MODÜL ADI: BİLİŞİM ETİĞİ VE BİLGİ GÜVENLİĞİ

A. ETİK VE BİLİŞİM ETİĞİ KAVRAMLARI

1- Etik Kavramı :

Etik sözcüğü, Yunanca “karakter” anlamına gelen “ethos” sözcüğünden türetilmiştir.

Sözlük anlamı olarak etik; töre bilimi, ahlak bilimi, ahlaki, ahlakla ilgili olarak tanımlanmaktadır Etik, ahlaki olanın özünü ve temellerini araştıran bilim, insan davranışları ile ilgili problemleri inceleyen felsefe dalı olarak tanımlanmaktadır.

Günümüzde etik kavramı, daha çok iş hayatı içerisindeki davranış biçimlerini irdeleyen, düzenleyen bir disiplin olarak görülmektedir.

Etik; doğruyla yanlışı, haklı ile haksızı, iyiyle kötüyü, adil ile adil olmayanı ayırt etmek ve doğru, haklı, iyi ve adil olduğuna inandığımız şeyleri yapmaktır. İşletme etiği ise insancıl değerlerin ışığında işletme görevlerinin doğru yerine getirilmesidir.

Etik davranışlar ahlakla ilgili olan davranışlar demektir. Bir davranış ahlaka uygun ise etik olarak adlandırılır.

2- Etik İlkeler :

Etik ilkeler yapılan işe ve göreve göre değişiklik gösterse de özünde hepsi ahlaklı davranışlar doğrultusunda gelişir.

Bazı etik ilkeler şunlardır:

* Görevini eksiksiz olarak yerine getirme bilinci

* Halka hizmet etme konusunda bilinçli olma

* Amaç ve misyona uygun şekilde davranabilme

* Dürüst ve tarafsız olabilme

* Nezaket kurallarına uyma ve saygılı olma

* Çıkar çatışmasına girmeme

* Menfaat sağlamaya çalışmaktan uzak durma

* Kamu mallarına zarar vermeme

* Savurgan davranışlarda bulunmama

* Gerçek dışı beyanat vermeme

* Rüşvet ve hediyeden uzak durma

* Bencillik yapmama, yolsuzluğa bulaşmama

* Yaranma ve dalkavukluktan uzak durma

3- Bilişim Etiği

Elektronik ve network(ağ ve internet) ortamında uyulması gereken kuralları tanımlayan normlar ve kodlar kısaca bilişim etiğini ifade eder.

Bilişim Etiğine, bilişim alanında uyulması gereken yazılı ve yazılı olmayan kurallar diyebiliriz

Bilişim etiğinin en önemli yanlarından biri, dünyanın neresinde olursa olsun, bilişim sektöründe çalışanların birbirleri ile ilişkilerinde belli davranış kalıplarına uygun davranmalarının gerekli olmasıdır

4- Bilişimde Temel Etik Sorunlar:

20. yüzyılın ikinci yarısından sonra, bilgisayar ve bilgisayar teknolojilerinin hızla gelişmesiyle birlikte, sanayi toplumu yerini, insan faktörünün ve bilginin daha önce görülmedik düzeyde ön plana çıktığı yeni bir toplum şekline bırakmıştır. Bu yeni topluma bilişim toplumu içinde bulunduğumuz çağ ise bilişim çağı olarak adlandırılmaktadır.

Bilişim toplumunda daha önce var olup da bilişim teknolojilerinin etkisiyle artan sorunlarla birlikte, birey ve toplumun bugününü ve geleceğini önemli ölçüde olumsuz olarak etkileyen ve tehdit eden yeni etik sorunların ortaya çıktığı gözlenmektedir.

Bilişim toplumunda ortaya çıkan etik sorunlardan bazıları şunlardır:

- Bilginin Doğruluğu

- Özel Yaşama İlişkin Sorunlar, Mahremiyet, Kişisel Haklar

- Bilgisayar Suçları

- Fikri Mülkiyet Hakları

- İşsizlik

- Sağlık Sorunları

- Sosyal İlişkiler, Ev Ofisleri ve Aileye İlişkin Sorunlar

- Sanal Ortam, Sanal İlişkiler

- Yapay Zeka

- Sosyal İlgi ve Teknoloji İlişkisi

5- Bilişimde Temel Hak ve Özgürlükler

Anayasa göre vatandaşların belli hak ve ödevleri vardır. Bunlar Kişi hak ve ödevleri, Sosyal haklar, Siyasi haklar olmak üzere üçe ayrılır.

Temel hak ve özgürlükleri öğrenmek için öncelikle hak ve özgürlük kelimelerinin anlamlarının bilinmesi gerekmektedir.

Hak: Kişilerin herhangi bir iş kapsamında istediğini yapma yetkisine hak denir.

Özgürlük: Kişilerin, başka bir insana zarar vermeden ve haklarını kısıtlamadan istediği her şeyi yapabilmesine özgürlük denir.

İnsanlar anayasada belirtilen haklara sahip olmakla beraber aşağıdaki kurallara da uymak zorundadır.

- Bilgisayar başka insanlara zarar vermek için kullanılamaz.
- Başka insanların bilgisayar çalışmaları karıştırılamaz.
- Bilgisayar ortamında başka insanların dosyaları karıştırılamaz.
- Bilgisayar hırsızlık yapmak için kullanılamaz.
- Bilgisayar yalan bilgiyi yaymak için kullanılamaz.
- Bedeli ödenmeyen yazılım kopyalanamaz ve kullanılamaz.
- Başka insanların bilgisayar kaynakları izin almadan kullanılamaz.
- Başka insanların entelektüel bilgileri başkasına mal edilemez.
- Kişi yazdığı programın sosyal hayata etkilerini dikkate almalıdır.
- Kişi, bilgisayarı, diğer insanları dikkate alarak ve saygı göstererek kullanmalıdır.

6- Kod Yazımında Etik Kurallar

IEEE(Institute of Electrical and Electronics Engineers- Elektrik ve Elektronik Mühendisleri Enstitüsü) tarafından bir yazılım geliştirilirken, yazılımı geliştiren kişilerin uyması gereken bazı etik kurallar belirlenmiştir. Kısaca bu maddeleri görelim:

- Yazılım Mühendisleri, kamusal yararları gözetmelidir.
- Yazılım Mühendisleri, is vereni ve müşterisinin isteklerini kamusal yararları gözeterek en iyi şekilde yapmalıdır.
- Yazılım Mühendisleri, hem ürün yaratırken hem de bakim yaparken en son teknolojik standartları kullanmalıdır.
- Yazılım Mühendisleri, ürün yaratırken veya gelişimi sırasında hukuksal kurallara uymalıdır.
- Yazılım Mühendisleri, ürün yaratırken etrafındaki herkesi teşvik edici hareketler sergilemeli ve onlara yârdim etmelidir.
- Yazılım Mühendisleri, kamusal yararları ve hukuk kurallarını göz önüne alarak kendini mesleki anlamda sürekli geliştirmelidir.
- Yazılım Mühendisleri, is arkadaşlarını her zaman destek olmalıdır, onların gelişimine yardım etmelidir.
- Yazılım Mühendisleri, hayat boyu yeniliklere açık olmalı kendini sürekli geliştirmelidir.

7- Sosyal Medya Etiği

Zamana ve mekâna bağlı olmadan; her türlü resim, video, söz ve yazıların paylaşıldığı, tartışmanın olduğu, soru sorulup cevap alındığı, anında iletişimin olduğu milyonlarca insanın kullandığı alana sosyal medya denir. Bu yüzden sosyal medya çok önemli ama bunu daha da önemli kılan etik değerlere uygun olan paylaşımların olmasıdır. Birçok etik ilke sıralanabilir ama biz önem arz eden birkaç değerden bahsedelim.

- Tarafsız olmak
- Yalan söylememek
- Toplumun değerleri ile çatışmamak
- Dedikodu yapmamak
- Kendin olmak
- Açık ve anlaşılır dil kullanmak

- Bağlayıcı açıklamalardan kaçınma (Bağlı bulunduğumuz kuruma, gruba ya da zümreyi dahil etmemek)
- Argo ve küfürden kaçınmak.
- Başkalarının özeline saygı duymak

8- İnternet Etiği

Çevrimiçi ortamlarda diğer insanların hak ve hukukuna saygılı olmak noktasında nelerin yapılıp nelerin yapılamayacağının bilgisine internet etiği denir. İnternet etiği, gerçek hayatta iletişimde olduğunuz insanlara gösterdiğiniz saygı ve nezaketin aynıyla internet ortamında da gösterilmesi için bazı kurallar içerir.

Herhangi bir hak ihlaline uğramamak ve kullanılan sistemi de zafiyete uğratmamak için çevrimiçi ortamları kullanırken kullanım politikalarına uygun davranılmalıdır.

- İnsanların iletişim özgürlüğüne sahip olduğu gibi erişim özgürlüğüne de sahip oldukları unutulmamalı, diğer kullanıcıların haklarına saygı gösterilmelidir. İnternet ortamında kimseye zorbalık/taciz yapılmamalı, kötü söz söylenilmemeli ve istemeden kimseye art niyetli davranışlar sergilenmemelidir.
- İnternet ortamında uygun olmayan (yasadışı) içerikleri indirmekten, paylaşmaktan veya saklamaktan kaçınılmalıdır. Bu tarz içeriklerin üretilmesi ve paylaşılmasının suç teşkil ettiği unutulmamalıdır.
- İnternet üzerinden yapılan herhangi bir paylaşımın, birdenbire milyonlarca kişiye erişebileceği her zaman hatırda tutulmalı ve çevrimiçi ortamlarda buna göre davranılmalıdır.
- Fikir ve sanat eserleri ile telif hakları ve lisanslama konusunda titiz davranılmalıdır. Telif hakkı olan materyallerin lisanssız kopyaları oluşturulmamalı veya bu materyaller indirme amaçlı kullanılmamalıdır. Sahibi olunmayan eserler topluluklarla paylaşılmamalıdır.
  Konuyla ilgili mevzuat hakkında aşağıdaki linkten bilgi sahibi olabilirsiniz: http://mevzuat.basbakanlik.gov.tr/Metin1.Aspx?MevzuatKod=1.3.5846&MevzuatIliski=0&sourceXmlSearch=fikir%20ve%20sanat&Tur=1&Tertip=3&No=5846
- Elektronik ortamlara bağlanan cihazlara, sistemlere veya sistemlerde bulunan bilgi kaynaklarına erişim yetkiniz yok ise girilemeyeceği ve kasıtlı olarak sisteme müdahale edilemeyeceği veya işleyişinde değişiklikler yapılamayacağı her zaman hatırda tutulmalıdır.

B.BİLGİ GÜVENLİĞİ YÖNETİMİ TEMEL KAVRAMLARI

1- Bilgi Kavramı

Bilginin sözlük anlamı incelenecek olursa, insan aklının alabileceği gerçek, olgu ve ilkelerin tümüne verilen ad veya bir konu ya da iş konusunda öğrenilen, öğretilen şeyler olarak tanımlandığı görülür.

Bilişim teknolojilerinde bilgi kavramı ise şu şekilde tanımlanır.

Bilişim ürünleri/cihazları ile bu cihazlarda işlenmekte olan verilerin tümüne “Bilgi(Veri)” denir.

2- Bilgi Güvenliği Kavramı

Bilgi güvenliği, bir varlık türü olarak bilginin izinsiz veya yetkisiz bir biçimde erişim, kullanım, değiştirilme, ifşa edilme, ortadan kaldırılma, el değiştirme ve hasar verilmesini önlemek olarak tanımlanır.

3- Bilgi Güvenliği Unsurları

Bilgi güvenliği "gizlilik", "bütünlük" ve "erişilebilirlik" olarak isimlendirilen üç temel unsurdan meydana gelir. Bu üç temel güvenlik öğesinden herhangi biri zarar görürse güvenlik zaafiyeti oluşur. Bu unsurları kısaca açıklamak gerekirse;

Gizlilik: Bilginin yetkisiz kişilerin eline geçmeme ve yetkisiz erişime karşı korunmasıdır.

Bütünlük: Bilginin yetkisiz kişiler tarafından değiştirilmemesidir.

Erişilebilirlik: Bilginin yetkili kişilerce ihtiyaç duyulduğunda ulaşılabilir ve kullanılabilir durumda olmasıdır.

Örneğin,

- İnternet bankacılığına ait hesap bilgimiz bir saldırganın eline geçince "**GİZLİLİK**" zarar görmüş olur.
- Bir web sayfasının içeriği saldırgan tarafından değiştirildiğinde "**BÜTÜNLÜK**" zarar görmüş olur.
- Bir web sayfasına erişim engellendiğinde "**ERİŞİLEBİLİRLİK**" zarar görmüş olur.

C.TEMEL GÜVENLİK PRENSİPLERİ

9- Bilgisayara Giriş Güvenliği Aşamaları

Bilgisayara giriş güvenliği, bilgisayarın içinde sakladığınız bilgilerin de güvenliği anlamına gelmektedir. Bu nedenle son derece önemlidir.

Bu konuda ilk adım fiziksel güvenliktir. Öncelikle bilgisayarınızın bulunduğu yerin güvenliği sağlanmalıdır. En çok karşılaşılan problemlerden birisinin dizüstü bilgisayarların çalınması olduğunu utmamak gerekir.

Bilgisayarınız açılırken kullanıcı adı ve parola sormuyorsa bilgisayarınızı bilgisayarınıza fiziksel olarak ulaşabilen herkes açabilir ve kişisel bilgilerinize erişebilir.

Fiziksel güvenliği sağladıktan sonra bilgisayarını "kullanıcı adı" ve "parola" ile açılmasını sağlamak gerekir.

Bu işlemi iki şekilde yapabilirsiniz:

- Bilgisayarınızın her açılışta(BIOS) parola sormasını sağlayarak,
- Bilgisayarınızda kurulu olan işletim sisteminin açılışında parola sormasını sağlayarak, farklı işletim sistemlerinde farklı adımlar izlemek gerekebilir.

10- Parola Güvenliği Aşamaları

En önemli kişisel bilgilerden olan parola çok farklı yöntemlerle ele geçirilebilmekte ve zararımıza kullanılabilmektedir. Bu yüzden parola güvenliği son derece önemlidir.

Bu sebeple;

- Kullanılan parolalar korunmalı ve paylaşılmamalı,
- Ara sıra değiştirilmeli,

- Herhangi bir yerde yazılı bulundurulmamalı
- Anti-virüs programı güncel tutulmalıdır.

Parolalar genel olarak iki şekilde ele geçirilebilir.

a- Tahmin ederek ya da deneme yanılma yolu ile ele geçirilebilir.
b- Parolanızın çalınması ile yani hırsızlık yaparak ele geçirilebilir.

Parolamız başkası tarafından ele geçirilirse veya böyle bir şüphemiz varsa;

İlk işi olarak parolamızı değiştirilmeli sonrasında ise aynı parola ya da çok benzerleri başka sistemlerde de kullanılıyorsa, onları da değiştirilmelidir.

Bu durumdan etkilenebilecek diğer kişilere haber vermemiz olası başka problemleri önüne geçmemize yardımcı olacaktır.

Benzer problemleri tekrar yaşamamak için, yeni oluşturacağın parolalar, tahmin edilmesi zor, yani güçlü parolalar olmalıdır.

Oluşturulan bir parolanın "güçlü" kabul edilebilmesi için aşağıdaki özellikleri göstermelidir.

- En az 8 karakterden oluşur.
- Harflerin yanı sıra, rakam ve "?, @, !, #, %, +, -, *, %" gibi özel karakterler içerir.
- Büyük ve küçük harfler bir arada kullanılır.

Bu kurallara uygun parola oluştururken genelde yapılan hatalardan dolayı saldırganların ilk olarak denedikleri parolalar vardır. Bu nedenle parola oluştururken aşağıdaki önerileri de dikkate almak gerekir.

- Kişisel bilgiler gibi kolay tahmin edilebilecek bilgiler parola olarak kullanılmamalıdır. (Örneğin doğum tarihiniz, çocuğunuzun adı, soyadınız, ... gibi)
- Sözlükte bulunabilen kelimeler parola olarak kullanılmamalıdır.
- Çoğu kişinin kullanabildiği aynı veya çok benzer yöntem ile geliştirilmiş parolalar kullanılmamalıdır.

Parolanızı korumak için:

- Kağıt ya da elektronik, herhangi bir ortamda açıkça yazılmış olarak bulundurulmamalıdır. Yazılı bulundurulması gerektiğinde saklanan ortamın güvenliği sağlanmalı ve parolalar kilit altında saklanmalıdır.
- Farklı sistemlerde farklı parola kullanılması olası riskleri azaltacaktır.
- Parolalar belirli aralıklarla değiştirilmelidir.

Sakızlar ve parolalar birbirine benzer. Parolalar kişiye özeldir, herkesin farklı bir sakız çiğnemesi gibi.

- Başkalarıyla paylaşılmaz. Herkesin sakızı/parolası farklıdır.
- Ara sıra yenilemek gerekir. Bayat bir sakız güzel değildir ve zor çiğnenir ortalıkta bırakılmaz, yoksa ciddi sorunlar yaratır. Çiğnenmiş bir sakız sokağa atıldığında olduğu gibi

11- E posta Güvenliği Aşamaları

Günlük hayatımızda haberleşme ve dosya transferi için çok sık kullandığımız e-postalar, dikkatli davranılmadığında kolayca insanlara zarar vermek, aldatmak ve bu yolla ekonomik çıkar elde etmek için kullanılıyor olabilirler.

Bu sebeple;

- E-posta adresleri herkese açık web sitelerinde paylaşılmamalı,
- Tanımadığınız kişilerden gelen her türlü e-postaya cevap verilmemeli,
- Kişisel ve mali bilgiler e-posta üzerinden hiç kimseyle paylaşılmamalı,
- E-posta içinde bulunabilecek bağlantılara tıklanılmamalı,
- İçeriği ne olursa olsun, başkalarına göndermeni isteyen e-postaları kimseye gönderilmemeli
- Güncel anti-virus ve güvenlik duvarı yazılımları kullanılmalı.

12- İnternet Erişimi Güvenliği Aşamaları

İnternet yaşamımızı birçok açıdan kolaylaştırsa da dikkatsiz kullanıldığı takdirde sorunlar yaşanmasına neden olabilir. Internet'te var olan tuzakları fark edebilmek ve hangi web sitesine güvenilebileceği, nasıl güvenli hareket edilebileceğine dikkat etmek önemlidir. Ayrıca;

- Özellikle internet ortamında, hassas bilgilerin paylaşımı güvenli iletişim yolları ile gerçekleştirilmelidir.
- Tuzak web sitelerine dikkat etmek ve güvenilmeyen web sitelerini ziyaret etmemek.
- E-posta mesajları ile gönderilen bağlantılara dikkat etmek
- Web sitelerinde gezerken yayılabilen zararlı programlardan korunmak için açılır pencere engelleyicisi kullanmak gereklidir.
- Bunların yanı sıra çocukların güvenliğini sağlamak anne babanın görevidir ve bu konuda alınabilecek tedbirler konusunda aileler hem kendilerini hem de çocuklarının bilinçli birer kullanıcı olmaları için özen göstermelidir.

13- Sosyal Medya Güvenliği Aşamaları

Bireylerin internet aracılığıyla bilişim teknolojilerini kullanarak birbirleriyle etkileşim sağlayan araç, hizmet ve sanal uygulamalara "Sosyal Medya denir".

Sosyal medya güvenliği için dikkat etmemiz gerekenler şunlardır:

- Hangi sosyal paylaşım sitesinde olursa olsun, resmi olmayan hiçbir sayfa ve profillere itibar edilmemesi gerekir.
- Kişisel bilgilerin herkese açık görünür şekilde yer almasına izin verilmemesi gerekir.
- Yapılan paylaşımların ne olduğuna, suç unsuru taşıyıp taşımamasına mutlaka dikkat edilmesi gerekir.
- Aynı şekilde gelen paylaşımların da suç unsuru taşıyıp taşımamasına, küfür, hakaret, sövme, aşağılayıcı sözler içerip içermemesine dikkat edilmelidir. Bu durumlar da size yönelen söz ve davranışlar hakkında suç duyurusunda bulunma hakkınız mevcuttur.
- Hiçbir yerde özel bilgilerinizin paylaşılmaması ve tanımadığınız kişilerin listenizde yer almasına izin vermemeniz gerekir.
- Fotoğraf veya videolar paylaşılmadan önce fotoğrafta yer alanlardan mutlaka izin alınmalıdır.

- Yer bildiriminde bulunurken aslında bulunduğunuz adresi ve konumunuzu da paylaştığınızı unutmayınız...
- Ekranlarda görülen her bilginin doğruluğu mutlaka sorgulanmalı ona göre hareket edilmelidir.
- Twitter ve Facebook gibi sosyal ağlarda gezinirken kaynağı belirtilmeyen aldatıcı linkler tıklanmamalı.
- Sosyal ağ sitelerinde etiketlenme gibi durumların yaşanmaması için mutlaka kişisel profil ayarlarından bu ayarların özenle onaylı olması gerektiğinden emin olunmalıdır.

14- Sosyal Mühendislikten Korunma Yöntemleri

Sosyal mühendislik, internet ortamında, insanların zafiyetlerinden faydalanarak çeşitli ikna ve kandırma yöntemleriyle istenilen bilgileri elde etmeye çalışmaktır. İnsanların karar verme süreçlerini değiştirmeye yönelik teknikler içerir.

Sosyal mühendislik yöntemleri çok çeşitli olmak ile birlikte en çok kullanılan yöntemler şunlardır.

a- **Telefon yolu ile:** En etkili sosyal mühendislik ataklarından biridir. Hedef kişi, bir dolandırıcı tarafından aranır ve arayan kişi yetkili biri gibi davranarak yavaş yavaş kişisel belgilere ulaşır veya istediği eylemleri yaptırır.

b- **Çöpleri Boşaltma (Dumpster Diving):** Önemli ve kötü niyetli kullanıma uygun birçok bilginin, kurumun veya şirketin çöplerinden derlenerek elde edilmesidir.

c- **İkna Etme:** Taklit etme, kendini sevdirme, riayet etme, sorumluluk yayma ve sade bir arkadaş olarak görünme yöntemlerini denerler

d- **On-Line Sosyal Mühendislik Sosyal ağları(Twitter, İnstagram, Facebook vb.)** : çok etkin kullanarak sizi arkadaşınız kadar iyi tanıyabilirler. Facebook aracılığıyla anne kızlık soyadını öğrenmek dakikalar almakta ve bu basit bilgi ile birçok işlem yapılabilmektedir.

Sosyal Mühendislikten korunmak için aşağıdakilere dikkat etmek gerekir.

- Kullanıcılar eğitilmelidir.
- Telefonda arayan hiç kimseye şifreler ve önemli bilgiler verilmemelidir.
- Büyük şirketlerde veya kurumlarda "yardım masası" denilen bölümler vardır. Bu bölümleri arayıp kimlik doğrulaması tam olarak yapılmalıdır.
- Uygun olmayan yöntem ve kanallardan kurumsal bilgiler paylaşılmamalıdır.
- Parola gizliliği prensibi, kurum genelinde uygulanmalıdır.
- Gerektiğinde, “Ben kurumsal hattan sizi arayayım” denilmelidir.
- Kurumsal gizlilik taşıyan evraklar, uygun yöntemlerle imha edilmelidir.
- E-Posta, posta ile gelen CD, yardımcı yazılımlar vs. kullanımında dikkatli olunmalıdır.

15- Dosya Erişim ve Paylaşım Güvenliği Aşamaları

Bilgisayarda bilgilerin kaydedildiği birimlere dosya adı verilir. Dosya içerisindeki bilgi; resim, yazı, çizim, ses gibi her şey olabilir.

Herhangi bir şekilde, ister paylaşıma açarak ister dosya paylaşım yazılımları kullanarak başkalarının erişimine imkan verdiğiniz zaman bilgisayarınızı korumak için güvenlik önlemleri almanız gerekir. Bunun için

- Paylaşıma açtığınız dosya veya klasörler, kimlerin hangi haklarla erişmesi gerektiği göz önünde bulundurularak yapılandırabilir.
- Kişisel veya önemli bilgilerin olduğu dosyalar şifrelenerek saklanabilir.
- Paylaştığınız dosya veya klasörlerin zaman zaman denetimini yapmak ve önceden verilmiş hakları güncellemek gerekir.
- Dosya paylaşım yazılımları kullanırken telif haklarını göz önünde bulundurarak paylaşımda bulunmak yasal açıdan önemlidir.

16- Sistem ve Verilerin Yedeklenmesi Aşamaları

Yazılım veya donanım hataları yaşandığında veri kaybı yaşanabilir. Yedekleme, bilgi kaybını azaltmak için önlem almaktır. Yedeklemenin önemi, değerli bir bilginin yitirilmesinden sonra daha iyi anlaşılır. Ancak yitirilen bilginin arkasından üzülmektense, akıllı davranıp yedek almak hem zaman kazandırır hem de iş gücü tasarrufu sağlar.

Verilerimizi:

- Dosyalarınızı veya verilerinizi farklı ortamlara (CD, DVD, USB gibi) kopyalayarak
- Yedekleme yazılımları ile yedeğini alarak sağlayabilirsiniz.

Neleri ne zaman yedekleyeceğiniz sorusuna cevap vermek ve bir yedekleme planı oluşturmak etkin yedekleme süreçleri için önemlidir.

17- Zararlı Yazılımlardan Korunma Aşamaları

Zararlı programlar bilgisayarımız üzerinde başka şahısların kontrol sahibi olmasını sağlarlar. Programlarımız bozulabilir, istediğimiz gibi çalışmamaya başlarlar. Dosyalarımız silinebilir. Kişisel bilgilerimiz başkalarının eline geçebilir.

Bu sebeple;

- Antivirüs (virüsten korunma) ve antispyware (casus yazılımdan korunma) programları kullanmalıyız
- Antivirüs ve antispyware programlarını güncel tutmalıyız
- İşletim sistemini güncel tutmalıyız (işletim sistemi yamalarını yapmalıyız)
- Güvenlik duvarı kullanmalıyız
- İnternette girdiğimiz sitelere ve indirdiğimiz dosyalara dikkat etmeliyiz
- Lisanslı programlar kullanmalıyız
- E-postaları açmadan önce içeriğinin güvenilirliğini kontrol etmeliyiz.

18- Mobil cihaz güvenlik aşamaları

Haberleşmeden bankacılığa, alışverişten elektronik cüzdana günlük hayatımızda her türlü iş için kullanmakta olduğumuz mobil haberleşme araçları olan cep telefonları, en önemli araç olarak hemen hemen her kişinin cebindeki yerini alırken hem akıllanıp kapasite ve yetenekleri artmakta hem de çok çeşitli siber tehditlerin hedefi haline gelmiş bulunmaktadır.

Bu konuda dikkat edilmesi gereken en önemli konuları şöyle sıralamak mümkündür;

- Bilmediğiniz kaynaklardan gelen ya da şüphe uyandıran elektronik postaları açmayınız,
- Bilmediğiniz kaynaklardan gelen ya da şüphe uyandıran elektronik postaların eklentileri üzerine tıklamayınız, bu ekleri cihazınıza indirmeyiniz,
- Cihazınıza kaynağından emin olmadığınız ve/veya işlevini bilmediğiniz yazlım yüklemeyiniz,
- Uygulama dükkanlarından indireceğiniz uygulama yazılımlarını dikkatlice seçiniz, özellikle ücretsiz olanları mümkün olduğunca indirmeyiniz,
- Cihazının içinde sakladığınız kritik bilgilerinizi (örneğin şifre dosyanız, kimlik belgeleriniz vs.) şifreleyiniz,
- Cihazınızın ayarlarını yaparken özellikle dışarıya gidecek ya da dışarıdan gelecek verileri (konum bilgisi vb.) otomatik hale getirmeyiniz, sizin onayınızı isteyiniz,
- Cihazınızı tanımadığınız kişilere vermeyiniz,
- Cihazınızı üreticilerin resmi tamir-bakım merkezleri dışında tamir ettirmeyiniz,
- Şüpheli kaynaklardan hediye telefon kabul etmeyiniz,
- Cihazınızda mutlaka virus koruma programı bulundurunuz,
- Cihazınızdaki yazılımları sık sık güncelleyiniz,
- Cihazınızı zaman zaman fabrika ayarlarına döndürünüz ve/veya formatlayıp yeniden kurunuz,

D.SİBER SUÇLAR VE İSTİSMARLAR

19- Siber Uzay Nedir?

- *"Siber" kelimesi İngilizce "Cyber" kelimesinden uyarlanıp kullanılmaya başlayan bir kelime olup "Bilgisayar ağlarına ait olan", "İnternete ait olan", "Sanal Gerçeklik" manalarına gelmektedir.*

Siber Uzay (Cyberspace), birbirine bağlı olan cihazlar teknolojisidir. Siber Ortam olarak da adlandırılan Siber Uzay yalnızca bilgisayar ağları üzerinden iletişim kurulan donanımları içeren bir çevredir.

Bu tanımın, öncelikle internet'i ve onun üzerindeki bütün Web servisini içerdiği açıktır. Ancak, buradaki "bütün veri kaynakları" deyimi Web servislerinden fazlasını kapsar. Telefon, telex, radyo, TV gibi elektronik olarak kumanda edilebilen bütün aygıtlar, kaydedilebilen ses ve görüntüler, filimler, fotoğraflar, grafikler, kitaplar, projeler... Bunların yanında, marketlerden alış-veriş, banka işlemleri, e-ticaret, sinema ve tiyatro görüntüleri,... **Bütün bunların bileşimi siber uzaydır.**

20- Siber Suç Nedir?

Her geçen gün teknolojinin ve bu teknolojilere erişilebilirliğin artmasına paralel olarak bilişim sistemlerine yönelik işlenen suçlar da artmaktadır. Siber Suç, bir bilişim sisteminin güvenliğini ve / veya buna bağlı verileri ve / veya kullanıcısını hedef alan ve bilişim sistemi kullanılarak işlenen suçlardır. Siber Suçu diğer suçlardan ayıran özelliği bir bilişim sistemi olmadan işlenememesidir. Bu suç türü bilgisayar ve internete özgü suçlar olarak da adlandırılabilir.

Örneğin, bir sisteme girerek, zarar verme, verileri silme, şifreleme, ele geçirme, veri ekleme, sistemin kullanımını engelleme, özel hayatın gizliliğine müdahale etme, iletişimi engelleme, iletişimi izinsiz izleme ve kayıt etme gibi eylemler siber suç kategorisinde değerlendirilir.

21- Siber Suç Çeşitleri

a) **İstenmeyen İletilerin Gönderilmesi:** Toplu mesaj veya istenmemiş yığın miktarda iletinin ticari amaçlarla gönderilmesi bazı devletlerin yasal dizgelerinde yasa dışı bir eylem olarak değerlendirilir.
b) **Dolandırıcılık:** Banka dolandırıcılığı, kimlik hırsızlığı, gasp etme, özelleştirilmiş bilginin çalınması eylemleri olduğu gibi diğer dolandırıcılık biçimleri bilişim sistemlerinin kullanılması ile sağlanabilir.
c) **Müstehcen veya Saldırgan İçerik:** İnternet sayfaları ve diğer elektronik iletişim araçları nahoş, müstehcen veya birçok neden ve çeşitlilikte saldırgan içerikler bulundurabilir.
d) **Rahatsızlık Verme, Taciz:** İçerik çok farklı biçimlerde ortaya çıkabilir olsa da, rahatsızlık verme veya taciz etme, doğrudan müstehcen ve küçültücü yorumlar bir cinsiyet, ırk, din, cinsel durum gibi belirli özellikleri ile kişileri doğrudan hedef almasıdır.
e) **Korkutma ve Hakaret:** Anayasada ifade özgürlüğü 25. maddede korunmaktadır. Her türlü ifade özgürlüğünü kapsamaz. Gerçekte, konuşulan veya yazılan gerçek tehdit söylem/yazım zarar verme veya korkutma kastı olması nedeniyle suç olarak tanımlanmıştır ve bu tehdit bir bilgisayar ağında yazılı/sözel olarak kullanılabilir.
f) **Uyuşturucu Kaçakçılığı ve Yasa Dışı Ürün Satışları:** Uyuşturucu madde tacirleri günümüzde giderek daha fazla oranda yasa dışı uyuşturucunun nakledilmesi ile satışında e-posta ve diğer internet teknolojilerinden şifreli yollarla yararlanmaktadırlar.
g) **Siber Terörizm:** Önemli sistemlerin mevcut güvenlik boşluklarını kullanarak bilgi alma, sisteme zarar verme gibi eylemlerin, yabancı istihbarat kurumlarının veya diğer gruplar tarafında gerçekleştirilmesidir.

22- Siber Suçun Sosyal ve Ekonomik Yaşama Etkisi

Gelişen teknolojiyle birlikte birçok suç türü internet ortamına taşınmıştır. Suçlunun mağdura birebir temas etmesini gerektiren birçok suç artık uzaktan işlenebilmektedir Günümüzde suç ekonomisinin kapsamı ve hacmi çok önemli boyutlara ulaşmıştır. Yetkililerinin açıklamalarına göre dakikada 4.800 cihazın birbirine bağlandığı internet ortamında yaşanan siber saldırıların dünyaya maliyetinin 2.1 trilyon doları bulabileceği belirtilmiştir. Siber saldırıların ekonomik yansımalarının zamanla daha da artacağı tahmin edilmektedir.

Siber suçların sadece ekonomik alanda yaptıkları olumsuz etkiler değil, ulusal güvenliğe ve mağdurların psikolojilerine yaptığı olumsuz etkiler de yadsınamaz.

23- Siber Suçların Tarihçesi

Bilgisayar ve internet alanında işlenen suçların tarihi 1960'lara kadar gitmektedir. İnternet'in anavatanı olan ABD, internet ve bilgisayar dünyasındaki tüm olumlu gelişmelerin öncülüğünü yapmasının yanında, İnternet'in bir suç vasıtası olarak kullanılmasında ve bu suçlara ilişkin düzenlemelerin yapılmasında da öncülüğü kimseye bırakmamıştır. Bilgisayarlar ve internet konusunda 1970'li yılların ortalarına kadar karşılaşılan ve suç teşkil eden eylemler, bugün için nispeten basit sayılabilecek düzeyde olmuştur. Zaman ilerledikçe bilgisayar ve internet teknolojisinin de gelişmesiyle bu teknoloji çok hızlı bir şekilde gelişmektedir. Bilgisayarlar yoluyla işlenen suçlar üzerine yapılan ilk çalışmalar, 1970'li yıllarda başlamıştır. 1980'li yıllardan sonra, iş hayatında ve günlük hayatta bilgisayar ve internet kullanımının yaygınlaşması ile birlikte, nitelik ve nicelik olarak değişikliğe uğrayan suç olgusu, bu sahanın da bir takım hukuki düzenlemelerle disipline edilmesi ihtiyacını ortaya çıkarmıştır. 1980'li yıllardan sonra, bilgisayar ve internet yoluyla işlenen suçların sadece ekonomik boyutlarının olmadığı ve bu tür suçların en az ekonomi kadar önemli, diğer bazı değerler aleyhine de işlenebileceği anlaşılmıştır. Bunun sonucu olarak da siber suç olgusu ortaya atılmış ve bu suçların ayrı bir disiplin altında incelenmesi gereği ortaya çıkmıştır.

24- Siber İstismar Kavramı

Bir çocuğun veya ergenin başka bir çocuk veya ergen tarafından internet, interaktif, dijital ve mobil teknolojiler kullanılarak tehdit edilmesi, aşağılanması, utandırılması, taciz edilmesi veya işkence edilmesi olarak değerlendirilmektedir.

İstatistikler siber zorbalığın günümüzde en büyük mağdurlarının çocuklar (0-18) olduğunu göstermektedir. Bunun nedeni ise gelişen teknoloji ve bu teknolojinin beraberinde getirdiği riskler noktasında en savunmasız grubun çocuklar olmasıyla açıklanmaktadır Öyle ki bu riskler hızla yaygınlaşan bir biçimde okulun sınırlarını aşmış çocukların-gençlerin evdeki odalarına kadar girmiştir. Çocuklar ve gençlerin yaşadığı siber zorbalık, akranlarının e-posta, Facebook, Whatsapp, vb. sosyal sohbet ortamları üzerinden veya doğrudan cep telefonlarına gelen sözlü veya yazılı mesajlarla rahatsız edilmesi, küçük düşürülmesi veya aşağılanması şeklinde de ortaya çıkmaktadır.

25- Türkiye'nin Siber Güvenlik Organizasyon Yapısı

Siber güvenlikle ilgili olarak kamu kurum ve kuruluşları ile gerçek ve tüzel kişiler tarafından alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla; Bakanın başkanlığında ***Siber Güvenlik Kurulu kurulmuştur***. Siber Güvenlik Kurulunda yer alacak bakanlık ve kamu kurum ve kuruluşları ile üyelerinin temsil düzeyi Bakanlar Kurulu tarafından belirlenir.

<u>Siber Güvenlik Kuruluna Üye Kurumlar Listesi</u>

- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (UDHB)
- Dışişleri Bakanlığı
- İçişleri Bakanlığı
- Milli Savunma Bakanlığı (MSB)
- Kamu Düzeni ve Güvenliği Müsteşarlığı
- Milli İstihbarat Teşkilatı (MİT)
- Genelkurmay Başkanlığı
- Bilgi Teknolojileri ve İletişim Kurumu (BTK)
- Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK)
- Mali Suçları Araştırma Kurulu
- Telekomünikasyon İletişim Başkanlığı (TİB

BİLİŞİM HUKUKU

1- Bilişim Suçlarının Türk Hukuk Düzenindeki Yeri

Ülkemizde de bilişim suçlarına yönelik tek bir kanun yoktur. Onun yerine mevcut kanunlara bilişim suçlarıyla ilgili hükümler eklenmiştir.

Türkiye'de bilişim alanında gerçekleştirilen yasal düzenlemeler, genel olarak AB direktifleri ile uyumlu olacak şekilde hazırlanmıştır. Bilişim suçları, her suçun kendi alanına ilişkin düzenlemeler içermektedir.

2- Bilişim Hukukunun Temel Kavramları

Bilişim hukuku, sayısal bilginin paylaşımını konu alan hukuk dalıdır. İnternetin kullanımına ilişkin yasal çerçeveyi belirleyen internet hukukunu kapsamaktadır. Bu bağlamda; gizlilik ve ifade özgürlüğü gibi kavramlar da bilişim hukukunu ilgilendirir.

Bilişim Hukukunun, Bilgi Teknolojisi Hukuku ve İnternet Hukuku başlıkları altında ikiye ayrılarak incelenmesi gerekir. Bilgi Teknolojisi Hukuku hem dijital hale getirilmiş bilginin hem de bilgisayar programlarının dağıtılması ile ilgili hükümleri düzenler. Bilgi güvenliğinin sağlanması ve elektronik ticaret konularında düzenlemeler içerir. Diğer taraftan İnternet Hukuku, İnternet'in kullanılması ile ortaya çıkan hukuki meseleleri inceler. İnternet Hukukunun hukukun birçok alanı ile etkileşim içerisinde bulunması gerekir. İnternet erişimi ve kullanımı, güvenlik, ifade özgürlüğü ve yargılama gibi hukukun diğer alanları ile ilişkilidir.

3- Bilişim Suçlarının Uluslararası Hukuk Düzenindeki Yeri

Her ülkenin doğru kabul ettiği bir internet hukuku bütünlüğü bulunmamaktadır. Her ülke şimdilik kendi politikası ve dünya görüşüne göre düzenleme yapmaktadır. Örneğin, bazı ülkelerde internete giriş izinle olabildiği gibi, bazılarında devletin kontrolünde olan tek bir servis sağlayıcı bulunabilmektedir.

4- Etik ile hukuk arasındaki ilişki

Etik ve hukuk kavramlarının, benzer yanlarının yanı sıra farklılıkları da mevcuttur. Ayrıca, zamanla bu iki kavramın birbiriyle iç içe geçtiği ve kimi zaman da bir etik ilkesinin bir hukuk kuralına dönüştüğü görülebilmektedir. Nitekim her iki kavram da belli ölçüde, insanların fiillerini ve davranışlarını düzenleme gayesindedir; insanların yaşantılarında tek başlarına değil, bir topluluk olarak yaşamaya gereksinim duyması ve bunun için var olması da yine her iki kavramın mevcudiyetinin önemine işaret etmektedir.