ETİK, GÜVENLİK VE TOPLUM

ETİK; bireylerin ahlaklı ve erdemli bir hayat yaşayabilmesi için, hangi davranışlarının doğru, hangilerinin yanlış olduğunu araştıran bir felsefe dalıdır.

ETİK DAVRANIŞ: Toplumca hoş görülen, kabul gören ahlaklı ve erdemli olarak kabul edilen davranışlara denir.

Etik davranışa örnek: Yaşlılara yardım etmek,

Doktorların hastalara iyi davranması

Etik dışı(etik olmayan) Davranışa Örnek:

Yere tükürmek,

Hırsızlık yapmak,

İnternette başkasına ait bilgileri ifşa etmek

Başkasına ait sosyal medya hesaplarını çalmak..

Bilgisayara virüs bulaştırmak

BİLİŞİM ETİĞİ: Bilişim teknolojilerinin ve İnternet'in kullanımı sırasında uyulması gereken kuralları tanımlayan ilkelere bilişim etiği denir.

BİLİŞİM TEKNOLOJİLERİNİN KULLANIMINDA YAŞANAN ETİK SORUNLARIN

fikri mülkiyet, erişim, gizlilik ve doğruluk

İNTERNET ÜZERİNDEN BİLGİ EDİNİRKEN NELERE DİKKAT ETMELİYİZ?

- Kullanıcıya bilgi aktaran kanal (İnternet sitesi, sosyal medya hesabı), kaynak belirtmelidir.
- Kaynağı belirtilmemiş bilgiye şüpheyle yaklaşılmalıdır.
- Elde edilen bilgiler üç farklı kaynaktan teyit edilmelidir.
- Bilgiyi aktaran İnternet sitesinin adresi kontrol edilmelidir. Alan adı uzantıları birçok İnternet sitesi için fikir verebilir.

İNTERNET ADRESİ YAPILARI

Bir internet site adresi aşağıdaki kısımlardan oluşur.

http://www.meb.gov.tr

adresini inceleyecek olursak; http: İletişim protokolü (internete bağlanma şekli)

www: World Wide Web in kısaltmasıdır. Geniş dünya ağı demektir. meb: Alan adıdır.

İnternet sitesinin internetteki ismidir. gov: internet sitesinin uzantı türüdür. Sitenin

hangi tür site olduğu hakkında bilgi verir.

tr: ülke kodudur. Web sitesinin hangi ülkeye ait olduğunu belirtir.

İnternet adresi uzantı türleri;

İnternet adresi uzantısı	*Hangi tür sitelere ait olduğu*
gov	Resmi kurum, devlet ait siteler Örn: www.usak.gov.tr (uşak valiliği sitesi) www.meb.gov.tr (milli eğitim bakanlığı sitesi)
com	Ticari amaçlı siteler için kullanılır. şahıs veya kurumsal olabilir. Örn: www.n11.com.tr www.facebook.com www.google.com
edu	Üniversite siteleridir Örn:www.usak.edu.tr Uşak üniversitesi sitesi www.ege.edu.tr ege üniversitesi sitesi
k12	İlk ve orta dereceli okul siteleri için kullanılır. Örn:www.izzettincalislarlisesi.meb.k12.tr (okul sitesi)
Org	Organizasyon, vakıf ve dernek gibi kar amacı güdmeyen kuruluşlar için kullanılır. Örn:www.yesilay.org.tr Yeşilay ın internet sitesi

Ülke kodları:

İnternet sitelerindeki ülke kodları o ülkenin kendi dilindeki yazılışının ilk iki harfidir.

Ülke kodu	Ait olduğu ülke
tr	Türkiye
de	almanya
ru	rusya
us	amerika
fr	Fransa

SİBER ZORBALIK NEDİR?

Bir birey veya grubun bilişim teknolojilerini diğer bireylere;

Zarar vermek,

Kötü niyetli,

Tekrarlayan şekilde kullanmasıdır.

Ayrıca siber zorbalık internet ortamında bilgisayarlar, telefonlar, tabletler ile whatsAPP, facebook, instagram, tiktok, snapchat, twitter, online oyunlar v.b ortamlar aracığıyla da yapılabilir.

Kısacası siber zorbalık internet ortamında veya bilişim teknolojileri aracılığıyla bir başkasına zarar verme işlemidir diyebiliriz.

Siber zorbalık davranışlarına örnekler;

SİBER ZORBA: Siber zorbalığı yapan kişiye denir.

SİBER MAĞDUR: Siber zorbalık davranışından etkilenen kişiye denir.

SİBER ZORBALIĞA MARUZ KALMANIZ DURUMUNDA YAPMANIZ GEREKENLER

1-öncelikle siber zorbalık yapan hesaba/kişiye cevap vermeyiniz.

2- Tartışmaya ve iletişime girmeyiniz.

3- Hesabı engelleyiniz.

4-Bu hesapları bulunduğu platformlarda bildir/şikayet et v.b gibi şikayet birimlerine şikayet ediniz. 5-Size yönelik siber zorbalık davranışı hala devam ederse, siber zorbalık davranışının ekran görüntüsünü kaydediniz veya mesaj ise silmeyiniz. Ve bir büyüğünüze veya Öğretmeninize haber veriniz.

6-Siber zorbalığa maruz kalan başka kişiler ile karşılaşırsanız bu üç maddeyi onlara da hatırlatınız.

PAROLALAR VE ŞİFRELER

Şifreler ve parolalar hayatımızda. Hemen hemen hepimizin bir sürü şifre ve parolaları var. Parolalarımızın ve şifrelerimizin başkaları tarafından kırılmaması için güçlü şifreler ve parolalar oluşturmalıyız.

Şifre veya parolalarımız başkasının eline geçerse;

- Ele geçirilen bilgiler yetkisiz kişiler ile paylaşılabilir ve şantaj amacıyla kullanılabilir.
- Parolası ele gecirilen sistem başka bir bilişim sistemine saldırı amacıyla kullanılabilir.
- Parola sahibinin saygınlığının zarar gormesine yol acabilecek eylemlerde bulunulabilir.
- Ele gecirilen parola ile ekonomik kayba uğrayabilecek işlemler yapılabilir.
- Parola sahibinin yasal yaptırım ile karşı karşıya kalmasına yol acabilir.

Güçlü Parola ve Şifre belirlerken Uyulması Gerekenler

- Büyük Harf, küçük harfler kullanılmalı
- Rakam ve Özel karakterler olmalı
- Noktalama işaretlerinden olmalı En az 8 basamaklı olmalı
- Belirli aralıklarla değiştirilmeliler
- Ardışık rakamlar ve harfler kullanılmamalıdır
- Doğum tarihi gibi tahmin edilebilecek karakterden şifre oluşturmuyoruz. Örn:güçlü parola örneği yazınız…

Şifre ve parolaların güvenirliği için;

- Hiç kimseyle paylaşmıyoruz
- Herhangi bir yazılı veya elektronik ortamlara yazmıyoruz
- Kullanılan farklı hesaplar için farklı parola ve şifreler kullanmalıyız

ZARARLI YAZILIMLAR

Yazılımcılar tarafından geliştirilen bilgi ve belgelerimizi ele geçirmek, sistemlerimize zarar vermek gibi kötü amaçlar için yazılmış yazılımlara denir.

ZARARLI YAZILIMLARIN BULAŞMA YÖNTEMLERİ

- Mail adreslerinden ve mail eklerinden
- Usb belleklerden
- Crackli korsan yazılımlardan
- Güvenilmeyen download sitelerinden
- Güvenilmeyen internet sitelerinden
- Anlık mesajlaşma ve sosyal medya ileti ve mesajlarından

ZARARLI YAZILIMLARA KARŞI ALINABİLECEK TEDBİRLER

- Güncel antivirüs programı kurulmalı ve sürekli güncel tutulmalı
- Güncel işletim sistemi kullanmak
- Korsan (crack) Yazılımlar kullanmamalıyız
- Tanımadığımız mail adreslerinden gelen mailleri ve özellikle eklerini açmıyoruz, Yada antivirüs programları ile taratıyoruz.
- Zararlı yazılım barındırabilecek güvenilmeyen web sitelerinden uzak duruyoruz.
- Güvenli olmayan download sitelerinden dosya vb indirme yapmıyoruz.
- Flash bellekleri sürekli taratmalıyız
- Güvenlik duvarı programları kullanabiliriz.

Bilgisayarımıza Virüs Bulaşmış olabileceğini nasıl anlarız?

- Bilgisayar yavaşlar, kasmaya başlar veya donar.
- Bilgisayar açılmayabilir.
- Bilgisayarda kendi kendi sayfalar veya dosyalar veya programlar açılabilir.
- Uygulamalar bozulabilir.
- Belge ve dosyalarımız silinebilir, bozulabilir
- Bilgisayarımıza değişik türde dosyalar kendini kopyalabilir.

□