

Herhangi bir deęişiklik yapılmadıęı,
her sunumda isim hakkı korunduęu
sürece ders notu olarak
kullanılmasında sakınca yoktur.
Emeęe gösterdięiniz hassasiyet için
teşekkür ederiz.



SAĞLIK BİLİŞİMİ VE BİLGİ GÜVENLİĞİ

Dr. Öğretim Üyesi Nuran AYDIN



AMAÇ ve İÇERİK

1. Veri ve Bilgi nedir ?
2. Bilgi Güvenliđi Neden Önemlidir
3. Bilgi Güvenliđine Yönelik Tehditler Nelerdir?
4. Bilgi Güvenliđi İçin Önlemler Nelerdir ?

VERİ NEDİR ?



BİLGİ NEDİR ?

VERİNİN İŞLENMİŞ HALİ

VERİ KORUMA ?
BİLGİ KORUMA ?

Tek başına bir verinin korunmasına ilişkin bir kanun ya da düzenleme yoktur

Veriler arasında ilişki ile ilgili düzenlemeler vardır

BİLGİ ya da BİLGİYE DÖNÜŞEBİLECEK VERİ KORUNMALIDIR

KURUMUNUZDA KAÇ TÜR BİLGİ VARDIR ?

GİZLİ

En kritik bilgiler
Sadece yönetim
kadrosu erişebilir.
Yetkisi olmayanın
erişmesi, yayması,
kullanması kurumu
zor durumda bırakır.

Sadece birim/ bölüm çalışanları
tarafından görülebilecek bilgiler

GİZLİ

Örneğin: hasta bilgileri, düşme raporu, denetim tutanağı vb

ERİŞİLEBİLİRLİK

Sadece
yetkilendirilmiş
kişilerin görebileceği
Haftalık faaliyet
raporları,
çalışma planları,
sunum hazırlıkları vb
kişisel bilgiler

ERİŞİLEBİLİRLİK

Kuruma açık bilgiler
Bültenler, araç hareket saatleri,

BİLGİNİN HANGİ ÖZELİKLERİNİ KORUMAMIZ GEREKİYOR?

GİZLİLİK : Bilginin yetkili olmayan kişiler, varlıklar ve süreçler tarafından erişilemez ve ifşa edilemez niteliğidir.

BÜTÜNLÜK : Bilginin doğruluk, bütünlük ve kendisine has özelliklerinin korunmasıdır.

ERİŞİLEBİLİRLİK: Bilginin yetkilendirilmiş kişiler tarafından istenildiğinde ulaşılabilir ve kullanılabilir olma özelliğine denir.

BİLGİ GÜVENLİĞİ NEDEN ÖNEMLİDİR?

- Birey/hasta/kuruma ait gizli ve hassas bilgiler herkese açık hale gelebilir
- Üçüncü şahıslar tarafından emanet edilen bilgiler ticari, teknolojik, adli bilgiler herkese açık hale gelebilir
- Kurum işlerliğini sağlayan bilgi ve süreçler herkese açık hale gelebilir
- Kurumun ismi, güvenilirliği, itibarı zedelenir
- İş sürekliliği zarar görebilir.....

BİLGİLERİ NEREDE SAKLIYORUZ / TUTUYORUZ/ BİRİKTİRİYORUZ /SERGİLİYORUZ ?



FİZİKSEL ORTAMLAR



BİLGİLERİ NEREDE SAKLIYORUZ / TUTUYORUZ/ BİRİKTİRİYORUZ /SERGİLİYORUZ ?

ELEKTRONİK ORTAMLAR



Bilgisayarlar

Mobil iletişim cihazları

E-posta,

USB,CD,Disk

Disket

Manyetik ortamlar

Ortak alan dosyaları vs

BİLGİLERİ NEREDE SAKLIYORUZ / TUTUYORUZ/ BİRİKTİRİYORUZ /SERGİLİYORUZ ?

SOSYAL ORTAMLAR

Sosyal medya araçları

Elektronik sohbet odaları

Elektronik konuşma uygulamaları

Telefon görüşmeleri

Görüntülü paylaşımlar

Ve tabii yemek ve kahve arası sohbetleri

BİLGİLERİ NEREDE SAKLIYORUZ / TUTUYORUZ/ BİRİKTİRİYORUZ /SERGİLİYORUZ ?

TANITIM ARAÇLARI

İnternet siteleri, kurum web sayfaları

Broşürler, Reklamlar, Sunumlar, Eğitimler, Görsel sunumlar.

www.acibademhemsirelik.com

The screenshot shows the homepage of the Acibadem Hemşirelik website. The header features the Acibadem logo and a navigation menu with items like 'ASG Hemşireliği', 'Kadrolarımız', 'Şubelerimiz', 'Eğitim', 'Yayınlarımız', 'Haberler', 'Hemşirelik Yasası', 'Linkler', and 'İletişim'. The main content area includes a 'Direktörümüzden' section with a photo of a nurse and a patient, and a text block about the organization's focus on research and education. Below this is a 'Haberler' section with a 'Geleceğe Bakış Projesi' article. The footer contains four promotional boxes: 'Göstergelerimiz' (Acibadem Sağlık Grubu Hemşirelik Hizmetleri olarak, hemşirelik kalite göstergelerimizi paylaşıyoruz.), 'Kariyer Fırsatları' (Açık pozisyonlara ulaşmak için tıklayınız.), 'Hemşirelik E-Dergi' (Acibadem Hemşirelik), and 'Hemşirelik Yasası' (Hemşirelik yasasına ulaşmak için tıklayınız.).

Bilgi Nedir?

Kurumumuzun işleri için kıymetli olan, korunması gereken bir varlıktır.

Koruma görevi kimin ?

YASALAR/YÖNETMELİKLER/ 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",

YASALAR/YÖNETMELİKLER/ MEVZUAT

- 26687 sayılı “İnternet **Toplu Kullanım Sağlayıcıları** Hakkında Yönetmelik,
- 26716 sayılı “İnternet Ortamında Yapılan **Yayınların Düzenlenmesine** Dair Usul ve Esaslar Hakkında Yönetmelik”,
- 26680 sayılı “Telekomünikasyon Kurumu Tarafından **Erişim Sağlayıcılara** ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik”,
- Sağlık Bakanlığı ve Bağlı Kuruluşlarınının **Elektronik Belge Yönetimi Sistemi** Uygulama Yönergesi,
- **Sağlık Bakanlığı Bilgi Güvenliği Politikaları Yönergesi.**

YASALAR/YÖNETMELİKLER/ MEVZUAT

- 28/02/2014 tarihli ve 5181.1272 sayılı Bakanlık Makamının onayı ile Bilgi Güvenliği Politikaları Yönergesi,
- 03/03/2014 tarihli ve 5181.1317 sayılı Bakanlık Makamının onayı ile Bilgi Güvenliği Politikaları Kılavuzu yürürlüğe girmiştir.
- 24/3/2016 Kişisel Verilerin Korunması Kanunu
- 09/02/2018 Kişisel Verileri Koruma Uzmanlığı Yönetmeliği

TEBLİĞ

Sermaye Piyasası Kurulundan:

BİLGİ SİSTEMLERİ YÖNETİMİ TEBLİĞİ

(VII-128.9)

<http://www.resmigazete.gov.tr/eskiler/2018/01/20180105-9.htm>

Veri gizliliği

MADDE 17 – (1) Kurum, Kuruluş ve Ortaklıklar, bilgi sistemleri faaliyetleri kapsamında gerçekleşen işlemlerin ve bu işlemler kapsamında iletilen, işlenen ve saklanan verilerin gizliliğini sağlayacak önlemleri alır. Gizliliği sağlamak üzere yapılacak çalışmalar asgari olarak aşağıda belirtilen hususları içerir:

a) Bilgi sistemleri yapısı ile iş ve işlem çeşitliliği göz önünde bulundurularak verilerin önem derecesine uygun önlemlerin alınması,

b) Verilere erişim haklarının kişilerin görev ve sorumlulukları çerçevesinde belirlenmesi, erişimlerin kayıt altına alınması, bu kayıtların yetkisiz erişim ve müdahalelere karşı korunması,

c) Veri gizliliğini sağlamada şifreleme tekniklerinin kullanılması durumunda, güvenilirliği ve sağlamlığı ispatlanmış algoritmaların kullanılması; geçerliliğini yitirmiş, çalınmış veya kırılmış şifreleme anahtarlarının kullanılmasının engellenmesi, verinin ve operasyonun önem düzeyine göre anahtarların değiştirilme sıklıklarının belirlenmesi.

(2) Kurum, Kuruluş ve Ortaklıklar, bilgi sistemleri faaliyetleri kapsamında gerçekleşen işlemlere ilişkin iletilen, işlenen ve saklanan önem derecesi yüksek verilerin kasten veya yanlışlıkla kurum dışına sızmasını önlemeye yönelik olarak gerekli önlemleri alır.

Kullanıcı Bilinci

Kullanıcının güvenlik bilinci birinci dereceden önemlidir

Bilgi sistem güvenlik açıklarının büyük kısmı kullanıcı hatasından kaynaklanmaktadır.

Kötü amaçlı girişimler (Hacker vb) çoğunlukla kullanıcı hatalarını kullanmaktadır

KULLANICIDA FARKINDALIK GELİŞTİRME ÖNEMLİ

Şifrelerimi

- a) hiç deęiřtirmem
- b) belli aralıklarla deęiřtiririm
- c) fikrim yok

Healthcare
Data Security
and Privacy:
It is your business

TEHDİTLERİ ÖĞRENELİM

KURUM İÇİ TEHDİTLER

• İYİ NİYETLİ TEHDİTLER

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

• KÖTÜ NİYETLİ TEHDİTLER

İşten çıkarılan çalışanın kuruma ait web sitesini değiştirmesi,
Bir çalışanın, ağda sniffer çalıştırarak e-postaları okuması,
Bir yöneticinin, geliştirilen ürünün planını rakip kurumlara satması.

KURUM DIŞI TEHDİTLER

• HEDEFE YÖNELİK SALDIRILAR

Bir saldırganın kurum web sitesini değiştirmesi,
Bir saldırganın kurum muhasebe kayıtlarını değiştirmesi,
Birçok saldırganın kurum sunucusuna hizmet aksatma saldırısı yapması.

• HEDEF GÖZETMEYEN SALDIRILAR

Virüs saldırıları (melissa, CIH – çernobil, vote),
Worm saldırıları (code red, nimda),
Trojan arka kapıları (netbus, subseven, black orifice).

DOĞAL/ FİZİKSEL TEHDİTLER

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

KÖTÜ NİYETLİ TEHDİTLER

Ağınıza, bilgisayarınıza zarar vermek ya da bilgileri çalmak ya da değiştirmek amacıyla yazılmış yazılımlardır.

Bilgisayar solucanları, Bilgisayar virüsleri, Truva atları, casusu yazılımlar , yığın mesajlar ...



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

TRUVA ATLARI



- Kullanıcıya, kullanışlı veya ilginç programlar gibi görünür
- Zararlı program barındıran veya yükleyen programdır
- Bilgisayarınızda uzaktan erişim kapısı açmak, internet bağlantınızı ortak kullanıma açmak, başka bir tarifeye yönlendirmek, sizin adınıza istemsiz e-posta göndermek vb işlemler yapabilir
- En tanınmış truva atı örnekleri, ub7, Poison Ivy, Bifrost, Pandora RAT (Türk yapımı), JRat, Prorat (Türk yapımı) sayılabilir.

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..)



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



ÖNLEMLER !!!!



KULLANICI ÖNLEMLERİ

TEMİZ MASA TEMİZ EKRAN

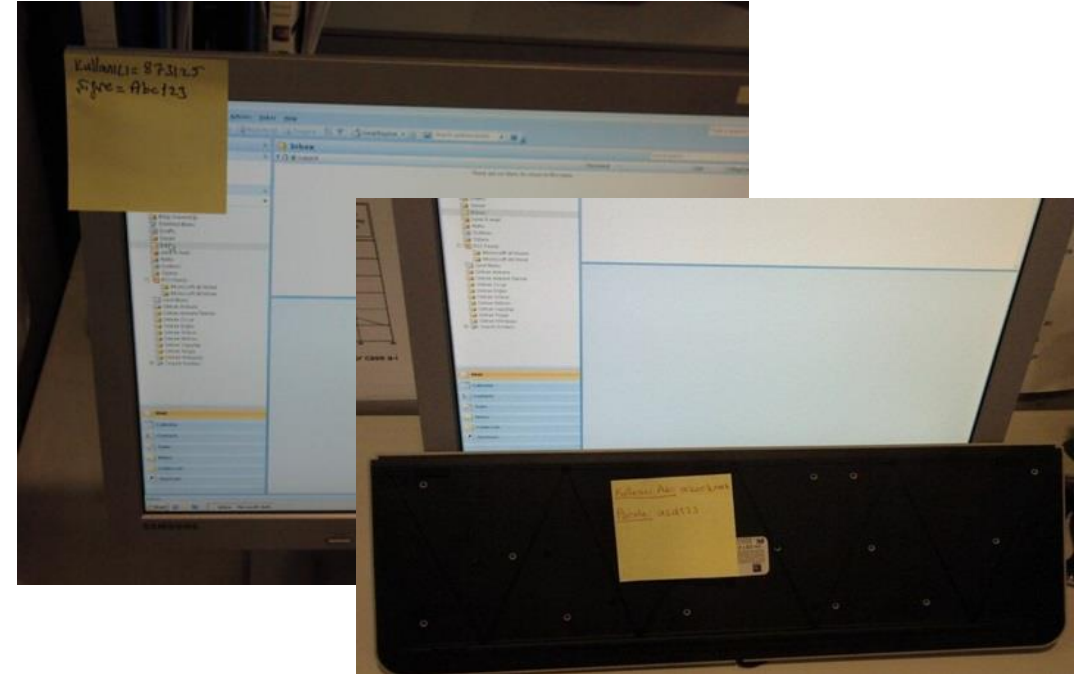
Çalışma masası ve bilgisayar ekranı üzerinde bilgiye yetkisiz ulaşım engellenmelidir.

Çalışma odaları ayrılırken kilitleyerek, 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



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)

Sözlükte bulunabilen kelimeler şifre olarak kullanılmamalıdır
Ardışık sayılar ve alfabetik karakterler kullanılmamalıdır.
Çoğu kişinin kullanabildiği aynı veya çok benzer yöntem ile geliştirilmiş şifreler kullanılmamalıdır.



GÜÇLÜ ŞİFRE

Cümlelerin baş harflerini birleştirebilirsiniz.

Günlük hayatınızdan kolay hatırlayacağınız herhangi bir cümle kullanabilirsiniz.

Benzer şekilde

- Atasözlerinden ,Şarkı sözlerinden, Şiirlerden vb
- seçeceğiniz cümlelerin aralarında rakamlar ve özel karakterler kullanarak çok daha güçlü bir parola oluşturmanız mümkün.
- Cümleleri olduğu gibi parola yapabilirsiniz

En az **8 karakter**den oluşur.

Harflerin yanı sıra, **rakam** ve "? , @ , ! , # , % , + , - , * , %" gibi **özel karakterler** içerir.

Büyük ve **küçük** harfler bir arada kullanılır.

Örneğin

- Yurtta Sulh Cihanda Sulh --> Y@S*C*S.
- 10 Yılda 15 milyon genç yarattık her yaştan. --> 10Y15mgyhy.
- Herseydahaguzelbirdunyaicin



E POSTA GÜVENLİĞİ

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

Birden çok kişiye veya bir gruba e-posta gönderirken kişilerin e-posta adreslerini **gizli karbon kopya (BCC) bölümüne** yazmak.

Bir web sitesinde yapılan işlem gereği e-posta adresi istendiğinde, **sitenin gizlilik politikasını** kontrol etmek

İstenmeyen e-postalara hiç bir şekilde **cevap yazmamak**

Özellikle kurum ve özel işleri ayırmak için, kullanım amacına göre **farklı e-posta adresleri** kullanmak

E POSTA GÜVENLİĞİ

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

SOSYAL MEDYA GÜVENLİĞİ

En çok kullanılan Sosyal Medya Uygulamalarının topladığı bilgiler

- Cihaz geçmişi
- Kimlik profil bilileri
- Konum
- Tarihçe
- Kişisel bilgiler
- Sosyal medya hesapları
- Telefon numarası
- Fotoğraf ve videolar
- Kayıtlı adresler
- Mülkiyet bilgileri
- Kayıtlı cihazlar
- Cihaz kimlik bilgileri

- *
- *
- *

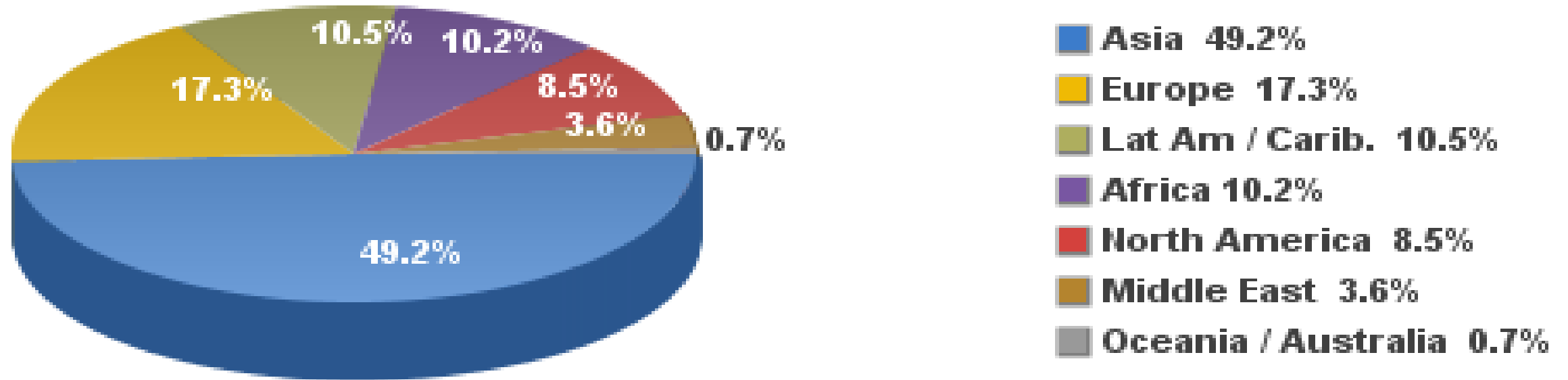
Bizler internet üzerinde bir karakter yaratma çabasında iken aslında birileri için birer **istatistikten** ve **dolandırılacak bir hesaptan** başka bir şey değiliz.



Eđitimden sonra bilinçlenen kullanıcılar hayatlarının sonuna kadar güvenli bir şekilde bilgisayar kullanmışlar...



Internet Users in the World by Regions - December 31, 2017



Source: Internet World Stats - www.internetworldstats.com/stats.htm

Basis: 4,050,247,583 Internet users in December 31, 2017

Copyright © 2018, Miniwatts Marketing Group



TURKEY

TR - 80,417,526 population (2017) - Country size: 773,473 sq km

Capital city: Ankara - population 4,630,735 (2012)

56,000,000 users in June, 2017, 69.6% penetration, per IWS.

56,000,000 Facebook users on June, 2017, 69.6% penetration rate.

<https://www.internetworldstats.com/europa2.htm#tr>

Yıllara Göre İnternet Kullanıcı Sayısı - Türkiye Telekomünikasyon Marketing Rapor

YEAR	Users	Population	% Pop.	Usage Source
2000	2,000,000	70,140,900	2.9 %	ITU
2004	5,500,000	73,556,173	7.5 %	ITU
2006	10,220,000	74,709,412	13.9 %	Comp. Ind. Almanac
2010	35,000,000	77,804,122	45.0 %	Comp. Ind. Almanac
2015	46,282,850	77,695,904	59.6 %	IWS

<https://www.internetworldstats.com/euro/tr.htm>

**DAHA FAZLASINI BİRLİKTE GERÇEKLEŐTİRMEK
İÇİN DERNEĐİMİZE ÜYE OLUNUZ**

<http://hembilder.org/>

