"SANA" YAPILAN "SANAL" SALDIRI:

BİLİŞİM SUÇLARININ İŞLENME YÖNTEMLERİ

Bayram YÜKSEKKAYA[1]

[1]Avukat, Adana Barosu.

ÖZET:

Bilişim suçları, hergün daha çok kişinin muhatap olduğu bir suç tipidir. Bu suç tipini diğer suç tiplerinden ayıran birçok özellik bulunmaktadır. Özellikle; her türlü fiilin sanal ortamda gerçekleşmesinden dolayı, kendine özgü ve karekteristik özellikleri bulunduğu açıktır. Bununla birlikte, fiziksel sınırların sanal ortamda bulunmamasından dolayı, uluslarası olarak işlenmesi de en kolay suç tiplerinden biridir.

İşte, bu kendine özgü ve karakteristik özellikleri nedeniyledir ki; bilişim suçlarına karşı farkındalık eşiği, maalesef ülkemizde tahmin edilenden dahi azdır.

Suçun işlendiği ortam fiziki değil, sanal bir ortam olduğundan ve her geçen gün, suçun işleniş tarzı, yöntemi ve boyutu değiştiğinden, sanal ortamın sakinleri, her türlü bilişim suçunun mağduru olabilmektedirler.

Biz bu makalemizde, bilişim suçlarının işlenme şekillerinin sadece bilinenlerinin bir kısmını aktarmaya çalışacağız. Zira hem her geçen gün yeni teknikler üretilmekte, hem de kullanıcıların büyük bir çoğunluğu teknik bilgi yönünden az bilgiye sahip olduklarından, teknikleri anlamakta güçlük çekmektedirler.

YÜKSEKKAYA LAW OFFICE, her türlü bilişim suçuna karşı, farkındalığı arttırmayı bir kamu görevi addederek, farkındalığı arttırmak için yayımlarda ve paylaşımlarda bulunmaktadır. Kullanıcıların; her klavye vuruşunu bilinçli yapmaları gerekliliği, bu makalenin sonunda çok daha iyi anlaşılacağı kanaatindeyiz.

BÖLÜM – 1

TANIM

Bilişim suçları, en basit tanımıyla sanal ortamda gerçekleştirilen suçlardır. Siber suçlar adı ile de anılan bu suç tipinin, diğer tüm suçlardan ayrılan özelliği, sanal âlem üzerinde işlenmesidir.

Bu nedenledir ki, tüm dünyada, kişisel (özel yahut tüzel) veya kamusal verileri korumak için sistemler geliştirilmekte ancak ne yazık ki, bu korumalar pek fayda getirmemektedir. Zira sanal âlemin usta failleri, yapılan koruma sistemlerini aşabilmektedirler.

Günümüz dünyasında, günlük yaşamın hemen hemen her alanı, internet ortamı ile entegre olmuş durumdadır. Alışverişten eğitime, hobiden bankacılığa kadar, akla gelebilecek tüm alanlarda kullanım alanına dönüştürülen internet âlemi, aynı anda suç dünyasının da ilgisini çekmekte geç kalmamıştır.

Suç ve fail ile mücadelede kullanılan klasik yöntemler ile hiçbir şekilde mücadele edilemeyecek olan sanal suç ve sanal faillere karşı, gerek ulusal gerekse uluslararası girişimler gerçekleştirilmiştir. Ulusal anlamda yasal düzenlemelere giden devletler, hem önleyici hem de cezalandırıcı normları hukuk sistemlerinde yer vermişlerdir. Ancak, uluslararası alanda çok rahat işlenebilecek suçların başında gelen bilişim suçları ile mücadele için, uluslararası sözleşmeler yapılmaya başlanmış, ülkeler siber suçlarla mücadele için hem fikir olmuşlardır.

Fakat çok büyük bir rahatlıkla söylenebilir ki, hem siber suç ve suçluluğunun çok teknik bir konu olması, hem bu konuda yeterli ve gerekli eğitimi veren kurumların azlığı hem de siber faillerin her geçen gün kendilerini yenilemeleri karşısında durağan hukuksal düzenlemeleri aşmalarındaki maharetler nedeniyle, hem ulusal hem de uluslararası girişimler siber suçlarla mücadelede hep yetersiz kalmıştır ve kalmaya da devam etmektedir.

Özellikle internet kullanıcılarını hedef alan ve onların kişisel bilgilerine ulaşmak, sahip oldukları bilgi ve belgeleri almak, neticeten de birçok suça vücut vermek amacıyla işlenen bilişim suçları, esasında klasik suçların sanal âlemdeki yansımasını gerçekleştirmektedirler.

Örneğin, bir mağdurun internet bankacılığı bilgilerine ulaşan siber failler, daha sonra o kişinin bankadaki parasını kendi hesaplarına aktarabilmektedir ki; bu klasik anlamdaki hırsızlık suçunun siber âleme yansımış bir halidir.

Aynı şekilde, mağdurun bilgisayarına yerleştirilen bir program sayesinde, bilgisayarında yer alan belgelere ulaşan fail, bu belgelere dayalı bir çok suça vücut verebilir. Örneğin mağdur, bir ticari şirketin muhasebecisi ise, şirketin tüm bilgileri siber fail tarafından ele geçirilebilir. Yine aynı yol ile bilgisayar ortamında hazırlanan ihale teklif belgelerine ulaşılarak, bir ihaleye şirketin vereceği teklifin ne olacağı yine siber fail tarafından ele geçirilebilir.

Bununla birlikte, yine mağdurun bilgisayarına yerleştirilen bir program ile, mağdurun bilgisayarında yer alan özel fotoğrafları siber fail tarafından ele geçirilebilmektedir. Daha sonra siber fail, elde ettiği bu fotoları bir şantaj aracı olarak kullanabileceği gibi, hiçbir şantaj fiili gerçekleştirmeden, internet ortamında yayımlayabilir.

Örnekler arttırılabilecektir. Görüldüğü üzere bilişim suçları, her ne kadar reel (gerçek) dünyada işlenen suçlara bizzat uyarlılık göstermese de, sanal dünyada vücut bularak, reel dünyada, belki de bizzat reel dünyada gerçekleştirilen suçlardan daha vahim bir şekilde etkisini gösterebilmektedir.

Son olarak belirtmeliyiz ki, insanlar devamlı suretle "internet bankacılığı" kullanmadıklarını ve bu nedenle bilişim suçlarının hiçbir şekilde konusu olmayacaklarını belirterek, bilişimi "internet bankacılığı"na indirgemektedirler. Bu yöndeki bir düşünce çok yanlıştır ve bu düşüncedeki insanlar esasında bizzat siber faillerin çok rahat avlayabildikleri potansiyel mağdurlardır. Örneğin, internet bankacılığı kullanmadığı için çok rahat olan birçok kişinin, sosyal medya hesabı siber faillerce ele geçirilerek, sosyal medya hesabında yer alan arkadaşlarından borç istemek ve almak yöntemiyle zarara uğratılmışlardır.

Görüldüğü üzere, sanal dünya internet bankacılığından ibaret değildir ve bu nedenledir ki, bilişim suçları da internet bankacılığına yönelik suçlarla da sınırlı kalmamaktadır.

BÖLÜM – 2

BİLİŞİM SUÇLARININ BAZI İŞLENME TEKNİKLERİ:

Aşağıda, bir kısım bilişim suçlarını işlemek amacıyla geliştirilen tekniklerden bahsedilmiştir. Unutulmamalıdır ki, bu teknikler, suçun oluşumu için uygulanan ve tespit edilen tekniklerin sadece bir kısmıdır. Her geçen gün yeni yeni teknikler geliştiren siber failler, bilişim suçlarını daha rahat işlemek için yeni yeni teknikleri de denemektedirler.

Anlatılan bu yöntemler, bazı teknik bilgilerin de bilinmesini gerektirdiğinden, elden geldiğince basite indirgenerek anlatılmıştır. Okuyucu, daha geniş ve teknik bilgiyi, birçok kaynaktan elde edebilecektir.

► ***Sosyal Mühendislik:***

Esasında sosyal mühendislik, siber fail tarafından ya en başta uygulanan yahut da diğer tüm yöntemler işe yaramaz ise uygulanmak zorunda kalınan bir yöntemdir.

Sosyal mühendisliğin ana teması, mağdur ile iletişime geçerek, mağdurda bir güven oluşturmak ve oluşturulan bu güvene bağlı olarak mağdurun bilgilerini ele geçirmek yahut da bilgisayarına sızmayı başarmaktır.

Klasik sosyal mühendisliği kullanan bir siber fail, mağdur ile öncelikle bir tanışma dönemi geçirmekte, bu dönemde mağdurda bir güven oluşturmaktadır. Oluşturulan bu güvene bağlı olarak siber fail, hedefini gerçekleştirmek için ataklara başlamaktadır.

Örneğin, mağdurun sosyal medya hesabını ele geçirmek isteyen bir siber fail, mağdur ile sosyal medya üzerinde arkadaş olur, sezdirmeden mağdur ile bir samimiyet oluşturarak, bu samimiyete bağlı ve karşı tarafça anlaşılamayacak şekilde sohbet ederken, mağdurdan bir kısım bilgiler alır. Zira siber fail, sohbet sırasında aldığı bu bilgiler ile sosyal medya şifresini ele geçirmek/değiştirmek için sorulan soruların cevabını alabilir, mağdurun annesinin kızlık soyadını öğrenerek kredi kartının bilgilerini ele geçirebilir vs. Böylece mağdur, failden hiç şüphe etmeden kendi eliyle teslim olmuş olur.

Aynı zamanda sosyal mühendislik kullanan bir siber fail, mağdurdan bilgisayarının kamerasını açmasını isteyebilir, mağdurla bu aşamaya gelecek bir samimiyet kurabilir. Daha sonra, kamerasını açan mağdurdan, bir kısım cinsel içerikli görüntüler oluşturmasını isteyebilir. Tüm bu görüntüleri, ekran görüntüsü kaydedici programlarla kaydeden siber fail, kayıtları tamamladıktan sonra, bu kayıtları mağdura karşı şantaj yapmak suretiyle kullanabilir.

Yahut da tüm sisteme girme yöntemini kullanan siber fail, son çare olarak sosyal mühendisliği kullanabilir. Mağdura bu yönden yaklaşarak istediğini ele geçirmek için sanal ortamda, sanal güven oluşturmaya çalışır.

Esasında sosyal mühendislik, kişisel girişim olarak görülse de organize bir yapı tarafından daha farklı boyutlarda da kendini gösterebilir. Örneğin, çok güvenilir gibi görünen bir alışveriş sitesi oluşturan siber failler, mağdurlarda bu alışveriş sitesinin güvenilirliği yönünde bir algı oluşturabilirler. Sitenin görünümü, sitede yer alan olumlu görüş bildiren ve yine siber failler tarafından oluşturulmuş kullanıcı mesajları, sosyal medyada yer alan ve site ile ilgili övücü görüş bildiren sahte hesaplar, güven oluşturan mailler, canlı müşteri hizmeti görünümü veren aramalar vs. yöntemi ile mağdurlar sitenin güvenilirliğine inanırlar. Oluşturulan alışveriş sitesinden sipariş veren kişilerin tüm kişisel verilerini, üyelik ve alışveriş talimatı formları ile ele geçiren siber failler, belli bir süre mağdur sayısını arttırdıktan sonra, asıl amaçlarını gerçekleştirmek için harekete geçerler ve tüm kredi kartlarını boşalttıkları gibi, sosyal medya aracılığıyla siteye üye olan kişilerin, sosyal medyadaki tüm bilgilerini de ele geçirmiş olurlar.

Görüldüğü gibi, sosyal mühendisliğin çok çeşidi bulunmaktadır ve kullanıcılar bu gibi olasılıklara karşı dikkatli ve duyarlı olmalıdırlar.

► ***Truva Atı:***

Herkes tarafından bilinen ve Yunan mitolojisinde Yunanlılar ile Akhalılar arasındaki savaşta, Akhalıların kale içine aldıkları bir Truva atının içinde gizlenen askerlerin, daha sonra gizlendikleri yerden çıkarak kaleyi ele geçirmeleri efsanesine uyarlılık gösteren Truva Atı tekniği, bilindik olduğu kadar işe yarayan bir tekniktir.

Kullanıcı, internetten indirdiği yahut kendisine mail ile gelen bir programı kurar iken, çok az yer kaplayan ve gerek virüs tarama programı gerekse diğer güvenlik duvarları tarafından zararlı gibi görünmeyen program, kurulum gerçekleştikten ve bilgisayarın içine girdikten sonra çalışmaya başlar. Truva Atı virüsleri, çoğalmazlar, sadece amaçları doğrultusunda çalışırlar ve sisteme bağlı virüs tarayıcısı kendisini fark etmeyebilir.

Truva Atı virüsleri, programı oluşturan kişinin tüm komutlarını bilgisayar içerisinde yerine getirir. Bu nedenle bilgisayar sistemine doğrudan bir zararı bulunmamaktadır. Ancak Truva Atı virüsünü yönlendiren siber fail ne isterse, onu yapar. İsterse tüm bilgisayarın çalışma sistemini bozabileceği gibi, isterse bilgisayardaki tüm bilgilerin aktarılmasını da sağlayabilir.

Bu nedenle kullanıcılar, en güncel ve güvenilir virüs programlarına sahip olmalıdırlar. Aynı zamanda, işletim sistemleri orijinal olmalı ve devamlı güncel tutulmalıdır. Ve en önemlisi, internette yahut kendilerine mail ile gelen her programı indirmemelidirler. Programı hazırlayan kişi yahut şirketten emin olmadan ve zararsız ve hatta bilgisayarın işlemesine yararlı gibi gözükse de, güvenilir olmayan programları bilgisayarlarına indirmemelidirler. Belli ve sık aralıklarla bilgisayarlarında virüs taraması yapmaları da zorunludur.

► ***Sistemi Ele Geçirme (Hacking) :***

Uzun zamandır, tüm bilgisayarlarda güvenlik duvarı ve virüs programları yer almaktadır. Ancak ne olursa olsun, tüm bu sistemleri, sistemleri yapanlardan dahi daha iyi bilen ve açıklarını çok iyi görebilen hacker denilen kişiler yetişmektedirler. Bilişim korsanı da denilen bu hackerlar, sistemi ele geçirerek, istedikleri her şeye ulaşmaktadırlar.

Bilişim korsanları, kişisel verilerden çok, kurumsal ve şirketsel verileri hedef almaktadırlar. Hatta bazı bilişim korsanları, sadece siyasi bir amaç için dahi çalışabilir. Hiçbir maddi kazanç gütmeyebilir. Bazı bilişim korsanlarının sadece internette yer alan pornografik yayın yapan siteleri çökertmek için çalıştığını dahi bilmekteyiz.

Esasında bilişim korsanlarına karşı, normal kullanıcıların yapabilecekleri çok şey yoktur. Zira bilişim korsanları, sistemin açıklarını kullanmaktadırlar ve kullanıcıyla doğrudan iletişime çoğu zaman geçmeseler de, yine bir kısım programlar kullanırlar. Bilişim korsanlarına karşı normal kullanıcıların yapmaları gereken en etkili yöntem, yazılımlarını orijinal ve güncel tutmak, gerekli olmadığı sürece, güvenilir görünümlü olsa dahi gereksiz hiçbir programı bilgisayara kurmamalarıdır.

► ***Solucanlar:***

Ağ solucanları da denilen bu programlar, sisteme girerek, girdikleri bilgisayarın bağlı olduğu ağda yer alan diğer bilgisayarlara da bulaşabilirler. Sisteme zarar verme zorunlulukları bulunmayan solucanlar, sisteme girmeye çalıştıklarında, karşılaştıkları güvenlik duvarı yahut virüs programını, kendi içerilerine yerleştirilmiş kütüphanelerinde yer alan şifrelerle aşmaya çalışırlar ve eğer karşılaştıkları virüs programı yahut güvenlik duvarı iyi oluşturulmamış ise, bu engelleri çok rahat aşabilirler.

Sisteme giren solucanlar, üzerlerinde taşıdıkları Truva Atı'nı sisteme bırakabilirler ya da doğrudan doğruya sistemi çökermeye yönelik girişimlerde bulunabilirler. Solucanların önemli özelliklerinden biri de, sistemde hiçbir iz bırakmamalarıdır. Görevlerini tamamladıktan sonra, sistem üzerinde yer alan ve kendilerini deşifre edecek tüm izleri de silerler.

Bu nedenle normal kullanıcıların, iyi ve güncel bir güvenlik duvarı ve virüs programına sahip olmaları, solucanlara karşı en etkili yöntemdir.

► ***Bukalemunlar:***

Çalışma yöntemi açısından Truva Atı'na benzeyen bukalemunlar, sisteme giriş bakımından Truva Atı gibi zararsız bir programmış gibi sisteme girerler. Sisteme girdikten sonra sistem içerisinde saklanma kabiliyetleri nedeniyle bu adı alan bukalemun programlar, sistem içerisinde çok iyi bir şekilde saklanarak, sisteme girdikten sonra gerçek amaçlarına uygun bir şekilde çalışmaya başlarlar.

Bilgisayar içerisinde yer alan tüm şifreleri, özel ve ulaşılması koruma altında olan tüm bilgileri, kullanıcı tarafından görünmeyen bir dosyaya yerleştiren bukalemun programlar, verileri çok iyi bir şekilde taklit edebilirler.

Bukalemun programlarının ortak özelliklerinden biri de, sisteme girdikten belli bir süre sonra, normal zamanlarda görünen, örneğin ***"güncelleme yapılacağından ötürü bilgisayar kapanacaktır"*** şeklinde, gayet normal görünümlü bir mesajın ortaya çıkmasını sağlamalarıdır. Zira yukarıda da denildiği gibi, verileri taklit edebilme özellikleri çok iyidir. Kullanıcı, her zaman karşılaştığı bu mesaja aldırmaz ve hatta bilgisayarı yönergeye uygun bir şekilde kapatma komutuna tıklar. Daha sonra, bukalemun yazılımını kullanan kişi, sisteme girerek istediği her şeyi yapar, ele geçirmek istediği tüm verileri alır.

Görüldüğü üzere, bukalemun yazılımlarına karşı da normal kullanıcıların yapabileceği yöntem, internetten çok ve gereksiz program indirmemeleri, iyi bir güvenlik duvarı ve güncel bir virüs programına sahip olmalarıdır.

►***Mantık Bombası:***

Esasında İngilizce çevirisi nedeniyle böyle bir isim alan bu virüs çeşidi, bir anlamda Truva Atı virüsünün bir modelidir. Zamanlı bomba da denilebilecek bu virüs türü, aynı Truva Atı gibi sisteme girmekte, daha sonra belli bir etkiyi beklemektedir. Bu etki yani bombayı harekete geçirecek fiil, bir zaman olabilir yani virüs zamana bağlı ayarlanmış olabilir yahut bir işlem gerçekleştirmeye *(word belgesi açma, tarayıcıyı kapama vs.)* bağlı hale getirilmiş olabilir. Ön koşul işlemi gerçekleştikten sonra, virüs çalışmaya başlar ve yıkıcı etki göstererek sistemi çökertir. Bu tip virüsler, tamamen sistemi çökertmeye yöneliktir. Ülkemizde 1999 yılında görülen Çernobil Virüsü, bu virüslere en iyi örnektir.

Truva Atı virüslerine karşı korumak için yapılması gerekenler, bu tip virüsler için de geçerlidir.

►*Bilişim Virüsleri:*

Bilişim virüsleri, en çok karşılaşılan ve belki de kişisel kullanıcıların en çok zarar gördüğü virüs türleridir. Bu virüsler, sisteme kendilerini gizleyerek girerler ve sistem içerisinde belli yerlere yerleşirler. Bilgisayarda yer alan ve en çok değişim aracı olarak kullanılan belgelere, fotoğraflara, flaş belleklere, CD'lere bulaşarak yayılırlar.

Esasında, kullanıcıların ***"bilgisayarıma virüs bulaşmış"*** dedikleri duruma neden olan bu virüslerdir. Ana amaçları bilgisayarın çalışma sistemini bozmak, zarar vermek ve yayılmaktır. Ancak bilgisayardaki verileri almak için de kullanılabilirler.

Bu virüslerin ana özellikleri çoğalmalarıdır. Ancak çoğalarak yayılabildikleri için, her daim çoğalmayı öngören bir yazılım üzerine kurulmuş programlardır. Bir anlamda mantarların sporları gibi çoğalmaya çalışırlar ve özellikle yayılmak için en çok kullanılan bölümlere yerleşirler.

Bu tip virüslerin oluşturduğu tahribatı gidermek çok zordur. Format adı verilen ve bilgisayardaki sistemi silip yeniden kurma manasına gelen işlem yapılsa dahi, yine de oluşan zararı tamamen yok etmek bazen mümkün olmayabilmektedir.

Bilişim virüsleri o kadar çeşitli hale gelmişlerdir ki, antivirüs programları dahi bu hususta çaresiz kalmış durumdadırlar. Hatta bazı otoriteler, bizzat antivirüs programları satan şirketler tarafından yeni virüsler üretildiğini, bu şekilde antivirüs programlarının satılması döngüsünün oluşturulduğu belirtilmektedir.

Belirtilen nedenlerle, piyasada kullanıcılara ücretsiz olarak dağıtılan antivirüs programları, bilişim virüslerine karşı çoğu zaman çaresiz kalmaktadırlar. Bu nedenle ücretli antivirüs programlarının alınması yönünde teşvik oluşturulmaktadır. Gerçekten de iyi bir şekilde bilgisayarı korumak için lisanslı ve ücretli bir antivirüs programı kullanma zorunluluk haline gelmiştir.

SONUÇ:

Yukarıda bilişim suçları hakkında ve bu suçların işlenme yöntemleri hakkında kısa bilgiler verilmiştir. Bir anlamda hukuki durumdan ziyade fiili durum hakkında bir ön bilgi mahiyetinde anlatımlarda bulunulmuştur.

Defaten belirtildiği gibi, belirtilen teknikler dışında daha birçok teknik vardır ve hatta bazıları yukarıda belirtilen tekniklerin bir araya getirilmesi ile de oluşturulabilmektedir.

Ancak, bireysel kullanıcıların dikkat etmeleri ve kesinlikle atlamamaları gereken husus şudur ki; bu konudaki farkındalıklarını arttırmalıdırlar.

Güncel ve güvenilir bir antivirüs programına sahip olmak, orijinal ve lisanslı bir işletim sistemi yüklü bilgisayar kullanmak, ilk alınması gereken önlemdir. Bu önlemler de yeterli gelmemekte, bilgisayara indirilen programlara dikkat etmek, bilgisayara kaydedilen tüm belge, fotoğraf ve dosyaları, bilgisayara takılan flaş bellekler ve CD'leri mutlaka kontrol etmek ve virüs taramasından geçirmek gerekmektedir.

Bilgisayarın çalışma sistemi çok iyi takip edilmelidir. En ufak bir tereddütte hemen çalışmaya ara vermek ve tüm bilgisayarı ayrıntılı bir virüs taramasından geçirmek gerekmektedir. Ayrıca virüs programını ve güvenlik duvarını kapatmayı öngören hiçbir programı bilgisayarda barındırmamak lazımdır.

Son olarak güvenli olmayan sitelere hiçbir şekilde girilmemesi önem arz etmektedir. Zira internet tarayıcıdan girilen her sitenin belli bazı bilgileri (resimler, yazılar vs.) tarayıcı tarafından hemen kaydedilmektedir. İşte bu kayıt sırasında dahi bilgisayara zararlı bir program/yazılım yüklenebilmektedir.

Bilgisayarın devamlı internete bağlı olup olmaması, bilgisayar içerisinde bulunan zararlı yazılım bakımından çok büyük bir önem arz etmemektedir. Zira zararlı yazılım, bilgisayar içerisinde çalışmaya ve verileri kaydetmeye devam etmektedir, internete bağlandığı anda bilgileri siber failin istediği yere, kullanıcının farkına varmayacağı şekilde aktarmaktadır.

Unutulmamalıdır ki, siber failler her türlü saldırıyı gerçekleştirmek için fırsat kollamaktadırlar. Bu nedenle internet kafe ve ortak kullanıma açık kablosuz bağlantı noktaları gibi yerlerde, internet bankacılığı tarzında önem arzeden işlemler yapılmamalı, şifre ile giriş yapılan sitelere zorunlu olmadıkça girilmemelidir.

Bilişim suçları ile ilgili en önemli korunma yöntemi, bu konuda bilgilenmek ve farkındalığın artmasıdır. Bu nedenle, sitemizde ve sosyal paylaşım sayfamızda, bu konu ile ilgili önemli ve temel olarak bilinmesi gereken bilgileri kamuya açık bir şekilde paylaşmaktayız.

Farkındalık, dikkat etmek demek değildir. Farkındalık, dikkatten daha öte bir uyanık bilince sahip olmak, tüm sürece hâkim olmaktır. Bunun da tek yolu, bilgi sahibi olmaktan geçmektedir. Bilgisi olmayanın bir fikri olmayacağı gibi farkındalığı da olmayacağı açıktır. Bu nedenle, tüm açık kaynaklardan bu konularla ilgili farkındalığınızı arttırıcı bilgiler edinilmesi ve edinilen bilgilerin uygulanması önem arz etmektedir.