Etik ve Güvenlik

Etik; doğru ile yanlışı, haklı ile haksızı, iyi ile kötüyü, adil ile adil olmayanı ayırt etmek, bunun sonucunda da doğru, haklı, iyi ve adil olduğuna inandığımız şeyleri yapmaktır.
Sanal ortamlarda iletişim kurarken doğru ve yanlış davranışları ayıran kurallara internet etiği denildiğini 6.sınıfta öğrenmiştik. Gerçek yaşamda suç olan ve etik olmayan davranışların sanal alemde de suç olduğunu ve etik olmadığını unutmamamız gerekiyor.
İnternet kullanımına yönelik temel etik kurallarında birkaçı aşağıdadır.

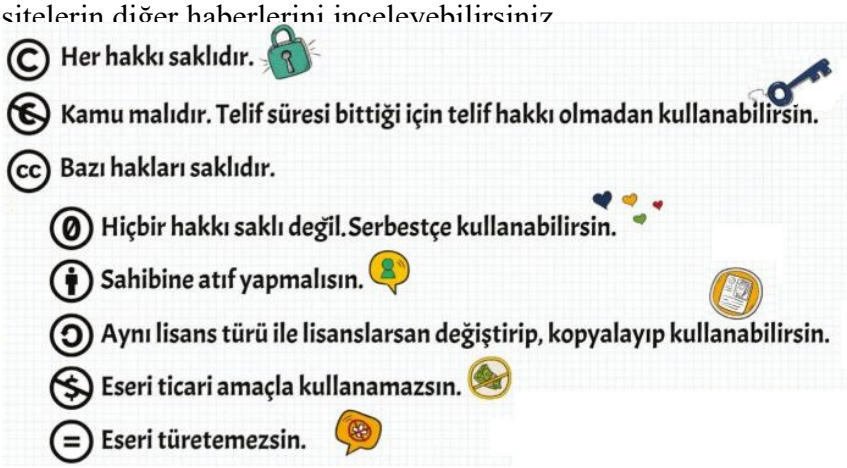
- ✗ İnternet'i, insanlara zarar vermek için kullanmamalıyız.
- ✗ Başkalarının İnternet'te yaptığı çalışmalara engel olmamalıyız.
- ✗ Başkalarının gizli ve kişisel dosyalarına İnternet yoluyla ulaşmamalıyız.
- ✗ Bilgilerin doğruluğuna tam olarak emin olmadan bilgileri savunmamalıyız.
- ✗ Parasını ödemediğimiz yazılımları kopyalayıp kendi malımız gibi kullanmamalıyız.
- ✗ Başkalarının elektronik iletişim kaynaklarını izinsiz kullanmamalıyız.
- ✗ Elektronik iletişim ortamını başkalarının haklarına saygı göstererek kullanmalıyız.
- ✗ İletişim sürecinde kullandığımız dilin doğuracağı sonuçları önceden düşünmeliyiz.
- ✗

Bunu paylaşmalı mıyım?

Yapılan araştırmalarda yalan haberin yayılma hızının, doğru haberin yayılma hızından 6-10 kat fazla oluğu tespit edilmiş. Bundan dolayı karşımıza çıkan bilginin doğrulunu güvenilir ve birden fazla kaynaktan kontrol etmeliyiz.
Bilgiyi güvenilir be bilinen bir kaynak üzerinden almalıyız.
Karşınıza çıkan her bilgi doğru olmayabilir. Eleştrisel yaklaşın, şüpheci olun.
Yalan haberlerde zaman ve görseller tutarsızlık gösterir.
Yanıltma, provokasyon, abartılı içerik olmadığından emin olun.
Montaj, alakasız görsel kullanılmış olabilir. Arama motorlarından görsellerin asıllarını bulmaya çalışın.
Haberi yayınlandığı veya kaynak gösterilen sitelerin diğer haberlerini incelevebilirsiniz

Fikri Mülkiyet Hakları ve Önemi

Fikri Mülkiyet : Zihinsel bir emeğin sonucunda ortaya çıkan ürünlerin, sahibine belli süre için tanınan patent, telif hakkı, endüstriyel tasarım hakkı gibi yasal haklardır.
Fikri mülkiyetin **hukuk** ve **etik** olmak üzere iki boyutu vardır.



Şekil 1: İşaretlerin Anlamları

Gizlilik ve Güvenlik

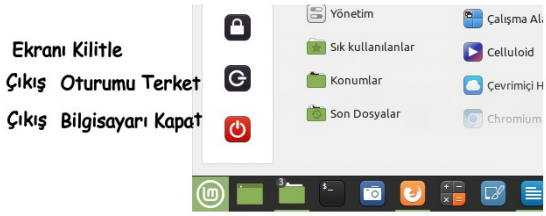
Pek çok alanda bilgisayar ve internet kullanımı hayatımızı kolaylaştırdığı gibi kaynaklı sorunlar bazı olumsuzluklara da sebep olabiliyor. Bu olumsuzluklara örnek olarak hırsızlık, dolandırıcılık, hakaret, taciz, istismar, hak ihlali, özel hayatın gizliliği...
Bilgi güvenliğin 3 temel unsuru vardır. (6.sınıfta konuyu işlemiştik)

1. **Gizlilik** : Bilginin yetkisiz kişilerin eline geçmemesi için alınan önlemler
2. **Erişebilirlik** : Yetkili olan kişilerin gerektiği zaman bilgiye ulaşmalarıdır.
3. **Bütünlük** : Bilginin silinmesi, zarar örmesi ve yetkisiz kişilerce değiştirilmesini engellemek içindir.

Şekil 2: Güvenlik Unsurları

Günümüzde bilgi güvenliğinin en zayıf noktasının **kullanıcı** olduğunu asla unutmayalım.

Çeşitli Ortamlara Güvenlik

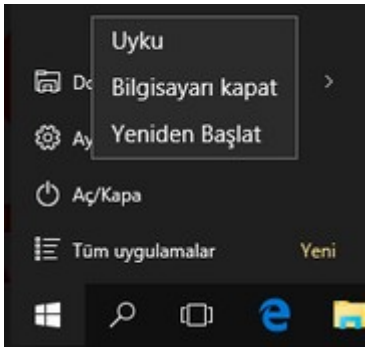


Şekil 3: Linux Mint 20.2 Cinnamon

Kullanıcılar kullanım sırasında güçlü şifre oluşturma, şifrelerini saklama, kişisel bilgilerini sanal alemde paylaşmama, sanal ayak izi bırakmamaya dikkat etmek gibi 5. ve 6. sınıfta gördüğümüz konular haricinde donanım ve yazılım seviyesinde güvenlik ayarlarına dikkat etmeliyiz.

Donanım seviyesinde:

a) Eğer bilgisayarımızı birçok kişi kullanıyorsa BİOS ayarlarından şifre verebilirsiniz. Böylece istemediğiniz kişilerin bilgisayarına format atmak gibi işlemleri yerine getirmesini engelleyebilirsiniz.



Şekil 4: Windows 10

b)Kullanıcı ve parola ekleme: Normal ayarlarda bilgisayarda tek kullanıcı olur isterseniz parola ekleyerek başkalarının erişmesini engelleyebilirsiniz ya da ikinci (gerekirse üçüncü bir) kullanıcı ekleyerek parola yardımıyla kullanıcıların başka kullanıcıların dosya ve ayarlarını görmelerini engelleyebilirsiniz. Bu işlemi Windows, Linux, Mac, Android cihazların hepsinde yapabilirsiniz. Uyarı: bilgisayarı kullanmadığınız zamanda kapatmak ya da "oturumu kapat" seçeneğini unutmayın.

Yazılım seviyesinde :

a) Ofis programlarında dosyalara parola eklenebilir.

b) Sıkıştırma programları kullanılarak klasör ve dosyalara parola eklenebilir.

Bu iki işlemde de okuma, yazma, salt okunur olarak açma izinlerine dikkat ederek istediğimiz seviyede güvenliğe ücretsiz bir şekilde ulaşabiliriz.

Güvenlik Tehditleri ve Alınabilecek Önlemler

Gerekli tedbirleri almazsak kullandığımız cihazlara zararlı yazılımlar bulaşabilir, yazılımlarımız hatta cihazlarımız bile zarar verebilir.

Basit birkaç önlemle yaşayabileceğimiz sıkıntıları engelleyebilir veya azaltabiliriz.

- Korsan yazılım kullanılma, dosya paylaşım programları, kaynağı belirsiz programlar, eposta ile gelen dosyaları taratmadan indirme, gelen bağlantılara kontrol etmeden tıklama, farklı cihazdan gelen taşınabilir belleği kontrol etmeden cihazımıza takma gibi işlemlerden uzak durmalıyız.
- Güncel antivirüs kullanımı, internette sayfalardan gelen uyarıları okumadan onaylamama, e postaları kontrol edip açma, sosyal medya ve mesajlaşma uygulamalarından gelen mesajları güvendiğimiz kişilerden bile gelse bile açmama, bu mecralarda gizlilik ayarlarını düzenleme... oluşabilecek sıkıntıları en aza indirmemizi sağlar.

Not: Şifre ve parola kelimeleri anlam yönüyle karıştırılabilmektedir. Basit olarak parola, okunduğunda anlam ifade eden, kişinin kendinin de bildiği, kendinin seçip kullandığı kelimelerdir. Şifre ise normal olarak okunduğunda bir anlam ifade etmeyen, kişiden kişiye farklı gösteren metinlerin çeşitli algoritmalar ile oluşturulan metinlerdir. Kısaca "**senin bildiğin parola, sistemin bildiği şifredir."** denilebilir. Önceki yıllarda dersimizde gördüğünüz "Sezar Şifresi"ni hatırlayınız.