

Oltalama (Phishing) Suçları

Av. Burak Üçüncü · 8 Ocak 2025 · 6 dk okuma

Bilişim teknolojilerinin hızla gelişmesiyle birlikte günlük yaşamın vazgeçilmez bir parçası haline gelen internet, sunduğu olanaklar kadar belirli riskleri de beraberinde getirmiştir. Alışveriş, bankacılık, eğitim, sağlık gibi sayısız alanda işlemlerimizi çevrimiçi platformlar üzerinden yürütmek, zaman ve mekan sınırlarını büyük ölçüde ortadan kaldırmaktadır. Ancak bu kolaylık, kötü niyetli kişilerin de hedef kitlesini genişletmiş durumdadır. Dolandırıcılık faaliyetleri, internetin sağladığı anonimlik ve hızlı etkileşim özellikleriyle yeni bir boyut kazanmış ve “siber dolandırıcılık” adı altında farklı yöntemlerle karşımıza çıkmaya başlamıştır. Bu yöntemlerden belki de en yaygını ve en tehlikelisi, “oltalama” ya da literatürde bilinen adıyla “phishing” yöntemidir.

Oltalama saldırıları, hedef alınan kişilerin zafiyetlerini kullanarak onların banka hesap bilgileri, kredi kartı bilgileri, şifreleri veya kişisel verileri gibi önemli bilgilerini elde etmeye yöneliktir. Fail, çoğu zaman kurumsal bir kimlik veya güvenilir bir şirket görünümünde davranarak mağdurları kendi tuzağına düşürmeye çalışır. Bu makalede siber dolandırıcılığın oltalama (phishing) yöntemi, Türkiye’deki yasal düzenlemeler ve olası yaptırımlar ele alınacaktır.

BÖLÜM II

Oltalama (Phishing) Nedir?

Oltalama, siber suçluların mağdurlardan menfaat elde etmek için kullandıkları bir tuzak yöntemidir. Özellikle e-posta, kısa mesaj (SMS), sosyal medya mesajı, sahte web siteleri ve hatta bazen telefon aramaları aracılığıyla yürütülen bu saldırılarda amaç, kişinin kimlik bilgilerini, finansal verilerini veya diğer önemli dijital hesap bilgilerini ele geçirmektir. Oltalama girişimlerinde en sık karşılaşılan senaryoda saldırganlar, kurumsal bir şirketin veya devlet kurumunun resmi bir temsilcisiymiş (savcı, polis, avukat vs.) gibi davranmaktadır. Mağdur, örneğin bankasından geldiğini zannettiği bir e-postada, hesabının güvenliğini kontrol etmek için bağlantıya tıklamasının istendiğini görür. Bu bağlantıya tıkladığında, bankanın sitesine çok benzeyen sahte bir sayfa açılır ve kişi burada kullanıcı adı, şifre, kart numarası gibi bilgilerini girdiğinde tüm bu veriler doğrudan saldırganın eline geçer.

Oltalama yöntemleri, kimi zaman da kişiye “ödül kazandınız, hediyenizi almak için tıklayın” gibi cazip vaatlerde bulunarak yanıt verme ihtimalini artırır. Dolandırıcıların kullandığı dil, genellikle aciliyet hissi yaratma veya duyguları manipüle etme üzerine kuruludur. Kişinin hesabında olağan dışı bir hareket tespit edildiği, kredi kartı bilgilerinin çalındığı ya da beklenmeyen bir masrafın oluştuğu söylenerek panik yaratmak, oltalamada yaygın bir taktiktir. Bazen de önemli bir alıcıdan (örneğin bir iş teklifi, kargo şirketi, resmi kurum) mesaj geliyormuş gibi görünerek merak duygusunu tetiklerler.

Teknolojik imkanların artması, saldırganların daha gerçekçi e-postalar ve taklit web siteleri hazırlamasına yardımcı olmaktadır. Kimi durumlarda logolar, kurumsal renkler ve yazı tipleri dahi birebir kopyalanır. Bu nedenle, özellikle finans kuruluşlarının ya da e-ticaret platformlarının kullanıcıları, bu tür ortalama girişimleri karşısında oldukça dikkatli olmalıdır. Aksi takdirde birkaç dakikada yaşanacak bir dikkatsizlik, banka hesabınızdaki bütün birikiminizin siber suçluların eline geçmesine neden olabilmektedir.

BÖLÜM III

Hukuki Açıdan Oltalama (Phishing)

Türk hukukunda "oltalama" şeklinde ayrı bir suç tipi yer almasa da, bu yöntemle işlenen eylemler Türk Ceza Kanunu (TCK) çerçevesinde çeşitli suç kategorilerine girebilmektedir. En yaygın karşılığı, TCK'da yer alan "dolandırıcılık" suçudur. TCK madde 157'de tanımlanan basit dolandırıcılık, hileli davranışlarla başkasının malvarlığına zarar verme şeklinde özetlenebilir. Ancak internetin veya bilişim sistemlerinin kullanılması suretiyle gerçekleştirilen dolandırıcılık eylemleri, çoğu zaman TCK madde 158'de yer alan "nitelikli dolandırıcılık" kapsamına girmektedir. Zira, bilişim sistemleri, banka veya kredi kurumlarının araç olarak kullanıldığı durumlar kanunda nitelikli hal olarak düzenlenmiştir.

Oltalamayla işlenen suçlarda fail, çoğunlukla mağdurun parasını doğrudan kendi hesabına transfer etmez. Bunun yerine farklı sahte hesaplar, aracı kişiler ya da kripto para cüzdanları kullanabilir. Ancak bu yöntemler, suçun niteliğini değiştirmez; hala bir aldatma ve menfaat temini söz konusudur. Bununla birlikte, TCK madde 243 ve 244'te düzenlenen bilişim sistemine girme, sistemi engelleme veya verileri bozma gibi suçlar da önem taşır. Oltalama sürecinde fail, kişinin bilgisayarına ya da sistemine zararlı yazılım yüklemişse, veri güvenliğini tehdit edecek eylemlerde bulunmuşsa bu hükümler de devreye girebilir. Benzer şekilde, mağdurun kredi kartı veya banka kartı bilgilerini rızası dışında ele geçirmek ve kullanmak, TCK madde 245 kapsamında ayrıca "banka veya kredi kartlarının kötüye kullanılması" suçunu da oluşturabilmektedir.

Bu suçlar re'sen takibe tabi olup, kolluk kuvvetleri veya savcılıklar herhangi bir ihbar veya şikayet olduğunda soruşturma başlatmakla görevlidir. Özellikle bankalar, müşterilerinden gelen şikayetleri ciddiye alarak bu konuda adli mercilere suç duyurusunda bulunabilmektedir. Failin işlediği fiil, birden fazla suç tanımına uygun olabilir. Bu ve benzer durumlarda içtima veya zincirleme suç hükümleri devreye girerek, suçun tipine ve mahiyetine göre değerlendirme yapılmakta ve fail bu yolla cezalandırılmaktadır.

BÖLÜM IV

Soruşturma ve Kovuşturma Süreci

Siber dolandırıcılığa maruz kaldığınızı düşündüğünüz anda, en önemli adım mümkün olduğunca hızlı ve doğru biçimde şikayette bulunmaktır. Oltalama saldırısına uğradığınızı fark ettiğinizde, hileli bağlantıya tıklamış ya da bilgilerinizi girmiş olsanız bile zaman kaybetmeden bankanızı arayarak kartlarınızı iptal ettirmeniz, hesap hareketlerinizi inceletmeniz ve gerekirse çevrimiçi hizmetlerinizi geçici olarak durdurmanız yerinde olur. Ardından, elinizdeki delillerle (gönderilen e-posta, sahte web sitesi linki, ekran görüntüleri) Cumhuriyet Savcılığına başvuruda bulunabilirsiniz. E-posta veya SMS gibi dijital delilleri kaybetmeden saklamanız, dosyanın açılması aşamasında işinizi kolaylaştıracaktır.

Savcılık, şikayetinizi aldıktan sonra soruşturma başlatarak kolluk kuvvetlerini görevlendirir. Siber suçlarla ilgili kolluk birimleri; IP adresi takibi, log kayıtlarının temini, bankacılık işlem kayıtlarının incelenmesi gibi teknik incelemeler yapar. Kimileri bu süreçte kimliklerini gizlemek için VPN, Proxy veya Tor gibi

anonimleştirme araçları kullanıyor olsa da, çeşitli veri analiz yöntemleriyle failin izine ulaşmak her zaman imkansız değildir. Özellikle banka hareketlerinde, SWIFT kayıtlarında veya para transferi yapılan hesaplarda mutlaka bir iz bırakılmaktadır. Kolluk kuvvetleri, bu izlerden yola çıkarak gerçeğe ulaşmaya çalışmakta, somut olayın mahiyetine göre başarı oranı değişmektedir.

Soruşturma tamamlandığında ve fail tespit edilip eylemiyle ilgili yeterli delil elde edilince, Savcılık kamu davasını açar. Bu aşamada şüpheli, "sanık" sıfatını alır ve ceza mahkemesinde yargılanmaya başlanır. Mahkeme, delilleri inceler, varsa tanıkları ve tarafları dinler. Dolandırıcılık fiilinin bilişim sistemi aracılığıyla işlenip işlenmediği, banka-kredi kurumlarının araç olarak kullanılıp kullanılmadığı gibi hususları göz önüne alarak sanığın eyleminin hangi kanun hükmünü meydana getirdiği, suçun unsurlarının oluşup oluşmadığına ilişkin değerlendirme yapacaktır.

BÖLÜM V

Mağdurun Hakları

Siber dolandırıcılığa karşı mağdurun hakları, klasik dolandırıcılık vakalarındaki haklarla büyük ölçüde aynıdır. İster bireysel kullanıcı olun, ister bir işletme sahibi, maruz kaldığınız zararı öncelikle kanıtlamanız ve bunu soruşturmaya konu etmeniz gerekir. Oltalama saldırıları özellikle hızlı hareket etmeyi gerektirir, çünkü saldırgan elde ettiği bilgilerle anında işlem yapabilir veya başka hesaplara yönlendirme gerçekleştirebilir. Bu yüzden, mümkün olan en kısa sürede hem ilgili bankaya hem de adli makamlara haber vererek mağduriyetinizi kayıtlara geçirmeniz gerekir. Süreci takip ederken avukat desteği almak, mağdurun haklarını daha etkin biçimde koruyabilmesini sağlar. Özellikle teknik detayların bolca yer aldığı dijital soruşturmalarda, avukatın siber suçlar alanında deneyim sahibi olan [bilişim hukuku avukatı](#) olması süreci büyük ölçüde kolaylaştırabilmektedir.

Ceza davasının yanı sıra mağdur, maddi zararın tazmini için hukuki yollara da başvurabilir. Dolandırıcılık sebebiyle belirli bir miktarda para kaybına uğramışsanız, faile karşı tazminat davası açmanız mümkündür. Bu noktada, yargılama sürecinde toplanan deliller ve failin suçlu bulunması, tazminat davasında da önemli dayanaklar oluşturur. Ayrıca, bazı durumlarda bankanın veya e-ticaret sitesinin kendi sorumluluğu gündeme gelebilir. Örneğin, platform güvenlik açıklarından dolayı böyle bir siber saldırı mümkün olmuşsa ve bu durum önlenemez nitelikteyse, mağdurun tazminat talebini bu kurumlara da yöneltmesi söz konusu olabilir. Her somut olayın şartları değerlendirilerek bu konuda karar verilir.

BÖLÜM VI

Oltalama Saldırılarına Karşı Alınabilecek Tedbirler

Oltalama eylemlerinin önemli bir kısmı, kullanıcı farkındalığının düşük olduğu durumlarda başarıya ulaşır. Dolandırıcıların bir bankayı ya da kurumsal firmayı taklit etmesi, kullanıcıların gözünü korkutabilir veya kandırabilir. Bu yüzden, siber dolandırıcılıkta en büyük savunma aracı yine kullanıcıların dikkatli olması ve temel bazı kuralları bilmesidir. Bankalar veya resmi kurumlar, genellikle "Şu bağlantıya tıklayın, bilgilerinizi girin" gibi isteklerle yaklaşmaz. Gerçek kurumlar, şüpheli gördükleri bir işlemde sizi arayabilir, ama kişisel şifrelerinizi veya kart PIN numaranızı sormazlar. Kişisel verileri paylaşmadan önce mutlaka gönderen kişinin gerçekliğini doğrulamak gerekir. E-postanın uzantısına, linklerin hedefine, alıcı adresine dikkatlice bakmak birçok oltalama girişiminin maskesini düşürür.

Çoğu oltalama saldırısında zararlı linklere tıklamak, sahte web sitelerine yönlendirilmekle sonuçlanır. Bu nedenle, gelen e-postada veya mesajda acil, ivedi ifadeler varsa, sizde bir güvensizlik hissi uyanıyorsa göndericinin bilinen telefon numarasını arayarak durumu teyit edebilirsiniz. Ayrıca düzenli olarak antivirüs yazılımları kullanmak, işletim sistemi ve yazılım güncellemelerini zamanında yapmak, güçlü şifreler tercih etmek ve iki faktörlü kimlik doğrulama yöntemlerini kullanmak, oltalama yöntemlerini zora sokar. Bu basit ama etkili önlemler, dijital dünya kullanımında olmazsa olmaz hale gelmiştir.

Hukuk dünyasında bilişim suçlarıyla mücadele, hem yasal düzenlemeler hem de pratik uygulamaların sürekli güncellenmesiyle her geçen gün gelişme katetmektedir. Savcılıklar ve kolluk kuvvetleri, siber suçlar birimlerini güçlendirerek bu alandaki faaliyetlerini etkin biçimde yürütmeye çalışmaktadır. Mağduriyetin asgariye indirilmesi için ise kullanıcı farkındalığı ve temel siber güvenlik prensiplerinin bilinmesi hayati öneme sahiptir. Şüpheli bir mesaj aldığınızda veya beklenmedik bir bağlantıya tıklamanız istendiğinde durup düşünmek, büyük kayıpların önüne geçecektir. Unutmamak gerekir ki, oltalama girişimlerinin başarılı olması, çoğu zaman insan hatasının ve dikkatsizliğin bir sonucudur.

Çevrimiçi sürüm: <https://burakucuncu.com.tr/oltalama-phishing-suclari>