BİLGİ GÜVENLİĞİ FARKINDALIK EĞİTİMİ NASIL OLMALI?

SUNA KÜÇÜKÇINAR

Uzman

Bilgi Güvenliği Birimi

sunay@metu.edu.tr

İBRAHİM ÇALIŞIR

Mühendis

Bilgi Güvenliği Birimi Yöneticisi

icalisir@metu.edu.tr

Ajanda

- Neden farkındalık eğitimi?
- Bu eğitimi ODTÜ içinde nerelerde verildi?
- Nelere değinmek lazım, biz nelere değiniyoruz?
- Nasıl anlatmak lazım?
- Soru - cevap

Neden farkındalık eğitimi?

- ✓ BG gün geçtikçe daha da önem kazanıyor
- ✓ İleri seviye güvenlik önlemleri kadar kullanıcıları BG hakkında bilgilendirme de önemli
- ✓ APT bir güvenlik trendi ve buna karşı kullanıcı farkındalığı önemli
- ✓ BGYS standartlarının da gereksinimidir

Farkındalık Eğitimi nerelerde verildi?

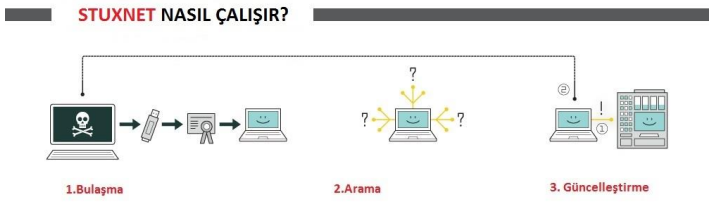
Kullanıcı Farkındalık Eğitimleri nerelerde verildi?

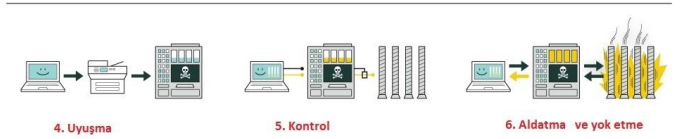
- Bilgi İşlem Daire Başkanlığı
  - ISO 27001 çalışmalarının parçası olarak danışman firma tarafından verildi
- Kütüphane ve Dokümantasyon Daire Başkanlığı
  - Kendileri talep ettiler, BGB verdi.
- Personel Daire Başkanlığı
  - Cryptolocker olayları sonrasında gelen talep sonrasında BGB tarafından verildi.
- İlerleyen zamanlarda başka birim/bölümlere de verilebilir

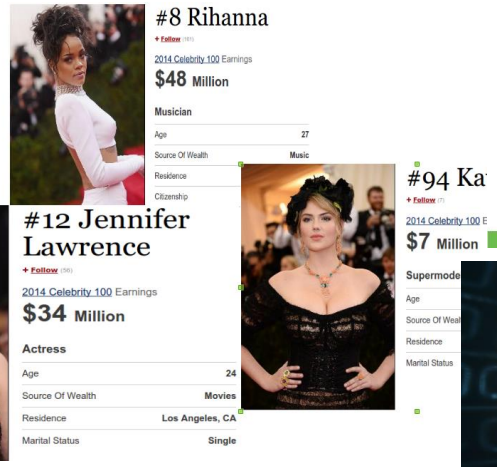
Neler Oluyor? Dünya

Dünyada Neler Oluyor

- Siber Savaş
  - Stuxnet, Estonya siber saldırıları, Çin vs Amerika vs
- Firma ve Kurumlara Saldırı
  - Sony, i-Cloud, Gmail, JP Morgan örnekleri
    - Sony Fury filminden beklenenden çok çok daha az para kazandı.
    - I-Cloud şifresini kaptıran kullanıcıların gizliliği ihlal edildi.
    - 5 miyon Gmail kullanıcısının şifreleri internete sızdı.
    - JP Morgan BG'ye 250 milyon $ harcamasına rağmen 1 milyondan fazla müşterisinin hesap bilgileri erişilebilir hale geldi.
- Kişilere Yönelik Saldırılar
  - Cryptolocker örneği (3.5 milyon $)







JPMorganChase

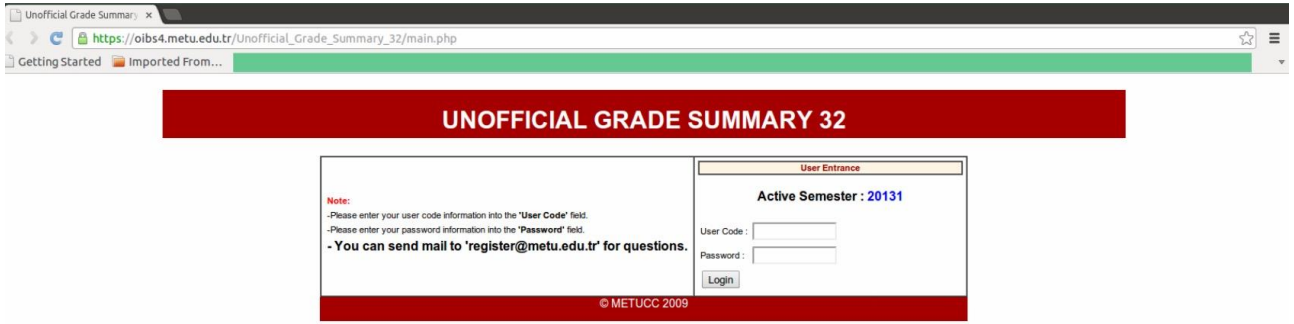
Neler Oluyor? Türkiye

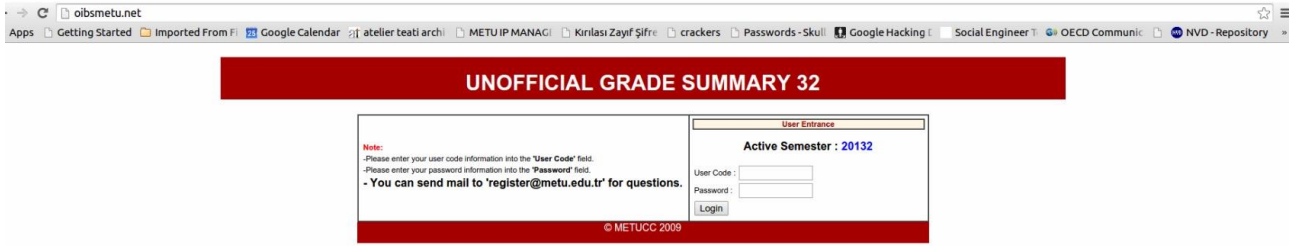
```
--- Syrian Electronic Army ----
fb.com/SEA.P.207
twitter.com/Official_SEA12
https://posta.icisleri.gov.tr/owa/
https://owa.icisleri.gov.tr/owa/
+-------------------------------------------+-------------------------+
| User                                      |  Password               |
+-------------------------------------------+-------------------------+
|                 @icisleri.gov.tr          |   sera2013.             |
|                 @icisleri.gov.tr          |   1073ugur              |
| mahm            @icisleri.gov.tr          |   *kard313n*            |
| asl             @icisleri.gov.tr          |   9815763               |
|                 @icisleri.gov.tr          |   123456-a              |
| yuce            @icisleri.gov.tr          |   123456-a              |
| ilk             @icisleri.gov.tr          |   123456-a              |
| mu              @icisleri.gov.tr          |   00009961              |
| i               @icisleri.gov.tr          |   in1616*b              |
| k               @icisleri.gov.tr          |   cg3984*b              |
| h               @icisleri.gov.tr          |   bs9413*h              |
| b               @icisleri.gov.tr          |   102505*bd             |
| 1               @icisleri.gov.tr          |   dz8341*b              |
| b               @icisleri.gov.tr          |   940016-tb             |
| ni              @icisleri.gov.tr          |   ch8161*g              |
| ne              @icisleri.gov.tr          |   123456-a              |
| mu              @icisleri.gov.tr          |   9961                  |
| bet             @icisleri.gov.tr          |   123456-a              |
| ful             @icisleri.gov.tr          |   170717                |
| i               @icisleri.gov.tr          |   70707                 |
| me              @icisleri.gov.tr          |   metin1965             |
| ma              @icisleri.gov.tr          |    68227052             |
| ay              @icisleri.gov.tr          |   5508177               |
| m               @icisleri.gov.tr          |   mehmet1966            |
|                 @icisleri.gov.tr          |   123456-a              |
| a               @icisleri.gov.tr          |   123456-a              |
| yas             @icisleri.gov.tr          |   123456-a              |
| ilh             @icisleri.gov.tr          |   123456-a              |
| ay              @icisleri.gov.tr          |   13&b_44&m             |
|                 @icisleri.gov.tr          |   123456                |
| u               @icisleri.gov.tr          |   mudanya               |
| fi              @icisleri.gov.tr          |   123456                |
| mesud           @icisleri.gov.tr          |   292464                |
| has             @icisleri.gov.tr          |   8726111733            |
```

- İçişleri Bakanlığı kullanıcı kodu ve şifrelerinin sızması
- HSBC Bankası tüm kredi kartı bilgileri kaptırdı
- Üniversitelere yönelik saldırılar
  - ODTÜ Duyuru sisteminin kırılması
  - Ankara Üniversitesi Twitter hesabının ele geçirilmesi

Neler Oluyor? ODTÜ

- Duyuru Sistemi kırıldı
- Bazı bölümlerin web sayfası ele geçirildi
- Cryptolocker vakaları yaşandı
  - PDB, YİTDB, İnşaat, Havacılık vs
- OİBS sisteminin tıpkı basımları türedi
  - oibsmetu.net
- 152 kullanıcı kodu parola ikilisinin ele geçirilmesi
  - Kaba kuvvet saldırıları





Gerçekler *

- **2,5** saniyede bir virüs!
- **%33**'ünü kendiniz fark edersiniz!
- **229 gün**de haberiniz olur!
- **180 gün**de tamamen izleri silip eski haline getirebilirsiniz!

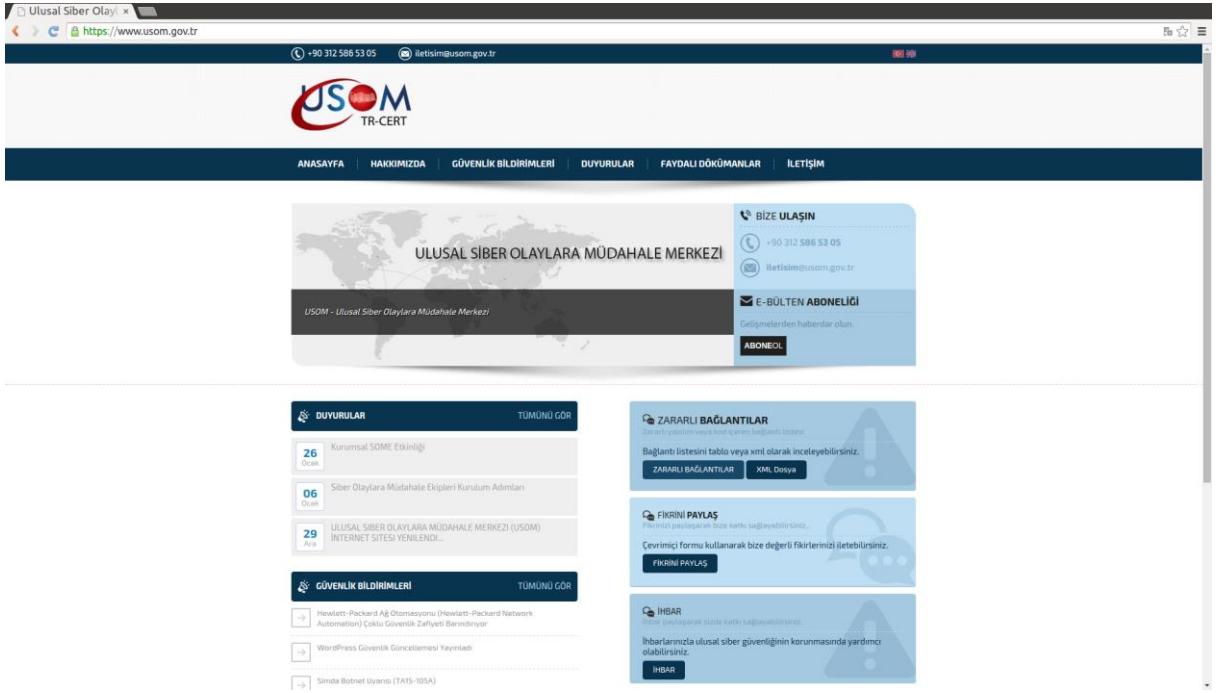
* SYMTURK SOME el kitapçığı

Neler yapılıyor?

Dünya
- NATO Cooperative Cyber Defence Center of Excellence

Avrupa Birliği
- Siber Güvenlik Politikası
- Siber Güvenlik Stratejisi

Türkiye
- Düzenleme
  - 5651 sayılı kanun ve ilgili yönetmelikler
- Uygulama
  - BTK
  - USOM
  - SOME



ODTÜ’de neler yapılıyor?

Kendi güvenlik uygulamalarınızı anlatın!

ODTÜ BİDB olarak biz neler yapıyoruz?

- ISO 27001 BGYS sertifikası
- SOME
- Uygulamalar
  - Güvenli Yazılım
  - Anti virüs
  - Port tabanlı güvenli duvarı
  - E-posta sistemi filtresi
  - Bilinçlendirme etkinlikleri
  - Güvenlik taramaları
  - 7/24 gözlem
- Yapmadıklarınızdan da bahsedin ki kendilerini çok da güvende hissetmesinler!

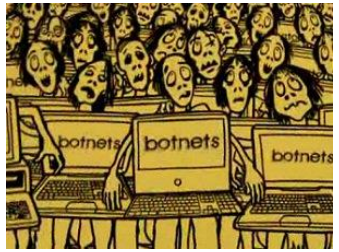
CERTIFICATE OF REGISTRATION

ORTA DOĞU TEKNİK ÜNİVERSİTESİ
BİLGİ İŞLEM DAİRE BAŞKANLIĞI

ISO/IEC 27001:2005

Neler anlatılmalı?

- Tehditlerin neler olduğuna değinilmesi
  - Virüs
  - Solucan
  - Truva Atı
  - Oltalama saldırısı
  - Casus Yazılımlar
  - Botnet
  - DoS/DDoS
  - APT
  - İnsanlar!
- Bu tehditlerin ilişkilendirilmesi



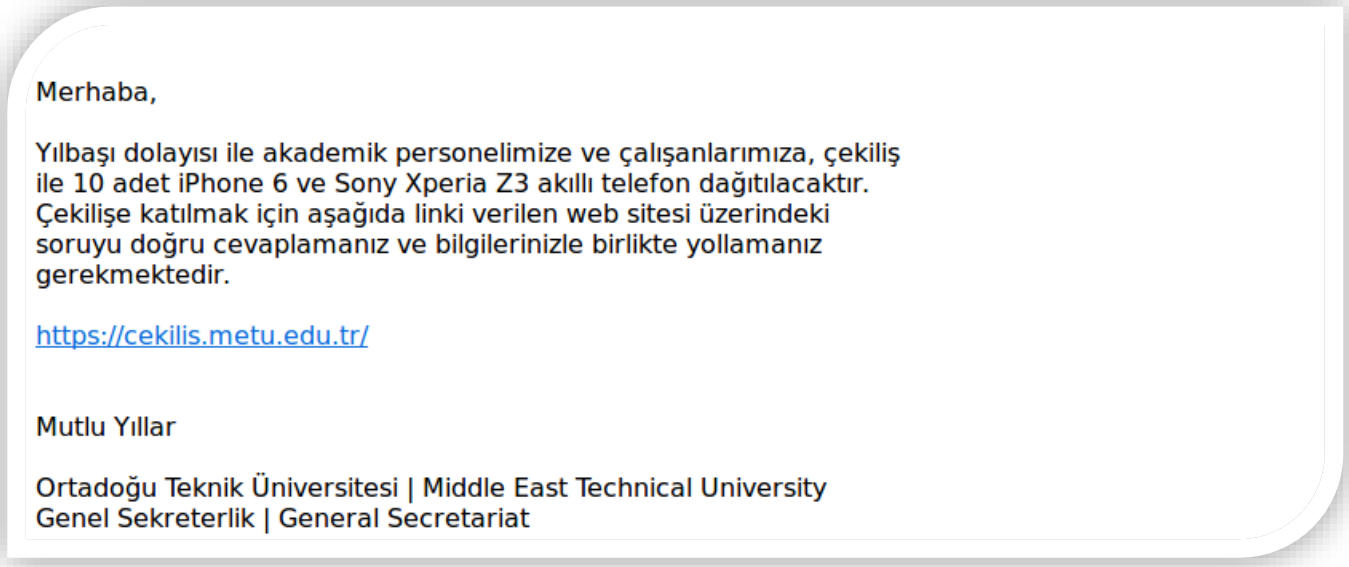
Neler anlatılmalı?

Neden etkileniriz?

- Güvenlik açıkları
  - İşletim sistemleri açıkları
  - Uygulamaların açıkları
  - Yanlış/eksik/hiç yapılandırma
- Güvenlik yazılımları eksikliği
- Kullanıcı hatası
  - E-posta eklentileri
  - USB bellek CD-ROM vs
  - İnternetten indirilen program ve dosyalar

Sosyal Mühendislik

- Nasıl ve neden yapılır?
  - Zararsız bilgi edinmek
  - Sadece sormak
  - Yardımcı olmak
  - Yardım istemek
  - Merak uyandırmak
  - Korkutmak
  - Sosyal ağlar
  - Vs
- Biz kendi testlerimizi anlattık
  - Grufoni oltalaması
  - Genel Sekreterlik oltalaması



Merhaba,

Yılbaşı dolayısı ile akademik personelimize ve çalışanlarımıza, çekiliş ile 10 adet iPhone 6 ve Sony Xperia Z3 akıllı telefon dağıtılacaktır. Çekilişe katılmak için aşağıda linki verilen web sitesi üzerindeki soruyu doğru cevaplamanız ve bilgilerinizle birlikte yollamanız gerekmektedir.

https://cekilis.metu.edu.tr/

Mutlu Yıllar

Ortadoğu Teknik Üniversitesi | Middle East Technical University
Genel Sekreterlik | General Secretariat

Önlem Almak

Fiziksel güvenlik

- Temiz masa temiz ekran politikasına uygun davranın.
- Odanızın kapısını kilitleyin.
- Bilgisayarınıza giriş parolası tanımlayın.
- Parola ile devre dışı kalan ekran koruyucu tanımlayın.
- Bilgisayar başından ayrılırken ekran koruyucusu devreye alın.

Önlem Almak

Parola Güvenliği

- Parola elde etme yöntemleri
  - Tahmin
  - Çalma
  - Deneme
- Nasıl bir parola
  - Büyük harf küçük harf rakam noktalama işaretleri
  - En az 8 harf
  - 3 ayda bir değiştir
  - Kolay tahmin edilebilecek parola tanımlama
    - 123456, qweasd, 1234-a, sunakucukcinar, 04071972 vs,
  - Her kullanıcı hesabı için aynı parolayı kullanma, bir kalıp belirle ve hesaplara göre uyarla

2014'ün en çok kullanılan şifreleri listesi:

1- 123456 (yerini korudu)
2- password (yerini korudu)
3- 12345 (17 sıra yükseldi)
4- 12345678 (1 sıra düştü)
5- qwerty (1 basamak düştü)
6- 1234567890 (yerini korudu)
7- 1234 (9 basamak yükseldi)
8- baseball (listeye yeni girdi)
9- dragon (listeye yeni girdi)
10- football (listeye yeni girdi)

2004 Çekirdeksiz Üzüm Sapı

- 04C$!zUS-GML --> Gmail
- 04C$!zUS-SPT --> Spotify
- 04C$!zUS-MT --> Metu
- 04C$!zUS-MRKF --> Markafoni

Önlem Almak

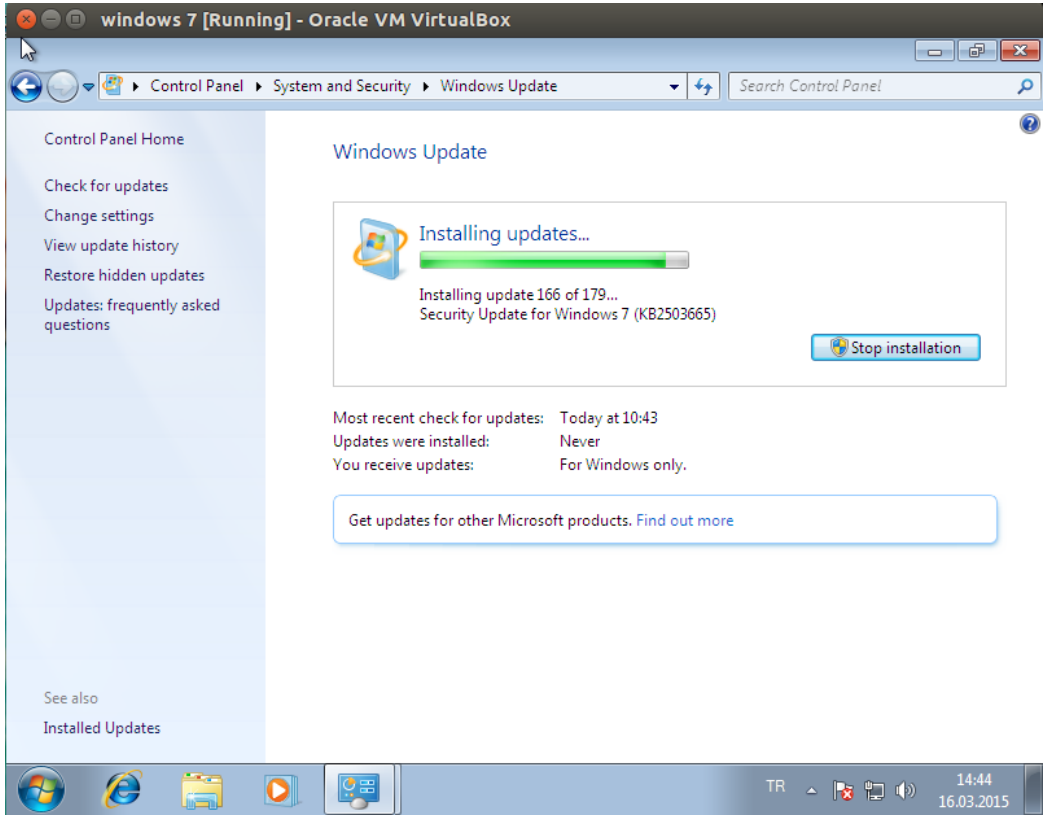
Parolayı Korumak

- Arkadaşlarınla paylaşmayın
- Yazılı ortamda saklamayın
  - Saklaman gerekiyorsa şifreleyerek saklayın!
- SMS ya da e-posta ile göndermeyin
- Telefonda söylemeyin
- **Sağduyulu olun!**

Önlem Almak

Güvenli Yazılım

- Güvenli ve lisanslı yazılım
  - Mtorrent örneği
- Yazılım güncellemelerini yapmak
- Hangi yazılımlar güncellenmeli
  - HEPSİ!!!



Acrobat and Reader 9.x and 8.x release notes

If you have trouble opening a note, right-click and save the file to your desktop.

Date	Release Notes	Release Type*	Focus
May 14, 2013	9.5.5	Q	**Latest and FINAL release**. This patch fixes specific security issues.
Feb 20, 2013	9.5.4	OOC	This patch fixes specific security issues.

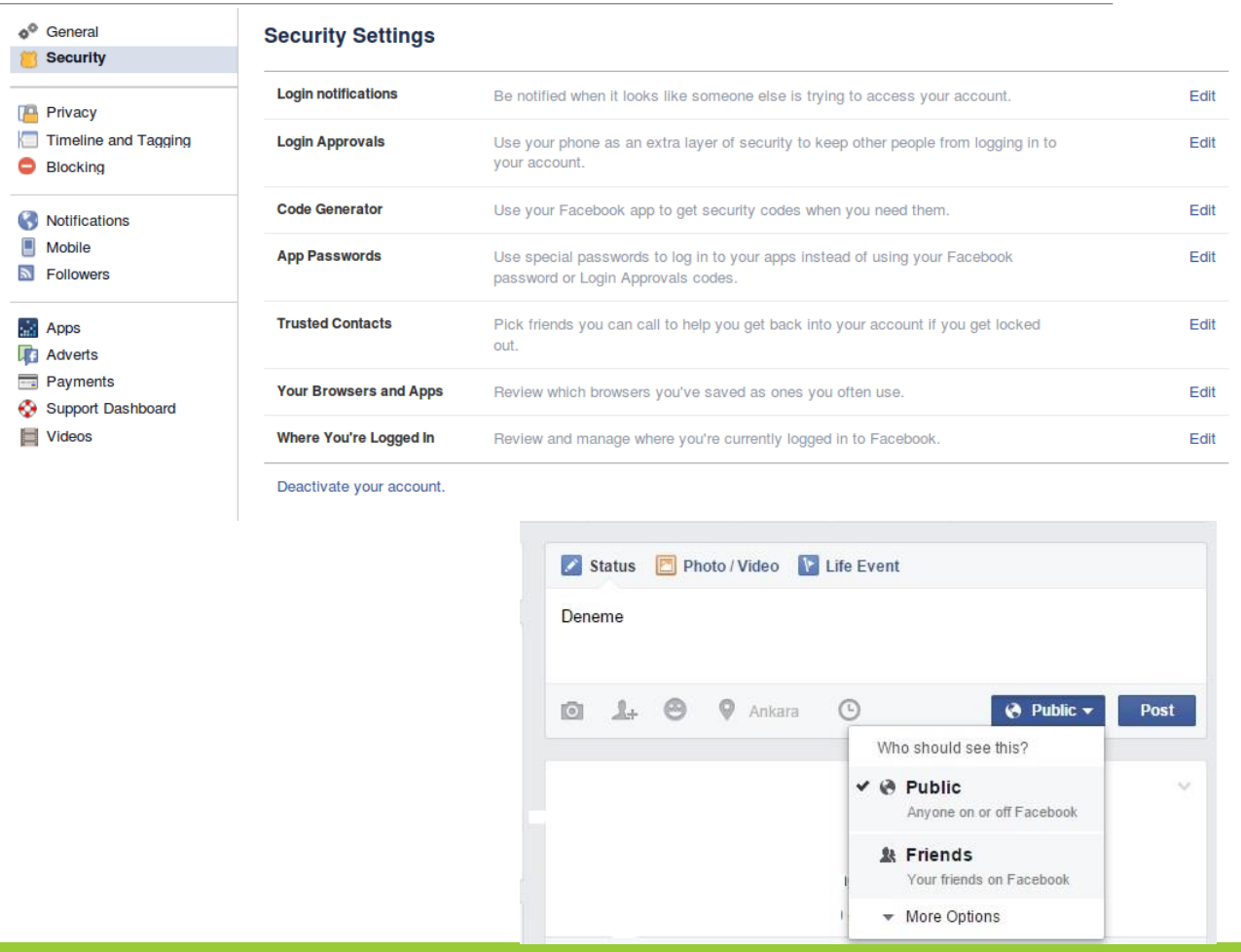
Önlem Almak

Güvenli Kullanım

- Admin haklarının kısıtlanması
  - PDB örneği
- E-posta
  - Kaynağına bakın
  - Eklentileri emin olmadıktan sonra açmayın
  - Sağduyulu olun!
- Internet
  - Şüpheli sitelerden uzak durun
  - Adresi kontrol edin
  - Gerekli yerlerde https gibi güvenli bağlantı olup olmadığını kontrol edin
  - Düşündüğünüz kadar şanslı olmayabilirsiniz

Sosyal Ağlar

- Paylaşımlar
  - Kiminle, farkında olarak mı paylaşıyorsun?
- Arkadaşlar
- Konum bilgisi
- Sadece kullanıcıların değil kurumsal sosyal medya hesaplarının güvenliği önemli!!!
  - TV5monde örneği!



Yedekleme

- Nasıl kaybederiz?
  - Zararlı yazılımlar
  - Yanlışlıkla silerek
  - Donanım arızası
- Önlem
  - Yedek alın
  - Kendi bilgisayarınız harici bir ortama alın
  - Planlı alın
  - Kullanılabilirliği test edin
- Cryptolocker örneği!

Nasıl anlatılmalı?

- Çarpıcı gerçekler
- Dünyada ve Türkiye’de olmuş olaylar
- Olabildiğince eğlenceli
  - Video koyabilirsiniz.
- En fazla 45 dakika x 2 oturum

Teşekkürler!

Soru ve Cevaplar?

security@metu.edu.tr