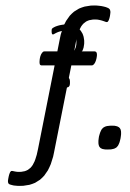
1.1. Etik Değerler

Etik; bireylerin ahlaklı ve erdemli bir hayat yaşayabilmesi için hangi davranışlarının doğru, hangilerinin yanlış olduğunu araştıran bir felsefe dalıdır. Temelinde barındırdığı güzel ahlaklı, adaletli ve iyi insan olma özellikleri değişmese de zamana, bilimsel gelişmelere ve toplumun gereklerine göre etik kavramına yüklenen anlam değişebilmektedir. Bir konuya ya da belirli bir meslek dalına özgü etik davranışların tamamı **etik değerler** olarak tanımlanabilir. Bir alanın evrensel etik değerlerinin belirlenmesi için o alanın toplum tarafından kabul gören ve görmeyen davranışlarının tanımlanması ve bireylerin bunlara uygun davranmalarının sağlanması gerekmektedir. Etik dışı eylemlere ilişkin yaptırımlar, çoğu zaman toplum tarafından belirlenmekte ve bu yaptırımlar gerekirse yasal düzenlemeler için belirleyici olmaktadır.



Günlük hayatımızın vazgeçilmez parçası hâline gelen bilişim teknolojileri; eğitim, sağlık, medya, iletişim, ticaret ve bankacılık gibi sektörler başta olmak üzere pek çok alanda yaygın bir şekilde kullanılmaktadır. Bilişim teknolojilerinde yaşanan bu hızlı değişim ve yaygınlaşma, istenen bilgiye her zaman ve her yerde erişebilme imkânı gibi faydalar sunmasının yanı sıra bu teknolojilerin tam olarak anlaşılmadan kullanımına yol açmakta ve bu durum da beraberinde pek çok sorun ortaya çıkarmaktadır. Bu anlamda yaşanan sorunlardan birisi de zaman ve mekân sınırı olmaksızın erişilen bilginin doğruluğunun ve kaynağının tespitidir. Gelişmekte olan ülkelerde toplumsal ve bireysel düzeyde artan rekabet ortamı, maddi kazanç sağlama ve bilginin kaynağından çok sonuca odaklanan yaklaşımlar, etiğin geri plana itilmesine yol açmaktadır. Gelişmiş toplumun önemli göstergelerinden birisi de gerek üretilen bilginin gerekse bu bilgiyi kullanan bireylerin etik kurallara uyup uymadıklarıdır. Geleceğin bireylerinin şekillenmesinde bilginin üretilmesi kadar bu bilgilerin etik kurallara göre üretilip paylaşılmasını da sağlamak önem kazanmaktadır. Bu da etiğin ne kadar önemli olduğunu göstermektedir.

1.2. Bilişim Teknolojileri ve İnternet Kullanımında Dikkat Edilmesi Gereken Etik İlkeler

Bilişim teknolojilerinin ve Internet'in kullanımı sırasında uyulması gereken kuralları tanımlayan ilkelere **bilişim etiği** denir. Bu ilkelerin temel amacı, bilişim teknolojileri ve İnterneti kullanan bireylerin yanlış bir davranış sergilemesine engel olarak onları güvence altına almaktır. Buna göre bilişim etiği, bilişim teknolojilerinin kullanımı esnasında toplum tarafından kabul gören uyulması gereken kurallar bütünüdür. Bilişim teknolojilerinin kullanımında yaşanan etik sorunların dört temel başlıkta (fikrî mülkiyet, erişim, gizlilik ve doğruluk) ele alındığı görülmektedir. Aşağıda bu başlıklara kısaca değinilmiştir.

1.2.1. Fikrî Mülkiyet

Bilişim teknolojileri alanında geliştirilen ürünler özellikle yazılım alanında ise arsa, ev, bilgisayar kasası gibi maddi bir varlığın dışında somut olmayan bir kavramın sahipliği söz konusu olmaktadır. Bu durumda bu sahipliğin ispatı çeşitli sıkıntılar doğurmaktadır. Aslında günümüzde bu sorunlar müzik, edebiyat alanları için de söz konusudur. Hatta sanat alanındaki bu etik sorun, doğrudan bilişim teknolojilerinin gelişmesi ile çığ gibi büyümüştür. Bu tür eserlerin günümüz teknolojisi ile kopyalanıp dağıtılmasının oldukça kolay olması, asıl sahibine dair bilginin korunmasında önemli bir engel olarak

karşımıza çıkmaktadır. "Eserlerin (bilişim alanı için geliştirilen yazılımlar) sahibi kimdir ve kimlerin-kullanımına izin verilmiştir?" sorularının cevabı fikrî mülkiyet başlığının altında irdelenmektedir.

Fikrî mülkiyet; kişinin kendi zihni tarafından ürettiği her türlü ürün olarak tanımlanmaktadır. Türk Dil Kurumu ise Bilim ve Sanat Terimleri Sözlüğünde fikrî mülkiyet kavramını "düşünü çalışması sonunda ortaya konulan yazın ve bilim ürünleri üzerindeki iyelik" olarak tanımlamıştır.

Fikrî mülkiyet denince karşımıza hukuki ve etik boyutlar çıkmaktadır. Kimi sorunlar yasal olup etik olmazken kimi de etik olup yasal olmayabilmekte ya da iki boyut birden temelsiz kalabilmektedir. Bu nedenle fikrî mülkiyete ilişkin yasalar, günümüz koşullarına uygun olarak güncellenmeye muhtaç olmaktadır. Telif hakkı, patent, şifreleme gibi kavramlar da bu gereksinim sonucunda ortaya çıkmıştır.

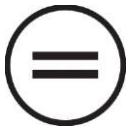
"Fikrî ve kültürel eserlerden bazıları Creative Commons (CC) organizasyonuna dâhildir. Creative Commons, telif haklan konusunda esneklik sağlamayı amaçlayan, eser sahibinin haklarını koruyarak, eserlerin paylaşımını kolaylaştırıcı modeller sunan, kâr amacı gütmeyen bir organizasyondur. Bu organizasyona dâhil olan eserler, kaynağı belirtmek ön şartıyla belirli kısıtlamalar göz önünde bulundurularak kullanılabilir."

Koşullar

Attribution - Atıf: Eserin ilk sahibinin belirtilmesi koşulu. Bu koşulu barındıran lisansa sahip eserlerde, eseri yaratan ilk kişinin mutlaka belirtilmesi gerekiyor.

Share Alike - Aynı Lisansla Paylaş: Lisans modelinin korunması koşulu. Bu koşula sahip eserlerin türetilmesi veya yeniden yayınlanması ancak onu barındıran yeni eserin de aynı lisansa sahip olması şartıyla gerçekleşebilir.

Non-Commercial - Ticari Olmayan: Eserin ticari amaçlı kullanılmaması koşulu. Bu koşulu şart koşan eserlerin türevlerinin veya orijinallerinin sadece ticari olmayan ürünlerde kullanılması mümkün (Ticari amaçlı kullanmak için eser sahibine başvurmak mümkün.).



No Derivate Works - Türetilemez: Eserin türevinin yaratılmaması koşulu. Bu koşulu içeren lisanslı eserlerin türevlerinin yapılmasına izin verilmemektedir eğer isteniyorsa sadece olduğu gibi kullanılması gerekir.

CC lisanslı eserler bu kısıtlamaların yalnızca birine sahip olabileceği gibi birden fazlasına aynı anda sahip olabilir. Bu eserlerin kısıtlamaları, eserin bulunduğu sayfanın alt kısmında görülebilir.

Bilişim dünyasında yazılımları lisanslarına göre, özgür yazılımlar ve ticari yazılımlar olmak üzere ikiye ayırabiliriz. Özgür yazılım dünyasına ait GPL'ye (General Public Licence - Genel Kamu Lisansı) sahip yazılımlar ücretsiz olarak (ya da özelleştirilmiş versiyonları düşük ücretlerle) kullanılabilirken, ticari faaliyet gösteren firmaların ürettiği yazılımların lisanslarıysa çoğunlukla yüksek bedeller karşılığında alınabilmektedir. Kişi ya da kuruluşlar yazılım seçimi yaparken ihtiyaçlarını doğru şekilde belirledikten sonra tercih yapmalıdır. Böylece yüksek maliyet ödemekten ve beklentileri karşılamayan program edinmiş olmaktan kaçınmış olurlar.

Lisanssız yazılım kullanmanın etik uygunsuzluk yanında teknik sakıncaları da vardır. Firmalarca sunulan yazılımlar, zaman zaman güvenlik açıklarını kapatmak ya da ek özelliklerle donanmak amacıyla güncelleme alır. Lisanssız kullanılan yazılımlar, bu güncellemeleri alamaz ve bilgi güvenliği açısından bilgisayarları savunmasız kılar.

1.2.2. Erişim

Bu başlık bilgiye erişimi anlatmaktadır. Sıradan bir vatandaş için herhangi bir bilişim teknolojisi ürününden bilgiye erişim olarak düşünülebilir. Örneğin herhangi bir arama sitesini kullanarak, istediğimiz bilgiye hızlıca erişebiliriz. Ancak bilgi daha özel bir formatta sunulmuş olabilir. Örneğin bir veri tabanında saklanıyor olabilir. Bu durumda karşımıza üç sorun çıkmaktadır:

1. Bilgiye erişebilecek düzeyde bilişim bilgisi,
2. Bilginin yararlılığını test edecek düzeyde bilgi okuryazarlığı,
3. Bilgiye erişmenin varsa maddi karşılığı olan ekonomik güç.

Günümüz insanı birinci sorunu aşmakta oldukça başarılı gibi görünürken, ikinci sorunun aşılmasında hâlâ güçlükler söz konusudur. Çünkü bilgi yığınları artmakta ve bu bilginin doğruluğunu test etmek güçleşmekte ayrıca son kullanıcı dediğimiz vatandaşın bunu test etme bilincinin eğitilmesi gerekmektedir. Üçüncü sorun olan ekonomik boyut için kütüphane veri tabanları bir çözüm olarak karşımıza çıkmaktadır. Bu durumda bilginin ücretsiz olması "Herkesin eşit derecede bilgiden yararlanmasını sağlar." çözüm önerisi, fikrî mülkiyet ile çelişecektir.

1.2.3. Gizlilik

Bir önceki başlıkta bahsettiğimiz gibi, bir arama sitesi kullanarak bilgiye hızlıca erişim, herhangi bir kişi için sıradan bir davranış hâline gelmiştir. Bugün herkes aklına gelen her şeyi özgürce Google ya da Yandex gibi arama motorlarında aramaktadır. Oysa ki her arattığımız şey ile birlikte hatta bilişim ortamında yaptığımız her eylem ile ardımızda "ekmek kırıntısı" olarak tabir edilen izler bırakıyoruz. Eğer birilerinin bizim bu bıraktığımız ekmek kırıntılarını takip ettiği hissine kapılırsak ne kadar rahatsız olacağımızı bir düşünün. Örneğin Google'da arama yaparken karşınıza çıkan reklamların, sizin daha önce ziyaret ettiğiniz siteler ve bunların içeriklerinden elde edilen verilerle tespit edilen ilgi alanlarınıza yönelik olduğunu görmüşsünüzdür. Sadece tarama yaparken değil, birçok kurum ve kuruluşa üye olurken dijital teknolojilerden yararlanıyoruz. Örneğin hastane kayıtları. Çoğu hasta hastane kayıtlarının başka kişilerle paylaşılmasını istemez, işte gizlilik dediğimiz kavram kişiye ait her türlü bilgiyi (ki bu bilgi sadece ad ve soyadı değil, kişinin duygu, düşünce, siyasi eğilim, dini inancı, planı, fantezi dünyası ve korku gibi bilgilerini de içerir) saklama becerisidir. Ancak bilginin saklanması dışında bu bilginin doğru kişilerle doğru zaman diliminde de paylaşılması gizlilik başlığını ilgilendirir. Örneğin hasta, bilgilerini doktoru ile paylaşmak zorundadır.

İzlenmekten kaçınmak için açık kaynak dünyasından alternatifler kullanılabilir.

Örnek olarak https://duckduckgo.com sitesini inceleyiniz.

1.2.4. Doğruluk

Tahmin edilebileceği gibi bilişim alanında şahsımıza ait bilgiler bizim dışımızdaki kişiler tarafından da kayıt altına alınabilmektedir. Ancak bu bilgilerin doğruluğu kimin sorumluluğundadır? Biz kendimize ait bilgileri kontrol etme hakkına sahip olmalıyız ve kendimize ait bilgileri kendimiz kodlayacaksak bunun sorumluluğunu da üstlenmek zorundayız. Ayrıca anonim bilgilerin doğruluğunun sorumluluğu kimde olmalıdır? Örneğin, içeriğini kullanıcıların oluşturduğu bilgi paylaşım siteleri (wiki

ortamları) açık sistemlerdir. Bu sistemlerdeki verilerin doğruluğunun garantisi kimdedir gibi sorular bu başlık altında ele alınmaktadır.

Uluslararası Bilgisayar Etik Enstitüsüne göre bilişim teknolojilerinin doğru bir şekilde kullanılabilmesi için aşağıda belirtilen 10 kurala uyulması gerekmektedir.

1. Bilişim teknolojilerini başkalarına zarar vermek için kullanmamalısınız.
2. Başkalarının bilişim teknolojisi aracılığı ile oluşturduğu çalışmaları karıştırmamaksınız.
3. Başkasına ait olan verileri incelememelisiniz.
4. Bilişim teknolojilerini hırsızlık yapmak için kullanmamalısınız.
5. Bilişim teknolojilerini yalancı şahitlik yapmak için kullanmamalısınız.
6. Lisanssız ya da kırılmış/kopyalanmış yazılımları kullanmamalısınız.
7. Başkalarının bilişim teknolojilerini izinsiz kullanmamalısınız.
8. Başkalarının bilişim teknolojileri aracılığı ile elde ettiği çalışmalarını kendinize mal etmemelisiniz.
9. Yazdığınız programların ya da tasarladığınız sistemlerin sonuçlarını göz önünde bulundurmalısınız.
10. Bilişim teknolojilerini her zaman saygı kuralları çerçevesinde kullanmalı ve diğer insanlara saygı duymalısınız.

Günümüzde Internet kullanıcıları, bilgiye kolay ulaşabilirken amaçları bu olmadığı zamanlarda da sıklıkla bilgi akışına maruz kalmaktadırlar. Bu bilgi akışı her zaman doğru ve iyi niyetli olmayabilir. Bu sebeple elde edilen bilgiler kullanılmadan önce bir dizi tedbir almak önemlidir. Bu tedbirler:

- 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. Örneğin;

o **.com** ya da **.net** alan adı uzantısına sahip İnternet siteleri ticari amaçlı sitelerdir.

o **.gov:** Devlet kurumlarının resmî sitelerinin uzantısıdır.

o **.org:** Ticari amacı olmayan vakıf, dernek ve organizasyonların kullandığı uzantıdır.

o **.edu:** Üniversite ve akademik kuruluşların siteleri için kullanılır.

o **,kl2:** Okul öncesi, ilkokul, ortaokul ve lise gibi eğitim kurumlarına ait uzantıdır.

Bilgi edinilen İnternet siteleri, uzantılarına göre değerlendirilerek kaynak güvenilirliği konusunda bir kanıya varılabilir. Türkiye Cumhuriyeti nin İnternet ülke kodu **.tr**'dir. Bu uzantıya sahip sitelere yönelik ülke içinde ayrı bir kontrol gerçekleştirildiği için bu sitelerin güvenilirliklerinin daha yüksek olduğu söylenebilir. Örneğin; Millî Eğitim Bakanlığının İnternet site adresi **meb.gov.tr,** Türkiye Erozyonla Mücadele ve Ağaçlandırma Vakfının adresi de **tema.org.tr'**dir.

Adresler incelendiğinde,

m c b .20V.tl*

Kurum/Kuruluş/Şirket Kategori Uzantısı Ülke Kodu

gu adresin Türkiye Cumhuriyeti'ne (.tr) ait bir devlet/hükümet (.gov) sitesi olduğu görülebilir.

tema.org.tr

Kurum/Kuruluş/Şirket Kategori Uzantısı Ülke Kodu

R , • , T••,• „ , •, ,

Bu adresin de 1 urkıye Cumhuriyeti nde (.tr) faaliyet gösteren bir vakıf ya da derneğe (.org) ait olduğu anlaşılabilir.

Düşünelim!D eneyelim

Bir arama sitesine "e-okul" ifadesini yazıp listelenen arama sonuçlarını inceleyerek hangisinin e-okul uygulamasının resmî sitesi olduğunu bulunuz.

İnternet sitelerinin adreslerini tanımak, yalnızca doğru bilgiye ulaşmak için gerekli değildir. Aynı zamanda karşılaşılabilecek sahtecilik ve bilgi hırsızlığından korunmak için de çok önemlidir. Bir önceki etkinlikte e-okul başlığıyla listelenen birbirinden farklı adresler görmüş olmalısınız, e-okul gibi hizmetlere ya da bankaların Internet sitelerine giriş yaparken bazı özel bilgiler girmeniz gerekir. Özel bilgilerinizi girdiğiniz sitenin doğru site olduğundan emin olmalısınız.

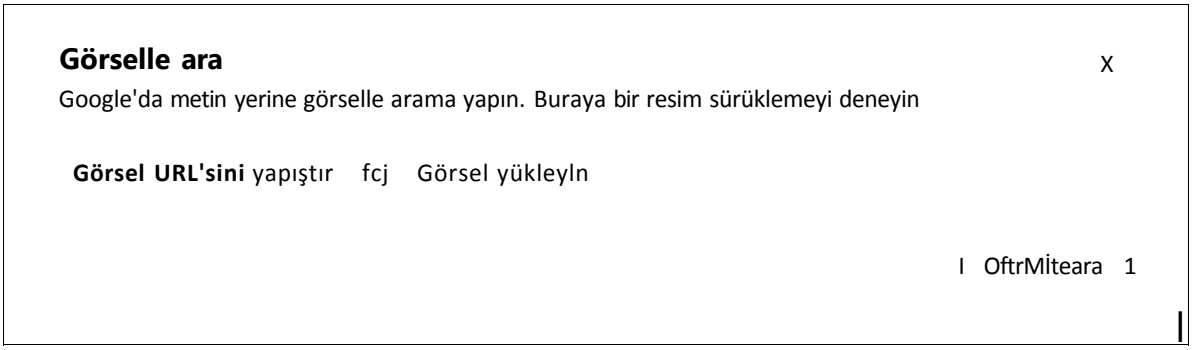
Altay Spor Kulübü Resmi Web Sitesi
vAvw.altay.org.tr/ »
Altay SDD; **Altay** Vakfı; Tesisler; Takımlar. A Takım (teknik ... BÜYÜK **ALTAY** 6-1 BEYLERBEYİ 100 YIL FOTOĞRAF ... İletişim Haberler. Müzemiz. **Spor** Okulları.
Kuruluş Öyküsü İletişim Ana Yönetim Başkanlar

Görselde bir arama sonucunu görmektesiniz. Arama sonuçlarının en üstündeki mavi renkli kısım başlıktır. Arama sonuçlarının başlıkları link/bağlantı niteliğindedir. Yani tıklandığında bir İnternet adresine yönlendirilirsiniz. Hangi adrese yönlendirildiğinizi arama başlığından değil, başlığın altındaki -yeşil renkli- adres bilgisinden anlayabilirsiniz. Görseldeki arama sonucunun başlığına tıklandığında Internet tarayıcınız www.altay.org.tr sayfasını görüntüleyecektir. Arama sonuçlarında görüntülenen diğer kısım olan siyah renkli metindeyse siteye ilişkin tanıtıcı bilgi ve açıklamalar görülebilir.

İnternet ortamında karşılaşılan bilgilerin doğruluğunu teyit etmek ve ayrıca sahteciliğe maruz kalmamak için İnternet sitelerinin adreslerini tanımanın önemini görmüş olduk. Bundan ayrı olarak özellikle sosyal medyada ya da bazen İnternet sitelerinde çeşitli görseller manipüle edilerek ya da olduğundan çok farklıymış gibi anlatılarak yanlış bilgilendirme, hatta kışkırtma yapılabilmektedir. Böyle durumlarda da görsele dayalı doğrulama yapmak mümkündür.

Bir paylaşım, insanları kışkırtıp şiddet olayları çıkarmak için yapılmış olabilir. Bu tip paylaşımları doğru kabul etmeden önce kontrol edilmek, istenmeyen olayların önüne geçecektir. Bunu anlamak için haberde kullanılan görselin üzerine sağ tıklayıp fotoğrafı bilgisayarınıza indirebilir ya da yine sağ tıklama seçeneklerindeki "bağlantı adresini kopyala" komutunu kullanabilirsiniz.

Bir arama sitesinin görsel arama sayfasını açıp işaretli yere tıkladığınızda sizden görsel yüklemenizi isteyecektir. Burada, bilgisayarınızda kayıtlı bir görseli yükleyebileceğiniz gibi görselin adresini ilgili alana girebilirsiniz.



Bu iki yoldan biriyle görselimizi yükledikten sonra arama motoru benzer görselleri listeleyecektir. Listelenen görseller arasında, aradığınız görselin aynısının daha önce paylaşıldığını görüyorsanız ilgili görseli tıklayabilir ve görselin bulunduğu Internet sitesini açabilirsiniz. Böylece, paylaşılan bilgiyi inanılır kılmak için kullanılan görselin İnternet'te farklı bir ortamdan alınan bambaşka bir görsel olduğunu görebilir ve paylaşılan bilginin doğru olmadığını belirleyebilirsiniz.

1.2.5. İnternet Etiği

İnternet kullanımı ile ilgili olarak dikkat edilmesi gereken etik ilkeler; kişilik haklan, özel yaşamın gizliliği ve veri güvenliği gibi başlıklar altında incelenebilir. İnternet ortamında uyulması gereken etik kurallar aşağıda verilmiştir:

- Bize yapılmasından hoşlanmadığımız davranışları başkalarına yapmaktan kaçınmalıyız.
- Bir durum karşısında internette nasıl davranmamız gerektiği konusunda kararsız kaldığımız zaman gerçek hayatta böyle bir durum karşısında nasıl davranıyorsak öyle davranmalıyız.
- İnternette karşılaştığımız ancak yüzünü görmediğimiz, sesini duymadığımız kişilere saygı kuralları çerçevesinde davranmalıyız.
- İnternet sadece belirli bir ırkın, topluluğun ya da ülkenin tekelinde değildir. Tüm dünyadan pek çok farklı kültür ve inanca sahip insan İnternet ortamında varlık göstermektedir. İnternet'i kullanırken her kültüre ve inanca saygılı olmak, yanlış anlaşılabilecek davranışlardan kaçınmak gerektiği unutulmamalıdır.
- İnternet'i yeni kullanmaya başlayan kişilerin yapacağı yanlış davranışlara karşı onlara anlayış gösterip yardımcı olmaya çalışmak ve yol göstermek gerektiği de unutulmamalıdır.
- Özellikle sosyal medya, sohbet ve forum alanlarındaki kişiler ile ağız dalaşı yapmaktan kaçınmalı, başka insanları rahatsız etmeden yazışmaya özen göstermeliyiz. Ayrıca, sürekli olarak büyük harfler ile yazışmanın İnternet ortamında bağırmak anlamına geldiği unutulmamalıdır.
- İnsanların özel hayatına karşı saygı göstererek kişilerin sırlarının İnternet ortamında paylaşılmamasına dikkat edilmesi gerektiği unutulmamalıdır.
- İnternette kaba ve küfürlü bir dil kullanımından kaçınarak gerçek hayatta karşımızdaki insanlara söyleyemeyeceğimiz ya da yazamayacağımız bir dil kullanmamalıyız.
- İnternet'i başkalarına zarar vermek ya da yasa dışı amaçlar için kullanmamalı ve başkalarının da bu amaçla kullanmasına izin vermemeliyiz.
- Internet ortamında insanların kişilik haklarına özen göstererek onların paylaştığı bilginin izinsiz kullanımından kaçınmamız gerektiği de unutulmamalıdır.

İnternet ortamında nasıl davranılması gerektiğini öğrenmiş oldunuz. Sizin doğru davranıyor oluşunuz, herkesin de size doğru davranmasını sağlayamayabilir. İnternet ortamında başkalarından kaynak-

lanan kötü davranışlara maruz kalabilirsiniz. İnternet etiğine uymayan bu davranışlara **siber (dijital) zorbalık** denir.

Siber zorbalığa maruz kalmanız durumunda yapmanız gerekenleri şöyle sıralayabiliriz:

Zorbalık yapan hesaplara cevap vermeyiniz, onlarla tartışmaya girmeyiniz. İlk yapmanız gereken, zorbalık yapan hesabı engellemektir.

Bu hesapları, bulunduğunuz sosyal medya platformundaki "Bildir/Şikâyet Et" bağlantısını kullanarak şikâyet ediniz. Böylece bu kişilerin size yaptığı etik dışı davranışları başkalarına da yapmasını engellemiş olursunuz.

Size yönelik etik dışı davranışlar artarak ve ağırlaşarak devam ederse bunların ekran görüntülerini ve mesajları kaydediniz. Bu kanıtlarla birlikte ailenizin ya da rehber öğretmeninizin gözetiminde hukuki yollara başvurunuz.

Siber zorbalığa maruz kalan başka kişiler de olabilir. Böyle durumlarda bu kişilere ne yapmaları gerektiği konusunda yardımcı olabilir, kötü kullanım bildirimini siz de yapabilirsiniz. Zorba bir hesap için kötü kullanım bildirimi sayısı fazla olursa o hesabın site yönetimi tarafından incelenmesi ve kapatılması daha çabuk olacaktır.

1.3. Bilgi Güvenliği

Bu bölümde;

"S Bilgi güvenliğinin önemini açıklayacak,

"S Bilgi güvenliğine yönelik tehditleri kavrayacak,

•S Sayısal dünyada kimlik yönetimi konusunda güvenlik açısından yapılması gerekenleri listeleyecek,

S Kişisel bilgisayar ve ağ ortamında bilgi güvenliğini sağlamaya yönelik işlemleri gerçekleştireceksiniz.

Bilim ve teknolojide yaşanan hızlı ilerleme, içinde bulunduğumuz 21. yüzyılın bilgi çağı olarak isimlendirilmesine yol açmıştır. Günümüzde bilişim teknolojilerinin yaygın kullanımı ile birlikte bilginin üretilmesi ve kullanılması büyük önem kazanmış ve bu teknolojiler aracılığı ile üretilen veri miktarında da büyük bir artış olmuştur. Bilgisayarlar ve akıllı cihazlar aracılığı ile başta İnternet olmak üzere bilgiye erişimin farklı yollarının ortaya çıkması da bilginin depolanması, iletilmesi ve korunması ile ilgili pek çok problemi de beraberinde getirmiştir. Bu problemlerden biri de kişisel ya da kurumsal bilgiyi erişilmez kılmaya, ele geçirmeye ya da değiştirmeye yönelik olanlardır. Kişisel ya da kurumsal düzeyde bizim için büyük önem teşkil eden her tür bilgiye izin alınmadan ya da yetki verilmeden erişilmesi, bilginin ifşa edilmesi, kullanımı, değiştirilmesi, yok edilmesi gibi tehditlere karşı alınan tüm tedbirlere **bilgi güvenliği** denir. Bilgi güvenliği, "gizlilik", "bütünlük" ve "erişilebilirlik" olarak isimlendirilen üç temel öğeden meydana gelmektedir. Bu üç temel güvenlik unsurundan birinin zarar görmesi durumunda güvenlik zaafiyeti oluşabilir.

Bilgi güvenliğini oluşturan unsurlardan **gizlilik,** bilginin yetkisiz kişilerin eline geçmemesi için korunmasıdır. Başka bir deyişle gizlilik, bilginin yetkisiz kişilerce görülmesinin engellenmesidir, e-posta hesap bilgisinin bir saldırgan tarafından ele geçirilmesi buna örnek verilebilir. **Bütünlük,** bilginin yetkisiz kişiler tarafından değiştirilmesi ya da silinmesi gibi tehditlere karşı korunması ya da bozulma-

maşıdır. Bir web sayfasında yer alan bilgilerin saldırgan tarafından değiştirilmesi, bütünlük ilkesinin bozulmasına örnek verilebilir. **Erişilebilirlik** ise bilginin yetkili kişilerce ihtiyaç duyulduğunda ulaşılabilir ve kullanıma hazır durumda olmasıdır. Bir web sitesine erişimin saldırı sonucunda engellenmesi erişilebilirlik ilkesinin ihlal edilmesine örnek olarak verilebilir.

1.3.1. Bilgi Güvenliğine Yönelik Tehditler

Bilgi ve bilişim teknolojileri güvenliğinde başlıca tehdit, korsan ya da saldırgan olarak adlandırılan kötü niyetli kişiler ve bu kişilerin yaptıkları saldırılardır. Bir bilişim teknolojisi sistemine sızmak, sistemi zaafiyete uğratmak, sistemlerin işleyişini bozmak ve durdurmak gibi kötü niyetli davranışlar; **siber saldırı** veya **atak** olarak adlandırılmaktadır. Günümüzde siber dendiğinde ilk akla gelen "Sanal Dünya (Internet)" olsa da bir cihazın siber kavramı içinde yer alması için Internet bağlantısına sahip olması gerekmez. **Siber** ya da **siber uzay;** temeli bilişim teknolojilerine dayanan, tüm cihaz ve sistemleri kapsayan yapıya verilen genel addır. Fiziki sınırları ve kuralları olmayan bu siber dünya içinde yaşanan saldırı, suç, terör, savaş gibi kötü niyetli hareketler daha çok elle tutulur, gözle görülür varlıklarımız için oluşturulmuş kurallar ve yasalar ile engellenemez/korunamaz. Korsanlar ya da saldırganlar, istediklerini elde edebilmek için çok farklı teknikler kullanabilirler. Bu tür saldırı türlerinin tanınması, doğru şekilde analiz edilmesi ve gereken tedbirlerin alınabilmesi siber güvenlik için çok önemlidir. Siber güvenlik; siber ortamda yaşanabilecek suç, saldırı, terörizm, savaş, gibi tüm kötü niyetli hareketlere karşı alınacak tedbirler bütünüdür. Siber ortamda yaşanabilecek kötü niyetli hareketler aşağıda tanımlanmıştır:

Siber Suç: Bilişim teknolojileri kullanılarak gerçekleştirilen her tür yasa dışı işlemdir.

Siber Saldırı: Hedef seçilen şahıs, şirket, kurum, örgüt gibi yapıların bilgi sistemlerine veya iletişim altyapılarına yapılan planlı ve koordineli saldırıdır.

Siber Savaş: Farklı bir ülkenin bilgi sistemlerine veya iletişim altyapılarına yapılan planlı ve koordineli saldırılardır.

Siber Terörizm: Bilişim teknolojilerinin belirli bir politik ve sosyal amaca ulaşabilmek için hükümetleri, toplumu, bireyleri, kurum ve kuruluşları yıldırma, baskı altında tutma ya da zarar verme amacıyla kullanılmasıdır.

Siber Zorbalık: Bilgi ve iletişim teknolojilerini kullanarak bir birey ya da gruba, özel ya da tüzel bir kişiliğe karşı yapılan teknik ya da ilişkisel tarzda zarar verme davranışlarının tümüdür.

Yukarıda bahsedilen saldırılar bireysel, kurumsal ve toplumsal hedeflere yönelik olabilmektedir. Bireysel saldırılarda ana hedefi kişisel bilgilerin ele geçirilmesi, değiştirilmesi ya da yok edilmesi oluştururken kurumsal ve toplumsal saldırılarda ise çoğunlukla kurumlar ve devletin zarara uğratılması hedeflenmektedir. Daha çok devletler arası düzeyde gerçekleşen siber savaşlarda ise ana hedef; sağlık, enerji, ulaşım, haberleşme gibi kritik altyapılardır.

1.3.2. Sayısal Dünyada Kimlik ve Parola Yönetimi

Her gün sıkça kullandığımız şifre ve parola kavramlarını inceleyecek olursak **"parola"** bir hizmete erişebilmek için gerekli olan, kullanıcıya özel karakter dizisidir. **"Şifre"** ise sanal ortamdaki verilerin gizliliğini sağlamak için veriyi belirli bir algoritma kullanarak dönüştüren yapıdır.

Bir bilişim sistemine erişimin belli kurallar çerçevesinde yapılması amacıyla o sistemi kullanmak isteyen kişilerin kullanıcı adı ve/veya parola ile erişim yetkisine sahip olduklarını ispatlamaları gerekmektedir. Buradaki kullanıcı adı ve parola, bilgiye erişim yetkisinin kanıtı olarak kullanılmaktadır.

Kullanıcı adı, her kullanıcıdan sadece bir tane olduğunu garantilemek amacıyla benzersiz bir bilgi olarak oluşturulur. Bu bilgi, bilişim sistemi tarafından otomatik olarak verilebileceği gibi kullanıcılardan kimlik No., öğrenci No. ya da e-posta gibi bilgiler istenerek de oluşturulabilir. Parola ise içinde büyük ya da küçük harfler, rakamlar ve özel karakterler barındıran bir karakter dizisidir.

Parola, bilgi güvenliğinin en önemli öğesidir. Parolanın da ele geçirilmesi durumunda oluşacak zarar, bir evin anahtarını ele geçiren hırsızın sebep olacağı zarardan çok daha fazla olabilir. Parolanın kötü niyetli kişiler tarafından ele geçmesi durumunda,

- Elde edilen bilgiler yetkisiz kişiler ile paylaşılabilir ya da şantaj amacıyla kullanabilir.
- Parolası ele geçirilen sistem başka bir bilişim sistemine saldırı amacıyla kullanılabilir.
- Parola sahibinin saygınlığının zarar görmesine yol açabilecek eylemlerde bulunulabilir.
- Ele geçirilen parola ile ekonomik kayba uğrayabilecek işlemler yapılabilir.
- Parola sahibinin yasal yaptırım ile karşı karşıya kalmasına yol açabilir.

Bilişim sistemlerinde parolanın ele geçirildiğinin ispatlanması ya da bu işi yapan kişilerin belirlenmesi çok zor olduğundan parolası ele geçirilen sistem üzerinde yapılacak kötü niyetli eylemler parola sahibinin ciddi yaptırımlar ile karşı karşıya kalmasına neden olabilir. Bir bilişim sistemine erişim için kanıt olarak kullanılan parolanın dikkatle belirlenmesi ve titizlikle korunması gerekir. Sadece rakamlardan oluşan 6 haneli bir parolanın özel programlar yardımı ile dakikalar içinde kırılması mümkündür. Güçlü ve kırılması zor bir parolanın oluşturulması için olabildiğince sayı, büyük/küçük harfler ile özel karakterler içermesine dikkat edilmesi son derece önemlidir. Başkalarının da kolaylıkla tahmin edebileceği qwerty, 123456 gibi ardışık harfler ve sayıların kullanılması, parolanın doğum yılı ya da mezuniyet tarihi gibi kişisel bilgi içermesi de zayıf parolalar için örnek gösterilebilir. Günümüzde saldırganların parolaları ele geçirmek ya da tahmin edebilmek için sosyal medyadan faydalandıkları da unutulmamalıdır. Sosyal medya aracılığı ile ulaşılabilen aile fertlerinin adı, doğum tarihi gibi bilgiler de parola belirlemek amacıyla kullanılmamalıdır. Saldırganlar, sosyal medya ortamlarını kendi çıkarları için kullanarak sosyal mühendislik adı verilen ikna ve kandırma teknikleri ile bu bilgileri elde edebilirler. Güçlü bir parolanın belirlenmesi için aşağıdaki kurallar uygulanmalıdır.

- Parola, büyük/küçük harfler ile noktalama işaretleri ve özel karakterler içermelidir.
- Parola, -aksi belirtilmedikçe- en az sekiz karakter uzunluğunda olmalıdır.
- Parola, başkaları tarafından tahmin edilebilecek ardışık harfler ya da sayılar içermemelidir.
- Her parola için bir kullanım ömrü belirleyerek belirli aralıklar ile yeni parola oluşturulması gerekir.

Parolanın güvenliği açısından, aşağıdaki kurallara dikkat edilmelidir:

- Parolanın başkalarıyla paylaşılmaması son derece önemlidir.
- Parolalar, basılı ya da elektronik olarak hiçbir yerde saklanmamalıdır.
- Başta e-posta adresinin parolası olmak üzere farklı bilişim sistemleri ve hizmetler için aynı parolanın kullanılmaması gerekir.

Bu durumda, bir kullanıcının onlarca parola üretmesi gerekebilir. Bu da parolaların unutulması sorununu beraberinde getirir. Böyle bir sorun yaşamamak için kullanıcılar kendilerine özgü kalıplardan yararlanmalıdırlar.

Örnek olarak;

Bir anahtar kelime belirlenerek kelime, parola kriterlerine uygun hâle getirilebilir. "Alsancak" kelimesi, parola oluşturma kriterleri göz önüne alınarak "Als@nc@k" şeklinde düzenlenebilir (8 karakter, büyük harf, küçük harf, sayı ve özel karakter içeriyor.). Bu anahtar kelimenin başına, ortasına ya da sonuna kullanılan platformun kısa ismi eklenerek o hizmete özgü parola oluşturulmuş olur. Tvvitter için Als@nc@kTW, Facebook için Als@nc@kFB gibi.

Bir anahtar cümle belirlenerek bu cümlenin bazı harfleri kullanılabilir. Örneğin "Muhtaç olduğun kudret, damarlarındaki asil kanda mevcuttur." cümlesindeki kelimelerin baş harfleri kullanılarak 7 karakter elde edilir. Bu yedi karakterin yanına, kullanılacak platformun kodu da eklendiğinde 9 karakterli bir parola elde edilebilir.

e-posta hesabı için: M0kd@kM@il, Instagram için: M0kd@kMig gibi...

- Anahtar kelime oluştururken;

G yerine 6,

g yerine 9,

Ş yerine $

a yerine @

i, 1 yerine 1 gibi karakterler kullanılabilir.

Düşünelim/Deneyelim

Hayalî bir kişinin üç farklı sosyal medya hesabı için güvenli parolalar oluşturunuz.

1.3.3. Kişisel Bilgisayarlarda ve Ağ Ortamında Bilgi Güvenliği

Bilgisayar ve İnternet teknolojisindeki hızlı ilerleme sonucunda üretilen veri, hiç durmadan artmaktadır. Özellikle İnternet kullanımının oluşturduğu büyük miktardaki bilgi, her gün milyonlarca insan tarafından kullanılmaktadır. Bu veriyi üreten, kullanan ve paylaşan insanların çok küçük bir kısmı ise İnternet'in tehlikeleri ve bilgi güvenliği konusunda bilgi sahibidir. Bilişim teknolojisinin kullanımında temel amaç bilgiye erişmektir. Ancak, teknolojinin hızlı ilerleyişi ile birlikte gelen güvenlik riskleri ve insanların bu konudaki yetersiz farkındalıkları bilgisayar ve İnternet kullanımı sırasında pek çok tehlikenin ortaya çıkmasına neden olmaktadır.

Bilişim sistemlerinin çalışmasını bozan veya sistem içinden bilgi çalmayı amaçlayan Virüs, Solucan, Truva Atı ya da Casus yazılım gibi kötü niyetlerle hazırlanmış yazılım veya kod parçaları zararlı programlar olarak adlandırılır.

Bu zararlı programlar,

- İşletim sisteminin ya da diğer programların çalışmasına engel olabilir.
- Sistemdeki dosyaları silebilir, değiştirebilir ya da yeni dosyalar ekleyebilir.
- Bilişim sisteminde bulunan verilerin ele geçirilmesine neden olabilir.
- Güvenlik açıkları oluşturabilir.
- Başka bilişim sistemlerine saldırı amacıyla kullanılabilir.
- Bilişim sisteminin, sahibinin izni dışında kullanımına neden olabilir.
- Sistem kaynaklarının izinsiz kullanımına neden olabilir.

Virüsler, bulaştıkları bilgisayar sisteminde çalışarak sisteme ya da programlara zarar vermek amacıyla oluşturur. Virüsler bilgisayara e-posta, bellekler, İnternet üzerinden bulaşabilir. Bilgisayarın yavaşlaması, programların çalışmaması, dosyaların silinmesi, bozulması ya da yeni dosyaların eklenmesi virüs belirtisi olabilir.

Bilgisayar Solucanları; kendi kendine çoğalan ve çalışabilen, bulaşmak için ağ bağlantılarını kullanan kötü niyetli programlardır. Sistem için gerekli olan dosyaları bozarak bilgisayarı büyük ölçüde yavaşlatabilir ya da programların çökmesine yol açabilir. Ayrıca sistem üzerinde arka kapı olarak adlandırılan ve saldırganların sisteme istedikleri zaman erişmelerini sağlayan güvenlik açıkları oluşturabilir.

Truva Atları, kötü niyetli programların çalışması için kullanıcının izin vermesi ya da kendi isteği ile kurması gerektiği için bunlara Truva Atı denmektedir. Truva Atları saldırganların bilişim sistemi üzerinde tam yetki ile istediklerini yapmalarına izin verir. Sisteme bulaşan bir Truva Atı ilk olarak güvenlik yazılımlarını devre dışı bırakarak saldırganların bilişim sisteminin tüm kaynaklarına, programlarına ve dosyalarına erişmesine olanak sağlar. Güvensiz sitelerden indirilen dosyalar, tanınmayan kişilerden gelen e-postalar ya da taşınabilir bellekler aracılığı ile yayılabilir.

Casus Yazılımlar, İnternetten indirilerek bilgisayara bulaşan ve gerçekte başka bir amaç ile kullanılsa bile arka planda kullanıcıya ait bilgileri de elde etmeye çalışan programlardır. Bunlar, sürekli reklam amaçlı pencerelerin açılması ya da İnternet tarayıcıya yeni araçların eklenmesine neden olabilir.

Zararlı Programlara Karşı Alınacak Tedbirler

- Bilgisayara antivirüs ve İnternet güvenlik programları kurularak bu programların sürekli güncel tutulmaları sağlanmalıdır.
- Tanınmayan/güvenilmeyen e-postalar ve ekleri kesinlikle açılmamalıdır.
- Ekinde şüpheli bir dosya olan e-postalar açılmamalıdır. Örneğin *resim.jpg.exe* isimli dosya bir resim dosyası gibi görünse de uzantısı *exe* olduğu için uygulama dosyasıdır.
- Zararlı içerik barındıran ya da tanınmayan web sitelerinden uzak durulmalıdır.
- Lisanssız ya da kırılmış programlar kullanılmamalıdır.
- Güvenilmeyen Internet kaynaklarından dosya indirilmemelidir.

Düşünelim/Deneyelim

Zararlı yazılımları ve bu yazılımların ne tür zararlar verebileceğini inceleyiniz.

2. PROBLEM ÇÖZME VE ALGORİTMALAR

Bu bölümde;

^ Genel problem çözme kavramlarını,

» Klasik bulmacaları ve çözümlerini detaylı biçimde öğreneceksiniz.