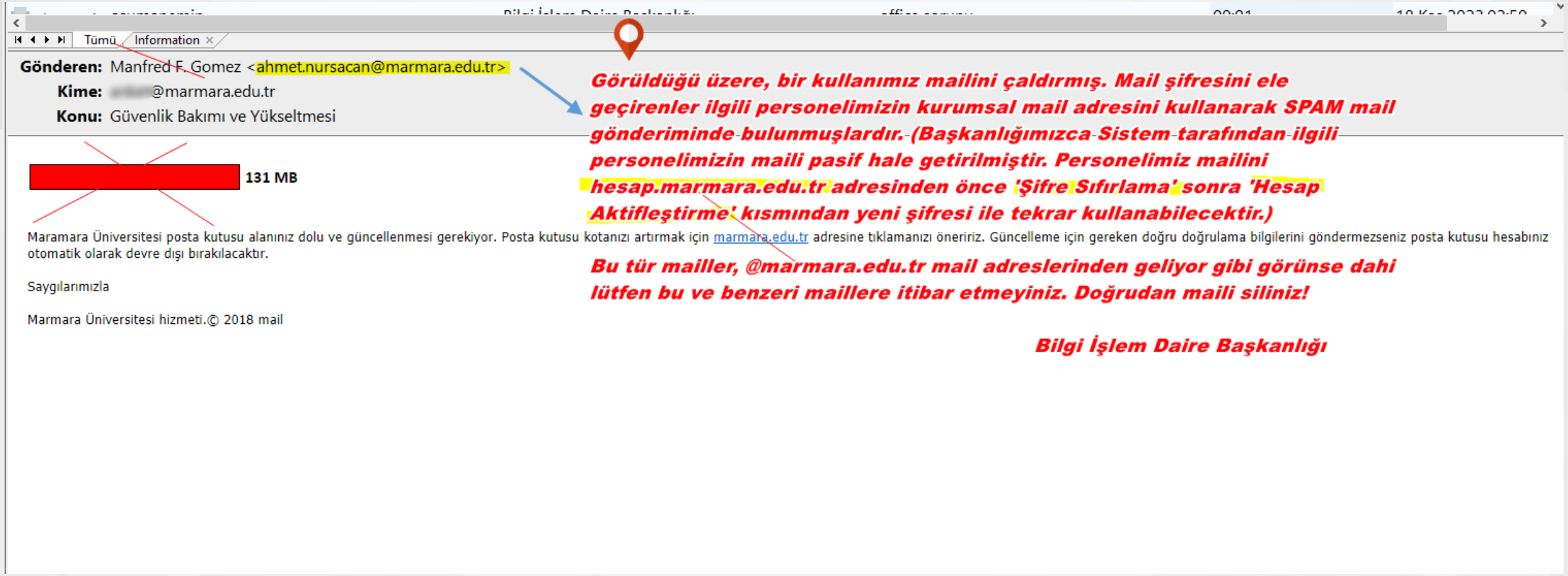
Phishing

* Pishing e-postaları içerisinde kötü niyetli bir link ya da döküman barındırır ve kullanıcıların bilgilerini çalmayı hedefler.
* Genelde **panik** gibi duygulara dayandırılarak hazırlandığından ve kullanıcının düşünmeden tepki vermesi için düşünülmüştür.
* Bu tip e-postalara içeriğini inceleyerek ve şüpheyle yaklaşarak bakmakta fayda var.

Phishing

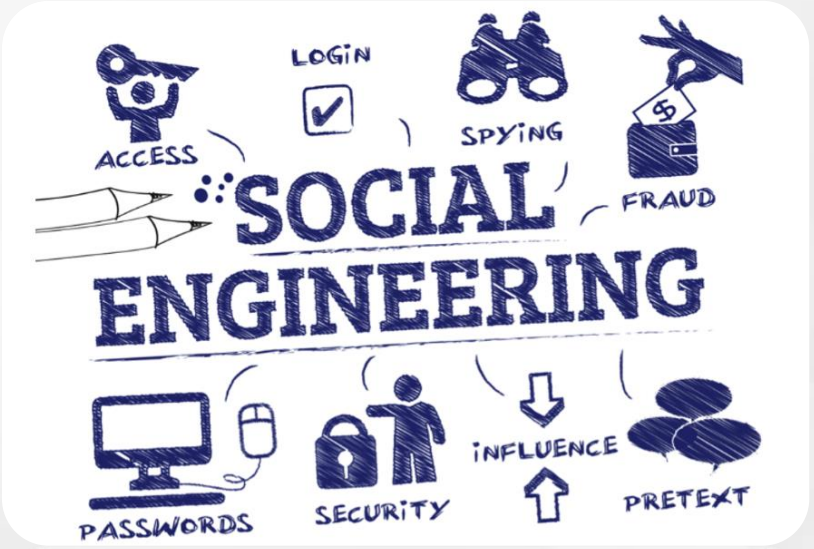

Bilgi ve İdari Daire Başkanlığı (Irén Anikó Madarasi) Kime: Tüm Öğrenci ve personel 09:01 18 Kas 2023,10:07
Bilgi ve İdari Daire Başkanlığı (Irén Anikó Madarasi) Kime: Tüm Öğrenci ve personel 09:01 18 Kas 2023,10:00
Tümü
Information
"Bilgi ve İdari Daire Başkanlığı (Iré\
Gönderen: \
n Anikó Madarasi)" <madarasi.iren_aniko@med.semmelweis-univ.hu>
Konu: Kime: Tüm Öğrenci ve personel
Sayın aktif e-posta kullanıcımız;
E-posta şifrenizin süresi 24 saat içinde dolacaktır, e-posta adresinizi ve şifrenizi lütfen korumak için, hemen güncellemek için BURAYA TIKLAYIN.
Teşekkür ederim.
Bilgi ve İdari Daire Başkanlığı
https://1eposta.wu...rms/zoo584112eipcw/
SPAM BAĞLANTIDIR!
SPAM maildir dikkate almayınız! Maildeki hiçbir bağlantıya tıklamayınız! Tıkladıysanız açılan ekranda hiçbir verinizi girmeyiniz! Veri paylaşımda bulunduysanız şayet hemen hesap.marmara.edu.tr adresinden Şifre Değiştirme menüsünden şifrenizi sıfırlayınız.
Bu tarz mailler bilgilerinizi çalmaya yönelik oluşturulan maillerdir. Hiç şüphe etmeden doğrudan maili siliniz!
Biz dahil hiçbir kamu kurumu kullanıcılarına bu şekilde mail göndermez ve en son gelen aldatıcı mailde görüldüğü gibi Bilgi İşlem Daire Başkanlığı'ndan gönderildiği algısı ile spam mail adresinden mail hesaplarınızı ele geçirmek üzere oluşturulan bu gibi maillere asla itibar etmeyiniz! Bilginize.
Bilgi İşlem Daire Başkanlığı

Phishing


Tümü
Information
Gönderen: Manfred F. Gomez <ahmet.nursacan@marmara.edu.tr>
Kime: @marmara.edu.tr
Konu: Güvenlik Bakımı ve Yükseltmesi
131 MB
Maramara Üniversitesi posta kutusu alanınız dolu ve güncellenmesi gerekiyor. Posta kutusu kotanızı artırmak için marmara.edu.tr adresine tıklamanızı öneririz. Güncelleme için gereken doğru doğrulama bilgilerini göndermezseniz posta kutusu hesabınız otomatik olarak devre dışı bırakılacaktır.
Saygılarımızla
Marmara Üniversitesi hizmeti.© 2018 mail
Görüldüğü üzere, bir kullanımız mailini çaldırmış. Mail şifresini ele geçirenler ilgili personelimizin kurumsal mail adresini kullanarak SPAM mail gönderiminde bulunmuşlardır. (Başkanlığımızca Sistem tarafından ilgili personelimizin maili pasif hale getirilmiştir. Personelimiz mailini hesap.marmara.edu.tr adresinden önce 'Şifre Sıfırlama' sonra 'Hesap Aktifleştirme' kısmından yeni şifresi ile tekrar kullanabilecektir.)
Bu tür mailler, @marmara.edu.tr mail adreslerinden geliyor gibi görünse dahi lütfen bu ve benzeri maillere itibar etmeyiniz. Doğrudan maili siliniz!
Bilgi İşlem Daire Başkanlığı

Sosyal Mühendislik Yöntemleri

- Sistem ve bilgiler üzerinde izinsiz erişim sağlayabilmek için insanların aldatılma yada hilekarlıkla kullanılmasıdır.
- Yardımcı olmaya istekli olma, başkalarına güvenme ve zor durumda kalmak istememe gibi zaaflarımızdan yararlanırlar.
- **Amaç**, dolandırıcılık, sistemlere erişmek, endüstriyel casusluk, kimlik hırsızlığı, sistemleri bozmak için gereken bilgiyi elde etmek.
- <u>Sosyal Mühendislik örnekleri:</u>
  - Bilgi almak için masum sebepler.
  - Güven sağlayıcı bilgiler vermek .
  - İşe yeni başlayan personel potansiyel açıktır!
  - Güvenliğin önemini vurgulayarak güven kazanma.
  - Üst yönetim kandırmacası.
  - Yardım isteme.
  - Yardım talep ettirme.



Sosyal Mühendislik Yöntemleri

- Bilgisayardan uzaklaştığınızda her zaman bilgisayar programlarındaki **oturumunuzu kapatın ve parolalı bir ekran koruyucu** kullanın. Aynı durum cep telefonları için de geçerlidir.

- Parolalarınızı hiçbir zaman başkalarıyla paylaşmayın. Ayrıca parolalarınızı **sık sık değiştirmeyi** unutmayın! Bu çok önemlidir.

- Katılmayı planladığınız etkinlikleri gösteren **çevrimiçi takvimleri ve seyahat programlarını** sosyal ağınızda olsa bile silin veya özel hale getirin. Güvendiğiniz kişilerin dışındakiler ile çevrimiçi paylaşımınızı sınırlamak için tüm çevrimiçi hesaplarınızda **gizlilik ayarlarını** kullanın.

Sosyal Mühendislik Yöntemleri

From: Bilgi İşlem <office365@micrsoft.com.tr>
Sent: Thursday, August 31, 2023 4:15 PM
To: [redacted]@marmara.edu.tr
Subject: Office 365 Kullanımı

Bu adres SPAM mail adresidir. Dikkat! Bu tarz mailler, Microsoft Firması mail adreslerinden geliyor dahi olsa bu ve benzeri içerikteki mailleri dikkate almayınız. SPAM MAİLDİR. Kesinlikle bilgilerinizi girmeyip, maili direkt siliniz.

office365@micrsoft.com.tr de "o" eksik dikkat ederseniz. "microsoft" doğrusu.

Gönderen mail adresine dikkat ediniz.

Microsoft | Microsoft 365

Sayın [redacted]

Office 365 Eğitim hizmetine **kesintisiz** devam edebilmek için , **01.09.2023 tarihine kadar** kullanıcı bilginiz ile aşağıdaki sayfaya giriş sağlayın.

Kaydolmak İçin Tıklayınız

Tıklamayınız! Bilgilerinizi girmeyiniz!

Microsoft Hesap Ekibi

Bir okul e-posta adresiyle kaydolduğunuzdan okulunuz Office 365 iletişimlerinizi v

Bu, zorunlu bir hizmet yazışmasıdır.
Bu ileti, takip edilmeyen bir e-posta adresinden gönderildi. Lütfen bu iletiyi yanıtlamayın.
Gizlilik | Yasal
Microsoft Office
One Microsoft Way
Redmond, WA
98052-6399 ABD

Bu eposta [redacted]@marmara.edu.tr adresine özel gönderilmiştir.

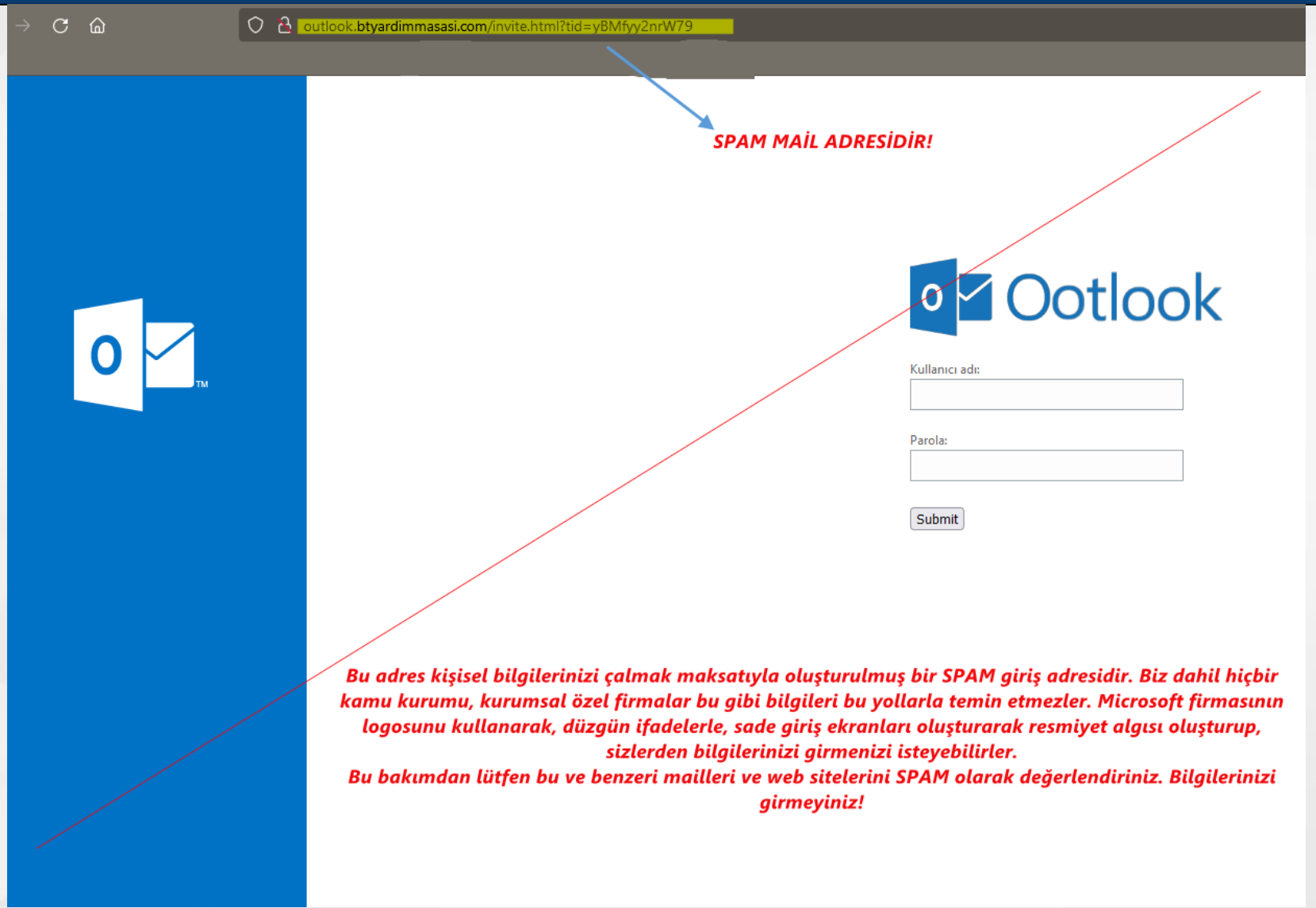
Bu mail, Bilgi İşlem Daire Başkanlığı tarafından, Sosyal Mühendislik Testi çalışması kapsamında Veri Güvenliği Farkındalığı oluşturmak amacıyla gönderilmiştir.

Biz dahil hiçbir kamu kurumu, bu ve benzeri mailler göndererek kişilerden bilgi güncellemesi talebinde bulunmazlar. Bu nedenle lütfen bu ve benzeri mailleri dikkate almayınız. Herhangi bir bilgi girişinde bulunmayınız ve direkt siliniz.

Bilgi İşlem Daire Başkanlığı
Marmara Üniversitesi

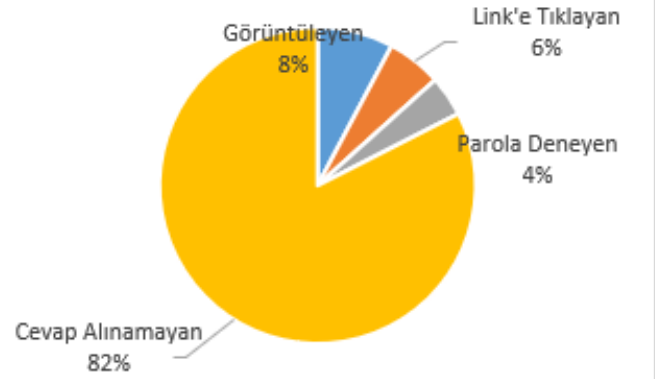
Senaryo 1

Sosyal Mühendislik Yöntemleri

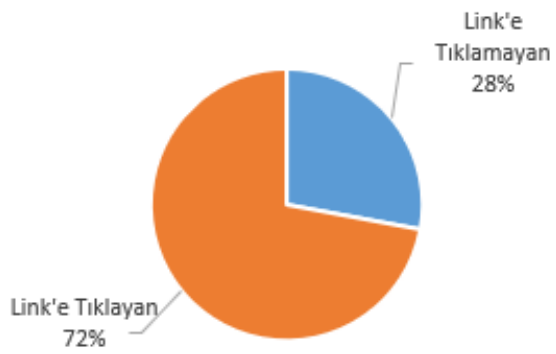


Sosyal Mühendislik Yöntemleri

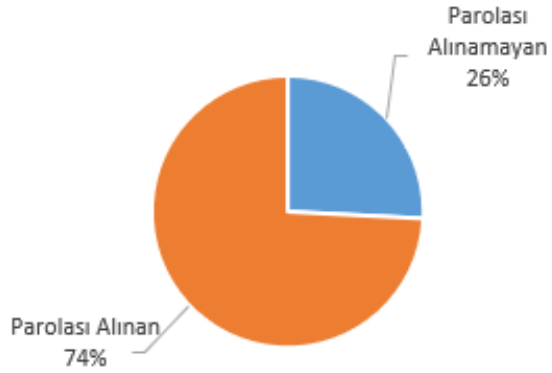
Başlangıç Zamanı	31/08/2023 11:49
Rapor Zamanı	**08**/09/2023 8:12:03
Gönderilen	**500**
Görüntüleyen	**43**
Link'e Tıklayan	**31**
Parola Deneyen	**23**
Cevap Alınamayan	**457**



Link'e Tıklama Oranı



Parola Deneme Oranı



(Yüzdelik dilim yalnızca link'e tıklamış kişiler üzerinden hesaplanmıştır.)

Sosyal Mühendislik Yöntemleri

Gönderen: Maaş Birimi <maasbirimi@marmar.com>
Kime: [redacted]@marmara.edu.tr
Konu: Eylül Ayı Maaş Bordrosu Gönderimi Hk.

Bu adres SPAM mail adresidir. Dikkat! Bu tarz mailler, Marmara Üniversitesi mail adreslerinden geliyor dahi olsa (mail çalınması durumlarında olabiliyor) bu ve benzeri içerikteki mailleri dikkate almayınız. SPAM MAİLDİR. Kesinlikle bilgilerinizi girmeyip, maili direkt siliniz.

Sayın [redacted]

Marmara Üniversitesi Eylül 2023 maaş bordronuzdaki gönderim bilgilerinizde eksiklik olduğu tespit edilmiştir. Bu bilgileri **01.09.2023 tarihi mesai bitimine kadar** aşağıdaki linkten doldurarak Personel Daire Başkanlığı Maaş Büromuza iletilmek üzere gönderiniz.

Bilgilerinizi Güncellemek İçin Tıklayınız

Tıklamayınız! Bilgilerinizi girmeyiniz!

Marmara – Maaş Bürosu

SPAM MAİLDİR!

Bu mail, Bilgi İşlem Daire Başkanlığı tarafından, Sosyal Mühendislik Testi çalışması kapsamında Veri Güvenliği Farkındalığı oluşturmak amacıyla gönderilmiştir.

Biz dahil hiçbir kamu kurumu, bu ve benzeri mailler göndererek kişilerden bilgi güncellemesi talebinde bulunmazlar. Bu nedenle lütfen bu ve benzeri mailleri dikkate almayınız. Herhangi bir bilgi girişinde bulunmayınız ve direkt siliniz.

Bu eposta [redacted]@marmara.edu.tr adresine özel gönderilmiştir.

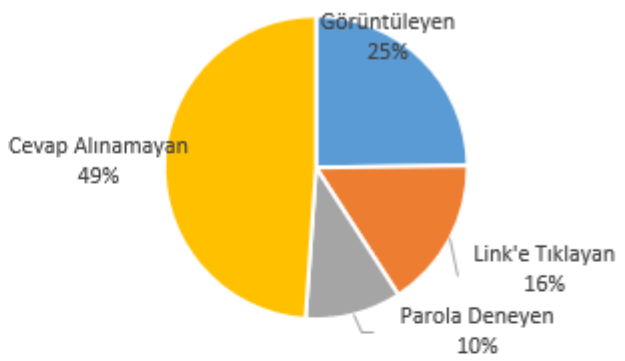
Bilgi İşlem Daire Başkanlığı
Marmara Üniversitesi

Senaryo 2

Sosyal Mühendislik Yöntemleri

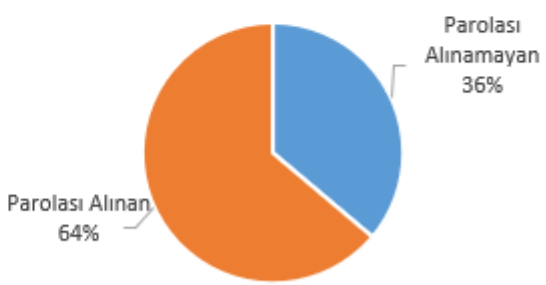
Sosyal Mühendislik Yöntemleri

Başlangıç Zamanı	31/08/2023 12:58
Rapor Zamanı	08/09/2023 12:03
Gönderilen	**4672**
Görüntüleyen	**1572**
Link'e Tıklayan	**1018**
Parola Deneyen	**650**
Cevap Alınamayan	**3100**



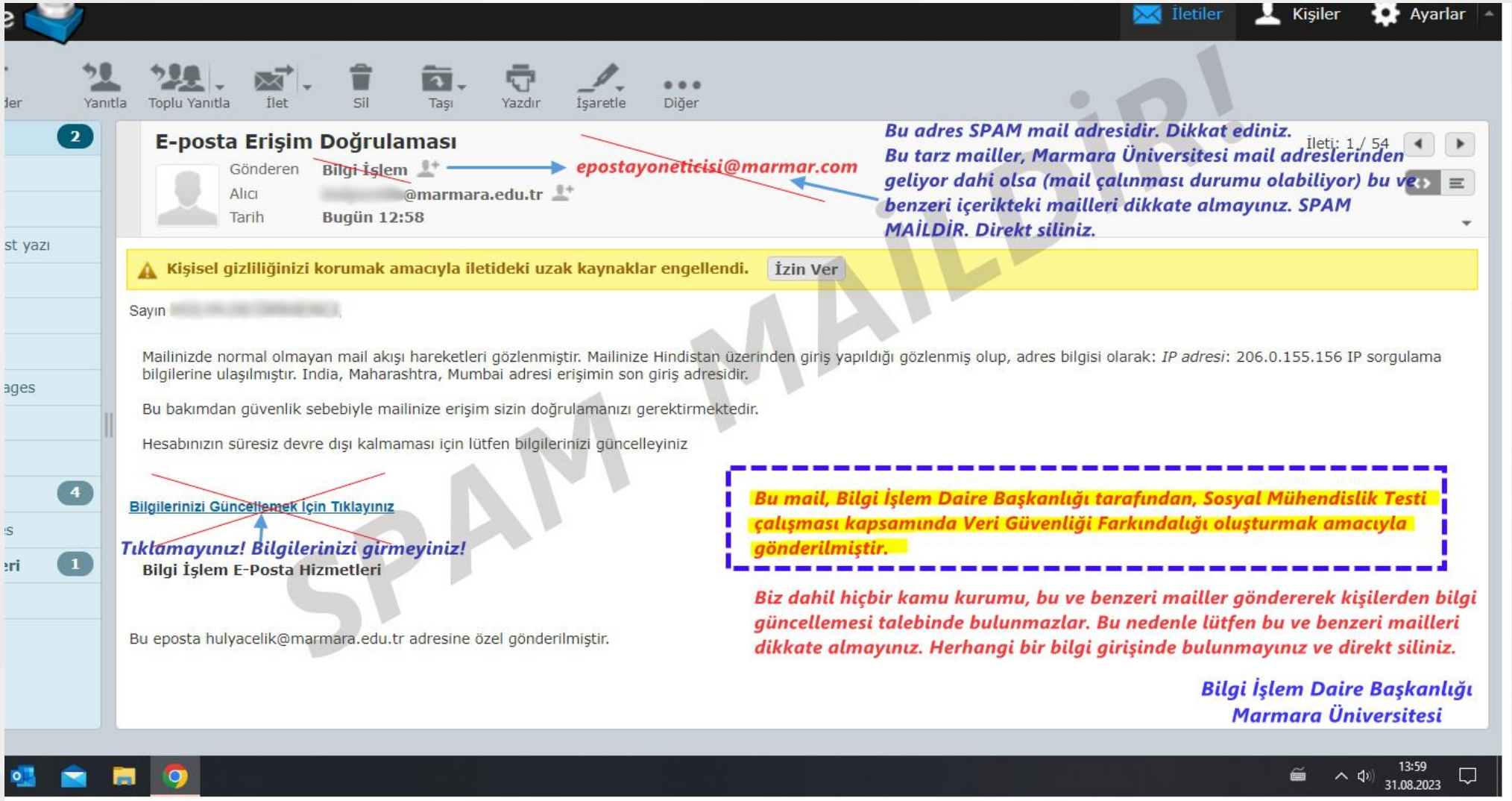
Link'e Tıklama Oranı

Parola Deneme Oranı



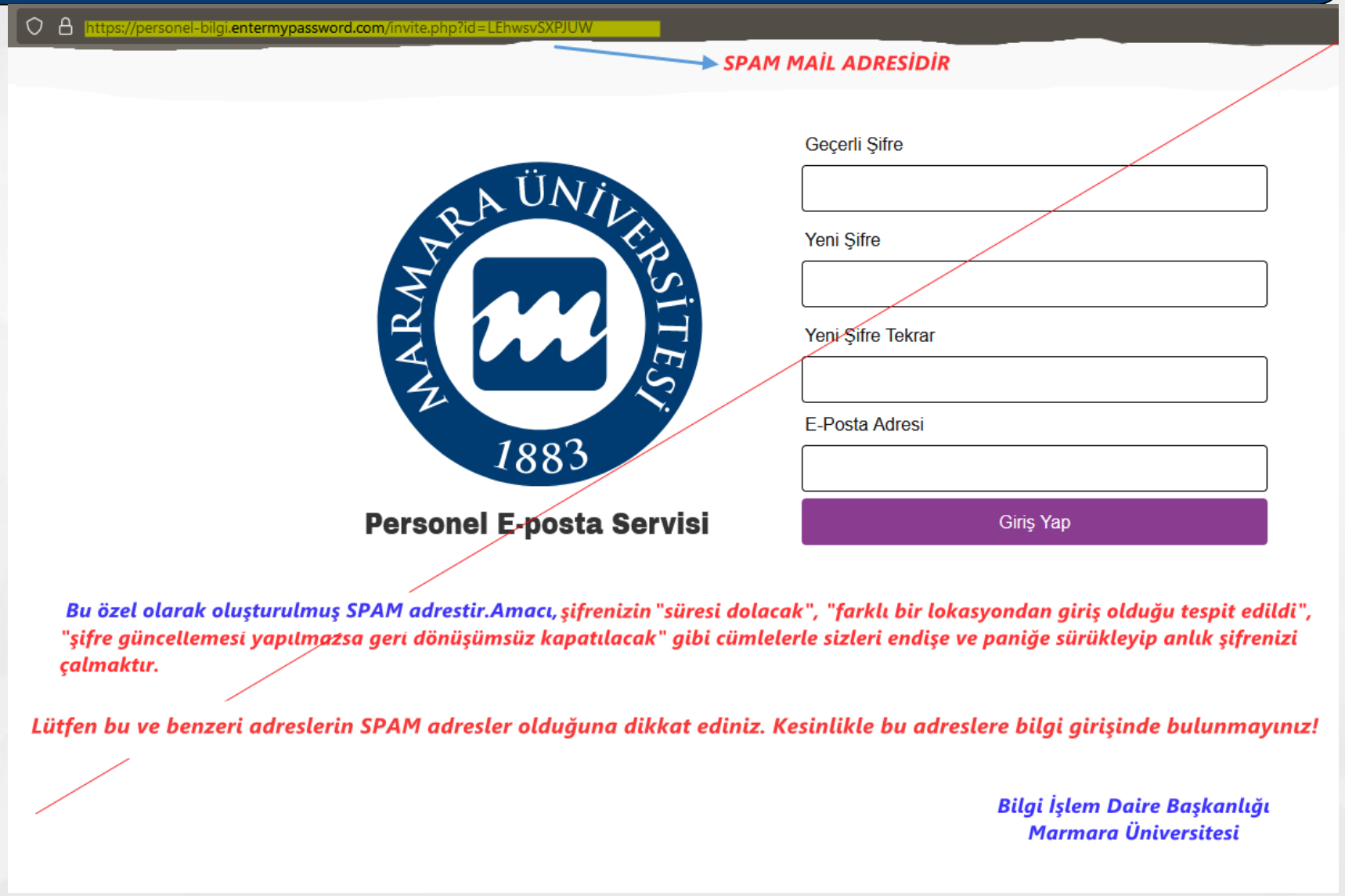
(Yüzdelik dilim yalnızca link'e tıklamış kişiler üzerinden hesaplanmıştır.)

Sosyal Mühendislik Yöntemleri



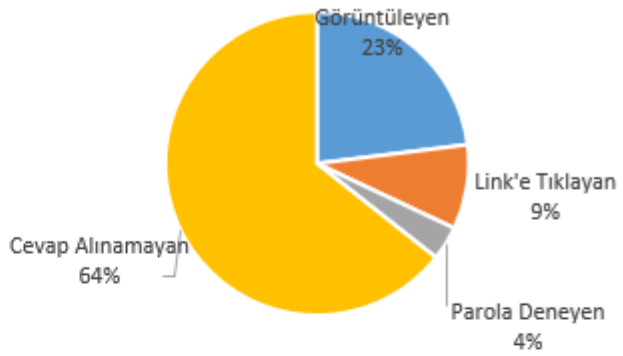
Senaryo 3

Sosyal Mühendislik Yöntemleri

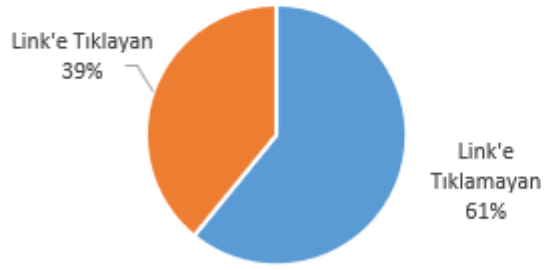


Sosyal Mühendislik Yöntemleri

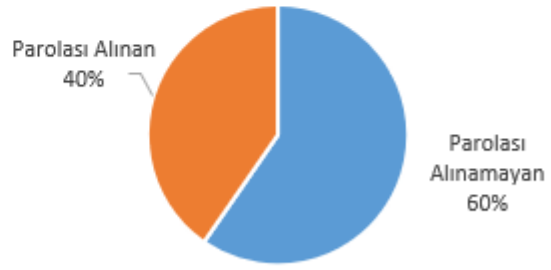
Başlangıç Zamanı	31/08/2023 12:58
Rapor Zamanı	08/09/2023 12:03
Gönderilen	505
Görüntüleyen	133
Link'e Tıklayan	52
Parola Deneyen	21
Cevap Alınamayan	372



Link'e Tıklama Oranı



Parola Deneme Oranı



(Yüzdelik dilim yalnızca link'e tıklamış kişiler üzerinden hesaplanmıştır.)

Bilgi Güvenliği İhlal Olayı

Bilgi Güvenliği İhlal Olayı, bilgi güvenliği ile uyuşmayan beklenmeyen veya istenmeyen olay olarak tanımlanabilir.

- Hizmet veya donanım kaybı,
- Sistemin yanlış veya aşırı yükle çalışması,
- İnsan hataları,
- Doğal afet durumu (Yangın, Sel, Deprem),
- Politikalara veya yönergelere uyulmaması,
- Fiziksel güvenlik düzenlemelerinin ihlali,
- Denetlenemeyen sistem değişiklikleri,
- Yazılım veya donanımın yanlış çalışması,
- Yetkisiz erişim denemeleri.

Bilgi Güvenliği İhlal Olayı

- Bilgi Güvenliği Politikalarını (Temiz Masa Temiz Ekran, Parola Politikası, Fiziksel Güvenlik) biliyor olacağız.
- Yetkili kişiyi bilgilendireceğiz. (Amiriniz, Bilgi Güvenliği Sorumlusu)
  - Telefon / yüzyüze
  - E-posta
  - destek.marmara.edu.tr →Bilgi Güvenliği sekmesi
  - https://bilgiguvenligi.marmara.edu.tr/bilgi-guvenligi/kisisel-verilerin-korunmasi/ihlal-olayi-bildirim-formu adresi üzerinden

Kurumsal Bilgi Güvenliği Dokümanları

bilgigüvenligi.marmara.edu.tr

BİLGİ GÜVENLİĞİ BİR ÜRÜN DEĞİL,

İÇİNDE STANDARTLARIN, UYGULAMALARIN VE EĞİTİMLERİN BULUNDUĞU

BİR SÜREÇTİR.

Katılımınız için teşekkür ederim.