Sosyal Mühendisliğin Bir Türü: Telefon Dolandırıcılığı

One Type of Social Engineering: Telephone Fraud

Mustafa Okudan[1], Hatice Tuğsavul[2], Neylan Ziyalar[2]

[1] İstanbul Üniversitesi-Cerrahpaşa, Adli Tıp Enstitüsü, Tıp Bilimleri Anabilim Dalı, İstanbul, Türkiye

[2] İstanbul Üniversitesi-Cerrahpaşa, Adli Tıp Enstitüsü, Sosyal Bilimleri Anabilim Dalı, İstanbul, Türkiye

Giriş

Dünya'da ve ülkemizde; özellikle 90'lı yılların sonunda herkesin telefon sahibi olması ile beraber dolandırıcılar, kişileri telefon üzerinden kandırıp mal varlıklarını tehlikeye atmaya başlamışlardır Özellikle kendini polis, savcı, banka memuru şeklinde tanıtan suçlular; masum vatandaşların tüm şahsi bilgilerini bilgisayar korsanları sayesinde ele geçirip kamuoyu gündemini teşkil eden konular üzerinden dolandırmaktadırlar. Dolandırılanların profilleri; eğitim seviyeleri, yaş ya da toplumdaki statüsüne bakılmaksızın çok geniş bir perspektifte dağılım göstermekte ve aralarında profesör, emekli general, savcı, yüksek rütbeli polis, öğretmen, sanatçı, ev hanımları, emekliler gibi bir çok meslek grubunu etkileyen bir mağdur havuzu oluşmaktadır (1).

İstanbul Emniyet Müdürlüğü Asayiş Şube Müdürlüğü, Yankesicilik ve Dolandırıcılık Büro Amiri Başkomiser Kıvanç Taşçı dolandırıcıların kim olduğunu gazetevatan.com'a verdiği demeçte şu sözlerle tanımlamaktadır:

"Vatandaşları hipnoz eden kişiler bunlar. Telefon açıyorlar size, çok güçlü bir senaryoları var. Bugüne kadar karakolun kapısından girmemiş namuslu Vatandaşlara kurdukları senaryoyu öyle bir anlatıyorlar ki, hipnoz oluyorsunuz! ve tüm dediklerine inanmaya başlıyorsunuz. Hukuk biliyorlar, öyle terimler kullanıyorlar ki, sanıyorsunuz karşınızdaki gerçekten bir savcı ya da polis. Bir call center kuruyorlar, tüm mali bilgilerinizi size telefonda söylüyorlar.. İnandırıcı olmak için her yolu deniyorlar. Dolandırıcılık suçu komplike bir suç. Eğer suçlu profili ikna ediciyse bu konuda kabiliyete sahipse çok kolay bir şekilde kandırabiliyor. Zaten bu iknadan sonra ortaya çıkan bir suç tipi olduğu için farkındalık sonra oluşuyor. Mağduriyet sonrası farkındalık olduğundan

önlemleri içermektedir (40). Bu süreçlerin uygulamaya koyulması, sadece şirket ortamında değil, aynı zamanda kişisel düzeyde de yararlı olabilir. Bireyleri çok fazla saldırıya karşı sorumlu tutmak ya da uygun politika ve prosedürleri izlememek, insanların bu saldırıların mağdurları olmasına izin vermektedir.

Yaşanan olayların sonuçlarına göre bilincin arttırılabilmesi için eğitim gereklidir (41). Sürekli gelişen veya değişen teknolojiye uyum sağlamak için, insanların sürekli eğitime ihtiyaçları vardır. Sosyal mühendislik taktiklerinin sürekli olarak gelişmesi, eğitim süreçlerinin sürekli değişen ortamla güncel kalması için düzenli olarak yapılması gerektiğini göstermektedir (42).

Tüm çalışanlar yalnızca güvenlik için değil, aynı zamanda çok seviyeli bir savunmanın bir parçası olarak direnç göstermek konusunda eğitilmelidir. Bir organizasyondaki anahtar personel; resepsiyonistleri, sekreterleri, müşteri hizmetlerini ve asistanları içerebilir. Bu kişiler bazı açılardan ilk savunma hattı niteliğindedir. Bu eğitim konuları sadece şirketler için değil, aynı zamanda kişisel düzeyde de kullanılmaktadır. Uygun direnç eğitimi verilmesi, saldırıya maruz kalanın bilgi vermek için kolayca ikna edilmemesini sağlayacaktır (43).

Eğitim ve farkındalığının etkili bir programa dönüştürülmesi ile tüm bireylerin en güncel bilgilere sahip olmaları sağlanabilir. Saldırganlar sürekli olarak yöntemlerini değiştirmekte ve saldırılar daha karmaşık hale gelmektedir (44). Değişimlere ayak uydurmak, bir sosyal mühendislik saldırısını önlemek konusunda çok önemlidir.

Sonuç olarak, sosyal mühendislik ve bir sosyal mühendislik saldırı çeşidi olan telefon dolandırıcılığı saldırılarının devam etmesi ve durdurulamamasının bilinmesi; ancak önlenebileceğinin fark edilmesi, bu saldırıları başarılı bir şekilde anlamanın anahtarıdır. Eğitim ve farkındalık temel olarak sosyal mühendislik saldırılarını önleyen faktörlerdir. Bir kişinin sosyal mühendislik saldırılarına karşı kullanabileceği en iyi savunma, çevresindekilerin farkında olmaktır. Kişi bu konu hakkında ne kadar çok şey bilirse, şüpheli bir durumla o kadar iyi başa çıkabilir. Teknoloji ne kadar değişirse değişsin; insanlar ikna edilmeye karşı her zaman savunmasız olacaktır. Bu nedenle, bir kişinin bu tür saldırılara karşı alabileceği en iyi önlem, çevresinde olup bitenin farkında olmaktır.

Kaynakça

1. Akbal, E., Doğan, Ş., ve Varol, N., 2016 'Karar Ağaçları ile Telefon Dolandırıcılığı Verilerinin Analizi', Fırat Üniversitesi Fen ve Mühendislik Bilimleri Dergisi, 29(01): 171-177.
2. Kara, B., 07.02.2016. http://www.gazetevatan.com/dolandiricilar-15-gunlugune-oto-galeri-kuruyor-912310-pazar-vatan/ (01.05.2018)
3. Murphy, L. L., 2017, 'Fraud', Salem Press Encyclopedia

4. Cross, C., 2016, 'They're Very Lonely': Understanding the Fraud Victimisation of Seniors', International Journal of Crime, Justice and Social Democracy, 5(4): 60-75. Araştırma Deseni. Siyasal Yayınevi, Ankara.
5. Bağcı, H., 2009. Sosyal mühendislik ve denetim. Denetişim Dergisi, Kış, ss. 42-51.
6. Conteh, N.Y. and Schmick, P.J., 2016. Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks, International Journal of Advanced Computer Research, 6 (23), ss. 31-38.
7. Wright, O., 2015, Hacking without computers - an introduction to social engineering. Alıntı: https://www.contextis.com/blog/hacking-without-computers-an-introduction-to-social-engineering 21 Eylül 2017.
8. Atkins, B. ve Huang, W., 2013. A study of social engineering in online frauds. Open Journal of Social Sciences, 1(03), 23-32.
9. Barışkan, M.A., 2017. Türkiye'deki siber güvenlik bilinci ve sosyal mühendislik ataklarına karşı savunma önlemlerinin geliştirilmesi. Yüksek Lisans Tezi. İstanbul: İstanbul Üniversitesi FBE.
10. Luo, X., Brody, R., Seazzu, A. ve Burd, S., 2011. Social engineering: the neglected human factor for ınformation security management. Information Resources Management Journal, 24 (3), ss. 1-8.
11. Bağcı, H., 2009. Sosyal mühendislik ve denetim. Denetişim Dergisi, Kış, ss. 42-51.
12. Tatar, Ü., 2011. Sosyal mühendislik saldırıları. 4. Ağ ve Bilgi Güvenliği Sempozyumu, 25-26 Kasım, TÜBİTAK-BİLGEM.
13. Akca, M.A., 2016. Sosyal mühendislik ile yapılan saldırıların doğal dil işleme teknikleri ile engellenmesine yönelik web servis geliştirilmesi. Selçuk Üniversitesi Mühendislik Fakültesi Dergisi, 4 (2), ss. 111-120.
14. Mitnick, K.D. ve Simon, W.L., 2006. Aldatma sanatı, Nejat Eralp Tezcan (Çev.). Ankara: ODTÜ Yayıncılık.
15. Luo, X., Brody, R., Seazzu, A. ve Burd, S., 2011. Social engineering: the neglected human factor for ınformation security management. Information Resources Management Journal, 24 (3), ss. 1-8.
16. Bağcı, H., 2009. Sosyal mühendislik ve denetim. Denetişim Dergisi, Kış, ss. 42-51.
17. Luo, X., Brody, R., Seazzu, A. ve Burd, S., 2011. Social engineering: the neglected human factor for ınformation security management. Information Resources Management Journal, 24 (3), ss. 1-8.
18. Çatak, F.Ö., 2016. Bilgi toplama ve sosyal mühendislik ders notları. İstanbul: İstanbul Şehir Üniversitesi.
19. Bayraktar, G., 2014. Harbin beşinci boyutunun yeni gereksinimi: siber istihbarat. Güvenlik Stratejileri Dergisi, 10 (20), ss. 119-147.
20. Barışkan, M.A., 2017. Türkiye'deki siber güvenlik bilinci ve sosyal mühendislik ataklarına karşı savunma önlemlerinin geliştirilmesi. Yüksek Lisans Tezi. İstanbul: İstanbul Üniversitesi FBE.
21. Hafızoğulları, Z., 2011. Türk ceza hukukunda dolandırıcılık suçları. Ankara Üniversitesi Yayınları.
22. Soyaslan, D. 2010. Ceza hukuku özel hükümler, Yetkin Yayınları, Ankara.
23. Bilen, M., 2012. Türk Ceza Hukuku'nda dolandırıcılık suçu. Doktora Tezi. Konya: Selçuk Üniversitesi SBE.
24. Yılmaz, A., 2015. Türkiye deki dolandırıcılık tipolojileri: dolandırıcılık olaylarının kategorik tasnifi ve yapılış şekilleri. Hacettepe Üniversitesi Sosyolojik Araştırmalar E-Dergisi, ss. 1-26.
25. Can, E.G., 2014. Dolandırıcılık suçu. Yüksek Lisans Tezi. Ankara: Çankaya Üniversitesi SBE.
26. Dursun, H., 2016. Türk ceza hukukunda dolandırıcılık suçu. Doktora Tezi. Ankara: Ankara Üniversitesi SBE.
27. Dursun, H., 2016. Türk ceza hukukunda dolandırıcılık suçu. Doktora Tezi. Ankara: Ankara Üniversitesi SBE.
28. Acılar, A. ve Baştuğ, A., 2016. İşletmelerde bir bilgi güvenliği tehdidi olarak sosyal mühendislik. Global Business Research Congress (GBRC), May 26-27, Istanbul, Turkey.
29. Yılmaz, A., 2015. Türkiye deki dolandırıcılık tipolojileri: dolandırıcılık olaylarının kategorik tasnifi ve yapılış şekilleri. Hacettepe Üniversitesi Sosyolojik Araştırmalar E-Dergisi, ss. 1-26.
30. Yılmaz, A., 2015. Türkiye deki dolandırıcılık tipolojileri: dolandırıcılık olaylarının kategorik tasnifi ve yapılış şekilleri. Hacettepe Üniversitesi Sosyolojik Araştırmalar E-Dergisi, ss. 1-26.
31. Altun, İ., 2016. Ortam Sanal Suç Gerçek.İskenderiye Kitap, İstanbul.
32. Cho, J. H., Cam, H., ve Oltramari, A., 2016. Effect of personality traits on trust and risk to phishing vulnerability: Modeling and analysis. in Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), 2016 IEEE International Multi- Disciplinary Conference, 7-13. IEEE. doi: 10.1109/COGSIMA.2016.7497779

33. Darwish, A., Zarka, A. E., ve Aloul, F., 2012. Towards understanding phishing victims' profile. in Computer Systems and Industrial Informatics (ICCSII), 2012 International Conference on, IEEE, 1-5.
34. Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F. ve Downs, J. 2010. Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 373-382. ACM.
35. Scheeres, J. W., 2008. Establishing the human firewall: Reducing an individual's vulnerability to social engineering attacks. Alıntı: http://www.dtic.mil/docs/citations/ADA487118
36. Akbal, E., Doğan, Ş., ve Varol, N., 2016 'Karar Ağaçları ile Telefon Dolandırıcılığı Verilerinin Analizi', Fırat Üniversitesi Fen ve Mühendislik Bilimleri Dergisi, 29(01): 171-177.
37. Türkiye Bankalar Birliği, Dolandırıcılık Eylemleri ve Korunma Yöntemleri, Aralık 2015.
38. Bağcı, H., 2009. Sosyal mühendislik ve denetim. Denetişim Dergisi, Kış, ss. 42-51.
39. T.C. Sağlık Bakanlığı, 2015. Sosyal mühendislik zafiyetleri ve sosyal medya güvenliği. 16 Aralık.
40. Baker, A. ve Matar, A. (Eds.) 2011. Threat: Palestinian political prisoners in Israel. Pluto Press.
41. Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F. ve Downs, J. 2010. Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 373-382. ACM.
42. Abraham, S., ve Chengalur-Smith, I., 2010. An overview of social engineering malware: Trends, tactics, and implications. Technology in Society, 32 (3), 183-196.
43. Gragg, D., 2002. A multi-level defense against social engineering. Alıntı: http://taupe.free.fr/book/psycho/social%20engineering/Social%20Engineering%20-%20Sans%20Institute%20-%20Multi%20Level%20Defense%20Against%20Social%20Engineering.pdf
44. Kellyk, 2016. Social engineering basics: How to educate your staff. Alıntı. https://www.tracesecurity.com/blog/social-engineering-for-dummies-how-to-educate-your-staff#.Wf47U1uCxdg