1.1 ETİK DEĞERLER

BİLİŞİM VE İNTERNET ETİĞİ:

(Bilişim Teknolojileri ve interneti kullanırken uyulması gereken kuralar)

1-) Kişisel bilgilerinizi (ad, soyadı, şifre, fotoğraf vb.)başkalarıyla paylaşmayınız.

2-) Tanımadığınız kişilerden gelen arkadaşlık isteklerini kabul etmeyin.

3-) İnterneti başkalarına zarar verme amaçlı kullanmayınız. (Dolandırma, küfür, hakaret, tehdit vb.)

4-) Başkasına ait içerikleri izinsiz olarak paylaşmayın, kullanmayın.(Telif Hakkı)

5-) Başkasına ait bilgileri kullanırken kaynağını belirtin.

6-) Lisanssız yazılım ve içerikler kullanmayın.

7-) Kaba ve küfürlü bir dil yerine, saygılı ve kibar bir dil kullanınız.

8-) Başkası adına sahte hesap/Profil/e-posta oluşturma gibi davranışlardan kaçınmalısınız.

9-) Başkalarının bilgilerini ele geçirme, değiştirme ve silme gibi davranışlardan kaçınmalısınız.

10-) Güçlü bir kullanıcı adı /şifre oluşturunuz ve kimseyle paylaşmayınız.

11-) İnternetteki uygunsuz içerikleri şikâyet edin.

BİLİŞİM SUÇLARI: Teknoloji kullanarak dijital ortamdaki kişi ve kurumlara maddi manevi zarar vermek. (dolandırıcılık, siber zorbalık, yasa dışı yayınlar, telif hakkı ihlali, siber saldırılar, sahte profil/hesap vb.)

FİKRİ MÜLKİYET: Kişinin kendi zihni tarafından ürettiği her türlü ürün. Hukuki ve etik boyutları vardır.

PATENT: buluş sahibinin buluş konusu ürünü belirli bir süre üretebilme, kullanabilme, satabilme veya ithal edebilme hakkını gösteren belge.

TELİF HAKKI: Kendi emeğimiz ile oluşturduğumuz ürünler üzerinde sahip olduğumuz haklar. Eseri kullanma, paylaşma, değiştirme vb. izinleri kapsar.

*Eserin izin verildiği ölçüde kullanılmasını sağlar

* Eser sahibin haklarını korur.

NOT: Başkasına ait ürünleri çoğaltmak, satmak suçtur.

Sahibinin izni olmadan çoğaltılan ve dağıtılan ürünlere **KORSAN** denir. **BANDROL** veya **BARKOD** ürünleri orijinal yapan koruma araçlarıdır.

LİSANS: Telif hakkına sahip olan eser sahibinin haklarını koruyan belge.

©	Her hakkı saklıdır.
℗	Kamu malıdır. Telif süresi bittiği için telif hakkı olmadan kullanılabilir.
cc	Bazı Hakları saklıdır. (Creative Commons) Sahibine atıf yapılmalı. Eser ticari amaçla kullanılamaz. Eseri türetemezsiniz.(eklemeler yapılamaz)

YAZILIM LİSANS ÇEŞİTLERİ

1-)Ücretsiz Yazılım (özgür yazılım/Freeware): Tamamı ücretsiz olarak kullanılan yazılımlar

2-) Lisanslı Yazılım: Yazılımı kullanabilmek için belli bir ücret ödenmelidir. Telif hakkı kapsamına girer.

3-)Beta (Geliştirme aşaması) Yazılım: Kullanıcılar tarafından yazılımın test edilerek eksik ve sorunların giderilmeye çalışıldığı yazılım.

4-) Demo Yazılım: Yazılımın kendisi ücretlidir. Ancak tanıtım amaçlı yazılımın bazı kısıtlı özelliklerini ücretsiz olarak kullanabildiğimiz sürümüne denir. Böylece piyasaya çıkarılacak yazılım kullanıcılara tanıtılmış olur.

5-) Paylaşılan Yazılım(Deneme sürümü/Shareware): Ücretlidir. Ancak kullanıcıya 30 ya da 15 günlük deneme süresi tanır, beğenilirse satın alınarak kullanılabilir.

TERİMLER:

İnternet: Dünyadaki tüm bilgisayarları birbirine bağlayan elektronik iletişim ağı.

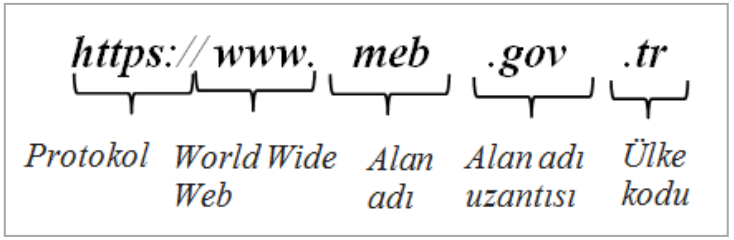
İnternet Tarayıcısı: İnternette istenilen bilgileri girilen kelimelere göre arayan programlardır.

- Google Chrome, İnternet Explorer,
- Yandex, Mozilla firefox, Opera vb.

Arama Motoru: İnternette arama yapılan web siteleri.

- www.google.com.tr
- www.yahoo.com.tr
- www.yandex.com.tr

URL: Web sitelerinin, internetteki yerini belirleyen bağlantı adreslerine verilen isimdir.



http: İnternet sayfalarının açılmasını sağlayan komutlar http ile iletilir. Web sayfalarının açılmasını sağlar.

- **https://** ile başlıyorsa site güvenlik sertifikasına sahiptir. Böyle siteler diğerlerine göre daha güvenlidir. Alışveriş, banka siteleri gibi kullanıcı adı, şifre vb. girilebilecek sitelerde kesinlikle bulunması gerekir.

Örnek: .au uzantısı Avustralya
.ch uzantısı İsviçre ülke kodlarıdır.

www (world wide web): Dünya çapında ağ anlamına gelir. Tüm web sayfalarında bulunur. Kısaca web denir.

Alan Adı Uzantıları:

.com: Ticari amaçlı siteler

.gov: Devlete ait olan siteler

.edu: Üniversitelere ait siteler

.org: Vakıf ve derneklere ait siteler

.k12: Okul öncesi, ilkokul, ortaokul ve lise kademesinde bulunan okulların siteleri

ÖRNEKLER:

- http://www.meb.gov.tr
- http://www.tema.org.tr
- https://www.kafkas.edu.tr
- https://www.hepsiburada.com.tr
- https://www.halkbank.com.tr
- https://www.kars.gov.tr (valilik)

SIRA SİZDE

Verilen internet adresinde soru işareti yerine hangisi gelmelidir?

kagizmanihl .meb ? .tr

.com .k12 .net .edu

İnternette bulduğumuz bir bilginin güvenilir olduğunu anlamak için ne yapmalıyız?

- ✓ Kullanıcıya bilgi aktaran kanal (İnternet sitesi, sosyal medya hesabı), kaynak belirtmelidir. (Kaynağı belirtilmemiş bilgiye şüpheyle yaklaşılmalıdır.)
- ✓ Elde edilen bilgiler üç farklı kaynaktan teyit edilmelidir.
- ✓ Bilgi edinilen İnternet siteleri, uzantılarına göre değerlendirilerek kaynak güvenilirliği konusunda bir kanıya varılabilir. (edu, gov, org gibi alan uzantılı siteler bilgi açısından daha güvenilirdir.)
- ✓ Https uzantılı internet siteleri daha güvenlidir.
- ✓ tr uzantılı siteler ülke geneli güvenlik kontrolünden geçirildiği için daha güvenilirdir.

SİBER: İnternete ait olan, interneti anlatan sanal ortam. Örnek: siber suç, siber saldırı, siber savaş vb.

Siber Suç: Bilişim Teknolojilerini kullanarak işlenen her türlü yasa dışı işlem.

Siber Saldırı: Hedef alınan kişi, kurum, şirket vb. bilişim alt yapılarına yapılan planlı saldırılardır.

Siber Savaş: Farklı bir ülkenin bilişim sistemleri ve altyapılarına yapılan planlı saldırılardır.

Siber Zorbalık: (Sanal ortamda yapılan zorbalık)
Aşağılamak, tehdit etmek, Hakaret etmek, Taciz etmek, sahte hesap oluşturmak, rızanız olmadan bilgilerinizi paylaşmak vb.

Neler yapılmalı?

1-)ENGELLEYİN (kişiyi engelle ve hesabının gizlilik ayarlarını değiştir.)

2-)UZAKLAŞIN (hemen sohbet penceresini kapat ve iletişim kurmaya devam etme.)

3-)ŞİKÂYET EDİN (Sosyal medya araçlarının Şikâyet Et/ Bildir bölümünü kullanın)

4-)YARDIM İSTEYİN (Büyüklerinizden yardım isteyin.)

Neler yapılmamalı?

1-)KANITLARI SİLME (zorbanın gönderdiği tüm iletileri, yorumları vb. saklayın.)

2-)YANIT VERME (zorbaya yanıt vermek onun zorbalığının artmasına neden olur.)

3-)MİSİLLEME YAPMA (Onun üslubuyla karşılık verme.)

4-)GÖZ YUMMA (Zorbalık yapan birini ve ya maruz kalan birini gördüğünde yardımcı olmaya çalış)

Modem: Bilgisayarın internete bağlanmasını sağlayan cihaz. Kablolu ve kablosuz çeşitleri vardır.

Kablosuz Ağ (wifi): İnternete kablo olmadan bağlanmayı sağlayan ağ sistemi.

E-posta: İnternet üzerinden gönderilen elektronik mektup(e-mail). Epostada ismimizden sonra kullanılan işaret "@" işaretidir. Örn: kubraozkn@gmail.com

Hoax (Aldatmaca e-posta):

Gelen e-postayı başkalarına göndermeni ya da herhangi başka bir eylemde bulunmanı sağlamak amacı ile, içinde aldatmaya ve kandırmaya yönelik ilginç bir konu (ölümcül hastalık, hediye, acil haber, uyarı, komplo teorisi) geçen e-postalardır. Örneğin;

- "Bilgisayarınızda ... dosyası varsa o bir virüstür. Hemen silmelisiniz." gibi bir mesaj
- "... havayolunun bu mesaji yolladığınız her 5 kişi için size bedava bir uçuş bileti sağlayacağı" gibi bir mesaj
- Yardım talebinde bulunan bir kişiden gönderilmiş mesaj olabilir

Phishing (oltalama e-posta):

Taklit (oltalama) e-postası, kimlik bilgilerini çalmak amacı ile, istenmeyen e-posta veya açılır pencere yoluyla yapılan bir aldatma yöntemidir.

Saldırgan önceden tasarlanan bir hikâye üzerinden, kullanıcıyı e-postanın güvenilir bir kaynaktan geldiğine inandırıp, özel bilgilerini (kredi kartı, şifre bilgileri vs…) ele geçirmeye çalışır.

SIRA SİZDE

Önemli bilgilerimizin başına neler gelebilir?

Önemli bilgilerimizi nasıl koruyoruz?

1.3.BİLGİ GÜVENLİĞİ:

Önemli bilgilerimize izin alınmadan yetkisiz erişilmesi, bilgilerimizin ifşa edilmesi, kullanılması, yok edilmesi gibi tehditlere karşı alınan tüm tedbirlere bilgi güvenliği denir. Bilgi güvenliğini oluşturan 3 ana unsur:

Gizlilik, Erişilebilirlik ve bütünlüktür.

Gizlilik: Önemli bilgilerin yetkisiz kişilerin eline geçmemesi bilgi gizliliğini ifade eder.

Örnek: Şirket ve kurumların bazı belgelerine sadece yetkili kişilerin erişebilmesi. (erişim kısıtlamaları)

Erişilebilirlik: Bilginin ihtiyaç duyulduğu anda erişilebilir olması. **Örnek:** Önemli bilgilerin hem bilgisayarda, hem hard diskte tutulması. Erişilebilirliği artırmak için alternatif yollar oluşturulmalıdır. Bilgilerin yedeğini almak vb.

Bütünlük: Bilgilerin yetkisiz kişiler tarafından değiştirilmemesini kapsayan unsurdur. **Örnek:** Hackerlerin verileri silmesi, bozması, yok etmesi bilgi güvenliğinde bütünlük ilkesi ile ilgilidir.

Bilgi güvenliğini Neler tehdit eder?

- İstenmeyen kişilerin erişebilmesi (Hack)
- Fiziksel zararlar (bilgisayarın bozulması, zarar görmesi vb.)
- Bilgilerin yazma, okuma, taşınma sırasında bozulması ve ya kaybolması(kullanıcı hataları)
- Bilginin yok edilmesi, silinmesi vb.
- Zararlı yazılımların bulaşması

Bilgi Güvenliği Nasıl sağlanır?

- Güvenlik yazılımları (antivirüs yazılımları)
- Yedek alma
- Verileri şifreleme (Dosyaya şifre koyma)
- Kullanıcı/yönetici oturumu açma
- Oturumu kapatma(sistemden çıkarken)
- Parola ile giriş (sisteme girerken)

Güçlü şifre oluştururken nelere dikkat edilmeli?

- En az 8 karakter kullan
- Sınıf, telefon numarası gibi kişisel bilgiler kullanma
- Beli örüntülerden oluşan şifre seçme (A1b2c3)
- Harf yerine sayı kullan (B yerine 8, S yerine 5 gibi.)
- Ara ara şifreni güncelle.(en geç 6 ay)
- Tüm hesaplarında aynı şifreyi kullanma
- Şifreni kimseyle paylaşma
- Sayı, Büyük, küçük harf ve Özel Karakterler(* ? + vb.) kullanmak şifreni daha güvenli yapar.
- Hesabından tamamen çıktığınıza emin olun.
- Oturumu Kapat. Örnek güvenli şifreler: 8iL9i5@y@r, F@ce800k

SIRA SİZDE

Kendinize Güçlü bir Şifre Oluşturun:

SIRA SİZDE

1) Alan Turing Kimdir?

2) Enigma makinesi nedir?

3) Turing testi nedir?

ZARARLI YAZILIMLAR:

NOT:

- Sisteminiz yavaşlamışsa,
- Bilgileriniz kayboluyorsa
- İstemediğiniz programlar, internet sayfaları kendi kendine açılıyorsa,
- Bilgisayar verdiğiniz komutları yerine getirmiyorsa,
- Bilgisayar isteğiniz dışı işlem yapıyorsa,
- Bazı dosyalarınız açılmıyorsa,

Sisteminize Zararlı Yazılım Bulaşmış olabilir!!

Zararlı Yazılımlar Neler yapabilir?

- Bilgisayardaki bilgileri çalabilir, başkasına gönderebilir.(e-posta hesabı, şifre, parola vb.)
- İşletim sisteminin veya diğer programların çalışmamasına, hatalı çalışmasına neden olabilir.
- Bilgisayardaki dosya ve klasörleri silebilir, kopyalayabilir, yerini değiştirebilir, yeni dosyalar ekleyebilir.
- Bilgisayarda yapılan her şeyi kaydeder. (Klavyede yazılan şeyler, Mouse hareketleri vb.)
- Ekranda can sıkıcı ve ya kötü amaçlı web sitelere yönlendiren açılır pencereler oluşturabilir.
- Diskteki tüm verileri silebilir, biçimlendirebilir.
- Bilgisayarınızı kullanarak siber saldırı yapabilirler.
- Güvenlik açığı oluşturur, bilgisayarı yavaşlatır.

Nasıl korunabiliriz?

- Güvenlik duvarını aktif olarak kullan
- Önemli bilgilerini yedekle.
- İşletim sistemini güncelle (Bazı işletim sistemleri daha güvenlidir.)
- Virüs koruma(Anti virüs) programı kullan.
- Emin olmadığın e-postaları açma
- Her bulduğun linkle tıklama
- Güvenilir olmayan sitelerden müzik, oyun, program, video indirme
- İnternet tarayıcı güvenlik ayarlarını üst düzeyde tut.
- Lisanssız yazılım kullanma

NOT: Bulaşmış virüs temizlenmiyorsa başka anti virüs programı ile temizle, eğer yine temizlenmiyorsa işletim sistemini biçimlendirin (format atın)

Zararlı Yazılım Çeşitleri:

Virüsler: Bir bilgisayardan diğerine yayılan, bilgisayarı olumsuz etkileyen yazılımlardır.
Spam: İnternette isteğimiz dışı aldığımız, kimin gönderdiği belli olmayan e-postalar.(reklam, virüs bulaştırma amacı ile gönderilir.)
Pop-up: İnternette gezinirken aniden açılan küçük pencere uygulamaları (reklamlar)

Solucan(WORM):Ağ üzerinden otomatik olarak yayılır. Güvenlik açığı oluşturur. Bilgisayarın çalışması için gerekli dosyaları bozarak bilgisayarın yavaşlamasına veya çökmesine neden olur.

Truva Atı(Trojen Horse): Güvenilir gibi görünen kötü amaçlı yazılımdır. Truva atının çalışması için kullanıcının izin vermesi ya da kendi isteği ile kurması gerekir:

- Flash bellek ile (bilinmeyen flashların bilgisayara takılması)
- Tanınmayan e-postaları açarak, linklere tıklanması
- Bilinmeyen sitelerden indirilen programlar ile

Casus Yazılım(Spyware): İnternetten izniniz olmadan bilgisayara yüklenen, bilgisayardaki bilgileri uzaktaki bir kullanıcıya gönderen yazılımdır.

Reklam Yazılımı(Adware): Bilgisayarınızda reklamları otomatik olarak gösteren zararlı yazılımdır. Herhangi bir işle meşgulken ekranda aniden reklam açar.

Rootkit: Bilgisayar üzerinde çalışan programları gizleyen programdır. Tespit edilmesi çok zordur. Bilgisayar uzaktan kontrol edilebilir, bilgisayarın video kamerası kullanılarak özel hayatın gizliliğine müdahale edilebilir, bilgisayarınız siber saldırılarda kullanılabilir.

Ransomeware (Fidyeci yazılım): Saldırgan tarafından istenen fidye ödenene kadar bilgisayara erişimi engelleyen yazılımdır.

Keylogger(Tuş takip programı): Klavyede basılan her tuşu, Mouse hareketlerini kaydeder. (kullanıcı adı, şifre, banka bilgileri, tc kimlik vb.)

DDoS Saldırısı: Hacker tarafından kontrol edilen Binlerce bilgisayarın(botnetlerin) aynı anda web sitesine erişmesini sağlayarak siteye erişimin engellenmesi(sitenin çökmesi) olayına denir. Planlı yapılan saldırılardır.

Botnet: Hackerler tarafından uzaktan kontrol edilen virüslü bilgisayara verilen ad. DDoS saldırısı yapmak için kullanılır.

SIRA SİZDE

Bir web sitesinin içeriğinin güvenli olup olmadığını nasıl anlarsınız?

Bir web sitesinin içeriğinin güvenli olduğunu nasıl anlarım?

- Web sitesi bilinen bir kuruma ya da markaya ait mi? (EVET)
- Web sitesinin doğrulayacak telefon, adres, e-posta vb. iletişim bilgileri bulunuyor mu? (EVET)
- Web sitesi kişisel bilgilerini istiyor mu? (HAYIR)
- İçeriğin kimin tarafından yazıldığı açık bir şekilde belirtilmiş mi? (EVET)
- İçeriği Oluşturulma tarihi belli mi? (EVET)
- Kaynağı belirtilmiş mi? (EVET)
- Sitenin alan uzantısı(gov, edu, org vb.) içerikle uyumlu mu? (EVET)

NOT: Güvenli bir web sitesi sizden kişisel bilgilerinizi (telefon , adres, tckimlik no) istemez.

İnternette Bilgilerini Korumak ve güvenli olmak için;

- İnternette kimlik bilgilerini isteyen sitelere karşı Dikkatli Ol!
- Bedava hediyelerden, programlardan ve yarışmalardan Uzak Dur!
- Eğlenceli görünen testler, hakkında bilgi toplamak için yapılmış olabilir. Düşün!
- Bilinen markalar ve ya kurumlar e-posta ile senden parola, kimlik bilgileri vb. kişisel bilgilerini istemez Unutma!
- Açılır Pencerelere(pop-up) ,gelen yarışma ve anketlere Katılma!
- Şüpheli bulduğun e-postanın içindeki bağlantıya (linke) Tıklama!
- Tanımadığın kişilerden gelen e-postayı açmadan önce Bir kez daha düşün!
- İçeriği arkadaşlarına da göndermeni isteyen e-postalar seni ve arkadaşlarını riske atabilir. E-postayı sil ve arkadaşlarını Uyar!
- Uygunsuz içerikleri Rapor et, Şikâyet et!