

BİLİŞİM SUÇU İLE KARŞILAŞTIĞINIZDA YAPABİLECEKLERİNİZ | WEBMASTER'LARIN DİKKATİNE | Bilişim Suçları Hakkında Bilmeniz Gerekenler.

1. Yasadışı siteler (web sayfaları) ile ilgili şikâyetlerinizi 155@iem.gov.tr adlı e-mail ihbar adresine bildirebilirsiniz.
2. Şahsınız ile ilgili şikâyetçi olduğunuz konular ile ilgili elde edebildiğiniz tüm deliller ile birlikte en yakın Cumhuriyet Başsavcılığına müracaat ederek şikâyetçi olabilirsiniz.
3. İl Emniyet Müdürlüğümüz tarafından yürütülmekte olan tüm tahkikatlarda Savcılık talimatı veya Mahkeme kararı esas alınmaktadır.
4. Şikâyetçi olduğunuz konular ile ilgili olarak yapılacak çalışma neticesinde ISP(İnternet Servis Sağlayıcının) yurt dışında bulunması durumunda Adli Makamlar tarafından yapılacak olan Adli İstinabe ile konunun takibi yapılabilmektedir.

BİLİŞİM SUÇLARI İLE İLGİLİ OLARAK MAĞDUR OLMADAN ÖNCE YAPILABİLECEKLERİNİZ

1. Şirketinize veya şahsınıza ait önemli bilgilerinizin yer aldığı bilgisayarınız ile özel güvenlik önlemleri almadan internete bağlanmayınız.
2. İnternet ortamında %100 güvenliğin hiçbir zaman sağlanamayacağını unutmayın!
3. Özellikle Chat ortamında bilgisayarınıza saldırılabileceğini;
4. Chat de tanıştığınız kişilere şahsınız, aileniz, adres, telefon, işiniz v.s. konularda şahsi bilgilerinizi vermemeniz gerektiğini unutmayın!
5. İnternet ortamında tanıştığınız kişilere kredi kartı bilgilerinizi vermeyin.
6. İnternet üzerinden yapılan yazışmalarınızda karşınızdaki kurumlarla özel bir yöntemle yazışmanızda fayda olacaktır. Bu şekilde sizin adınıza birlikte ticaret yaptığınız şirketlere asılsız bilgiler veya sizi kötüleyici bilgiler gönderilse bile karşı taraf bunun sizden gelmediğine emin olacaktır.

TÜRKİYEDE BİLİŞİM SUÇLARI Teknoloji her geçen gün ilerlemekte, her geçen gün farklı suç türleri ortaya çıkmaktadır. Bu kapsamda değişime ve gelişime en açık olan suçtu ise bilişim suçları oluşturmaktadır. Bu nedenle bu suç türünün de ayrı bir başlık altında incelenmesi gerekmektedir. Globalleşen dünyada yeni bir teknolojik gelişme bütün dünyaya yayılmaktadır. Bunun sonucunda da ülkemizde de gelişen teknolojiye bağlı olarak yeni bilişim suçları ortaya çıkmaktadır. Bilişim suçlarını oluşturan maddi vakıalara örnek olarak şunları verebiliriz. • Başkalarının adına e-mail göndererek özellikle ticari ve özel ilişkileri zedeleme. • Başkalarının adına web sayfası hazırlamak ve bu web sayfasının tanıtımı amacıyla başkalarına e-mail ve mesaj göndermek ve bu mesajlarda da mağdur olan şahsın telefon numaralarını vermek. • Kişisel bilgisayarlar ya da kurumsal bilgisayarlara yetkisiz erişim ile bilgilerin çalınması ve karşılığında tehdit ederek maddi menfaat sağlanması • Şirketlere ait web sayfalarının alan adının izinsiz alınması ve bu alan adlarının karşılığında yüklü miktarlarda para talep etmek. • Özellikle Pornografik içerikli CD kopyalamak ve satmak • Sahte evrak basmak Suçların türünü yukarıda sayılmış olan maddi vakalar oluşturmaktadır. Suçu işleyebilmek için türlü yollar kullanılabilmekte,bunun ötesinde bu tür suçların işlenmesindeki asıl amaç eylemin sonucundaki menfaat olmaktadır.11.06.1999 tarihinde Birleşmiş Milletler ve Avrupa Birliği tarafından hazırlanan "Bilişim Suçları" raporuna göre ; suç çeşitleri altıya ayrılmaktadır.Bunlardan birincisi "Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim ve Dinleme" olarak tanımlanır.İkinci olarak tanımlanan

bilişim suçtu "Bilgisayar Sabotajı" dır.Bir diğer suç kavramı "Bilgisayar Yoluyla Dolandırıcılık" tır.Başka bir siber suçtu ise "Bilgisayar Yoluyla Sahtecilik" kavramıdır.Beşinci suç türü ise "Kanunla Korunmuş Bir Yazılımın İzinsiz Kullanımı" şeklindedir.Son olarak tanımlanan bilişim suçtu ise "Diğer Suçlar" başlığı altında Yasadışı Yayınlar,Pornografik Yayınlar (Büyük ve Çocuk Pornografisi),Hakaret ve Sövme olarak değerlendirilmektedir. [Computer Sabotage , Unauthorized Access,Computer Fraud ,Child-terbiyesiz bir şey yazdım Porn] Buna benzer yine İnternet ortamında işlenen suçlarla mücadele etmek maksadıyla, 23 Kasım 2001 tarihinde Budapeşte"de imzaya açılan,Avrupa Ülkeleri ile Kanada,Japonya,Güney Afrika ve ABD dahil 33 devlet tarafından imzalandığı halde henüz Avrupa Birliği ile flört eden Türkiye"nin imzalamamış olduğu; Avrupa Konseyi Siber Suç Sözleşmesine göre;bilgisayar veri ve sistemlerinin gizliliğine,bütünlüğüne ve kullanımına açık bulunmasına yönelik suçlar kapsamında hukuka aykırı erişim,yasa dışı müdahale,verilere müdahale,sistemlere müdahale,cihazın kötüye kullanımı

fiilleri;bilgisayarla ilişkili suçlar çerçevesinde ise sahtecilik,dolandırıcılık,telif haklarının ve benzeri hakların ihlaline ilişkin fiiller ve içerikle ilişkili olarak çocuk pornografisine yönelik fiiller,cezalandırma konuları arasında sayılmış;bu hususlarda ulusal ve uluslar arası alanda gerekli etkin yaptırım ve işbirliğine ilişkin düzenlemeler belirtilmiştir.Avrupa devletlerinin bir çoğu (Almanya, İtalya, Finlandiya, Avusturya, Yunanistan, İsveç, Danimarka, Norveç ve Hollanda gibi) mevcut yasal hükümlere eklemeler yapmış; ABD, İngiltere ve İrlanda gibi Anglosakson sistemine dahil bazı devletler ise bu konularda özel düzenlemelere gitmişlerdir. Türkiye'de son yıllarda bilgisayar kullanımının artması ve her sokak başında internet cafelerin kurulması sonucu sanal alemdeki suç oranları hızla artmaya başlamıştır. Hırsızlık, dolandırıcılık, soygun, terörizm, sabotaj ve kaçakçılık gibi pek çok suç dijital ortama taşınmıştır. Türkiye'de işlenen bilişim suçları her geçen yıla göre yüzde 100 e yakın bir artış göstermektedir. Bilgisayar kullanımının bu kadar artması nitelikli suçların hızla artmasına sebep olmuştur. Türkiye'de Emniyet Genel Müdürlüğü (EGM) Bilgi İşlem Daire Başkanlığı Bilişim Suçları Araştırma Büro Amirliği bilişim suçlarının araştırılıp incelenmesinde ve bilişim suçlarına verilen önemde etkin olmuştur. İstanbul, Ankara, İzmir, Adana, Konya, Bursa, Malatya, Diyarbakır bilişim suçlarının en çok işlendiği iller olarak karşımıza çıkmaktadır. Emniyet Genel Müdürlüğü, il emniyet müdürlüklerindeki verileri alarak, Türkiye'deki bilgisayar suçlarının haritasını çıkarmıştır. Takibi şikâyete bağlı suçlar, Interpol aracılığıyla intikal eden suçlar ve polisin bizzat ilgilendiği suçlardan oluşmaktadır.1998 yılında Türkiye'de işlenen bilişim suç sayısı 5 iken, 1999'da bu sayı 15'e yükselmiş. 2000 yılında 80'i bulan suç dosyasının sayısı, 2001 yılına gelindiğinde 136'yı bulmuş. Her geçen yılda artış göstererek ilerlemiştir. Elde edilen sonuçlar, Türkiye'deki bilgisayar suçlarının, lisans haklarının ihlali, dolandırıcılık, sahtecilik, yasadışı yayınlar ve bilgisayar sabotajı şeklinde geliştiğini göstermektedir. Sanal âlemdaki dolandırıcılık suçlarının büyük bir kısmı kredi kartları üzerinden yapılmaktadır. Değişik yöntemlerle ele geçirilen kredi kartı numaralarıyla bilgisayar üzerinden alışveriş yapılması en yaygın yöntem olmaktadır. Otomatik para çekme makineleri olarak bilinen ATM dolandırıcılığı ise kredi kartlarından sonra ikinci sırada yer almaktadır. Kredi kartlarının ATM cihazında sıkıştırılması, değişik hilelerle şifrelerin öğrenilmesi veya kartların hırsızlık yoluyla elde edilmesi suretiyle dolandırıcılık yapılmaktadır. Evrak, para, Milli Piyango bileti, kimlik kartları, sigorta poliçeleri, pasaportlar ve yazarkasa fişlerinin sahteleri sahtecilik suçları da bu kapsamda yapılmaktadır. Lisans hakları ihlali içinde en yüksek oranı yüzde 82 ile filmlerin çoğaltılması oluşturmaktadır. Bilgisayar oyunları ve müzik CD'lerinin çoğaltılması da sanal âlemin diğer lisans hakkı ihlalleridir. Interpol verileri, yasadışı yayın suçları arasında ilk sıranın yüzde 40'la çocuk pornografisine ait olduğunu göstermektedir. Genel anlamdaki pornografik yayınların oranı da yüzde 25. Bunlar, daha çok internet kafe gibi ortamlarda pornografik içeriklerin gösterimi ve CD'lerinin satışından oluşmaktadır. Terör içerikli web sayfaları hazırlanması suretiyle işlenen suçların oranı ise yüzde 30. Şikâyete bağlı suçlardan kişilik haklarına saldırı ve hakaret ise yüzde 5 oranında işlenmektedir. Türkiye'de Emniyet Teşkilatı'nda bilişim ile ilgili temel, 1982 yılında Bilgi İşlem Daire Başkanlığının kurulmasıyla atıldı. 1997 yılında ise Bilişim Suçları Bürosu kuruldu. 2001 yılında bu büronun adı İnternet ve Bilişim Suçları Şube Müdürlüğü olarak değiştirildi. Bu birimin dışında da diğer daire başkanlıkları altında Bilgi İşlem Şube müdürlükleri kuruldu. Bu daireler kendi görev alanlarına giren konularda bilişim suçları ile mücadele etmektedir. Ayrıca merkez teşkilatı içinde bir Bilgisayar Suçları ve Bilgi Güvenliği Kurulu ve Üst Kurul oluşturulmuştur. 2001 yılında Kaçakçılık ve Organize Suçlar Daire Başkanlığı ile Birleşmiş Milletler tarafından ortaklaşa kurulan TADOC (Turkish Academy Against Drug

and Organised Crime) bünyesinde de Bilişim Suçları Araştırma Merkezi oluşturulmuştur. Bu merkez faaliyetlerini daha çok bu suçlar ile mücadelede, ilgili birimlere yön göstermek amacıyla akademik destek niteliğinde çalışmalar yapmaktadır. Bu merkezi yapılanmanın yanında büyük illerde de bilgi işlem büroları kurulmuş ve bu alanda karşılaşılan sorunlar ile ciddi anlamda mücadele etmeye başlanmıştır. Türkiye'de genel olarak, ülkemizde bilişim suçları denince akla iki olay gelmektedir: Kredi kartları ve pornografik CD'ler başta olmak üzere telif haklarının konusunu teşkil eden korsan CD'ler. Bilişim suçlarına ilişkin olarak yapılan üçlü sınıflandırma göz önüne alınırsa bilgisayar aracılığıyla işlenen suçların ülkemizde daha yaygın olduğu görülmektedir. Ancak bilgisayar sistemleri aracılığıyla işlenen suçların birçoğu takibe bağlı suçlardan olduğu için mağdurların şikâyeti olmadan resen ele alınmamaktadır. Örneğin elektronik posta yoluyla yapılan bir tehditte, tehdit edilen kişi veya kurum bunu polise bildirmese polisin bu olaydan haberdar olması ve işlem yapması mümkün olmamaktadır. Riptech'in yayınladığı rapora göre, siber saldırılar en fazla ABD'de olurken, Türkiye 6. sırada yer almaktadır. Türkiye'de işlenen bilişim suçlarına ait

oransal veriler ise şu şekildedir. Lisans hakları ihlallerinin yüzdesi % 4 müzik % 14 oyun % 82 film

BİLİŞİM SUÇLARI NELERDİR Bilişim suçlarının çok çeşitli tanımları vardır. Bunlardan, Avrupa Birliği Uzmanlar Komisyonu'nun Mayıs 1983'deki Paris Toplantısı'nda „bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranış“ olarak tanımlanmıştır. Özünde bilişim suçları terimi, teknolojileri kullanarak işlenen bir suç unsurudur. Bilişim Suçlarının Türlerini belirlemekte sorun olarak karşımıza çıkmaktadır. Bilişimle ilgili suç türlerini çok değişik şekillerde ortaya koymak mümkündür. Ancak, konuyu makul bir seviyede ele alarak, en çok görülen ve en ağır nitelikli olan suç türlerinin ele alınmasında yarar vardır. Suçun işlenmesindeki esas konuyu suçlar arasındaki farklar oluşturur. Bir hedefe ulaşabilmek için türlü yollar kullanılabilir, bunun ötesinde asıl amaç hedeftir. Yani suçun türleri arasındaki farkı oluşturan esas etken suçun işlenmesindeki amaçtır. Bu haliyle Suçların türleri TCK da suç teşkil edecek tüm suçları kapsayabilmekte veya bu suçlara zemin hazırlamaktadır. Suç çeşitleri ayrımında, 11.06.1999 tarihinde Birleşmiş Milletler ve Avrupa Birliği tarafından hazırlanan "Bilişim Suçları" raporuna göre; suç çeşitleri altıya ayrılmaktadır. Bunlardan birincisi "Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim ve Dinleme" olarak tanımlanır. İkinci olarak tanımlanan bilişim suçu "Bilgisayar Sabotajı" dır. Bir diğer suç kavramı "Bilgisayar Yoluyla Dolandırıcılık" olarak kabul görür. Başka bir siber suç ise "Bilgisayar Yoluyla Sahtecilik" kavramıdır. Beşinci suç türü ise "Kanunla Korunmuş Bir Yazılımın İzinsiz Kullanımı" şeklindedir. Son olarak tanımlanan bilişim suçu ise "Diğer Suçlar" başlığı altında Yasadışı Yayınlar, Pornografik Yayınlar (Büyük ve Çocuk Pornografisi), Hakaret ve Sövme olarak değerlendirilir. Bu suç türlerini teker teker açıklayacak olursak; **1) Bilgisayar Sistemlerine ve Servislerine Yetkisi Erişim ve Dinleme** "Erişim" sistemin bir kısmına, bütününe, bilgisayar ağı veya içerdiği verilere, programlara; yine programlar, casus yazılımlar veya virüsler vb. ile ulaşma anlamındadır. Günümüzde özel hayatın gizliliğinin korunması için kanunlarda gerekli müeyyideler konulması ile birlikte dinlemeler ,erişimler ,izinsiz özel ve şirket bilgisayarlarına ve sistemlerine girmek suç olarak kabul edilmiştir.. Günümüzde telefon dinlemeleri veya kişilerin özel mülklerine girmek nasıl savcı izni olmadan mümkün olmamakta ise yine kişiler veya kurumlar arası haberleşmenin bilgisayar üzerinden dinlenmesi veya izinsiz bilgilerin alınması da kişi özel mülkü ya da kişilerin şahsiyetlerine taciz olarak kabul edilmektedir ve suç oluşturmaktadır.

Ülkemizde bu konuda TCK'nin (Türk Ceza Kanunu) 243. maddenin 1. ve 2. fıkrasında açıkça belirtilmiştir. Bu bölümde incelenmesi gereken konulardan biri de casus yazılımlardır. Bu yazılımlar hukuki olarak suç sayılmamaktadır, fakat bu konuda tartışmaya açık bir kavram olduğu da bir gerçektir. **-Casus Yazılımlar Ve Etkileri** Casus yazılımlar bir bilgisayara kurulduktan sonra bilgisayarınıza girdikten sonra bilgisayarınızda farklı etkiler bırakarak, ya da bilgisayarınız içerisinde deyim yerindeyse casusluk yaparak rahatsız eden yazılımlar olarak ifade edilir. Casus yazılımların belli başlı amaçları; eriştiği ya da kurulduğu bilgisayarlardaki verileri, gezilen siteleri, bilgisayar içeriğindeki bilgilerin işe yarayan kısımlarını belli bir hedefe (doğrudan merkeze) göndermesine ya da bilgisayardan istenmeyen reklamların çıkmasına, internette reklam indirmesine yol açmaktadır. Tartışmaya açık olarak bu tür yazılımlar Kanunen suç sayılmamaktadır. Bu yazılımları, yine bu yazılımların lisans anlaşmasıyla kullanılmasını kabul ederek yüklediğinizden, bu tür yazılımları kanuni olarak gösterilmektedir. **2) Bilgisayar Sabotajı** Bu suç türü iki şekilde karşımıza çıkmaktadır. 1. Bilgisayar teknolojisi kullanarak sistemine sızılan bilgisayardaki bilgilerin silinmesi, yok edilmesi ve değiştirilmesi. 2. Hedef alınan sisteme uzaktan erişerek değil de bilakis fiziksel zarar vererek ya da sistem başında bulunarak bilgisayardaki bilgileri silmek, yok etmek veya değiştirerek zarar verilmesi. Burda önemli olan mala verilen zarardan ziyade içindeki bilgilere verilen zarar önem arz eder. Yetkisiz erişimin aktif sahası olarak da nitelendirilen "Bilgisayar Sabotajı", yalnız sisteme erişimle kalmamakla birlikte, eriştiği sistem (bilgisayar),ın içerdiği bilgileri silme veya değiştirme olarak ifade edilir. Bir bilgisayara veyahut sisteme yetkisiz erişim sağlayanlar; sadece eriştiği bilgileri incelemekle, kopyalamakla kalmıyor, bu bilgileri değiştirebiliyor, silebiliyor ya da bu bilgileri kanun dışı kullanmak isteyenlere satabiliyor. Türkiye'de "Bilgisayar Sabotajı" TCK(Türk Ceza Kanunu)'nun 243/ 3 ile 244/1 ve 2 maddelerine göre suçtur. Virüsler, Wormlar ve Zombiler kötü amaçlı olarak yazılmış kodlardır. Bu tür kötü amaçlı yazılmış kodlar, başkalarına zarar vermediği sürece suç sayılmamaktadır. Fakat bu tür kodlar; kişi ya da kurumlara intikal eder ve zarar verirse suç teşkil etmeye başlar. Yoksa sırf kod yazımı saikten öte bir anlam ifade etmemelidir. Türkiye'de kötü amaçlı kodları yazma bunu yaymaya ilişkin açık bir hüküm bulunmamaktadır. Bu nedenle Kötü amaçlı kodlarla bilgisayarlara zarar verme, doktrinde genellikle "sistem

ve unsurlarına yönelik nas-i izar suçu" olarak adlandırılmaktadır, oysa sabotaj konusunda belirttiğimiz TCK maddelerine bu bölümü de dahil etmek daha uygun olacaktır. **3)Bilgisayar Yoluyla Dolandırıcılık** Dolandırıcılık genel bağlamda "Hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlamaya" denmektedir. Bilişim kavramı olarak "Dolandırıcılık" bilgisayar veya iletişim araçlarıyla kişileri şaşırtma, aldatma, kandırma olarak tarif edilebilir. **Bilgisayar Yoluyla Dolandırıcılık suçu;** Kredi kartlarının bir benzerinin yardımcı programlarla oluşturulması yoluyla Yetkisiz ve izinsiz erişilen bilgilerin kopyasını olmak şeklinde Finans bilgilerinin tutulduğu programlarla yapılan değişiklik ile istenilen kişinin hesabına istenildiği kadar para aktarmak suretiyle Kişiler arasında mali alışverişi olan kişilerin adına mail vs. Şeklinde iletişim kurarak;

kişileri kandırarak, işlenmektedir. Ülkemizde bu tür suçlar TCK(Türk Ceza Kanunu)"da 158.maddenin (1). Fıkrasının (f) bendinde,244.maddenin (3).fıkrasında ve 245.maddesinin (1). Fıkrasında hüküm altına alınmıştır. **4)Bilgisayar Yoluyla Sahtecilik** Klasik olarak tabir edildiğinde, Bir şeyin aslına benzetilerek yapılan düzmece olarak tarif edilebilmektedir. Bazen ileri teknoloji ürünü cihazlar kullanılarak, bazen de çok basit web programcılığı (Fakemail, Phishing) yöntemiyle sahtecilik yapılmaktadır. Günümüzde başkalarının adına e-mail göndererek, ticari ve özel ilişkileri zedelenmesini sağlamak, başkalarının adına web sitesi hazırlamak ve bu web sitesinin tanıtım amacıyla başkalarına e-mail ve mesaj göndererek (iletişim kurarak) ve bu mesajlarda da mağdur olan şahsın telefonlarını vererek, sahte para, sahte evrak, sahte bilet vb. basma yönetimiyle bu suç işlenmektedir. Ülkemizde bu tür suçlara yönelik kanunlarda henüz net bir tanımlama yapılmamıştır.Fakat yeni TCK(Türk Ceza Kanunu)"nın 158. maddesinin f bendi uygulanabilirliği söz konusudur. **5) Kanunla Korunmuş Bir Yazılımın İzinsiz Kullanımı** "Kanunla Korunmuş Bir Yazılımın İzinsiz Kullanımı" yazılımların; yasadışı yöntemlerle kopyalanmasını, çoğaltılmasını, satılmasını, dağıtılm asının ve kullanılmasını ifade eder. Ülkemizde 5846 no"lu Fikir ve Sanat Eseleri Kanunu (FSEK) lisanslı yazılımları satın alan kişiye bir adet kopyalama hakkı vermekte, daha fazla kopyanın yapılmasını, satılmasını, yazılımın kiralanmasını yasaklamaktadır. **6)Yasadışı Yayınlar** Yasadışı olarak kabul edilen unsurların bilgisayar sistemleri, ağları, internet aracılığıyla yayınlanması ve dağıtılması olarak ifade edilir. Kanunun yasaklamış olduğu bu materyaller; web siteleri(sayfaları), elektronik postalar, haber grupları, forumlar, iletişim sağlayan her türlü araç, optik araçlar tarafından kayıt yapan tüm sistemler olarak kabul edilir. Yasadışı yayınları üç gruba ayırmak mümkündür.Bunlardan birincisi,vatanın bölünmez bütünlüğüne aykırı olarak hazırlanmış terör içerikli internet siteleridir(sayfalarıdır).Bu tür siteleri hazırlayanların asıl amacı sansür konulmuş Anayasaya aykırı fikirlerini , interneti kullanarak yaymak ,bu sayede de kendilerine taraf toplayarak vatanın bütünlüğünü bozacak düşüncelerini ifade etmektir.. Yasadışı yayınların bir diğeri ise toplumun genel ahlakına, ar ve haya duygularına aykırı düşen yayınlardır. Bunlar pornografik görüntü veya yazılar şeklinde olmaktadır. Türkiye"de TCK (Türk Ceza Kanunu)"da 77,102,103 ve 104. maddeleriyle büyük ve çocuk pornografisi yasaklanmıştır. İnternet aracılığıyla fiilen işlenen suçlardan üçüncüsü ise; bir kişiye, kuruma vb. karşı yapılan hakaret ve sövme suçudur. Bu suç türü internet üzerinden başkalarının adına uygun olmayan e-mailler göndererek kişi ya da kurumların itibarını zedelemek suretiyle olabilmektedir. Bir başka yol ise yine kişi ya da kurumların sahip oldukları adın, lakabın web üzerinden satın alınarak, kişi aleyhine yayında bulunmak suretiyle medyana gelebilmektedir. Kısaca 6 Ana başlık altında toplanan Bilişim Suçları Türlerinin birçoğu yasalarımızda suç olarak düzenlenmiş ve bu sayede koruma altına alınmıştır. Lakin günümüz teknolojisinin hızlı ilerlemesi, internetin sürekli yaygınlaşması nedeniyle, bu gün suç türleri arasında sayılmayan yeni birçok zarar amaçlı kullanımlar oluşacaktır. Yasalarımız teknolojik gelişmelerle aynı hızda ilerlemez ve yenilenmezse, bu tür fiillere karşı kanunlarımızda boşluk oluşacak, bu fiilleri işleyerek büyük zararlar doğuran şahıslara karşı hiçbir müeyyide uygulanamayacaktır. Bu halde Devlet yetkilileri, Hukukçular ve Emniyet Mensupları sürekli yeni gelişmeleri takip ederek yasal boşlukların giderilmesi konusunda çalışma yapmalıdırlar ki, İnternet yoluyla yapılan iletişim hizmetlerin en üst düzeyde güvenliği sağlanabilmiş olsun. Güvenli iletişim imkânlarımızın devam edebilmesi için İnternet kullanıcıları olarak bizlerde, yukarıda belirtilen suç türleri içine giren, yasaya aykırı olduğunu bildiğimiz eylemleri ve bu eylemlerin

uygulayıcılarını en kısa sürede emniyet birimlerine bildirmemiz gerekmektedir. Bu sayede bu tür suçların yaygınlaşmasına engel olunabilecektir. **Tanımı** Bilişim Suçlarıyla ilgili olarak karşımıza birçok tanım çıkmaktadır; Bilgisayar suçları, dijital suçlar, internet suçları, siber suçlar, ileri teknoloji suçları v.b.Tüm

bunlar ayrı bir tanım olmakla beraber bilişim suçları terimi kullanıldığında bahsedilen bu teknolojileri kullanarak işlenen tüm suçları kapsamaktadır. Bilişim kelime anlamı olarak; insanların teknik, ekonomik ve toplumsal alanlardaki iletişimde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla düzenli ve akılcı bir şekilde işlenmesi olarak kabul edilmektedir. Bilişim Suçları Halk deyişi ile; Bilgisayar Suçları” olarak tanımlanabildiği gibi “İletişim Suçları”, “İnternet Suçları”, “Dijital Suçlar”, “Teknolojik Suçlar”, gibi tanımlamalar da yapılmaktadır. Bilişim Suçlarını Avrupa da ki ilk tanımı ise şu şekilde; AET Uzmanlar Komisyonu”nun [8]Mayıs 1983 yılında Paris Toplantısında yaptığı tanımlamaya göre; “Bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanun, gayri ahlakî ve yetki dışı gerçekleştirilen her türlü davranıştır.” denmektedir. Genel manada bilişim suçları tanımı ise; Her türlü teknoloji kullanılarak, kanuni olmayan yollarla kişisel ya da kurumsal bilgisayarlarda, sistemler üzerinde zarar verici etki bırakmaktır. Bilişim teknolojilerinde suç meydana gelebilmesi için mutlaka teknoloji kullanılmalıdır. Bu teknoloji bilgisayar, kredi kartı, telefon, pos makinesi, elektronik bir cihaz olarak düşünülebilir. Bilişim Suçlarının Hukuki tanımı ve TCK daki yeri; Bilgileri otomatik bir sisteme tabi olan bilgisayar ,bilgisayar programları ile iletişim teknolojilerinin verilerini hukuka aykırı bir biçimde ele geçiren, ele geçirerek değiştiren, yok eden, erişilmez kılan böylece bir başkasının zarara uğratılmasının sağlanması veya kendisine ve başkasına maddi bir çıkar sağlanması Bilişim Suçunu oluşturmaktadır..5237 sayılı Türk ceza kanununda ayrı bir başlık halinde düzenlenen bilişim suçları kanununun 243, 244 ve 245. maddeleri ile tanımlanmaktadır. **BİLİŞİM SUÇLARININ TÜRLERİ NELERDİR?** Suçların türleri TCK da suç teşkil edecek tüm suçları kapsayabilmekte veya bu suçlara zemin hazırlamaktadır. Suçların işleme şekilleri; Hakaret, küfür, kredi kartı yolsuzlukları, sahte belge basımı, bilgilerin çalınması ve buna bağlı olarak devam edebilecek suçları kapsamakla, birlikte bunlarla sınırlı olmayıp, gündün güne değişiklikler göstermektedir. İl Emniyet Müdürlüğümüz Bilgi İşlem Şube Müdürlüğümüz 1999 yılından itibaren değişik birimlerden ve Cumhuriyet Başsavcılıklarından gelen talepler doğrultusunda çalışmalarına başlamıştır. 1999 yılında başlayan çalışmalarımız talebin atması nedeniyle Bilgi İşlem Şube Müdürlüğü içerisinde bulunan Bilgi Sistemi Büro Amirliği bünyesinde çalışmalarını sürdürmüştür. 2002 yılından itibaren Emniyet Genel Müdürlüğü bünyesinde İnternet ve Bilişim Suçları Şube Müdürlüğü kurulması sonucu taşra teşkilatı olarak Şube Müdürlüğümüz içerisinde Bilişim Suçları Büro Amirliği adı altına çalışmalarını sürdürmektedir.

ÜLKEMİZDE EN ÇOK KARŞILAŞILAN BİLİŞİM SUÇLARINDAN ÖRNEKLER

Başkalarının adına e-mail göndererek özellikle ticari ve özel ilişkileri zedeleme.

Başkalarının adına web sayfası hazırlamak ve bu web sayfasının tanıtımı amacıyla başkalarına e-mail ve mesaj göndermek ve bu mesajlarda da mağdur olan şahsın telefon numaralarını vermek.

Kişisel bilgisayarlar ya da kurumsal bilgisayarlara yetkisiz erişim ile bilgilerin çalınması ve karşılığında tehdit ederek maddi menfaat sağlanması

Şirketlere ait web sayfalarının alan adının izinsiz alınması ve bu alan adlarının karşılığında yüklü miktarlarda para talep etmek

Özellikle Pornografik içerikli CD kopyalamak ve satmak

Sahte evrak basımı gibi çok farklı konuları içerebilmektedir.

NOT: Unutmayın bu tür suçların tek mağduru siz değilsiniz. Karşılaşmış olan durumdan utanmadan tüm deliller ile birlikte en yakın Cumhuriyet Başsavcılığına başvurunuz.