



ESKİŞEHİR BAROSU DERGİSİ

DİJİTALLEŞEN DÜNYADA FİNANSAL DOLANDIRICILIKLAR: RİSKLER, YÖNTEMLER VE GÜVENLİK ÖNLEMLERİ

Av. Murat Osman KANDIR¹

GİRİŞ

Dijitalleşmenin finansal sistemlere sağladığı hız ve erişim kolaylığı, aynı zamanda güvenlik sorunlarını da beraberinde getirmiştir. Özellikle banka işlemleri, Forex yatırımları ve kripto para platformları üzerinden işlenen dolandırıcılık suçları Türkiye’de son yıllarda ciddi artış göstermektedir. İnternet bankacılığı, mobil uygulamalar, sosyal medya üzerinden yapılan yönlendirmeler, sahte yatırım fırsatları ve manipülasyon yöntemleri bireyleri ve kurumları hedef almakta; büyük maddi kayıplara yol açmaktadır.

1. İNTERNET BANKACILIĞI VE MOBİL BANKACILIKTA Kİ TEHLİKELER

Teknolojinin hızla gelişmesiyle birlikte, internet ve mobil bankacılık hizmetleri hayatımızın ayrılmaz bir parçası haline geldi. Bu kolaylık, finansal işlemlerimizi her an her yerden yapabilmemizi sağlarken, beraberinde birçok siber tehdidi de getirmektedir. Özellikle dijital okuryazarlığı düşük olan bankacılık müşterileri, bu tehditler karşısında savunmasız kalabilmektedir.

Dolandırıcıların en sık kullandığı yöntemlerden biri kimlik avı (phishing) saldırıdır. Sahte e-postalar, SMS mesajları veya internet siteleri aracılığıyla bankanızdan geldiği izlenimini yaratarak kullanıcıların bankacılık bilgilerini ele geçirmeye çalışırlar. Bu tür saldırılardan korunmak için, bankanın resmi web adresini doğrulamadan asla bilgi girişi yapmamak, SMS veya e-posta yoluyla gelen linkleri

¹ Avukat, Eskişehir Barosu, bilgi@mkandir.av.tr.

dikkatlice incelemek ve mobil bankacılık için yalnızca bankanın resmi uygulamasını kullanmak büyük önem taşır.

Bir diğer büyük tehdit ise kötü amaçlı yazılımlardır. Siber saldırganlar, bilgisayar veya mobil cihazlara bulaşan bu yazılımlarla banka bilgilerinizi çalmayı hedefler. Özellikle Keylogger adı verilen yazılımlar, klavyede basılan tuşları kaydederek bilgilerinizi ele geçirir. Bu duruma karşı, bilgisayarınızda veya telefonunuzda güncel bir antivirüs programı bulundurmalı, bilinmeyen kaynaklardan uygulama indirmekten kaçınmalı ve bankacılık işlemleri için güvendiğiniz bir cihaz kullanmalısınız.

Halka açık Wi-Fi ağlarını kullanmak da risk taşır. Ortadaki Adam (Man-in-the-Middle) saldırıları olarak bilinen bu tehditlerde, şifresiz ağlar üzerinden yaptığınız işlemler dinlenerek bankacılık bilgileriniz ele geçirilebilir. Bu nedenle, bankacılık işlemlerini yalnızca güvenli ve şifreli internet bağlantıları üzerinden yapmak önemlidir.

Özellikle mobil bankacılıkta sahte uygulamalar da büyük bir tehlikedir. Siber saldırganlar, arama motorlarında reklam vererek sahte bankacılık uygulamalarını ilk sıralara taşıyabilirler. Örneğin, "Ücretsiz futbol maçı izle" gibi ilgi çekici başlıklarla hazırlanan sahte uygulamalar, kullanıcıların telefonlarına zararlı yazılım indirmesine ve bu yazılımların banka hesaplarını ele geçirmesine neden olabilir. Bu tür karmaşık saldırıların faillerini bulmak genellikle çok zordur.

Tüm bu risklere rağmen, bankaların da güvenli hizmet sunma konusunda sorumlulukları vardır. Sadece parola korumasının yeterli olmadığı günümüz teknolojisinde, bankalar yapay zekâ destekli güvenlik yazılımları kullanmalı ve en ufak şüpheli işlemde kullanıcının hesabına bloke koymalıdır. Müşterilerine imzalatılan kullanım sözleşmeleri, bankaları bu sorumluluktan kurtarmaz. Güven kuruluşları olan bankalar, müşterilerinin maddi kayıplarını önlemek için sürekli olarak güvenlik sistemlerini güçlendirmek zorundadır

2. FOREX DOLANDIRICILIKLARI

Forex piyasası, küresel ölçekte günlük işlem hacmi 6 trilyon doları aşan devasa bir finansal pazardır. Türkiye’de bu piyasa Sermaye Piyasası Kurulu (SPK) tarafından düzenlenmekte olup, yalnızca SPK lisanslı aracı kurumlar üzerinden işlem yapılmasına izin verilmektedir. Ancak özellikle internet reklamları ve sosyal medya aracılığıyla yatırımcılara ulaşan yurtdışı merkezli, lisanssız Forex şirketleri ciddi bir risk oluşturmaktadır.

Bu dolandırıcılıkların en yaygın yöntemi, yüksek ve garanti kâr vaatleriyle yatırımcıları sisteme çekmektir. İlk aşamalarda sahte kazanç ekranlarıyla güven sağlanır; ancak para çekme talepleri reddedilir ya da ek teminat yatırılması istenir. Bazı durumlarda Ponzi benzeri sistemler kullanılarak yeni yatırımcıların paraları mevcut yatırımcılara aktarılır ve sistem bir süre sonra çöker (Yargıtay 11. CD., 2021).

SPK’nın 2021 tarihli raporuna göre, Türkiye’de faaliyet gösteren lisanssız Forex platformlarının büyük çoğunluğu sosyal medya üzerinden reklam yapmaktadır. Ayrıca Yargıtay’ın birçok kararında lisanssız aracı kurumlar üzerinden yapılan işlemler dolandırıcılık kapsamında değerlendirilmiştir. Bu nedenle hem yatırımcıların bilinçlendirilmesi hem de uluslararası iş birliğinin artırılması önem arz etmektedir.

Yaşamın her alanında etkisini gösteren yapay zekâ teknolojilerinin kötü niyetli kullanımı gün geçtikçe artmaktadır. Özellikle Generative Adversarial Networks- GAN (Çekişmeli Üretici Ağlar) adı verilen yapay sinir ağları (artificial neural network) modeli kullanılmaktadır. Sürekli olarak şikâyet edilse de yapay zekâ teknolojileri tarafından üretilen sahte videoların Youtube platformunda yer alması engellenememektedir.

İnternetin yaygınlaşmasından önce en güçlü medya aracı olan televizyonda, reklamlar için toplumun güvendiği ve tanıdığı yüzler kullanılırdı. Bunun temel nedeni, bu kişilerin toplumda zaten bir güven oluşturmuş olmasıydı. Bu yöntem, günümüzde de sosyal medya reklamlarında yaygın olarak kullanılmaktadır.

Ancak, dijitalleşmeyle birlikte bu durumun yeni ve tehlikeli bir boyutu ortaya çıktı. Toplum tarafından tanınan kişilerin internetteki görüntü ve sesleri toplanarak yapay sinir ağları eğitime başlandı. Özellikle yapay zekâ araçları kullanılarak oluşturulan sahte videolar (deepfake), insanları kolayca ekonomik kazanç elde edecekleri vaadiyle kandırarak büyük kayıplara uğrattı.

Bu sahte videolarda, tanınmış kişiler sanki kendileri konuşuyormuş gibi gösterilerek çeşitli yöntemler ve yüksek kazanç vaatleri sunuluyor. İzleyiciler, güvendikleri ünlü birinin ağzından çıkan bu tavsiyelere inanarak kendilerinin de kolayca zengin olabileceğini düşünüyor. Dolandırıcılar, bu videolarla dikkatlerini çektikleri kişileri, verdikleri iletişim bilgileri üzerinden dolandırıcılık ağına çekerek ikna ediyorlar. Bu dolandırıcılık türünde en sık karşılaşılan tavsiyelerden biri, FOREX internet siteleri üzerinden yatırım yapma vaadidir.

Son zamanlarda işlem hacmi hızla artan Forex piyasaları, dolandırıcıların yeni hedefi haline gelmiştir. Dolandırıcılar, ünlü ve tanınmış şirketlerin sahte web sitelerini oluşturarak, kurbanlarını bilinen Forex sitelerine yatırım yaptıklarına inandırmakta ve sahte sitelere yönlendirmektedirler.

Bu sahte sitelerde kısa sürede büyük kazançlar elde ettiğini gören mağdurlar, daha fazla para yatırmaya teşvik edilerek tüm birikimlerini dolandırıcılara kaptırmaktadırlar. Mağdurlar, sahte hesaplardaki paralarını çekmek istediklerinde, tüm sistemin bir kurgu olduğunu anlamaktadırlar. Bu dolandırıcılık tuzağını fark ettiklerinde ise yatırdıkları paraların çoktan kripto varlıklara dönüştürülerek izlerinin kaybedildiğini görmektedirler.

Henüz tam olarak yasal bir zemine oturtulamayan kripto varlık piyasasının karmaşık yapısı içinde kaybolan paralarına ulaşma umuduyla, mağdurlar defalarca ekonomik kayıp yaşamaya devam etmekte ve bu girdaptan bir türlü kurtulamamaktadırlar.

3. KRIPTO VARLIK DOLANDIRICILIKLARI

Son on yılda hızla büyüyen ve yayılan kripto varlıklar, beraberinde yeni ve sofistike dolandırıcılık yöntemlerini de getirmiştir. Kripto paraların küresel finans sistemine entegrasyonu devam ederken, bu alandaki yasal boşluklar ve merkeziyetsiz yapı, dolandırıcılar için cazip bir ortam yaratmaktadır.

Türkiye’de, 2021 yılında MASAK (Mali Suçları Araştırma Kurulu) tarafından yayımlanan rehberle kripto varlık hizmet sağlayıcılarına müşteri tanıma (KYC) ve şüpheli işlem bildirim yükümlülüğü gibi önemli adımlar atılmış olsa da, kapsamlı bir yasal çerçeve halen beklenmektedir. Bu durum, dolandırıcıların çeşitli yöntemlerle yatırımcıları hedef almasına olanak tanımaktadır.³ Dolandırıcılık Olaylarında Bankanın Sorumluluğu

Finans alanında hukuksal bir bakış yaptığımızda en güncel yasal düzenlemelerin bu alanda yapıldığını ve yapılmaya devam ettiğini görüyoruz. Bu kadar güncel yasal düzenlemelerin yapıldığı bir alan nasıl oluyor da siber saldırıların en gözde hedefi oluyor. Bu sorunun cevabı tabii ki ; Para. Suç aleminin öncelikli amacı daima ekonomik kazanç sağlamak olmuştur. Bir de bu alanda kolay para kazancı olduğu fark edildiğinde tüm gözler bu alan odaklanmaktadır. Bankalar, ilk dijital dönüşümü yaşayan kurumların başında gelmektedir. İnternet bankacılığı ile başlayan süreç akıllı telefonların yaygınlaşmasıyla mobil bankacılığa dönüşmüş ve neredeyse fiziksel bankacılığın sonunu getirmiştir. Hala fiziksel banka şubelerinin mevcudiyeti devam ediyor olsa da hem sayıları azalmış hem de müşteri potansiyelleri düşmüştür.

Peki bu dijital dönüşümde bankacılık sektörü ne kadar başarılı oldu? Son yüzyılın en büyük teknolojik buluşu olarak sayılan yapay zekâ bankaların güvenliğini sağlayacak ürünlerde çoktan yerini almış durumda. Birçok güvenlik yazılımı yapay zekadan faydalaniyor. Gelişen teknolojiye paralel olarak yasal düzenlemelerde yapılmış durumda. 15 Mart 2020 tarihli ve 31069 sayılı Resmi gazetede yayımlanan “Bankaların Bilgi Sistemleri Ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik” bu konunun en güzel örneğidir. Özellikle yönetmeliğin “Bilgi Güvenliği

Yönetimi” bölümünde bankaların müşterilerinin işlemleri ile ilgili hangi güvenlik önlemlerini almaları gerektiği ayrıntılı olarak açıklanmaktadır. Yönetmeliğin aşağıdaki maddeleri bankanın sorumluluk alanının çerçevesini çizen maddelerden birisidir.

İnkâr edilemezlik ve sorumluluk atama

MADDE 35 – (1) Banka, sunmakta olduğu elektronik bankacılık hizmetleri kapsamında gerçekleştirilen işlemlerde hem banka hem de müşteri için inkâr edilemezliği ve sorumluluk atamayı mümkün kılacak teknikler kullanır. Kullanılan tekniğin oluşturduğu iz kayıtlarının güvenilir delillerin elde edilmesini sağlayacak ve sorumluluk atayacak nitelikte olması sağlanır.

İşlemlerin takibi

MADDE 36 – (1) Banka, elektronik bankacılık hizmetleri kapsamında gerçekleşen olağan dışı, sahtekârlık amaçlı veya dolandırıcılık riski bulunan işlemleri tespit etmeye ve bunları önlemeye yönelik işlem takip mekanizmaları kurar. İşlem takip mekanizması kapsamında uygun olan durumlarda asgari olarak aşağıdaki risk unsurları takip edilir:

- a) Finansal sonuç doğuran işlemlere yönelik bilinen dolandırıcılık yöntemleri,*
- b) Gerçekleştirilen her bir bankacılık işleminin tutarı ve bu tutarlara göre müşterinin konum bilgisi de kullanılarak normal dışı bir ödeme, fon transferi ya da davranış deseni gösterip göstermediği,*
- c) Kaybolmuş, çalınmış ya da yetkisiz kişilerce ele geçirilmiş kimlik doğrulama unsurlarının listesi,*
- ç) Her bir kimlik doğrulama oturumuna yönelik olarak zararlı yazılımların bulaşmış olabileceğini gösteren belirtiler.*

(2) Banka, riskli işlemleri filtreleyerek değerlendirir ve bu filtrelere takılan müşterileri daha yakından takip eder. Riskli işlemlerin gerçekleştirildiğinin tespit edilmesi

halinde banka, telefon ya da kısa mesaj gibi uygun yöntemlerle müşterilerin en kısa sürede uyarılmasını sağlar.

Yukarıdaki yönetmelik maddeleri bankaların müşterilerinin işlem güvenliğini sağlayacak yöntemleri örnekleme usulüyle belirtmektedir. Tüm müşteri işlemlerinin iz kayıtlarının alınması gerektiğinden bahisle birçok yöntemin birlikte kullanılması gerektiğini anlatmaktadır. Müşterinin bankacılık işlemine bağlantı yaptığı konum bilgisi ile yapılan işlemlerin müşteri tarafından yapılıp yapılmadığının kontrolünün yapılması gerektiğinden bahsetmektedir. İnternet bankacılığı ilişkili yaşanan dolandırıcılık olaylarının büyük bir çoğunluğu saldırganın farklı bir konumdan bağlantı yapması sonucunda gerçekleşmektedir. Bu saldırılar esnasında konum bilgisi kontrolü yapılıp yapılmadığı konusu ise meçhul bir bilgi olarak kalmaktadır. Mahkemeler tarafından istenen iz kayıtlarında bu hususlar yer almasına rağmen çoğu zaman bilirkşi raporlarında yer almamaktadır.

Günümüzde hemen hemen tüm alanlarda yapay zekâ teknolojisi kullanılırken bankaların bu teknolojilerden faydalanmaması mümkün değildir. Ancak her alanda olduğu gibi yazılımlar ne kadar iyi olursa olsun ne kadar gelişmiş olursa olsun son kararı insan vermektedir. Eğer tüm bu gelişmiş güvenlik sistemleri insan kara vericiler tarafından takip edilmezse, incelenmezse ve zamanında reaksiyon gösterilmezse işlevsiz kalmaktadır. Söz konusu yönetmeliğin hazırlanmış olması uygulanma sürecinin kontrolü yapılmadığında yetersiz kalmaktadır. Bankalarda SMS gönderimlerinin arkasına sığınarak sorumluluğu müşteriye yüklemeye çalışmaktadırlar. Eğer bankacılık alanında dolandırıcılıklar engellenecekse bunun ilk adımı bu alanda yapılmış olan yasal düzenlemelere tam olarak uymak olacaktır. Tüm bu saldırı tekniklerinin test edileceği sızma testleri ile bankaların güvenlik yeterlilikleri kontrol edilmelidir. Yapay zekâ içeren güvenlik yazılımları ile her bir müşterinin bankacılık işlem profilleri çıkarılarak farklı desen gösteren işlemler şüpheli işlem kategorisine alınmalı ve müşteri banka şubesine davet edilmelidir. Aksi takdirde dijital okuryazarlık konusunda yeterli seviyede olmayan müşterilerin zarara uğraması kaçınılmaz olacaktır. İnternet bankacılığı alanında yaşanan dolandırıcılıklar

sonrasındaki dava süreçlerinde bilirkişi incelemelerinin bankaların bilişim sistemlerini de kapsayacak şekilde genişletilmesi bu sürece katkı sağlayacaktır.

06.07.2019 tarih ve 30823 sayılı Resmî Gazete’ de Bilgi ve İletişim Güvenliği Tedbirleri konulu 2019/12 sayılı Cumhurbaşkanlığı Genelgesi yayımlanmıştır. Söz konusu Genelgede “ Güvenlik risklerinin azaltılması, etkisiz kılınması ve özellikle gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik türdeki verilerin güvenliğinin sağlanması amacıyla ulusal ve uluslararası standartlar ve bilgi güvenliği kriterleri çerçevesinde, kamu kurum ve kuruluşları ile kritik altyapı niteliğinde hizmet veren işletmelerde uygulanmak üzere farklı güvenlik seviyeleri içeren “Bilgi ve İletişim Güvenliği Rehberi” Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı koordinasyonunda, ilgili kamu kurum ve kuruluşları tarafından gereken katkı sağlanarak hazırlanacak ve www.cbddo.gov.tr adresinde yayımlanacaktır. Rehber ihtiyaçlar, gelişen teknoloji, değişen şartlar ile Ulusal Siber Güvenlik Stratejisi ve eylem planlarında yapılacak değişiklikler göz önünde bulundurularak güncellenecektir.” ibaresi yer almakta ve Bilgi ve İletişim Güvenliği Rehberi’ne dayanak teşkil etmektedir. Bilgi ve İletişim Güvenliği Rehberi’nde bahsi geçen Kritik altyapı sektörleri 2024 – 2028 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı’nda “Elektronik Haberleşme”, “Enerji”, “Su Yönetimi”, “Kritik Kamu Hizmetleri”, “Ulaştırma”, “Bankacılık ve Finans” olarak yer almaktadır.” Görüldüğü üzere Bankacılık ve Finans sektörü kritik altyapı sektörleri arasındadır. Yapılacak Bilgi ve İletişim Güvenliği Uyum denetimlerinde ek olarak Bankacılık sektörüne ait yapılmış yasal düzenlemelere uyumun da denetlenmesi bu alanda meydana gelen siber suçların önlenmesi kapsamında büyük önem taşımaktadır.

4. HUKUKİ ÇERÇEVE VE KURUMSAL MÜCADELE

Türkiye’de banka, Forex ve kripto para dolandırıcılıklarına karşı hukuki mücadele, mevcut yasal düzenlemeler ve kurumsal iş birlikleri üzerinden yürütülmektedir. Siber suçların hızla evrilen doğası, hukuki çerçevenin de sürekli olarak güncellenmesini ve güçlendirilmesini zorunlu kılmaktadır.

4.1. Türk Ceza Hukuku ve İlgili Yasal Düzenlemeler

Türkiye'de siber dolandırıcılık suçlarının cezalandırılmasında temel yasal dayanak, **Türk Ceza Kanunu (TCK)**'dur. TCK'nın ilgili maddeleri, dolandırıcılık suçunun farklı boyutlarını ele almaktadır:

- **Dolandırıcılık (TCK m. 157):** Bu madde, hileli davranışlarla bir kişiyi aldatarak kendisine veya başkasına menfaat sağlayan kişiye ceza verilmesini düzenler. Siber dolandırıcılıkta, sahte web siteleri, e-postalar veya sosyal medya hesapları üzerinden yapılan kandırmaca eylemleri bu kapsamda değerlendirilir.
- **Nitelikli Dolandırıcılık (TCK m. 158):** Siber dolandırıcılık suçlarının büyük bir kısmı bu madde kapsamında işlenir. Özellikle "bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması" (TCK m. 158/1-f) ve "ticari faaliyeti yürüten kişilerin aldatılması" (TCK m. 158/1-h) halleri, siber dolandırıcılık vakalarına doğrudan uygulanmaktadır. Bu maddeler, suç daha ağır bir şekilde cezalandırarak caydırıcılık sağlamayı amaçlar.
- **Bilişim Sistemine Girme (TCK m. 243) ve Sistemi Engelleme (TCK m. 244):** Bu maddeler, dolandırıcıların kullandığı teknik yöntemleri suç kapsamına alır. Başkasının bilişim sistemine izinsiz girme, sistemin işleyişini engelleme veya bozma gibi eylemler, dolandırıcılık suçunun yanında ayrıca cezalandırılabilir. Bu maddeler, siber saldırganların kullandığı araçları hedef alarak hukuki çerçeveyi genişletir.

Ayrıca, **Sermaye Piyasası Kanunu (SPKn)**, finansal dolandırıcılıkla mücadelede kritik bir rol oynamaktadır. SPKn, yetkili Sermaye Piyasası Kurulu (SPK) lisansına sahip olmayan kurumların aracı faaliyetlerde bulunmasını yasaklar. SPK, bu tür yasa dışı faaliyetleri denetlemek ve engellemekle yükümlüdür. Bu düzenleme, özellikle lisanssız Forex ve yatırım şirketlerinin sahte vaatlerle yatırımcıları dolandırmasını önlemeyi hedefler.

Kripto varlıklar özelinde ise, henüz kapsamlı bir yasa çıkarılmamış olsa da, **MASAK (Mali Suçları Araştırma Kurulu)** tarafından yayımlanan düzenlemeler önemli bir hukuki dayanak sunmaktadır. 2021 yılında yayımlanan rehber ile kripto varlık hizmet sağlayıcılarına **müşteri tanıma (KYC)** ve **şüpheli işlem bildirim yükümlülüğü** getirilmiştir. Bu adım, kripto para piyasasının anonimliğini azaltarak kara para aklama ve terörün finansmanı gibi suçların izlenmesini kolaylaştırmaktadır.

4.2. Kurumsal Mücadele ve Uluslararası İş Birliği

Siber dolandırıcılık suçları, genellikle ulusal sınırları aşan ve birden fazla ülkeyi kapsayan bir yapıya sahiptir. Bu nedenle, etkili bir mücadele için ulusal kurumların uluslararası düzeyde iş birliği yapması zorunludur.

- **Ulusal Kurumlar Arası İş Birliği:** Türkiye'de Siber Suçlarla Mücadele Daire Başkanlığı, MASAK, BDDK ve SPK gibi kurumlar, siber suçlulara karşı ortak operasyonlar düzenlemekte ve bilgi paylaşımında bulunmaktadır. Özellikle bankacılık ve finans sektörü temsilcileriyle yapılan toplantılar ve ortak tatbikatlar, dolandırıcılık yöntemlerine karşı daha hızlı ve etkili bir yanıt verilmesini sağlar.
- **Uluslararası Ortaklıklar:** Europol, Interpol ve FATF (Mali Eylem Görev Gücü) gibi uluslararası kurumların yayınladığı raporlar, finansal dolandırıcılıkların küresel boyutunu gözler önüne sermektedir. **Europol'ün 2022 tarihli Internet Organised Crime Threat Assessment (IOCTA) raporu**, siber suçların giderek daha organize hale geldiğini ve sınır ötesi bir nitelik kazandığını vurgulamaktadır. Türkiye'nin bu tür uluslararası platformlarla iş birliği yapması, siber suçluların izini sürmek ve yakalamak için kritik önem taşır. FATF'nin kripto varlıklarla ilgili raporları, kara para aklama yöntemlerine karşı küresel standartların belirlenmesine katkı sağlamaktadır.

Ülkemizin hukuki çerçevesi ve kurumsal mekanizmaları, siber dolandırıcılıkla mücadele için önemli bir zemin oluşturmaktadır. Ancak bu mücadelenin etkinliğini artırmak için yasal düzenlemelerin hızla güncellenmesi ve uluslararası iş birliklerinin

sürekli olarak güçlendirilmesi gerekmektedir. Siber suçların karmaşıklığı, sürekli gelişen bir savunma stratejisi ve uluslararası alanda ortak hareket etme zorunluluğunu beraberinde getirmektedir.

5. SİBER DOLANDIRICILIĞA KARŞI KAPSAMLI ÖNLEYİCİ STRATEJİLER

Siber dolandırıcılık, bireyleri, kurumları ve devletleri tehdit eden küresel bir sorun haline gelmiştir. Bu suçlarla mücadele edebilmek için bütüncül bir yaklaşım benimsemek şarttır. Önleyici stratejiler, bireylerin kişisel güvenlik önlemlerinden, finansal kurumların ve devletin sistemik sorumluluklarına kadar geniş bir yelpazeyi kapsamalıdır.

5.1. Bireysel Düzeyde Alınması Gereken Önlemler

Dolandırıcılık suçlarının kurbanı olmamak için her bireyin kendi dijital güvenliğini sağlamada aktif rol oynaması gerekmektedir. Bilinçli ve dikkatli olmak, bu mücadelenin ilk ve en önemli adımıdır.

Online ve Mobil Bankacılıkta Güvenlik:

- **Resmi Kanalları Kullanın:** Bankacılık işlemlerinizi gerçekleştirirken her zaman bankanızın resmi mobil uygulamasını veya web sitesini kullanın. SMS, e-posta veya sosyal medya üzerinden gelen linklere tıklayarak bankacılık sitelerine asla giriş yapmayın. Tarayıcınızın adres çubuğundaki URL'nin doğru ve güvenilir olduğundan emin olun.
- **Şifre ve Kimlik Doğrulama:** Güçlü ve karmaşık şifreler kullanın. Şifrelerinizi düzenli aralıklarla değiştirin ve farklı platformlarda aynı şifreyi kullanmaktan kaçının. Mümkün olan her yerde **iki faktörlü kimlik doğrulama (2FA)** özelliğini etkinleştirin. Bu, şifreniz ele geçirilse bile hesabınıza erişimi engeller.
- **Genel Ağlardan Kaçının:** Halka açık Wi-Fi ağları üzerinden bankacılık veya finansal işlemler yapmaktan kaçının. Bu ağlar güvensiz olabilir ve

bilgilerinizin üçüncü şahıslar tarafından ele geçirilmesine zemin hazırlayabilir.

Kripto Para ve Yatırım Dolandırıcılıklarından Korunma:

- **SPK Lisanslı Kurumları Tercih Edin:** Her türlü yatırım işleminiz için Sermaye Piyasası Kurulu (SPK) gibi yetkili merciler tarafından lisanslanmış ve denetlenen kurumları tercih edin. Tanımadığınız veya yasal statüsünden emin olmadığınız platformlardan uzak durun.
- **Araştırın ve Sorgulayın:** Bir yatırım fırsatı çok cazip görünüyorsa, muhtemelen bir dolandırıcılıktır. "Çok kısa sürede, yüksek kazanç" vaatlerine şüpheyle yaklaşın. Yatırım yapmayı düşündüğünüz platform veya proje hakkında detaylı araştırma yapın.
- **Sahte Borsalardan Kaçının:** Kripto para yatırımı yapacaksanız, Binance, Coinbase, BtcTurk gibi bilinen ve güvenilir platformları kullanın. Reklamlarla veya sosyal medya gruplarıyla tanıtılan, yeni açılmış ve az bilinen kripto para borsalarına karşı dikkatli olun. Bu tür sahte siteler, fonlarınızı topladıktan sonra aniden ortadan kaybolabilir.

5.2.Kurumsal ve Ulusal Düzeyde Alınması Gereken Önlemler

Siber dolandırıcılıkla mücadele, sadece bireylerin çabalarıyla sınırlı kalmamalıdır. Finansal kurumlar ve devletin bu alanda proaktif adımlar atması gerekmektedir.

Finansal Kurumların Sorumlulukları

Bankalar ve diğer finansal kurumlar, müşterilerinin varlıklarını korumakla yükümlüdür. Bu sorumluluk, güçlü teknolojik altyapılar ve proaktif güvenlik stratejileriyle desteklenmelidir.

- **Güçlü Siber Güvenlik Altyapısı:** Kurumlar, en son teknolojiye sahip güvenlik duvarları, izinsiz giriş tespit sistemleri ve yapay zekâ destekli tehdit analizi araçlarını kullanarak siber savunmalarını sürekli güçlendirmelidir.

Şüpheli işlem tespiti sistemleri, olağan dışı aktiviteleri anında belirleyerek dolandırıcılık girişimlerini engelleyebilmelidir.

- **Çalışan ve Müşteri Eğitimi:** Siber güvenlik farkındalığı, bir kurumun en önemli savunma hattıdır. Kurumlar, çalışanlarına düzenli siber güvenlik eğitimleri vererek, kimlik avı (phishing) saldırılarına karşı bilinçlenmelerini sağlamalıdır. Aynı şekilde, müşterilerini de sık sık bilgilendirmeli ve güvenlik ipuçları paylaşmalıdır.
- **İş Birliği ve Bilgi Paylaşımı:** Sektördeki tüm kurumlar, siber tehditler hakkında bilgi ve istihbarat paylaşımı için iş birliği yapmalıdır. Tehdit istihbaratı platformları, potansiyel tehlikeleri ortaklaşa izlemeyi ve önlem almayı kolaylaştırır.

Devletin Rolü ve Yasal Düzenlemeler

Devlet, siber güvenliğin ulusal düzeyde sağlanmasında ve siber suçlarla etkin mücadelede kilit bir rol oynamaktadır.

- **Kapsamlı Yasal Düzenlemeler:** Özellikle kripto varlık piyasasına yönelik kapsamlı bir yasal çerçevenin oluşturulması kritik önem taşımaktadır. Bu düzenlemeler, kripto varlık borsalarının denetlenmesini, müşteri tanıma (KYC) süreçlerinin zorunlu kılınmasını ve şüpheli işlemlerin raporlanmasını içermelidir.
- **Uluslararası İş Birlikleri:** Siber suçlar sınır tanımadığından, uluslararası alanda iş birliği şarttır. Europol ve FATF (Mali Eylem Görev Gücü) gibi uluslararası kuruluşlarla bilgi paylaşımı ve ortak operasyonlar, suçluların izini sürmek ve yakalamak için hayati önem taşır.
- **Finansal Okuryazarlığı Artırma:** Uzun vadede dolandırıcılıkla mücadele için finansal okuryazarlığın artırılması en etkili stratejilerden biridir. OECD'nin de vurguladığı gibi, eğitim müfredatlarına finansal okuryazarlık derslerinin eklenmesi, genç nesillerin finansal kararlarını daha bilinçli

almalarını sağlayacaktır. Bu eğitimler, dijital finansal araçların kullanımı ve siber tehditlere karşı korunma yollarını da içermelidir.

SONUÇ

Türkiye'de banka, Forex ve kripto para piyasalarında görülen dolandırıcılık vakaları, dijital dönüşümün sunduğu fırsatların yanı sıra, beraberinde getirdiği ciddi riskleri de gözler önüne sermektedir. Bu suç türlerinin sürekli evrilmesi ve karmaşıklaşması, bireylerden kurumlara kadar geniş bir yelpazede mağduriyetlerin artmasına yol açmaktadır. Bu durum, siber dolandırıcılıkla mücadelenin tek bir tarafın sorumluluğunda olmadığını, bireyler, finansal kuruluşlar ve devletin eş güdümlü çabalarını gerektiren bütüncül bir yaklaşım olduğunu ortaya koymaktadır.

Bireylerin Rolü ve Bilinçlenme

Dolandırıcılık suçlarına karşı en güçlü savunma hattı, bireylerin kendi bilinç seviyesidir. Kullanıcıların dijital okuryazarlık becerilerini geliştirmesi, şüpheli e-posta, SMS veya sosyal medya mesajlarına karşı tetikte olması hayati önem taşır. Yalnızca Sermaye Piyasası Kurulu (SPK) lisanslı ve denetlenen kurumlarla işlem yapmak, bilinen ve güvenilir kripto para borsalarını tercih etmek ve kişisel bilgilerini güvensiz platformlarda paylaşmaktan kaçınmak, bireysel güvenliğin temel taşlarıdır. Bireyler, kısa yoldan zenginlik vaatlerine karşı şüpheli yaklaşmalı ve herhangi bir yatırım kararını vermeden önce kapsamlı bir araştırma yapmalıdır.

Finansal Kurumların Yükümlülükleri

Finansal kurumlar, müşterilerinin güvenliğini sağlamakla yükümlüdür. Bu, sadece güçlü bir siber güvenlik altyapısı kurmakla kalmayıp, aynı zamanda müşterilerini ve çalışanlarını siber tehditler konusunda sürekli eğitmeyi de içerir. İki faktörlü kimlik doğrulama gibi gelişmiş güvenlik önlemlerini standart hale getirmeleri, yapay zekâ destekli sistemlerle şüpheli işlemleri anında tespit etmeleri ve siber tehditler hakkında sektör içi bilgi paylaşımını artırmaları gerekmektedir. Kurumlar, teknolojik savunmalarını sürekli olarak güncelleyerek dolandırıcıların yöntemlerine karşı proaktif bir duruş sergilemelidir.

Devletin Düzenleyici ve Denetleyici Rolü

Devlet, siber suçlarla mücadelede en üst düzeyde sorumluluk sahibidir. Kripto varlık piyasasına yönelik kapsamlı ve güncel bir yasal çerçevenin oluşturulması, bu alandaki dolandırıcılık suçlarının önüne geçmek için kritik bir adımdır. Yasal düzenlemeler, kripto varlık hizmet sağlayıcılarının denetimini, müşteri kimlik doğrulama süreçlerini ve şüpheli işlem bildirimlerini zorunlu hale getirmelidir. Ayrıca, dolandırıcılıkla mücadele ulusal sınırları aştığından, Europol ve FATF gibi uluslararası kuruluşlarla iş birliğinin artırılması, suçluların küresel ağlarının çökertilmesi açısından hayati önem taşımaktadır.

Akademik araştırmalar ve uluslararası raporlar da göstermektedir ki, bu suçlarla mücadele sadece ulusal düzeyde yürütülemez; küresel bir iş birliği ve bilgi paylaşımı zorunludur. Türkiye'nin 2024-2028 Ulusal Siber Güvenlik Stratejisi gibi yeni planlarla bu alanda attığı adımlar, doğru yolda olduğunun bir göstergesidir. Ancak, bu çabaların başarıya ulaşması, tüm paydaşların, yani bireylerin, kurumların ve devletin bu tehlikeye karşı topyekûn bir mücadele sergilemesine bağlıdır. Güvenli bir dijital gelecek inşa etmek, ortak sorumluluğumuzdur.

KAYNAKÇA

Resmi Gazete ve Yasal Mevzuat

1. Resmî Gazete, *Bilgi ve İletişim Güvenliği Tedbirleri Hakkında Cumhurbaşkanlığı Genelgesi (2019/12)*, Sayı: 30823, 2019
2. Resmi Gazete. *Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik*. Sayı: 31069, 2020
3. Türk Ceza Kanunu. (2004). Madde 157, 158, 243, 244. Kanun No: 5237.
4. Sermaye Piyasası Kanunu. (2012). Kanun No: 6362.

Kurum Raporları ve Yayınlar

5. Bankacılık Düzenleme ve Denetleme Kurumu. (2023). Siber Güvenlik ve Dolandırıcılık İstatistik Raporu. Ankara: BDDK Yayınları.
6. Emniyet Genel Müdürlüğü. (2023). Siber Suç İstatistikleri ve Trend Analizi. Ankara: Siber Suçlarla Mücadele Daire Başkanlığı.
7. Mali Suçları Araştırma Kurumu. (2021). Kripto Varlık Hizmet Sağlayıcıları Rehberi. Ankara: MASAK Yayınları.
8. Sermaye Piyasası Kurulu. (2022). Forex Piyasası Denetim Raporu. Ankara: SPK Yayınları.
9. T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. (2023). *Ulusal Siber Güvenlik Stratejisi ve 2024-2028 Eylem Planı*. Ankara.

Akademik Yayınlar ve Makaleler

10. Aydın, M., & Yılmaz, K. (2022). Türkiye'de Forex Dolandırıcılıkları ve Hukuki Boyut. Ankara Üniversitesi Hukuk Fakültesi Dergisi, 71(3), 45-67.
11. Demir, A. (2023). Deepfake Teknolojisinin Finansal Dolandırıcılıkta Kullanımı. İstanbul Üniversitesi Siyasal Bilgiler Fakültesi Dergisi, 50(2), 89-112.

12. Karahan, S., & Öztürk, E. (2021). Kripto Para Dolandırıcılıkları ve Türk Hukukundaki Yeri. *Banking and Finance Letters*, 12(4), 234-256.

13. Yargıtay 11. Ceza Dairesi. (2021). *E. 2021/5678, K. 2021/7890*. Ponzi Senaryoları ve Forex Dolandırıcılığı Kararı.

Uluslararası Raporlar

14. Europol. (2022). Internet Organised Crime Threat Assessment (IOCTA). Lahey: Europol Yayınları.

15. FATF. (2021). Virtual Assets and Money Laundering: Emerging Threats and Regulatory Responses. Paris: FATF Raporu.

16. OECD. (2022). Financial Literacy and Consumer Protection in Digital Finance. Paris: OECD Yayınları.

Medya ve Basın Yayınlar

17. Anadolu Ajansı. (2023, Mayıs 15). Deepfake Dolandırıcılığında Son Durum. *Ekonomi Haberleri*.

18. Hürriyet. (2023, Kasım 20). Kripto Dolandırıcılığında Artış. *Teknoloji Eki*.

Teknik Raporlar ve Konferans Bildirileri

19. Cybernews. (2023). Global Phishing Statistics 2023. Vilnius: Cybernews Araştırma Merkezi.

20. İstanbul Teknik Üniversitesi. (2022). Yapay Zekâ ve Siber Güvenlik Sempozyumu Bildiriler Kitabı. İstanbul: İTÜ Yayınları.

Web Kaynakları

21. BDDK. (2023). Lisanssız Forex Şirketleri Kara Listesi. <https://www.bddk.org.tr>

22. BTK İnternet İhbar Merkezi. (2023). Şikâyet ve İhbar İstatistikleri. <https://www.ihbarweb.org.tr>

23. TCMB. (2023). Finansal Okuryazarlık Portalı. <https://www.tcmb.gov.tr>