Bilgi Güvenliği Farkındalık Eğitimi
Aralık 2019

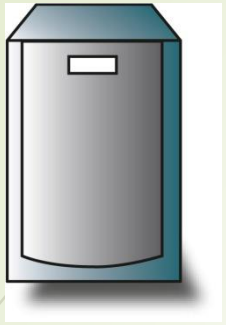
BİDB-Ayşen USLU

Bilgi Nedir ?

- **Bilgi**, verinin işlenmiş şeklidir.
- **Bilgi**, kopyalanabilir ve taşınabilirdir.

Bilgi nerelerde bulunur?

- ✓ Kağıtta
- ✓ Elektronik ortamda
- ✓ Maillerde
- ✓ Videolarda
- ✓ Web sayfasında
- ✓ Konuşmalarda
- ✓ vb…



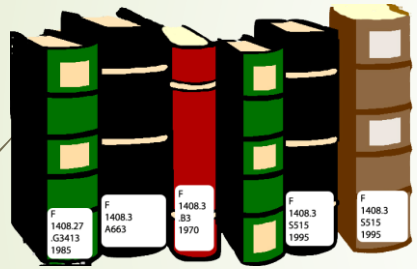
Sunucu

İstemci

Dizüstü bilgisayar

Kablosuz ağlar

Medya

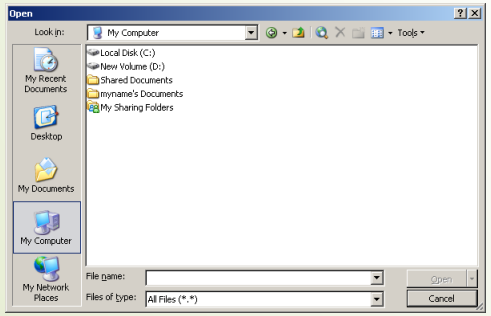


Dokümanlar

Kurum çalışanları

Yazıcı çıktıları

Radyo-televizyon yayınları



Yazılımlar

Cep telefonları, PDA'lar

Fotoğaf makineleri r

Bilgi güvenliği nedir?

- Bilgi varlıklarının, gizliliğini, bütünlüğünü ve erişilebilirliğini korumayı amaçlayan çalışma alanıdır.

Bilgi Güvenliğinin Amacı

- ✓ Veri bütünlüğünün korunması
- ✓ Yetkisiz erişimin engellenmesi
- ✓ Mahremiyet ve gizliliğin korunması
- ✓ Sistemin devamlılığının sağlanması

Bilginin gizliliğini korumaktan ne anlamalıyız?

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

Bilginin bütünlüğünü korumaktan ne anlamalıyız?

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

Bilginin erişilebilirliğini korumaktan ne anlamalıyız?

- Erişilmesi gereken bilgi her zaman erişilebilir olmalıdır.

ISO 27001 Bilgi Güvenliği Yönetim Sisteminin Kurulması

- Kapsamın belirlenmesi
- Rol ve sorumlulukların belirlenmesi
  - BGYS Komisyonu- Görev Tanımları
- Komisyon Üyelerimiz :

Vedat YURT	- BGYS Komisyon Başkanı
Ayşen USLU	- Bilgi Güvenliği Yöneticisi
Mustafa ŞAHİN	- BGYS Komisyon Üyesi
Orhan KOÇDEMİR	- BGYS Komisyon Üyesi
Volkan KALKAN	- BGYS Komisyon Üyesi

- Farkındalık eğitimlerinin verilmesi

Üniversitemizdeki BGYS Politikaları nerede bulunur?

- bilgigüvenligi.marmara.edu.tr adresinde güncel haliyle yayınlanmaktadır.

Bilgi Güvenliği Politikası ne işe yarar ?

- Personele, yaptıkları iş kadar, iş yapış yöntemlerinin ve işledikleri bilginin değerini farkettirir.
- Kurumu, bilgi kaybı nedeni ile uğrayacağı zarardan korur.
- Riskleri yönetilebilir kılar.
- Toplam kalitenin artmasına neden olur.

UYARILAR !!!

- BGP sadece Bilgi Teknolojilerini ilgilendiren bir politika değildir.
- Riskleri sıfıra indirmez, yönetilebilir kılar.
- Kendi kendini uygulayamaz.
- Başta yönetim kurulunun, ardından personelin katkısı gerekir.
- Zaman geçtikçe güncellenmesi gerekir.
- Sadece İdari yada Teknik bir politika değildir.

- Güvenliğin sadece küçük bir kısmı teknik güvenlik önlemleri ile sağlanır.
- Büyük kısım ise kullanıcıya bağlıdır.

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.
- Teknik önlemler kullanıcı hatalarını önlemede yetersiz kalmaktadır.
- Kullanıcılar tarafından dikkat edilmesi gereken kurallar sistemlerin güvenliğinin sağlanmasında kritik bir öneme sahiptir.

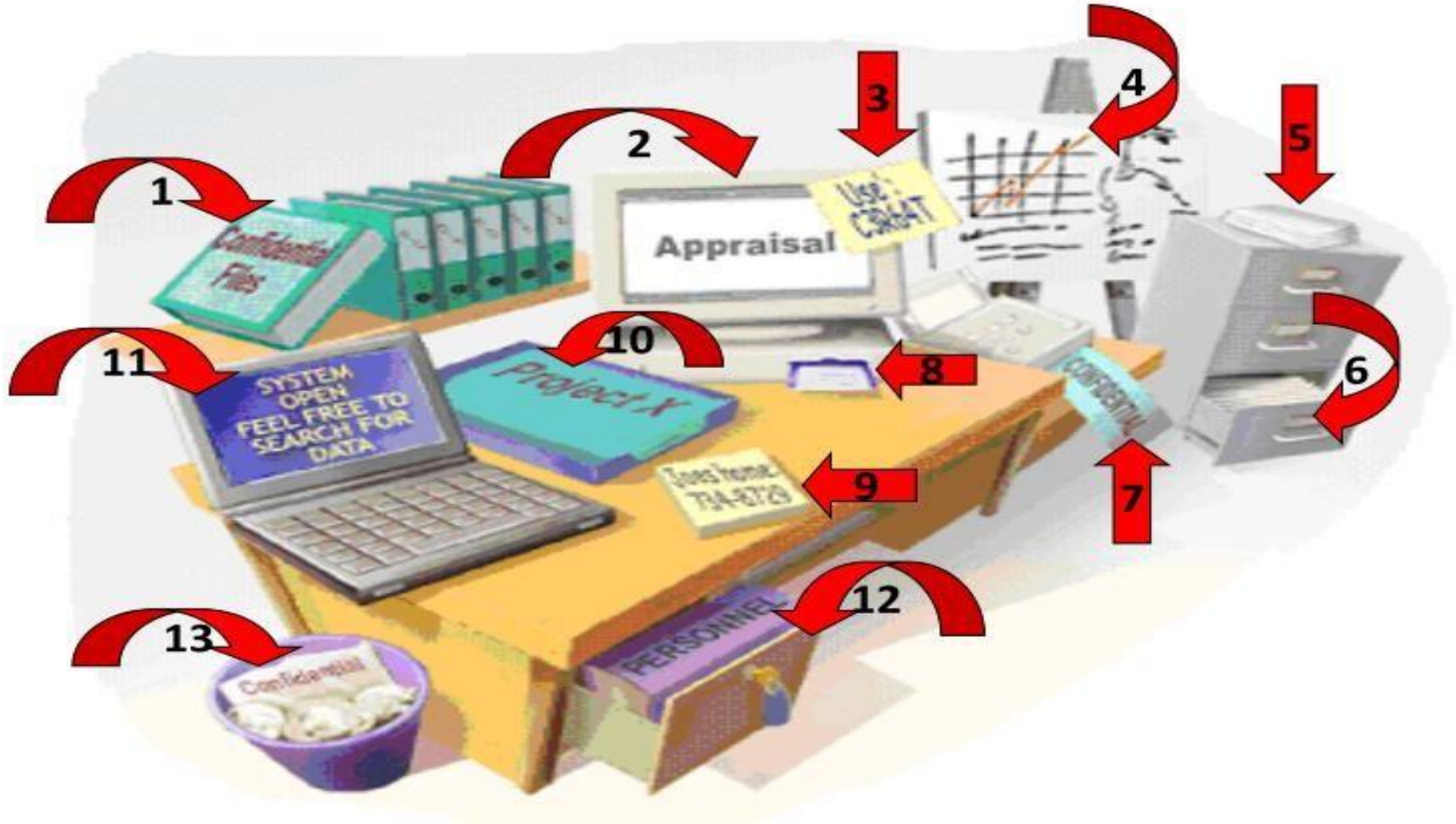
Personelden beklenenler

Fiziksel güvenlik :

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

Personel den beklenenler

Çalışma ortamı temizliği (Temiz Masa İlkesi)



Temiz masa temiz ekran

- 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.
  - Etiketleme- Gizli-KIRMIZI
  - Etiketleme- Hizmete Özel-SARI
  - Etiketleme- Genel-YEŞİL
- Gizlilik dereceli evraklar, işlevini tamamladıktan sonra imha edilmelidir.
- Gelen ve giden mesaj notları ve faks makineleri ve yazıcılar başıboş olarak bırakılmamalıdır.
- Kuruma ait antetli kağıtlar kilitli dolaplarda tutulmalıdır.

Temiz masa temiz ekran

- Hassas ve sınıflandırılmış bilgi basıldığında yazıcıdan hemen alınmalıdır.
- Bilgisayarların masaüstlerinde kuruma ait özel bilgiler içeren dokümanlar bulundurulmamalıdır.
- Bilgisayarlara ait olan şifreler kesinlikle kağıt ortamlara yazılı bir şekilde bırakılmamalıdır.
- Ofis ve çalışma ortamlarındaki yazı tahtaları kullanıldıktan sonra temizlenerek bırakılmalıdır.
- Ofis ve çalışma ortamlarında bulunan başı boş USB/CD gibi medyalar, bilgisayarlara takılmamalıdır. Gerekli yerlere teslim edilmelidir.

Personelden beklenenler

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 beklenenler

- 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

Kötü Şifre Örnekleri

- 12345
- abcdef
- 1978
- 11111
- 13579
- aaaaa
- bbbbbbb
- 123123 …

- deniz
- deniz1998
- Deniz123

Personelden beklenenler

- 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.
- En geç 5 dk içinde devreye girecek parolalı Otomatik Ekran Koruma kullanıcı bilgisayarlarında yapılandırılmalı.

Virüsler

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.

- Virüsler
  - Bilgi Güvenliği için gerçek ve kesin bir tehdit oluştururlar
  - Bilgiye zarar verebilir,
  - yok edebilir,
  - yetkisiz kişilerin eline geçmesini sağlayabilir

Personelden beklenenler

- Virüsler nasıl bulaşır ?
  - İnternet yada ağ üzerinden
  - USB bellek yada harici disklerden
  - Korsan \ Lisanssız yazılım CD lerinden
  - E-Posta yoluyla

Phishing:

- Phishing mailleri 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 düşünülmüş bu tip maillere içeriğini inceleyerek ve şüpheyle yaklaşarak bakmakta fayda var.

E-posta Güvenliği

- 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.

Sistem Güvenliği: Pishing Saldırısı

Sayın müşterimiz;
Ağustos ayından itibaren T.C Merkez Bankası'nın aldığı karara dayanarak tüm internet bankacılığı sistemlerinde TCMB'ye bağlı tüm bankaların (AKBANK, ANADOLU BANK, ASYA BANK, GARANTİ BANKASI, FORTIS BANK, FİNANSBANK, HSBC BANK, ŞEKERBANK, T.C İŞ BANKASI, TURKEYFINANS, TEB, TEKFENBANK, TEKSTILBANK, KOÇBANK, KUVEYTTÜRK, YAPI VE KREDİ BANKASI, VAKIFBANK) SSL yazılımları ve internet bankacılığına hizmet eden bilgisayarlar güncellenmektedir. Bu güncelleme nedeniyle sistemler yenileneceğinden, hem aktif internet bankacılığı kullanıcılarını tespit etmek, hem de güvenlik açısından sizlere daha iyi bir hizmet verebilmek için bilgilerinizi teyit etmeniz gerekecek ve yeni veritabanımıza kaydedilecektir. Bilgilerinizin teyidi ve yeni veritabanına eklenmesi zorunludur. Teyit işlemi yapılmadığı taktirde Ağustos ayından sonra internet bankacılığını kullanabilmeniz için TCMB Ankara Şubesi'nden bilgilerinizi teyit edip yeni veritabanına kaydettirmeniz gerekecektir. Aşağıdaki linkten bilgilerinizi internet üzerinden teyit edebilir, ya da TCMB Ankara Şubesi'nden bilgilerinizi teyit edebilirsiniz.

İnternet üzerinden teyit işlemini yapmak için aşağıdaki linke tıklayın;
http://tcmb.gov.tr.teyit.merkezbanka.org/guncelleme.php?sid=d3fd99df91df76dfs

DİKKAT: Lütfen TCMB üzerinden gelmeyen mailleri dikkate almayınız. TCMB üzerinden gelmeyen mailleri güvenliğiniz için bize bildirin. Teyit işlemleriyle hiçbir banka doğrudan ilgilenmemektedir. Bütün teyit işlemleri TCMB tarafından organize edilmektedir. Teşekkürler.

Adres: İstiklal Cad. 10 Ulus, 06100 Ankara, Türkiye
Telefon : (312) 310 3646

---------- Forwarded message ---------
From: **Bilgi Islem** <bilgi_islem@marmara.edu.tr>
Date: Wed, Oct 9, 2019 at 2:04 PM
Subject: ÖNEMLİ! Kişisel Verilerin Korunma Kanunu (KVKK) Hk.
To: <falkaya@marmara.edu.tr>

Üniversitemiz Kullanıcılarının Dikkatine,

Üniversitemizde ISO 27001 BGYS çalışmaları kapsamında bazı iyileştirmeleri hızlıca tamamlamamız gerekiyor.

Üniversitemizde bulunan bilgisayarları, yazıcıları, sunucuları domain yapısına entegre ederek tek çatı altında yönetim sağlayabileceğiz ve güvenlik politikalarını uygulayabileceğiz. Bilgisayarlarınız da oluşacak problemlere daha kısa zamanlı çözümler sağlanabilecek.

Tek bir ortak şifreyle Bilgisayarınıza, Mail Adresinize, Yazıcılara, Ortak Dosya Paylaşım Klasörünüze ve Wifi' ye erişebiliyor olacaksınız. Bu kapsamda ortak şifre olarak kullanmak istediğiniz şifrenizi güncellemeniz gerekmektedir.

Önemli! : Bu şifrenin tüm sistemlerde geçerli olacağını unutmayınız. Saldırganlar tarafından yapılacak olan şifre saldırılarına karşı güvenlik seviyesi yüksek bir şifre belirlenmesi ve sosyal mühendislik saldırılarına karşın dikkatli olunması gerekmektedir. Şifrenizi kimseyle paylaşmayınız.

Şifre Güncellemelerinin en geç 11.10.2019 günü mesai bitimine kadar aşağıdaki linkten yapılması gerekmektedir.

Şifrenizi sadece buraya tıklayarak güncelleyebilirsiniz.

Marmara Üniversitesi

Sosyal Mühendislik

Sosyal Mühendislik:

- Sistem ve bilgiler üzerinde izinsiz erişim sağlayabilmek için insanların aldatılma yada hilekarlıkla kullanılmasıdır.
- Yardımcı olmaya istekli olma, başkalarına güvenme ve zor durumda kalmak istemem gibi zaaflarımızdan yararlanırlar.
- Amaç > Dolandırıcılık, sistemlere erişmek, endüstriyel casusluk, kimlik hırsızlığı, sistemleri bozmak için gereken bilgiyi elde etmek.

Sosyal Mühendislik örnekleri:

- Bilgi almak için masum sebepler
- Güven sağlayıcı bilgiler vermek
- Yeni başlayanlar potansiyel açıktır
- Güvenliğin önemini vurgulayarak güven kazanma
- Üst yönetim kandırmacası
- Yardım isteme
- Yardım talep ettirme

Nasıl Korunulur?

- Bilgisayarınıza ve cep telefonları gibi Web'e erişimi olan diğer aygıtlara fiziksel erişim konusunda tetikte olun. Siber takipçiler, kurbanlarını izlemek için yazılım ve donanım aygıtları kullanır (bazen siz farkında bile olmadan bilgisayarınız arkasına takılıdır).
- Bilgisayardan uzaklaştığınızda her zaman bilgisayar programlarındaki oturumunuzu kapatın ve parolalı bir ekran koruyucu kullanın. Aynı durum cep telefonları için de geçerlidir. Çocuklarınız ve eşiniz de aynı iyi alışkanlıkları geliştirmelidir.
- İyi parola yönetimi ve güvenliği konusunda alıştırma yapın. Parolalarınızı hiçbir zaman başkalarıyla paylaşmayın. Ayrıca parolalarınızı sık sık değiştirmeyi unutmayın! Bu çok önemlidir.
- Adınızı ve aile bireylerinizin adını aratarak internette sizinle ve çocuklarınızla ilgili ne tür bilgiler bulunduğuna bakın. Sosyal ağları da aramak konusunda çekingen olmayın (arkadaşlarınızın ve meslektaşlarınızın ağları da dahil olmak üzere) ve özel ya da uygunsuz olan her şeyi kaldırın.

- Katılmayı planladığınız etkinlikleri gösteren çevrimiçi takvimleri ve seyahat programlarını sosyal ağınızda olsa bile silin veya özel hale getirin. Bu bilgiler bir takipçinin ne zaman nerede olmayı planladığınızı öğrenmesine neden olabilir.
- Güvendiğiniz kişilerin dışındakiler ile çevrimiçi paylaşımınızı sınırlamak için tüm çevrimiçi hesaplarınızda gizlilik ayarlarını kullanın. Bu ayarları kullanarak birisi sizin adınızı aradığında profilinizin görünmemesini sağlayabilirsiniz. İnsanların yayınladıklarınızı ve fotoğraflarınızı görmemesi için onları engelleyebilirsiniz de.
- Birisinin günlük etkinliklerinizi takip etmek için casus yazılım kullandığından şüpheleniyorsanız ve tehlikede olduğunuzu düşünüyorsanız, yardım almak için kamuya açık bilgisayarlar veya telefonlar kullanın. Aksi takdirde, siber takipçi yardım almaya çalıştığınızı öğrenir ve bu da sizin için daha da büyük bir tehlike oluşturabilir.
- Her zaman olduğu gibi birisinin bir kimlik avı saldırısı veya virüs bulaşmış olan bir Web sitesi aracılığıyla bilgisayarınıza casus yazılım yüklemesini önlemek için iyi, güncellenmiş güvenlik yazılımı kullanın. Hangi güvenlik yazılımlarının mevcut olduğunu görmek için cep telefonunuzun uygulama mağazasına gidin. Güvenlik yazılımları, aygıtınızda casus yazılımları tespit etmenizi sağlayabilir ve takip edilme riskini azaltabilir.

Bilgi Güvenliği İhlali ne demektir?

Bilgi güvenliği ile uyuşmayan beklenmeyen veya istenmeyen olay.

Bilgi güvenliği ihlallerine örnekler aşağıda listelenmiştir:

- 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.

BG İhlal Olayında ne yapacağız?

- Bilgi Güvenliği Politikalarını (Temiz masa Temiz Ekran, Parola Politikası, Fiziksel Güvenlik) biliyor olacağız.
- Yetkili kişiyi bilgilendireceğiz. (BGYS Komisyonu-Bilgi Güvenliği Yöneticisi)
  - Telefon
  - E-posta
  - Yüz yüze
  - destek.marmara.edu.tr →Bilgi Güvenliği sekmesi
- Acil Durum İletişim Bilgileri
  - 0 216 337 5252
  - 0 216 345 5433

Bilgi güvenliği için yapabileceklerimiz

Ofis ve odaların fiziksel güvenliği
Doküman ve evrakların korunması
Bilgisayarlarımızın güvenliği
Bilgilerin/dosyaların yedeklenmesi
Taşınabilir bilgisayarlar
Taşınabilir diskler
Yanlışlıkla yapılan işlemler (silme, değiştirme vb.)

✓ Şifrelerimi

a) hiç değiştirmem
b) belli aralıklarla değiştiririm
c) fikrim yok

✓ **Bence en güvenli şifre**

a) 2805
b) a1,dCe!r
c) fenerbahce

- ✓ **Gerekirse, şifremi kimlere söyleyebilirim?**

a) yöneticime
b) bilgi işlem personeline
c) hiç kimseye

- ✓ Çay almak için bilgisayarımın başından kalkarken, ekran kilidini devreye sokmam

a) gerekmez
b) gerekir
c) kararsız kaldım

- ✓ Restoran, kafe gibi yerlerde arkadaşlarımla iş konularında konuşmamamda hiçbir mahsur yok.

a) doğru
b) yanlış
c) hangi restoran ya da kafe olduğuna bağlı

- ✓ **Kurumumun güvenliğini ilgilendirecek bir olay farkettiğimde...**

a) gerekli yerlere haber veririm
b) benim görevim değil
c) kararsız kaldım

- ✓ Facebook, twitter gibi ortamlarda işle ilgili bilgi paylaşmamda mahsur yok

a) evet yok
b) hayır var
c) hangi bilgi olduğuna göre değişir

✓ **Bilgi güvenliğini sağlamak**

a) Bilgi işlemin görevidir
b) Yönetimin görevidir
c) Hepimizin görevidir

✓ İnternette araştırıp edindiğim bütün bilgiler

a) güvenilirdir
b) güvenilmezdir
c) kısmen güvenilirdir

- ✓ İş bilgisayarıma, gerekli gördüğüm bir programı yükleyebilirim

a) doğru
b) yanlış
c) izin almam gerekir

✓ **Toplantı odasında bir USB buldum.**

a) Hemen gidip bilgisayarıma takmalıyım
b) Hemen gerekli yerlere haber vermeliyim
c) Beni ilgilendirmez orada kalsın

- ✓ E –posta hesabıma tanımadığım birinden e-posta geldi. Fatura ile ilgiliymiş,

a) Üzerine gelip silerim
b) Ben bir şey almadım ama ne faturasıymış bakayım

- ✓ Doğru kullanıldığında, en basit ve en ucuz güvenlik yöntemlerinden birisi ,

a) Bilgisayarı ayda bir formatlamak.
b) Parola kullanmak
c) Bilgisayarı diğer çalışanlarla ortak kullanmak.

✓ Bilginin gizliliği neyi ifade etmektedir?

a) Bilginin kimsenin göremeyeceği yerde saklanması
b) Bilgiye yalnızca yetkisi olan kişiler tarafından erişilmesi.
c) Bilginin kopyasının çıkartılıp saklanması.