BİLİŞİM ETİĞİ VE BİLGİ GÜVENLİĞİ

Programlama Temelleri – Hafta 1

Etik Nedir?

İnsanların kurduğu bireysel ve toplumsal ilişkilerin temelini oluşturan değerleri, normları, kuralları; doğru – yanlış ya da iyi – kötü gibi ahlaksal açıdan araştıran bir felsefe disiplinidir.

Bir başka tanıma göre ise etik; doğru ile yanlışı, haklı ile haksızı, iyi ile kötüyü, adil ile adil olmayanı ayırt etmek ve **DOĞRU, HAKLI, İYİ ve ADİL** olduğuna inandığımız şeyleri yapmaktır.

Etik İlkeler

- ✓ 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

Bilişim Nedir?

Bilişim; insanların teknik, ekonomik ve toplumsal alanlardaki iletişimde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığı ile düzenli ve akılcı biçimde işlenmesi, bilginin elektronik cihazlarda toplanması ve işlenmesi bilimidir.

Bilişim; bilginin aktarılması, organize edilmesi, saklanması, tekrar elde edilmesi, değerlendirilmesi ve dağıtımı için gerekli kuram ve yöntemlerdir.

Bilişim Etiği Nedir?

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

Bu normlar ve kuralların temel amacı elektronik ortamdaki kullanıcıların minimum zarar ve maksimum fayda ile bu ortamı kullanmasını güvence altına almaktır.

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

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.

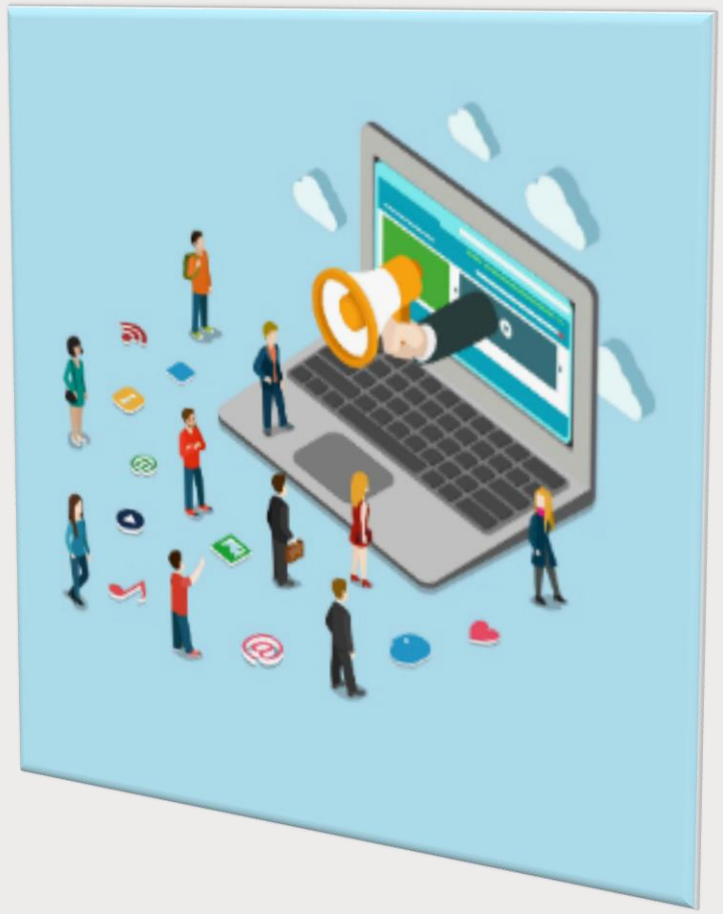
İnsanlar anayasada belirtilen haklara sahip olmakla beraber aşağıdaki kurallara da uymak zorundadır.

- ✓ 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.

Bilgisayar Etiği Nedir?

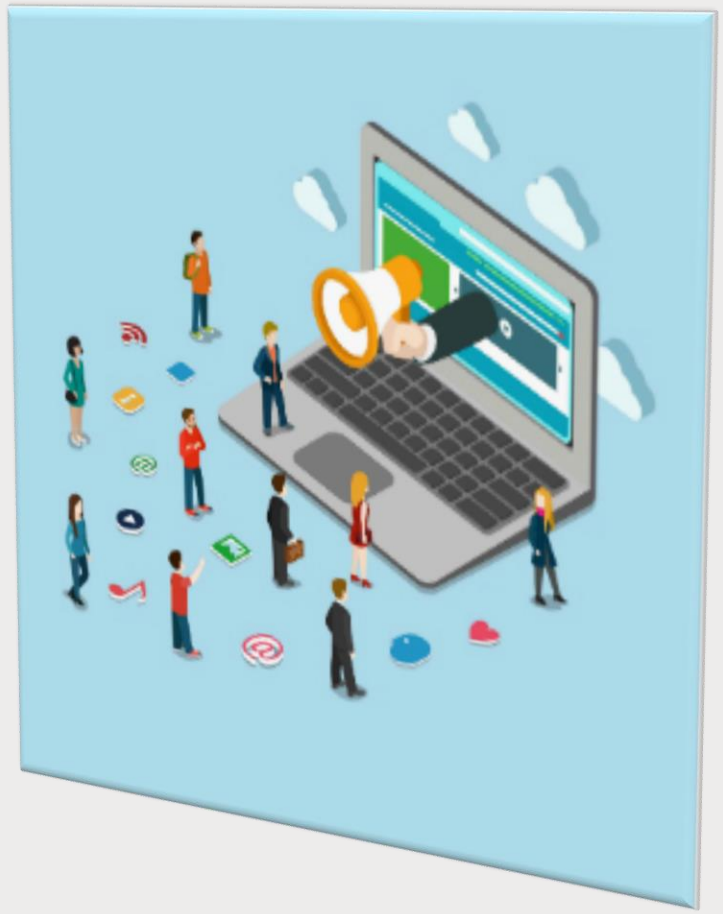
Bilgisayar Etiği Enstitüsü (Computer Ethics Institute) tarafından ortaya konan 10 etik kural şunlardır.

- ✓ Bilgisayarı başkalarına zarar vermek için kullanma
- ✓ Başka insanların bilgisayar çalışmalarını karıştırma
- ✓ Başka insanların dosyalarını karıştırma
- ✓ Bilgisayarı hırsızlık yapmak için kullanma
- ✓ Bilgisayarı yalan bilgiyi yaymak için kullanma



Bilgisayar Etiği Nedir?

- ✓ Bedelini ödemediğin yazılımı kullanma
- ✓ Başka insanların bilgisayar kaynaklarını izin almadan kullanma
- ✓ Başka insanların entelektüel bilgilerini kendine mal etme
- ✓ Yazılan programın sosyal hayata etkilerine dikkat et
- ✓ Bilgisayarı; saygı duyulacak, hakkında bahsedilecek şeyler için kullan



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, işvereni 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.

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

İnternet Etiği Nedir?

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.

İnternet Etiği Nedir?

- ✓ 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.
- ✓ 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.

İnternet Etiği Nedir?

İnternet üzerinde kabul edilebilir ya da kabul edilemez davranışları belirleyen kurallara internet etiği denir. İnternet etiği hakkında 10 kural vardır. Bunlar;

- ✓ İnsan olduğunuzu unutmayın.
- ✓ İnternet ortamında da gerçek hayatta olduğu gibi davranın.
- ✓ Sanal ortamda bulunduğunuz yerin bilincinde olarak davranışta bulunun.
- ✓ İnsanların zamanlarına saygı gösterin.
- ✓ İnternette güzel görünün.

İnternet Etiği Nedir?

- ✓ Bilgilerinizi paylaşın.
- ✓ Ateşli tartışmalarda kontrolünüzü kaybetmeyin.
- ✓ İnsanların özel hayatlarına saygı gösterin.
- ✓ Gücünüzü kötüye kullanmayın.
- ✓ İnsanların hatalarına karşı bağışlayıcı olun.

Bilişim Etiği İle İlgilenen Kurumlar

- ✓ Bilim Teknolojileri ve İletişim Kurumu
- ✓ Telekomünikasyon İletişim Başkanlığı
- ✓ Türkiye Bilişim Vakfı
- ✓ Türkiye Bilim Teknoloji Araştırma Kurumu
- ✓ Türkiye Bilişim Derneği
- ✓ Bilişim Sektörü Derneği

Kanunlar

- ✓ 5651 Sayılı Kanun (İnternet Erişiminin Kontrol Altına Alınması)
- ✓ 5846 Sayılı Kanun (Fikir ve Sanat Eserleri)
- ✓ Türk Ceza Kanununda yer alan Bilişim Suçları
  - ✓ *243: Bilişim Sistemine Girme*
  - ✓ *244: Sistemi Engelleme Bozma*
  - ✓ *245: Banka ve Kredi kartlarını kötüye kullanma*
  - ✓ *246: Tüzel kişiler hakkında güvenlik tedbirleri uygulanması*

Kanunlar

- ✓ Türk Ceza Kanununda yer alan Bilişim Suçları
  - ✓ *135: Kişisel verilerin kayıt edilmesi*
  - ✓ *136: Kişisel verilerin hukuka aykırı olarak ele geçirilmesi*
  - ✓ *138: Verileri yok etme*
  - ✓ *132: Haberleşmenin gizliliğini ihlal etme*
  - ✓ *124: Haberleşmenin engellenmesi*
  - ✓ ***125: Bilişim Sistemi kanalı ile hakaret***
  - ✓ *142: Nitelikli hırsızlık*
  - ✓ *158: Nitelikli dolandırıcılık*
  - ✓ *226: Müstehcenlik*

Bilgi Güvenliği Yönetimi Temel Kavramları

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.

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.

Bilgi Güvenliği Yönetimi Temel Kavramları

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 zafiyeti oluşur. Bu unsurları kısaca açıklamak gerekirse;

- ✓ **Gizlilik:** Bilginin yetkisiz kişilerin eline geçmeme ve yetkisiz erişime karşı korunmasıdır.
- ✓ **Bütünlük:** Bilginin doğruluğunun, tamlığının ve kendine has özgünlüğünün korunmasıdır.
- ✓ **Erişilebilirlik:** Bilginin yetkili kişilerce ihtiyaç duyulduğunda ulaşılabilir ve kullanılabilir durumda olmasıdır.

Bilgi Güvenliği Yönetimi Temel Kavramları

ÖRNEĞİN;

- ✓ 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

Kişisel Bilgiler

- ✓ TC Kimlik Numarası
- ✓ Kredi Kart Numarası
- ✓ Parola
- ✓ Adres
- ✓ Telefon
- ✓ Anne Kızlık Soyadı

vb..

Kurumsal Bilgiler

- ✓ Personel Bilgileri
- ✓ Bilgisayar Bilgileri
- ✓ Sunucu Bilgileri
- ✓ E – Posta Hesap Bilgileri
- ✓ Web Sayfası Bilgileri
- ✓ Müşteri Bilgileri
- ✓ Raporlar ve Planlar

vb..

Bilgi Güvenliği Yönetimi Sistemi Prensipleri

ISO 27001 Bilgi Güvenliği Yönetim Sistemi ilke olarak bulunan dokuz prensip birbirini tamamlamakta olup bir bütün olarak okunmalıdır. Bu ilkeler, politik ve uygulama seviyeleri de dahil olmak üzere tüm kullanan bireyleri ilgilendirmektedir. Bizlere rehber olan ilkeler çerçevesinde kullanıcıların üstlenmiş oldukları sorumlulukların rollerine göre değişiklik gösterebilmektedir. Daha kaliteli bir güvenlik anlayışının derlenmesi ve uygulamaların benimsenmesi için üretimi, eğitimi, bilgi paylaşımı sayesinde tüm kullanıcılara yardımda bulunmaktadır. Bilgi sistemleri ve ağlarının güvenilirliğini artırma çalışmaları, demokratik toplumsal değerleriyle, özellikle de kişisel mahremiyet ile ilgili esas olan konular ve bilginin serbest ve açık bir şekilde gereksinimi ile uyum gösterebilmektedir.

Bilgi Güvenliği Yönetimi Sistemi Prensipleri

Bilinç

Kullanıcı bireyler, bilgi sistemleri ve sahalarının güvenliğinin ihtiyaçlarını ve güvenliğini artırmak için neler yapabilecekleri konusunda bilinçli olmalıdır. Bilgi ağlarının ile sistemlerinin güvenliği bakımından, riskler ve mevcut korunma şekilleri konularda bilinç ilk savunma temelini oluşturmaktadır. Bilgi ağları ile sistem hem dış hem de iç risklerden etkilenebilecek vaziyettedir. Kullanıcı bireyler güvenlik anlamında oluşan noksanlıkların kontrolleri altındaki ağlara ve sisteme yüksek miktarda zarar geleceğini bilmelidirler ve birbiriyle bağımlı olan sistemler nedeniyle diğer kullanıcı bireylere da zararları dokunabileceklerini hiç bir zaman unutmamalıdırlar. Kullanıcı bireyler, ağ içindeki yeri ve sistemlerin güncelleştirilmesi ile güvenliği yükseltmek maksadıyla yapacakları iyi örnekler ve başka kullanıcı bireylerinde ihtiyaçların hakkında bilgi sahibi olmalıdır.

Bilgi Güvenliği Yönetimi Sistemi Prensipleri

Duyulan Tepki

Kullanmakta olan bireyler, güvenlik tehditlerini engellemek, belirlemek ve karşı tepki gösterebilmek maksadıyla bir ortaklık içinde olmalı ve zamanında faaliyete geçmelidirler. Kullanan bireyler, bilgi ağlarının ve sistemlerinin birbirlerine olan bağlantılı yapısını ve potansiyel aksaklıklarını hızlı bir şekilde ve geniş alanlara yayılabileceğini unutmayarak güvenlikle ilgili tehditler karşısında ortaklık içerisinde olmalı aynı anda müdahalede bulunmalıdırlar. Tehlike ve zafiyet konusundaki bilgileri mümkün oldukça birbirleriyle paylaşmalı, güvenlik tehlikelerine karşı koymak, müdahale etmek, saptamak amacıyla atik ve etkili bir ortaklık çerçevesinde ihtiyaç olan prosedürler faaliyete geçirmelidirler. Gerekli izinlerin verildiği aşamalarda sınırları aşan bilgi paylaşımı da buna dahil edilebilir.

Bilgi Güvenliği Yönetimi Sistemi Prensipleri

Sorumluluk Alma Görevi

Tüm kullanıcı bireyler bilgi ağları ve sistemlerin ehemmiyetinden sorumlu tutulmaktadır. Yerel bilgi ağlarına ve sistemlerine ve bağlı olan kullanıcı bireyler, sistemlerin ehemmiyeti konusunda kendilerine ayrılan sorumlulukların farkında olmaları gerekmektedir. Kendilerine ayrılan rollere uygun bir yöntemler davranmalıdırlar. Kullanıcı bireyler kendi ait olan politika, yöntem, uygulama, tedbir alma prosedürlerini düzenli bir şekilde irdelemeleri ve uygun bulunup bulunmadıklarını değerlendirmelidir. Mamul ve hizmet sağlayan, yenileyen ve tasarlayan kullanıcı kişiler, kullan bireylerin mamul ve hizmetlerin ehemmiyetini fonksiyonlarını daha ayrıntılı anlamaları ve bu konuda kendi yükümlülüklerinin bilincinde olabilmeleri için ağ ve sistem güvenliği konusuna dikkat etmeli ve güncellemeleri de olmak üzere gerekli bilgileri sunmalıdır.

Bilgi Güvenliği Yönetimi Sistemi Prensipleri

Risklerin Değerlendirilmesi

Kullanmakla olan bireyler risk analizlerini yapmalıdır. Tehlike ve hassasiyetleri anlatan risk analizleri, fiziksel, teknoloji ve insani etmenleri, siyasal ve üçüncü taraf hizmetleri gibi önem arz eden iç ve dış sebepleri kapsayacak biçimde geniş bir kesime temsil edilmelidir. Risk değerlendirmeleri kabul gören risk seviyesinin saptanmasını belirler ve korunması lazım bilginin önemi ve yapısı doğrultusunda bilgi ağ ve sistemlerin karşılıklı olduğu potansiyel tehlike risklerini yönetmek maksadıyla gereken kontrollerin seçimine yardımcı olur. Bilgi sistemlerinin giderek daha bağımlı bir duruma gelmeleri nedeniyle risk analizleri, diğer kullanmakta olan bireylerden yaşanan yahut onları etkileyebilecek potansiyel kazaları da göz önünde bulundurmalıdırlar.

Bilgi Güvenliği Yönetimi Sistemi Prensipleri

Etik Kurallar

Kullanılan bireyler birbirlerine karşı yasal çıkarlarına saygı duymalıdırlar. Bilgi ağ ve sistemlerin toplumumuz içinde ne kadar süratli bir şekilde yaygınlaştığı düşünülürse, kullanan bireylerin faaliyetlerinin veya tepkisizliklerinin diğerlerine zarar getirebileceğini anlamaları gerekmektedir. Bu maksatla ahlaki davranışlar çok önem arz edip kullanan şahısların en güzel şekilde uygulamaları benimsemeye ve geliştirmeye itina göstermeli, güvenlik gereksinimlerini göz önünde bulunduran faaliyetlere teşvik ederek, diğer kullanan tarafların çıkarlarına saygı etmemelidirler

Bilgi Güvenliği Yönetimi Sistemi Prensipleri

Güvenlik Tasarımı Ve Faaliyetleri

Kullanan şahıslar, güvenliği, bilgi ağları ve sistemini ve önemli bir faktör olarak ele almalıdır. Güvenliği sağlam kılmak için sistemler, politikalar, ağlar ve uygun şekilde uygulanmalı, tasarlanmalı ve koordinasyon edilmelidir. Bu çalışmaların önemli bir organı da, tanımlanmış tehlike ve hassasiyetlerden kaynaklanabilecek hasarları engellemek ya da minimuma indirmek için uygun engelleme yöntemleri ve çözümlerinin benimsenmeli ve tasarlanmalıdır. Hem tekniksel hem de teknik olmayan korunma şekilleri ve çözümleri gerekli olup bunlar, faaliyetlerin sistem ve ağlarında bulunan bilginin önemi ile orantılı olmalıdır. Güvenlik, hizmet, ürün, sistem ve aların temel bir elemanı olmalı ve sistem tasarımı ve mimarisinin ayrılmaz bir nesnesi boyutuna gelmelidir. Uç kullananlar için güvenlik tasarımı genelde kendi ağları için ürün ve hizmetleri seçmek ve yapılandırmak manasına gelmektedir.

Bilgi Güvenliği Yönetimi Sistemi Prensipleri

Yeniden Analiz Etme

Kullanan bilgi ağların ve sistemin ehemmiyetini incelemeli ve yeniden analiz etmeli; güvenlik ile alakalı politika ve uygulama prosedürlerde düzenlemeleri yapmalıdır. Sürekli bir şekilde yeni ve değişen tehlike ve hassasiyetler ortaya çıkmaktadır. Kullanan bireyler değişen bu tehlike ile mücadele etmek amacıyla güvenliğin bütün elemanların devamlı olarak irdelemeli ve yeniden değerlendirmeli ve düzenlemelidir.

Bilgi Güvenliği Yönetimi Sistemi Prensipleri

Demokrasi

Bilgi ağları ve sistem güvenliği, demokratik toplumun en önemli değerleriyle uyumlu olmalıdır. Güvenlik faaliyetleri, ifade ve düşünce özgürlüğü, bilgi ve iletişimin güvenilirliği, bilginin serbestliği, kişisel bilginin muhafaza edilmesi, açıklık ve şeffaflık gibi değerler toplum ile uyumlu bir şekilde yürütülmelidir.

Bilgi Güvenliği Yönetimi Sistemi Prensipleri

Güvenlik Yönetimi

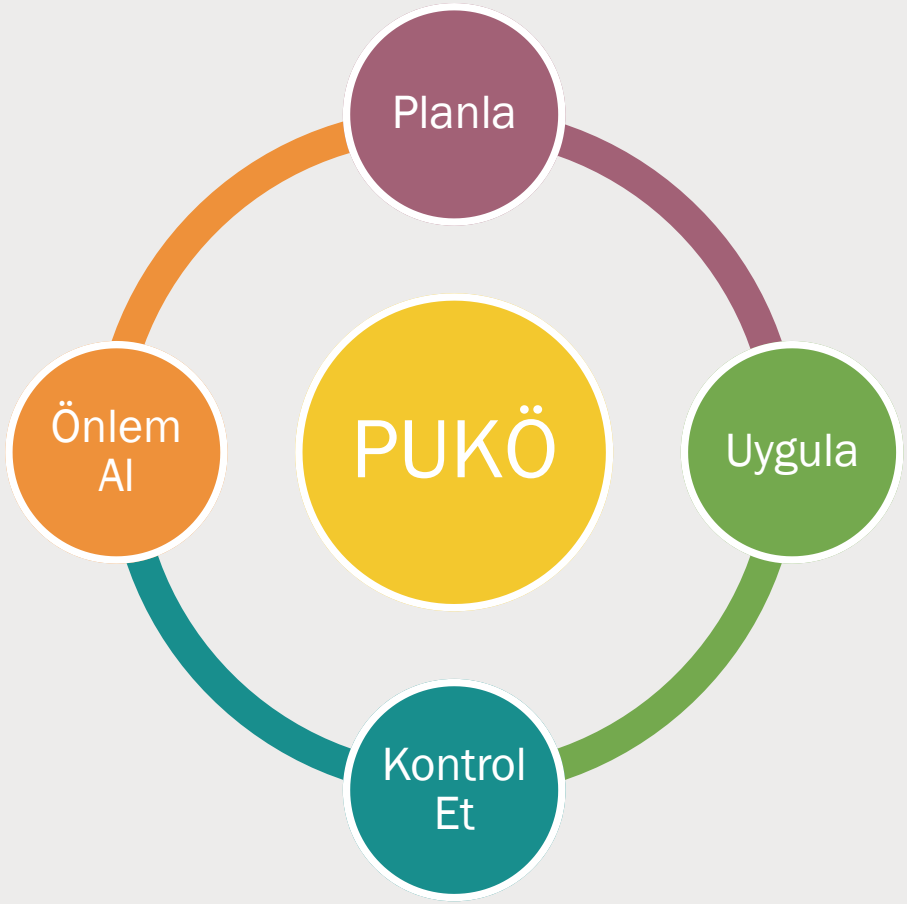
Kullanan bireyler güvenlik yönetimiyle alakalı kapsamlı bir yaklaşım benimsemelidir. Güvenlik yönetimi, risk analizlerine dayalı ve kullanan bireylerin tüm faal düzeylerini ve işlemlerinin her anlamda kapsayacak biçimde dinamik olmalıdır. Yeni tehlikelere karşı ileri görüşlü analizler içermeli, bakım, sistem onarımı, arızalara karı önlem, inceleme, saptama ve müdahale gibi konulara önem vermelidir.

Bilgi sistem ve ağ güvenliği uygulamaları, prosedürleri ve önlemleri tutarlı bir güvenlik sistemi oluşturabilmek adına koordine edilmeli ve bütünleştirilmelidir. Güvenlik yönetimi gereksinimleri, kullanıcının rolüne, katılım seviyesine, riske ve sistem gereksinimlerine bağlıdır.

PUKÖ Döngüsü

Sürekli İyileştirme döngüsü olarak bilinen PUKÖ Döngüsü, Deming Döngüsü veya Shewhart döngüsü olarak da adlandırılmaktadır.

PUKÖ Döngüsü bir değişimi yada çalışmayı gerçekleştirmek için kullanılan ve dört adımdan oluşan basit bir araçtır. Özellikle döngü denmesinin sebebi tek seferlik değil, tekrar tekrar kullanılarak sürekli iyileştirmenin gerçekleştirilmesidir.



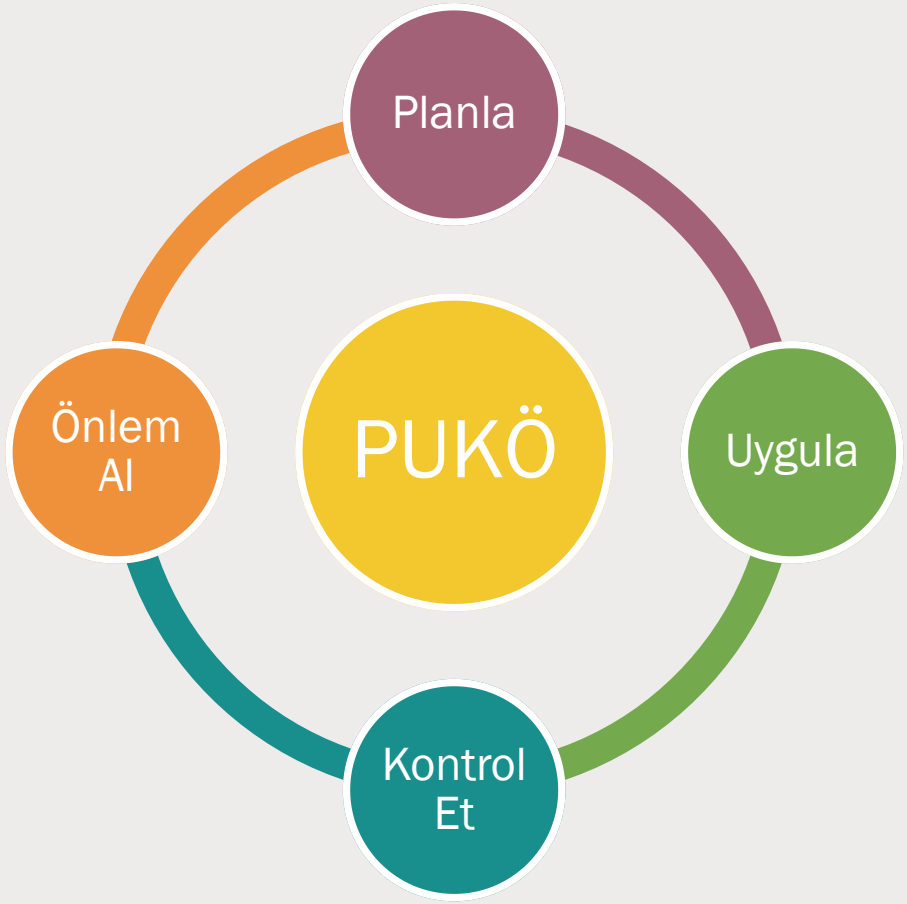
PUKÖ Döngüsü

Plan: İşi, projeyi veya süreci nasıl yapacağını planla

Uygulama: Planladığın gibi uygula

Kontrol Et: İstediğin sonuçlara ulaşabildin mi? Ne tür sorunlar ve hatalar çıktı kontrol et. Ölç ve analiz yap.

Önlem Al: Bir sonraki planlamanı kontrol aşamasında yaptığın öğrenmeyle iyileştir ve geliştir. Bu şekilde tekrar PUKÖ' nün planlama aşamasına geç ve tekrar tekrar PUKÖ' yü çevir.



Bilgi Güvenliği Yönetim Sistemi (BGYS)

Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçası. BGYS, “Planla – Uygula – Kontrol Et – Önlem Al (PUKÖ)” modelini benimser.

Planla: BGYS’ nin kurulması Sonuçları kuruluşun genel politikaları ve amaçlarına göre dağıtmak için, risklerin yönetimi ve bilgi güvenliğinin geliştirilmesiyle ilgili BGYS politikası, amaçlar, hedefler, prosesler ve prosedürlerin kurulması.

Uygula: BGYS’ nin gerçekleştirilmesi ve işletilmesi BGYS politikası, kontroller, prosesler ve prosedürlerin gerçekleştirilip işletilmesi.

Kontrol Et: BGYS’ nin izlenmesi ve gözden geçirilmesi BGYS politikası, amaçlar ve kullanım deneyimlerine göre proses performansının değerlendirilmesi ve uygulanabilen yerlerde ölçülmesi ve sonuçların gözden geçirilmek üzere yönetime rapor edilmesi.

Önlem Al: BGYS’ nin sürekliliğinin sağlanması ve iyileştirilmesi BGYS’ nin sürekli iyileştirilmesini sağlamak için, yönetimin gözden geçirme sonuçlarına dayalı olarak, düzeltici ve önleyici faaliyetlerin gerçekleştirilmesi.

Bilgi Güvenliği Politikası Ne İşe Yarar?

- ✓ Rekabet avantajını, itibarı, güveni korur
- ✓ Hukuki cezaları önler.
- ✓ Bilgi varlıklarını korur.
- ✓ Tasarımları korur.
- ✓ Tescilleri korur.
- ✓ Yazılımları korur.
- ✓ Elektronik dosyaları korur.
- ✓ Ticari sırları korur.
- ✓ Finansal ve kişisel bilgileri korur

Bilgi Güvenliğinin Hedefleri

- Tehditlerin farkında olma
- İşlerin devamlılığını sağlama
- Kayıpları en aza indirme
- Kuruluşların varlıklarının her koşulda gizliliği, erişebilirliği ve bütünlüğünü koruma

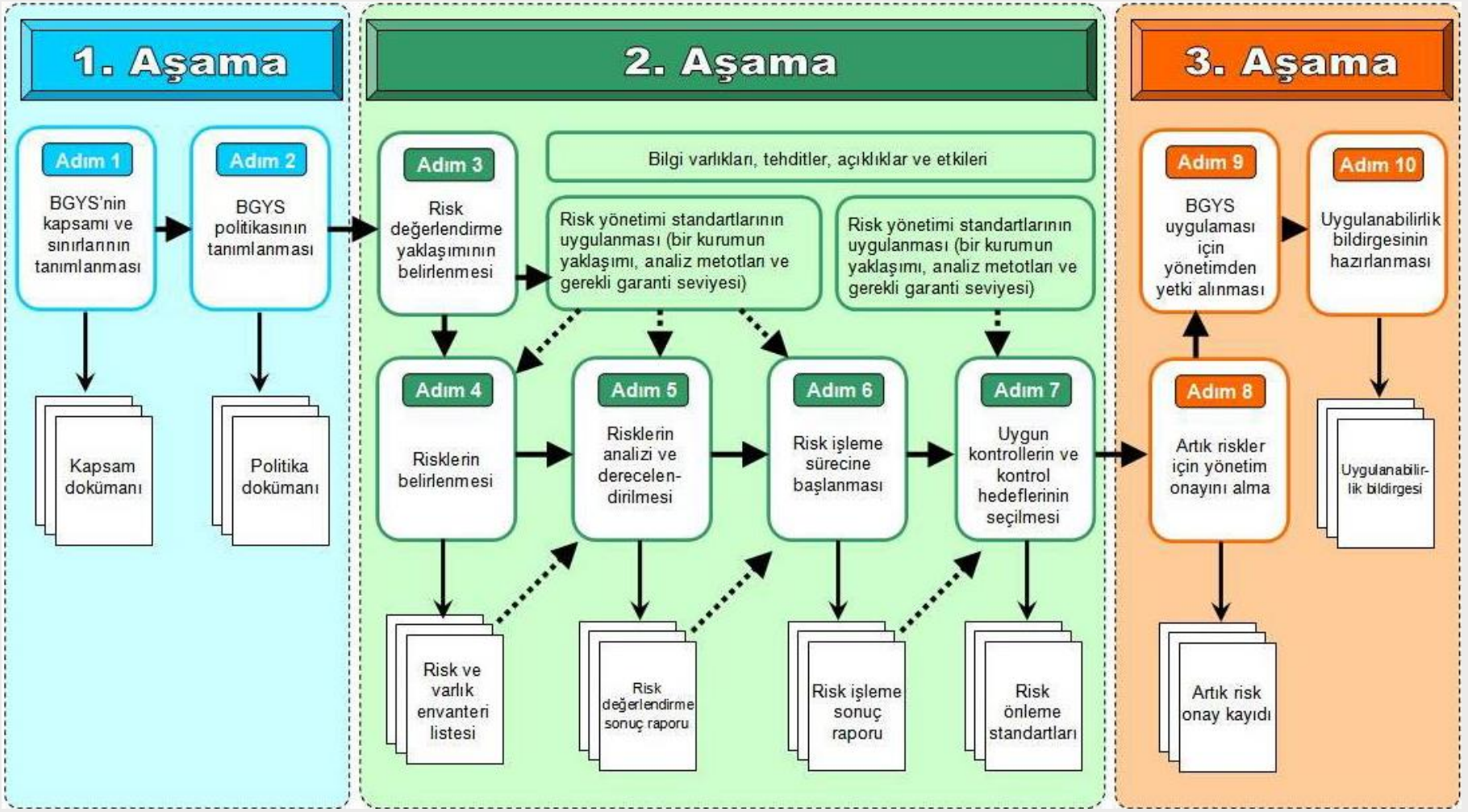
Bilgi Güvenliği İhlalleri Nelere Mal Olur?

- ✓ Para : Oluşabilecek tüm maddi kayıplar.
- ✓ İş Kaybı : Bilginin oluşturulmasında harcanan iş ve emek gücü kaybı.
- ✓ İmaj : Sektörde oluşan firma isminin, etiketin zarar görmesi.
- ✓ Güven : Müşteriler ile, tedarikçi firmalar ile, bayiiler ile ve birlikte çalışılan veya çalışılabilecek kurumlar ile güven kaybı oluşması.
- ✓ Zaman : Bilginin oluşturulmasında harcanan zamanın kaybolması.
- ✓ Hukuksal Problemler : Para Cezaları, Hapis Cezaları..

BGYS Neden Gereklidir?

- ✓ Bilgi kaynaklarına erişimin denetlenmesi
- ✓ Personelin, yüklenicilerin ve alt yüklenicilerin güvenlik konusunda farkındalık düzeyinin yükseltilmesi ve önemli güvenlik konularında bilgilendirilmesi.
- ✓ Bilgi varlıklarının bütünlüğünün ve doğruluğunun sağlanması.

BGYS Kurulumu



ISO 27001 Ana Başlıkları

- ✓ Güvenlik Politikası Bilgi Güvenliği Organizasyonu
- ✓ Varlık Yönetimi
- ✓ İnsan Kaynakları Güvenliği
- ✓ Fiziksel ve Çevresel Güvenlik
- ✓ Haberleşme ve İşletim Yönetimi
- ✓ Erişim Kontrolü
- ✓ Bilgi Sistemleri Edinim, Geliştirme ve Bakımı
- ✓ Bilgi Güvenliği İhlal Olayı Yönetimi
- ✓ İş Sürekliliği Yönetimi
- ✓ Uyum

Son Kullanıcı Farkındalığı

- ✓ Şifre Güvenliği
- ✓ E-Posta Güvenliği
- ✓ Sosyal Mühendislik

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.

Şifre Güvenliği

En önemli kişisel bilgi şifrenizdir. Hiç kimseyle herhangi bir şekilde paylaşılmamalıdır. Mümkünse bir yere yazılmamalıdır. Yazılması gerekiyorsa güvenli bir yerde muhafaza edilmelidir. Güvenli olmadığını düşündüğünüz mekanlarda kurumsal şifrelerinizi kullanmanızı gerektirecek uygulamaları kullanmayınız

Güçlü Şifre Özellikleri

- ✓ En az sekiz karakterli olmalıdır.
- ✓ Hem dijit hem de noktalama karakterleri ve ayrıca harflere sahip olmalıdır (0-9, @, !, &, =, } ?, \)
- ✓ Büyük ve küçük harf karakteri kullanılmalıdır.
- ✓ Kişisel bilgilerle ilişkili olmamalıdır (çocuğunuzun ismi, evlenme yıldönümü vs)
- ✓ Örnek: Güçlü bir şifre: AG685kt?!

E-Posta Güvenliği

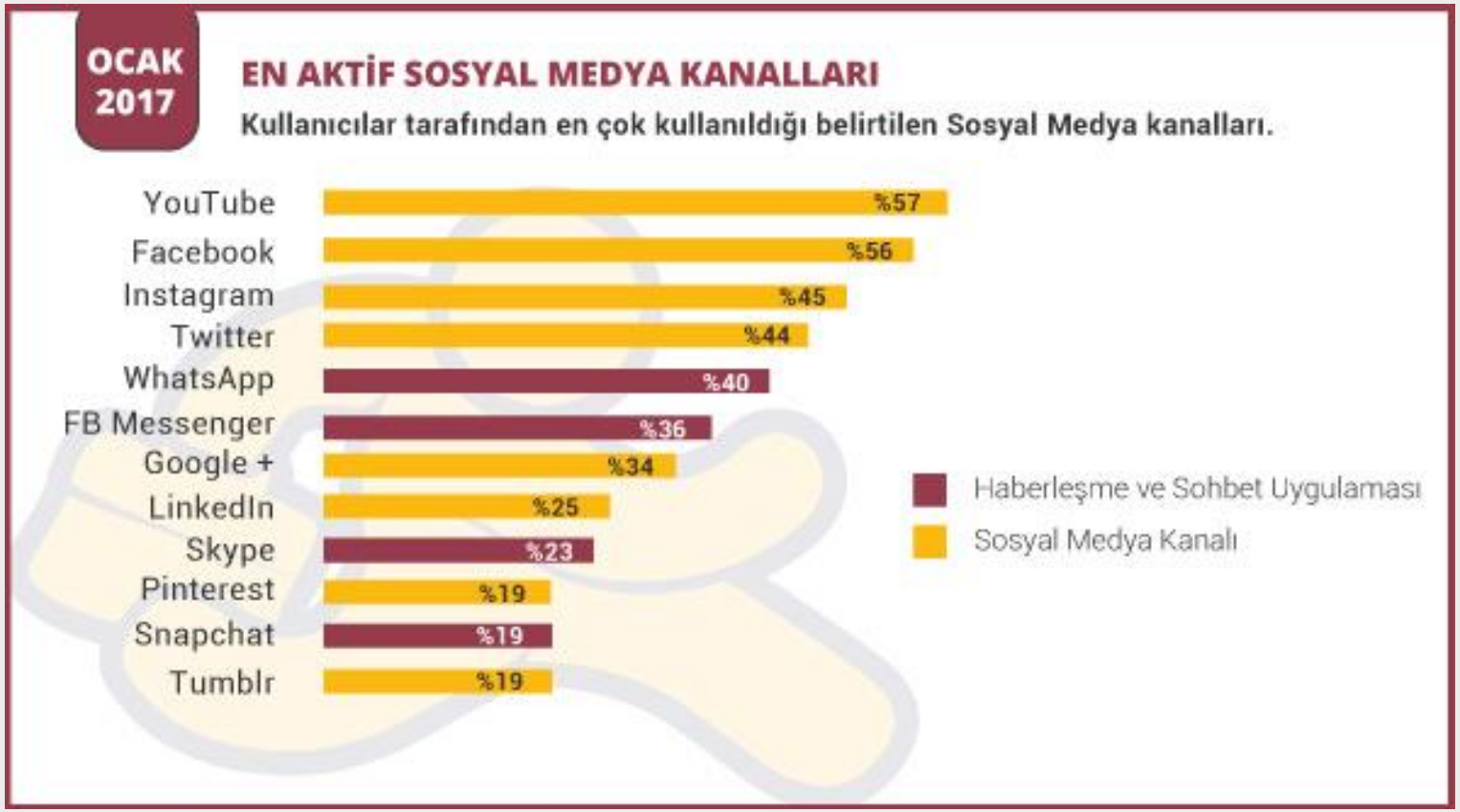
Ne Yapma(ma)lıyım?

- ✓ Kişisel kullanım için internetteki forumlara üye olunması durumunda kurum e-posta adresleri kullanılmamalıdır.
- ✓ Kullanıcıların kullanıcı kodu / şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.
- ✓ Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere azami biçimde özen gösterilmelidir.
- ✓ Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında hemen silinmeli ve kesinlikle başkalarına iletilmemelidir.
- ✓ Spam, zincir e-posta, sahte e- posta vb. zararlı e-postalara yanıt yazılmamalıdır.

Sosyal Mühendislik

- ✓ Yalan Söyleme tekniğinin siber alemdeki tanımıdır. Bilgi Güvenliğinin en zayıf halkası olan insan üzerinden açıklık elde etme çalışmasıdır.
- ✓ Sistem ve bilgiler üzerinde izinsiz erişim sağlayabilmek için insanların aldatılma yada hilekarlıkla kullanılmasıdır.
- ✓ Yardımcı olmaya istekli olma, başkalarına güvenme ve zor durumda kalmak istemem gibi zaaflarımızdan yararlanırlar.
- ✓ Amaç; dolandırıcılık, sistemlere erişmek, endüstriyel casusluk, kimlik hırsızlığı, sistemleri bozmak için gereken bilgiyi elde etmek.

Sosyal Mühendislik Kanalları



Alınacak Önlemler

- ✓ Taşıdığınız, işlediğiniz verilerin öneminin bilincinde olunmalıdır.
- ✓ Kötü niyetli kişilerin eline geçmesi halinde oluşacak zararları düşünerek hareket edin.
- ✓ Arkadaşlarınızla paylaştığınız bilgileri seçerken dikkat edin. Özellikle telefonda, e-posta veya sohbet yoluyla yapılan haberleşmelerde şifre gibi özel bilgilerinizi kimseye söylemeyin.
- ✓ Şifre kişiye özel bilgidir, sistem yöneticinize bile telefonda veya e-posta ile şifrenizi söylemeyin. Sistem yöneticisi gerekli işlemi şifrenize ihtiyaç duymadan da yapacaktır.

Sosyal Medya Güvenliği

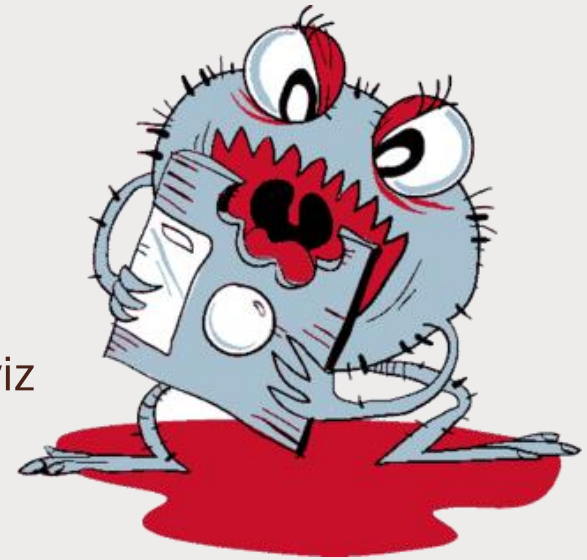
- ✓ Hangi sosyal paylaşım sitesinde olursa olsun, resmi olmayan hiçbir sayfa ve profillere itibar edilmemesi gerekir.
- ✓ Kişisel bilgilerin herkese açık görünür şekilde yer almasına izin verilmemesi gerekir.
- ✓ Yapılan paylaşımların ne olduğuna, suç unsuru taşıyıp taşımamasına mutlaka dikkat edilmesi 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.

Mobil Cihaz Güvenliği

- ✓ 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 virüs koruma programı bulundurunuz,
- ✓ Cihazınızdaki yazılımları sık sık güncelleyiniz,
- ✓ Cihazınızı zaman zaman fabrika ayarlarına döndürünüz ve/veya formatlayıp yeniden kurunuz,

Zararlı Yazılımlardan Korunma

- ✓ 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.



Dosya Erişim ve Paylaşım Güvenliği

- ✓ 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

Araştırma Konuları

- ✓ Bilgi hırsızlığı için kullanılan yöntemler nelerdir? Araştırınız.
- ✓ Bilgisayarlara yapılan internet saldırıları nelerdir? Araştırınız.
- ✓ Türkiye' de yaşanan bilgisayar korsanlığı ile ilgili en büyük olaylar nelerdir? Araştırınız.
- ✓ Hacker kime denir? Kaç çeşit hacker vardır? Araştırınız.
- ✓ Kişisel Bilgisayarımızın güvenliği için almamız gereken önlemler nelerdir?
- ✓ Kişisel bilgilerimizin güvenliği için almamız gereken önlemler nelerdir?
- ✓ Dünyada ve ülkemizde tanınan ünlü hacker kişi ve grupları kimlerdir?