Co-funded by the Erasmus+ Programme of the European Union

InCyT Eğitim Modülleri

Çalışanlar için Bilgi Güvenliği **Ünite No: (4) 7. Hafta** **Birim (Modül) adı: (Sosyal Mühendislik)**	
Öğrenme Aktiviteleri	❑**Web semineri** ❑**Alıştırmalar** ❑ **Çalıştay** ❑ **Sunum** ❑ **Diğer** Streaming Webinar, Metin, Öz Değerlendirme Alıştırmaları, Tartışma forumlarında ve eğitmen/mentor ile düzenlenen oturumlarda cevaplarla alıştırmalar, e-portfolyolar
Öğrenme Sorumlusu	• David Sommer · • Ileana Hamburg
Öğrenme Etkinliği Hedefleri	1. Sosyal mühendislik saldırı teknikleri 2. Sosyal Mühendislik Eğitiminin Önemi 3. Kimlik Avı Saldırılarından Nasıl Korunursunuz? 4. Disiplinlerarası bir bakış açısıyla sosyal mühendislik
Kazanılacak Beceriler	• **TS3 Ağ güvenliği** • **TS4 Penetrasyon (istismar edilebilir güvenlik açıkları) testi** • **SS3 Bilişsel ve davranış analizi**
Öğrenme aktivitesinin süresi	2 hafta
Öğrenme rdonatımları	***Neye ihtiyaç var?*** • İnternet erişimi • İnternet Tarayıcısı • MS Office365

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Modül hakkında kısa bilgi

Giriş
Sosyal mühendislik, bilgi güvenliği için önemli ve çok sık bir tehdittir. Bu modül, sosyal mühendisliğin yaşam döngüsünü, bir saldırının nasıl gerçekleştiğini ve önlenebileceğini kısaca açıklamaktadır. Özellikle kimlik avı, en popüler sosyal mühendislik saldırılarından biri olarak tanımlanmaktadır. Birçok şirket saldırıları önlemek için teknik çözümler kullanır, ancak personel eğitimli değilse teknolojik önlemler çok etkili değildir. Bu birimin amaçlarından biri de budur. Öğrenciler, ilgili metni okuyarak, akış web seminerlerini izleyerek ve alıştırmaları kendi hızlarında çözerek bu yönler hakkında bilgilendirilebilirler. Tüm bu dokümanlar dijital interaktif proje platformundadır. Öğrenciler cevaplarını Öz değerlendirme alıştırmalarında test edebilirler. Diğer alıştırmalarla ilgili cevaplar ilgili tartışma forumuna kaydedilmeli ve haftada bir kez ortak organize toplantıda mentorla tartışılmalıdır. Öğrenci, özellikle toplantılar sırasında diğerleriyle işbirliği içinde çalışabilir ve mentorluk yapabilir. Eğitimin yansıtılması ve değerlendirilmesi için önemli olan e-portfolyo geliştirmeleri desteklenecektir.

Öğrenme Materyalinin İçeriği

Sosyal mühendislik nedir?

Sosyal mühendislik, saldırganın elde edememesi gereken verilere, belgelere ve bilgilere erişmek için çoğu zaman psikolojik yöntemler kullanarak insanları manipüle etmek olarak tanımlanabilir. Yıllar önce çeşitli sosyal mühendislik biçimleri bulunabilir, ancak teknolojinin iş ve yaşamın ana yönlerinde artan kullanımı nedeniyle, tehditler büyür ve durdurulması zor karmaşık bir süreç haline gelir. Sosyal mühendislik, günümüzde bilgi güvenliğine yönelik önde gelen tehditlerden biridir ve etkili bir siber suç biçimidir. Başarılı bir sosyal saldırının potansiyel yansımaları insanlar ve kuruluşlar için çok tehlikeli olabilir. Örneğin, 2019'da, bir tür sosyal mühendislik suçu olan kimlik avı, diğer tüm saldırı türlerinden daha fazla birçok veri ihlalinden sorumluydu.

Birçok sosyal mühendislik saldırısında mali scoplar ve sop örgütleri önemli miktarda para kaybetti. Örneğin, FBI'a göre 2020'de ABD 4,2 milyar dolar zarar etti (Abbate, 2020).

Şirketler iş kesintisine maruz kalabilir - verimlilik kaybı, çalışanların moralinde bir düşüş ve organizasyonun toparlanması için zorluklar. Bu sürecin sonuçları olabilir, genellikle bir olay müdahale ekibi kovulur, gelecekteki saldırıları önlemeye yardımcı olacak güvenlik yazılımı sağlanmalı ve çalışanlar yeniden kalifiye edilmelidir. Şirketler, bir sosyal mühendislik saldırısı

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

durumunda itibar kaybına da uğrayabilirler çünkü müşteriler kuruluşun kendisini koruyabileceğine ikna olmuyorlar.

Sosyal Mühendislik Eğitiminin Önemi

Oksiyal mühendisliğine karşı korunmak zordur,çünkü saldırganların kullandığı taktikler bireylerin davranışlarına dayanır ve çalışanların sosyal mühendislik saldırılarını tanımak için karşılık gelen eğitimleri yoksa, kurban düşme riski büyüktür.

Sosyal mühendislik eğitimi, güvenlik farkındalığı programlarına dahil edilebilir ve çalışanlara bu tür saldırıları tanımak ve hem kendilerini hem de organizasyonlarını korumak için ihtiyaç duydukları bilgi ve araçları verir (Weßelmann, 2008).

Tehditlerin en aza indirilmesinde sosyal mühendislik eğitiminin önemi nedeniyle, başta daha az kaynağa sahip olan KOBİ'ler olmak üzere birçok kuruluşun, sosyal mühendislik de dahil olmak üzere siber farkındalık eğitimini çok ciddiye almalarına ve çalışanlarına takip etme olanakları sunmalarına yardımcı olunmalıdır (Mimecast Katkıda Bulunan Yazar, 2021).

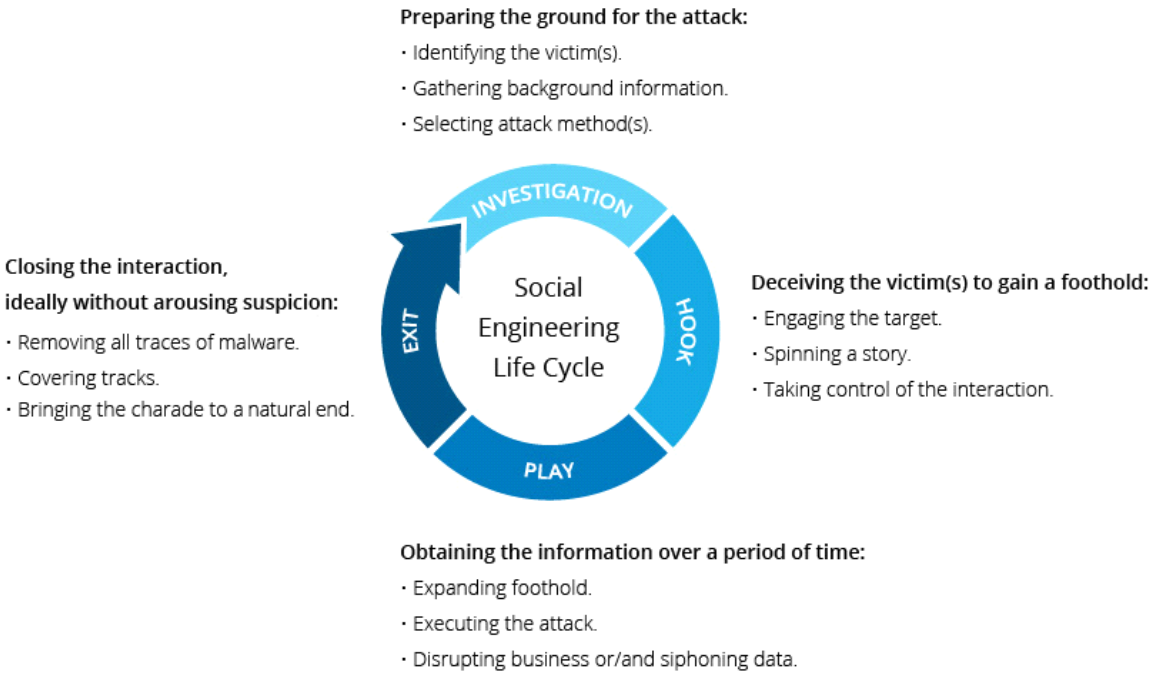
Örneğin, 2022 yılına kadar büyük kuruluşların %60'ının güvenlik bilincini dikkate alması planlanmaktadır (SAT 2019 için Gartner Magic Quadrant).

Sosyal Mühendislik Saldırısı Yaşam Döngüsü

Genellikle sosyal mühendislik saldırıları daha fazla adımda yapılır. Saldırgan önce saldırı için gerekli olan giriş noktaları ve zayıf güvenlik protokolleri gibi gerekli arka plan bilgilerini toplamak için hedeflenen kurbanı araştırır. Ardından, saldırgan kurbanın güvenini kazanmaya çalışır ve hassas bilgi haline gelme veya kritik kaynaklara erişim izni verme gibi genellikle güvenlik uygulamaları olmayan eylemler için uyaranlar sağlar. Şekil 1'de bir saldırının yaşam döngüsü açıklanmaktadır.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union



Şekil 1: Saldırı Yaşam Döngüsü (https://www.iacpcybercenter.org/resource-center/what-is-cyber-crime/cyber-attack-lifecycle/)

Social mühendisliği özellikle tehlikelidir, çünkü yazılım ve işletim sistemlerindeki güvenlik açıklarına değil, daha çok insan hatasına dayanmaktadır. Meşru kullanıcılar tarafından yapılan m istake'leri tahmin etmek, bunları tanımlamak ve durdurmak kötü amaçlı yazılım tabanlı bir müdahaleden daha zordur.

Sosyal mühendislik saldırı teknikleri

Sosyal mühendislik saldırıları farklı biçimlere sahiptir ve insan etkileşiminin dahil olduğu her yerde yapılabilir. Dijital sosyal mühendislik saldırılarının en yaygın biçimleri şunlardır:

Baiting

Yemleme saldırıları, kurbanın merakını yakalamaya çalışır. Kullanıcıları kişisel bilgilerini çalan veya sistemlerine kötü amaçlı yazılım bulaştıran bir tuzağa çekerler. En sık yemleme şekli, kötü amaçlı yazılımları dağıtmak için fiziksel medya kullanır. Örneğin, kötü amaçlı yazılım bulaşmış flash sürücüler, potansiyel kurbanların onları gördüğünden emin olunan göze çarpan alanlarda (örneğin, banyolar, asansörler, hedeflenen bir şirketin otoparkı). Yem, şirketin bordro listesi olarak sunan bir etiket gibi otantik bir görünüme sahiptir. Kurbanlar yemi alır ve bir iş veya ev bilgisayarına yerleştirir, bu da sisteme otomatik bir kötü amaçlı yazılım yüklemesine neden olur. Yemleme saldırıları mutlaka fiziksel dünyada yapılmaz. Çevrimiçi yemleme biçimleri , kullanıcıları kötü

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

amaçlı yazılım bulaşmış bir uygulamayı indirmeye teşvik eden kötü amaçlı sitelere yönlendiren cazip reklamlardan oluşur.

Korkutma Yazılımı

Kurbanlar yanlış alarmlar ve hayali tehditler haline gelir. Kullanıcılar sistemlerine kötü amaçlı yazılım bulaştığını düşünür ve yalnızca saldırgan için yararı olan veya kötü amaçlı yazılımın kendisi olan yazılımları yüklemeleri gerekir. Scareware, aldatma yazılımı, hileli tarayıcı yazılımı ve dolandırıcılık yazılımı olarak kabul edilir. Yaygın bir korkutma yazılımı örneği, web'de gezinirken kendi tarayıcınızda "Bilgisayarınıza zararlı casus yazılım programları bulaşmış olabilir" gibi metinlerle meşru görünen açılır pencere afişleridir. Ya aracı yüklemeyi (genellikle kötü amaçlı yazılım bulaşmış) ya da kurbanı kendi bilgisayarına virüs bulaşacağı kötü amaçlı bir siteye yönlendirmeyi önerir. Scareware ayrıca, kullanıcılara değersiz / zararlı hizmetler satın almalarını sağlayan spam e-posta yoluyla da dağıtılır.

Pretexting

Attacker, yalanlar aracılığıyla bir dizi aracılığıyla bilgi edinir. Dolandırıcılık (dolandırıcılık) genellikle kritik bir görevi yerine getirmek için bir mağdurdan hassas bilgilere ihtiyaç duyan bir fail tarafından başlatılır. Saldırgan genellikle iş arkadaşlarını, polisi, banka ve vergi yetkililerini veya bilme hakkına sahip diğer kişileri taklit ederek kurbanlarıyla güven kurarak başlar. Saldırgan, kurbanın kimliğini doğrulamak için gerekli olan soruları sorar ve bu sayede önemli kişisel verileri toplar. Bu sahtekarlık kullanılarak birçok önemli bilgi ve kayıt toplanabilir, örneğin sosyal güvenlik numaraları, kişisel adresler ve telefon numaraları, telefon kayıtları, personel tatil tarihleri, banka kayıtları ve hatta fiziksel bir tesisle ilgili güvenlik bilgileri.

Kimlik avı

En popüler sosyal mühendislik saldırı türlerinden biridir; Kimlik avı dolandırıcılığı (sahtekarlık), mağdurlarda merak veya korku uyandırmayı ve onları hassas bilgiler vermeye, kötü amaçlı web sitelerine bağlantılara tıklamaya veya kötü amaçlı yazılım içeren ekleri açmaya teşvik etmeyi amaçlayan e-posta ve kısa mesaj kampanyalarıdır. Bir örnek, çevrimiçi bir hizmetin kullanıcılarına gönderilen ve gerekli parola değişikliği gibi acil işlem gerektiren bir politika ihlali konusunda onları uyaran bir e-postadır. Yasal olmayan bir web sitesine bir bağlantı içerir - görünüşte meşru sürümüyle neredeyse aynıdır - ve kullanıcı mevcut kimlik bilgilerini ve yeni şifresini girer. Bilgiler saldırgana gönderilir. Kimlik avı kampanyalarında birçok kullanıcıya aynı veya neredeyse aynı iletiler gönderildiğinden, tehdit paylaşım platformlarına erişimi olan posta sunucuları için bunları algılamak ve engellemek daha kolaydır.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Spear kimlik avı

Bu, kimlik avı saldırısının özel bir biçimidir, çünkü saldırgan belirli kişileri veya kuruluşları seçer. Saldırganlar, saldırılarını daha az belirgin hale getirmek için mesajlarını kurbanlarının özelliklerine, iş pozisyonlarına ve bağlantılarına uyarlar. Mızraklı kimlik avı, failden (yasadışı eylemi gerçekleştiren kişi) daha fazla çaba gerektirir ve hazırlanması haftalar ve aylar sürebilir. Bu tür saldırıları tespit etmek çok zordur ve daha iyi başarı oranlarına sahiptirler. Örnek olarak, mızraklı kimlik avı senaryosu, (mevcut) bir kuruluşun BT danışmanı olarak bir veya daha fazla çalışana e-posta gönderen bir saldırganı içerir. Tam olarak danışmanın normalde yaptığı gibi imzalanır ve alıcılar bunun gerçek bir mesaj olduğunu düşünür. İleti, kurbanların parolalarını değiştirmelerini gerektirir ve onlara saldırganın kimlik bilgilerini çaldığı kötü amaçlı bir sayfaya yönlendiren bir bağlantı sağlar.

Kimlik Avını Algılama

Dolandırıcılar (hileli iş yapan kişiler), kişisel bilgilerini iletmeleri için kişileri kandırmak amacıyla e-posta veya kısa mesajlar kullanır. Parolaları, hesap numaralarını veya sosyal güvenlik numaralarını çalmaya çalışırlar. Bu bilgileri alırlarsa e-postaya, bankaya veya diğer hesaplara erişebilirler. Dolandırıcılar her gün olduğu gibi binlerce kimlik avı saldırısı başlatır ve genellikle başarılı olurlar. Dolandırıcılar genellikle taktiklerini günceller, ancak kurbanların kimlik avı e-postasını veya kısa mesajını tanımasına yardımcı olan aşağıdaki gibi bazı işaretler vardır:

- Kimlik avı e-postaları ve kısa mesajları, tanıdığınız veya güvendiğiniz bir şirketten geliyormuş gibi görünebilir. Bir bankadan, kredi kartı şirketinden, sosyal ağ sitesinden, çevrimiçi ödeme web sitesinden veya uygulamasından veya çevrimiçi bir mağazadan geliyormuş gibi görünürler.
- Kimlik avı e-postaları ve kısa mesajları genellikle kurbanları bir kişi bağlantısına tıklamaları veya bir eki açmaları için kandırmak için bir hikaye anlatır. Bazı şüpheli etkinlikler veya giriş girişimleri fark ettiklerini söyleyebilir, hesap veya ödeme bilgileriyle ilgili bir sorun olduğunu iddia edebilir, bu kişinin bazı kişisel bilgilerini onaylaması gerektiğini, sahte bir fatura eklemesi gerektiğini, kişinin ödeme yapmak için bir bağlantıya tıklamasını istediğini, kişinin devlet parası için kaydolmaya uygun olduğunu söyleyebilir, ve saire.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Şekil 2'de kimlik avının gerçek dünyadaki bir örneği gösterilmektedir.

E-posta, kişinin bildiği ve güvenebileceği bir şirketten geliyor gibi görünüyor: Netflix. Hatta bir Netflix logosu ve başlığı bile kullanıyor.

E-postada, faturalandırma sorunu nedeniyle kendi hesabınızın beklemede olduğu belirtiliyor.

E-postada genel bir selamlama var, "Merhaba Sevgilim." Kişinin işletmede bir hesabı varsa, muhtemelen böyle bir genel selamlama kullanmaz.

E-posta, kişiyi ödeme ayrıntılarınızı güncellemek için bir bağlantıya tıklamaya davet eder.

Bu e-posta gerçek görünebilir, ancak gerçek değildir. Bunun gibi e-postalar gönderen dolandırıcıların, taklit ettikleri şirketlerle hiçbir ilgisi yoktur. Kimlik avı e-postaları, dolandırıcılara bilgilerini veren kişiler için gerçek sonuçlar doğurabilir. Ayrıca, sahtekarlık yaptıkları şirketlerin itibarına zarar verebilirler.

Kimlik avına karşı koruma

Kendi e-posta spam filtreleri, birçok kimlik avı e-postasını kendi gelen kutusundan uzak tutabilir.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Ancak dolandırıcılar her zaman spam filtrelerini geride bırakmaya çalışırlar, bu nedenle ekstra koruma katmanları eklemek yararlıdır.

Koruma yöntemleri:

- Güvenlikyazılımı kullanarak kendi bilgisayarını döndürmek için, yazılım güvenlik tehditleriyle başa çıkmak için otomatik olarak güncellenmelidir.
- Kendi cep telefonunu p rotect etmek için, yazılım otomatik olarak güncellenmelidir.
- Kendi hesaplarını protect etmek için çok faktörlü kimlik doğrulama kullanılmalıdır.

Kendi hesabında oturum açmak için ek kimlik bilgileri şu şekilde gruplandırılabilir:

- Parola, bir kimlik doğrulama uygulaması veya bir güvenlik anahtarı aracılığıyla alınır.
- Kendi parmak izinin, retinanın veya yüzün taranması.

Çok faktörlü kimlik doğrulama, dolandırıcıların karşılık gelen kullanıcı adı ve şifreyi almaları durumunda diğer hesaplarda oturum açmalarını zorlaştırır. Kendi verilerini, kendi ev ağına bağlı olmayan yedeklemelerle korumak önemlidir. Kendi computer dosyaları harici bir sabit sürücüye veya bulut depolama alanına kopyalanmalıdır. Ayrıca, kendi telefonundaki veriler kopyalanmalıdır.

Kimlik Avı Saldırısından Şüphelenen Bir Kişiye Karşı Harekete Geçme

- Bir bağlantıya tıklamanızı veya eki açmanızı isteyen bir e-posta veya kısa mesaj gelirse şu soruyu sorun: Şirkette hesabım var mı veya benimle iletişime geçen kişiyi tanıyor muyum?
- Cevabınız "Hayır" ise, bu bir kimlik avı dolandırıcılığı olabilir. Kimlik avını tanıma, kimlik avı dolandırıcılığının belirtilerini arama, mesajı bildirme ve ardından silme bölümündeki ipuçlarını gözden geçirmeniz gerekir.
- Cevabınız "Evet" ise, bilgileri e-postaya koymadan bir telefon numarası veya gerçek bir web sitesi kullanarak şirketle iletişime geçin, çünkü birttachments ve bağlantılar zararlı kötü amaçlı yazılım yükleyebilir.

Kimlik Avı E-postasına Yanıt Verme

Kaybedilen bilgilere dayanarak atılması gereken belirli adımlar vardır

- Bir tarama çalıştırın.
- Kimlik avı e-postası veya kısa mesajı alınırsa bildirin.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Disiplinlerarası bir bakış açısıyla sosyal mühendislik

Ağ bağlantılı günümüz dünyası ve internetin ve teknolojinin yoğun kullanımı, sosyal mühendislik saldırıları için katalizörlerdir. Sistem korumaları, bazı sosyal mühendislik saldırılarını hafifletmek için yararlıdır, ancak yeterli değildir. Federal Soruşturma Bürosu'nun internet suçları, sosyal mühendislik ve iş e-posta dolandırıcılık planlarının artan kullanımının son birkaç yılda milyarlarca dolarlık kayıplara neden olduğunun altını çizdi (Abbate, 2020). Yine, bilgisayar korsanlarının yöntemleri, bu fenomeni ve tüm karmaşıklıklarını, özellikle işletmeleri nasıl etkilediği bağlamında anlamak için disiplinlerarası bir yaklaşım kullanmak gerekir. Lyinelemeli incelemeler, farklı disiplinlerden bakış açılarını vurgulamaktadır: bilgi teknolojisi, psikoloji, iş ve etik. Şekil 3 bu görüşü göstermektedir (Washo, 2021).

Bilgi teknolojileri disiplini

Sosyal mühendislik, gerçek bilgi sistemleri ve bunların işletmedeki kullanımları bağlamında tartışılamaz. Teknik savunmalar bir risk azaltma biçimi olarak kullanılabilir ve kontrol stratejilerinin kullanılması önerilir. Çok faktörlü kimlik doğrulama, kuruluşların sistemlere erişen kişinin gerçekten bu erişime sahip olması gerektiğini onaylaması için yaygın ve genellikle etkili bir yoldur. Örneğin, kullanıcı adı ve parola içeren bir oturum açma işlemi, kullanıcının kimliğinin doğrulanması için bir yol olacaktır. Ek bir faktör, kullanıcıyı daha fazla doğrulamak için sanal özel ağ (VPN) oturum açma işleminin kullanılması olabilir.

Psikoloji disiplini

Sosyal mühendislik aldatma ile bağlantılıdır, bu nedenle kavramı anlamaya yönelik psikolojik bir yaklaşım, hem saldırganın hem de mağdurun düşüncelerini ve davranışlarını anlamak için önemlidir. Psikolojik yöntemlerin kullanımı sosyal mühendislik için önemlidir, çünkü davetsiz misafirleri tanımlamak için kullanılan güvenlik duvarları ve sistemler gibi korumaları desteklemek için kullanılırlar (Bullee, Montoya, Pieters, Junger, & Hartel, 2018). Belirli bir şirketteki tüm bilgi teknolojisi ağı, yalnızca belirli bir sistemin bireysel kullanıcısı kadar güçlüdür. Aslında, çalışanların davranışları ve eylemleri, veri ihlallerinin önde gelen nedenlerinden biridir.

İş Perspektifi

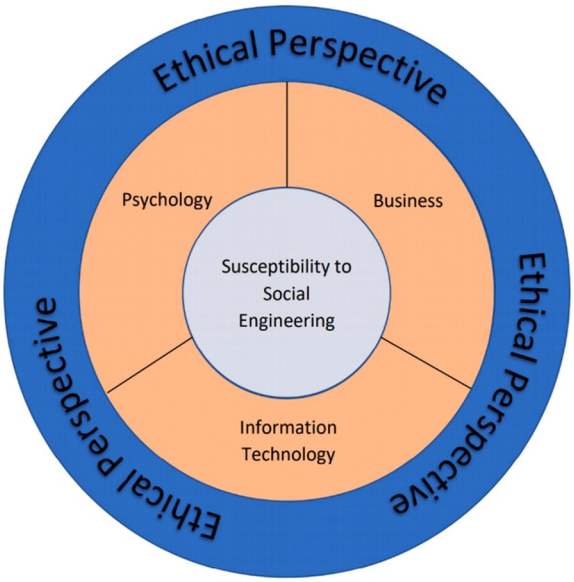
Sosyal mühendislik birçok işletme türünü etkiler ve kuruluşların yapılandırılma ve yönetilme şekli üzerinde etkileri vardır. Konu, sosyal mühendislik saldırılarını etkileyen faktörleri belirlemek için iş perspektifinden ele alınabilir. Bu bakış açısı, aşağıdaki iş alanlarıyla ilgiliyse faydalıdır: eğitim ve gelişim, belgelenmiş politikalar, iç denetim prosedürleri, bütçeler ve organizasyon kültürü. Bu alanlardan herhangi birindeki eksiklik saldırılara katkıda bulunabilir.

Etik Bakış Açısı

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Etik, sosyal mühendislik ve konuyla ilgili araştırmalar bağlamında önemlidir. Başka bir insanı manipüle etme fikri birçok etik ilkeyi ihlal eder. Bir sosyal mühendislik olayı olması durumunda, mağdurların tedavisi değişebilir, ancak çoğu zaman, saldırının gerçekleşmesine izin vermek için yeterli muamele edilmezler. Ne yazık ki, genellikle ideal çalışanlarda bulunan güven, yöneticiler, müşteriler, iş arkadaşları ve ziyaretçiler gibi başkalarını memnun etme istekliliği ve otoriteye uymaya hazır olma gibi nitelikler genellikle bir bireyi sosyal mühendisliğe duyarlı kılan özelliklerle aynıdır (Mouton, Malan, Kimppa, & Venter, 2015).



Şekil 3: Disiplinlerarası bir bakış açısıyla sosyal mühendislik (Washo, 2021)

Farklı disiplinlerden literatür taraması, karmaşık sosyal mühendislik konusunu incelemek için entegre bir yaklaşıma duyulan ihtiyacı açıklamaktadır. Her disiplin, konunun nasıl anlaşılacağı ve yorumlanacağı, çeşitli saldırı türlerine karşı korunma ve sosyal mühendisliğin hem insani hem de örgütsel açıdan etkisinin nasıl anlaşılacağı hakkında bilgi sağlar. Bununla birlikte, her disiplinin konuyu yorumlaması yalnızca diğer disiplinler bağlamında bakıldığında yararlıdır.

Soru:

Sorular Tartışma Forumu kısa bir açıklama ile cevaplandırılacaktır. Mentorluk oturumları sırasında cevaplar mentor ile tartışılacaktır.

1. Kimlik Avı nasıl tanınır: yani Kimlik avı e-postaları ve kısa mesajları genellikle kurbanların bir bağlantıya tıklamasını veya bir eki açmasını belirlemek için bir hikaye anlatır.
2. Kimlik Avı Saldırılarından Nasıl Korunursunuz?

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

3. Lütfen Sosyal Mühendislik ile bağlantılı bazı disiplinleri adlandırın ve bu bağlantıları kısaca açıklayın.

Ekler:

1. Sunum
2. Video filmler

Başvuru:

Abbate, P., (2020). İnternet Suçları Raporu 2020 URL'si: (https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf)

Bullee, J., Montoya, L., Pieters, W., Junger, M., HYPERLINK "http://refhub.elsevier.com/S2451-9588(21)00074-9/sref14"&HYPERLINK "http://refhub.elsevier.com/S2451-9588(21)00074-9/sref14" Hartel, P. (2018). Sosyal mühendislik saldırılarının anatomisi üzerine: Başarılı atakların literatüre dayalı diseksiyonu. KÖPRÜ "http://refhub.elsevier.com/S2451-9588(21)00074-9/sref14"Araştırmacı Psikoloji ve Suçlu Profilleme Dergisi, 15 KÖPRÜ "http://refhub.elsevier.com/S2451-9588(21)00074-9/sref14"(1), 20KÖPRÜ "http://refhub.elsevier.com/S2451-9588(21)00074-9/sref14"–45.

Lee, T. (2020). Daha iyi güvenlik farkındalığı için doğru öğretmenleri işe alın. URL: https://www.gartner.com/smarterwithgartner/hire-the-right-teachers-for-better-security-awareness

Mimecast Katkıda Bulunan Yazar (2021). Emploeyees için Sosyal Mühendislik Farkındalık Eğitimi. URL: https://www.mimecast.com/blog/what-is-social-engineering/

Mouton, F., Malan, M., Kimppa, K., & Venter, H. (2015). Sosyal mühendislik araştırmalarında etiğin gerekliliği. Bilgisayar ve Güvenlik, 55, 114–127. https://doi.org/10.1016/j. KÖPRÜ "https://doi.org/10.1016/j.cose.2015.09.001"cose.2015.09.001

Washo, A. (2021). Sosyal mühendisliğe disiplinlerarası bir bakış: Araştırma için harekete geçme çağrısı. URL: https://www.researchgate.net/publication/353448049_An_interdisciplinary_view_of_social_engineering_A_call_to_action_for_research

Weßelmann, B. (2008). Sosyal mühendisliğe karşı önlemler: Eğitim, farkındalık önlemlerini tamamlamalıdır. İçinde: Datenschutz und Datensicherheit. DuD. 601–604.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.