Zapobieganie inżynierii społecznej

Większość, jeśli nie wszystkie, poważnych naruszeń, które miały miejsce w ostatnich latach, dotyczyła jakiegoś elementu inżynierii społecznej. Nie pozwól, aby przebiegli przestępcy oszukali Ciebie lub Twoich bliskich. W tym rozdziale dowiesz się, jak się chronić

Nie ufaj technologii bardziej niż ludziom

Czy podałbyś swoje hasło do bankowości internetowej przypadkowemu nieznajomemu, który poprosiłby Cię o nie po tym, jak podszedł do Ciebie na ulicy i powiedział, że pracuje dla Twojego banku? Jeśli odpowiedź brzmi „nie" - jak z pewnością powinno być - musisz wykazać się takim samym brakiem zaufania, jeśli chodzi o technologię. Fakt, że na Twoim komputerze wyświetla się wiadomość e-mail wysłana przez jakąś stronę, która twierdzi, że jest Twoim bankiem, a nie przypadkowa osoba, która zbliża się do Ciebie na ulicy i zgłasza podobne roszczenie, nie jest powodem, aby dawać temu e-mailowi więcej zaufania, niż byś przyznał nieznajomy. Krótko mówiąc, nie dajesz ofert od nieznajomych, którzy zbliżają się do Ciebie na ulicy, na korzyść wątpliwości, więc nie rób tego w przypadku ofert przesyłanych drogą elektroniczną - mogą one być jeszcze bardziej ryzykowne.

Rodzaje ataków socjotechnicznych

Ataki phishingowe są jedną z najczęstszych form ataków socjotechnicznych. Ataki phishingowe czasami wykorzystują technikę zwaną pretekstem, w której przestępca wysyłający wiadomość phishingową fabrykuje sytuację, która zarówno zyskuje zaufanie celów, jak i podkreśla przypuszczalną potrzebę szybkiego działania zamierzonych ofiar. W e-mailu phishingowym pokazanym na Rysunku 8-1 zwróć uwagę, że nadawca podszywając się pod bank Wells Fargo, umieścił w e-mailu łącze do prawdziwego Wells Fargo, ale nie udało mu się odpowiednio ukryć adres wysyłkowy. W Części 2 omówiono typowe formy ataków socjotechnicznych, w tym wiadomości e-mail typu spear phishing, smishing, smishing, spear smishing, vishing, spear vishing i oszustwa CEO. Popularne są również dodatkowe typy ataków socjotechnicznych:

* Przynęta: osoba atakująca wysyła wiadomość e-mail lub wiadomość na czacie - a nawet publikuje post w mediach społecznościowych, w którym obiecuje komuś nagrodę w zamian za wykonanie jakiejś czynności - na przykład mówiąc osobie docelowej, że jeśli wypełni ankietę, otrzyma darmowy przedmiot . Czasami takie obietnice są prawdziwe, ale często nie są i są po prostu sposobem na zachęcenie kogoś do podjęcia określonego działania, nie brać inaczej. Czasami tacy oszuści żądają uiszczenia niewielkiej opłaty za wysyłkę nagrody, czasami rozpowszechniają złośliwe oprogramowanie, a czasami zbierają poufne informacje. Istnieje nawet złośliwe oprogramowanie, które jest przynętą. Nie myl przynęty z przynętą. To ostatnie odnosi się do formy czujności, w której ludzie udają łatwowierność, potencjalne ofiary i marnują czas i zasoby oszustów poprzez powtarzające się interakcje, a także (czasami) gromadzą informacje o oszustach, które można przekazać prawu egzekwowania lub publikowane w Internecie, aby ostrzec innych przed oszustem.

* Quid pro quo: napastnik stwierdza, że potrzebuje osoby do podjęcia działania w celu świadczenia usługi dla zamierzonej ofiary. Na przykład osoba atakująca może udawać menedżera ds. Wsparcia IT oferującego pomoc pracownikowi w instalacji nowej aktualizacji oprogramowania zabezpieczającego. Jeśli pracownik współpracuje, przestępca przeprowadza go przez proces instalacji złośliwego oprogramowania.

* Podszywanie się pod media społecznościowe: niektórzy napastnicy podszywają się pod inne osoby w mediach społecznościowych w celu nawiązania z nimi połączeń w mediach społecznościowych

ofiary. Strony, pod które ktoś się podszywa, mogą być prawdziwymi ludźmi lub nieistniejącymi bytami. Oszuści odpowiedzialni za podszywanie się pod inne osoby pokazane na rysunku 8-3 i wiele innych tego typu kont często kontaktują się z osobami, które śledzą te konta, udając autora, i proszą obserwujących o dokonanie różnych „inwestycji".

* Kuszące e-maile: te e-maile próbują nakłonić ludzi do uruchomienia złośliwego oprogramowania lub kliknięcia zatrutych linków, wykorzystując ich ciekawość, pragnienia seksualne i inne cechy.

* Tailgating: Tailgating to fizyczna forma ataku socjotechnicznego, w którym napastnik towarzyszy upoważnionemu personelowi, gdy zbliża się do drzwi, do których jest upoważniony, ale nie atakujący, przechodzi i nakłania ich, aby przepuścili go z upoważnionym personelem. Atakujący może udawać, że przeszukuje torebkę w poszukiwaniu karty dostępu, twierdzić, że zapomniał swojej karty lub po prostu zachowywać się towarzysko i podążać za upoważnioną stroną.

* Fałszywe alarmy: Podnoszenie fałszywych alarmów może również skłonić ludzi do umożliwienia nieupoważnionym osobom robienia rzeczy, na które nie wolno im pozwolić. Rozważmy przypadek, w którym napastnik uruchamia alarm przeciwpożarowy wewnątrz budynku i udaje mu się wejść do normalnie zabezpieczonych obszarów przez drzwi awaryjne, z których ktoś inny wcześniej szybko wyszedł z powodu tzw. sytuacji awaryjnej.

* Dziura wodna: Dziura wodna łączy hakowanie i inżynierię społeczną wykorzystując fakt, że ludzie ufają określonym stronom, na przykład mogą klikać linki podczas przeglądania witryny tej strony, nawet jeśli nigdy nie klikali linków w e-mailu lub SMS-ie. Przestępcy mogą uruchomić atak na wodopój, naruszając odpowiednią witrynę i umieszczając na niej zatrute linki (lub nawet umieszczając bezpośrednio na niej złośliwe oprogramowanie).

Fałszywe wirusy: Przestępcy wykorzystują fakt, że ludzie są zaniepokojeni cyberbezpieczeństwem i prawdopodobnie niezasłużenie zwracają uwagę na wiadomości, które otrzymują z ostrzeżeniem o zagrożeniu w sieci. Wiadomości e-mail z fałszywymi wirusami mogą zawierać zatrute łącza, kierować użytkownika do pobrania oprogramowania lub instruować użytkownika, aby skontaktował się z pomocą techniczną za pośrednictwem adresu e-mail lub strony internetowej. Ataki te mają wiele odmian - niektóre ataki rozpowszechniają je jako masowe wiadomości e-mail, podczas gdy inne wysyłają je w wysoce ukierunkowany sposób. Niektórzy uważają, że oprogramowanie typu scareware, które przeraża użytkowników, aby uwierzyli, że muszą kupić określone oprogramowanie zabezpieczające (opisane w rozdziale 2), jest formą oszustwa związanego z wirusami. Inni nie, ponieważ „straszenie" scareware jest dokonywane przez złośliwe oprogramowanie, które jest już zainstalowane, a nie przez fałszywą wiadomość, która udaje, że złośliwe oprogramowanie jest już zainstalowane

* Awarie techniczne: przestępcy mogą z łatwością wykorzystywać irytację ludzi problemami technologicznymi, aby podważać różne technologie bezpieczeństwa.

Na przykład, jeśli przestępca podszywający się pod witrynę internetową, która zwykle wyświetla obraz bezpieczeństwa w określonym obszarze, umieści „symbol zepsutego obrazu" w tym samym obszarze witryny klonowanej, wielu użytkowników nie dostrzeże zagrożenia, ponieważ są przyzwyczajeni do oglądania zepsutych symbole graficzne i kojarzyć je raczej z awariami technicznymi niż zagrożeniami bezpieczeństwa.

Sześć zasad wykorzystywanych przez inżynierów społecznych

Psycholog społeczny Robert Beno Cialdini w swojej pracy z 1984 r. Influence: The Psychology of Persuasion, wyjaśnia sześć ważnych, podstawowych pojęć, które ludzie starający się wpływać na

innych często wykorzystują. Inżynierowie społeczni, którzy chcą oszukać ludzi, często wykorzystują te same sześć zasad, więc przedstawiam ich krótki przegląd w kontekście bezpieczeństwa informacji. Poniższa lista pomoże Ci zrozumieć i zinternalizować metody, których mogą używać oszuści, aby zdobyć Twoje zaufanie:

* Dowód społeczny: ludzie robią rzeczy, które widzą, że robią inni.

* Wzajemność: ludzie na ogół często wierzą, że jeśli ktoś zrobił dla nich coś miłego, są winni tej osobie zrobienie czegoś miłego.

* Autorytet: ludzie zwykle są posłuszni autorytetom, nawet jeśli nie zgadzają się z autorytetami, a nawet jeśli uważają, że to, o co są proszeni, jest niewłaściwe.

* Polubienie: Ogólnie rzecz biorąc, ludzie są łatwiej przekonani przez ludzi, których lubią, niż przez innych.

* Spójność i zaangażowanie: jeśli ludzie zobowiązują się do osiągnięcia jakiegoś celu i internalizują to zobowiązanie, staje się to częścią ich własnego wizerunku i prawdopodobnie będą próbować dążyć do celu, nawet jeśli pierwotnym powodem dążenia do celu jest nie już w ogóle istotne.

* Niedobór: jeśli ludzie myślą, że dany zasób jest rzadki, niezależnie od tego, czy jest on rzeczywiście rzadki, będą go chcieli, nawet jeśli go nie potrzebują.

Nie nadmiernie udostępniaj w mediach społecznościowych

Nadmierne udostępnianie informacji o przestępcach w mediach społecznościowych za pomocą materiałów, które mogą wykorzystać do inżynierii społecznej Ciebie, członków Twojej rodziny, współpracowników w pracy i znajomych. Jeśli na przykład ustawienia prywatności zezwalają każdemu, kto ma dostęp do platformy mediów społecznościowych, na przeglądanie opublikowanych przez Ciebie mediów, ryzyko wzrasta. Wiele razy ludzie przypadkowo udostępniają całemu światu posty, które przeznaczone są tylko dla niewielkiej grupy ludzi. Ponadto w wielu sytuacjach błędy w oprogramowaniu platformy mediów społecznościowych stworzyły luki w zabezpieczeniach, które umożliwiały nieupoważnionym stronom przeglądanie mediów i postów, które miały ustawienia prywatności uniemożliwiające taki dostęp. Weź również pod uwagę swoje ustawienia prywatności. Materiały rodzinne z ustawieniami prywatności umożliwiającymi przeglądanie ich członkom niebędącym członkami rodziny mogą powodować różnego rodzaju problemy związane z prywatnością i wyciekać odpowiedzi na różne popularne pytania służące do uwierzytelniania użytkowników, takie jak „Gdzie mieszka najstarsze rodzeństwo?” lub „Jakie jest nazwisko panieńskie Twojej matki?”

Nie polegaj na ustawieniach prywatności w mediach społecznościowych, aby chronić prawdziwie poufne dane. Niektóre platformy mediów społecznościowych umożliwiają szczegółową ochronę opublikowanych elementów, podczas gdy inne nie. Udostępnione niektóre elementy mogą pomóc przestępcom w inżynierii społecznej Ciebie lub kogoś, kogo znasz. Ta lista nie jest wyczerpująca. Ma raczej na celu zilustrowanie przykładów, które pobudzą Twoje myślenie o potencjalnych zagrożeniach związanych z tym, co zamierzasz opublikować w mediach społecznościowych, zanim to zrobisz. W poniższych sekcjach opisano informacje, które należy udostępniać ostrożnie w mediach społecznościowych. Liczne inne typy postów w mediach społecznościowych niż te, które wymieniam w poniższych sekcjach, mogą pomóc przestępcom w organizowaniu ataków socjotechnicznych. Pomyśl o potencjalnych konsekwencjach przed opublikowaniem i odpowiednio ustaw ustawienia prywatności swoich postów.

Twój harmonogram i plany podróży

Szczegóły Twojego harmonogramu lub harmonogramu innej osoby mogą dostarczyć przestępcom informacji, które mogą im pomóc w zorganizowaniu ataku. Na przykład, jeśli opublikujesz, że będziesz uczestniczyć w zbliżającym się wydarzeniu, takim jak ślub, możesz zapewnić przestępcom możliwość wirtualnego porwania Ciebie lub innych uczestników - nie wspominając o zachęcaniu innych do atakowania Twojego domu za pomocą próby włamania kiedy dom prawdopodobnie będzie pusty. (Wirtualne porwanie odnosi się do przestępcy żądającego okupu w zamian za ten sam powrót kogoś, kto twierdzi, że został porwany, ale który w rzeczywistości nie został porwany). Podobnie ujawnienie, że będziesz leciał konkretnym lotem, może dać przestępcom możliwość wirtualnego porwania Cię lub próby oszustwa typu CEO przeciwko Twoim współpracownikom. Mogą podszywać się pod Ciebie i wysłać e-maila z informacją, że lecisz i możesz nie być osiągalny telefonicznie w celu potwierdzenia instrukcji, więc po prostu idź i postępuj zgodnie z nimi. Unikaj też publikowania informacji o wakacjach lub wycieczce członka rodziny, co może zwiększyć ryzyko wirtualnego porwania (i rzeczywistego fizycznego zagrożenia dla tej osoby lub jej rzeczy).

Informacje finansowe

Udostępnianie numeru karty kredytowej może prowadzić do nieuczciwych obciążeń, a zaksięgowanie numeru konta bankowego może prowadzić do nieuczciwych działań bankowych. Ponadto nie ujawniaj, że odwiedziłeś lub miałeś interakcję z konkretną instytucją finansową lub lokalizacje, w których przechowujesz swoje pieniądze - banki, konta kryptowalut, domy maklerskie i tak dalej. Może to zwiększyć prawdopodobieństwo, że przestępcy będą próbowali wejść na Twoje konta w odpowiednich instytucjach finansowych. W związku z tym takie udostępnianie może narazić Cię na próby włamania do Twoich kont, a także ukierunkowane ataki typu phishing, vishing i smishing oraz wszelkiego rodzaju inne oszustwa związane z inżynierią społeczną. Publikowanie informacji o potencjalnych inwestycjach, takich jak akcje, obligacje, metale szlachetne lub kryptowaluty, może narazić Cię na cyberataki, ponieważ przestępcy mogą założyć, że masz znaczne pieniądze do kradzieży. (Jeśli zachęcasz ludzi do inwestowania lub publikowania różnych innych form postów, możesz również naruszyć SEC, CFTC lub inne przepisy). Możesz również otworzyć drzwi przestępcom podszywającym się pod regulatorów i skontaktować się z Tobą w celu zapłacenia grzywny za opublikowanie informacje niewłaściwie.

Informacje osobiste

Na początek unikaj umieszczania członków rodziny w sekcji Informacje na swoim profilu na Facebooku. Sekcja That About zawiera linki do ich profili na Facebooku i wyjaśnia widzom charakter odpowiednich relacji rodzinnych z każdą wymienioną stroną. Wymieniając te relacje, możesz ujawnić wszelkiego rodzaju informacje, które mogą być cenne dla przestępców. Nie tylko prawdopodobnie ujawnisz nazwisko panieńskie swojej matki (odpowiedź na pytanie-wyzwanie!), Ale możesz także podać wskazówki, gdzie dorastałeś. Informacje znalezione w Twoim profilu zapewniają również przestępcom listę osób do inżyniera społecznościowego lub kontaktu w ramach wirtualnego oszustwa związanego z porwaniem. Powinieneś także unikać udostępniania następujących informacji w mediach społecznościowych, ponieważ może to podważyć pytania uwierzytelniające i pomóc przestępcom w inżynierii społecznej Ciebie lub Twojej rodziny:

* Drugie imię twojego ojca

* Urodziny Twojej matki

* Gdzie poznałeś drugą połówkę

* Twoje ulubione miejsce na wakacje

* Nazwa pierwszej szkoły, do której uczęszczałeś

* Ulica, na której się wychowałeś

* Typ, marka, model i / lub kolor Twojego pierwszego samochodu lub samochodu innej osoby

* Twoje ulubione jedzenie lub napoje

Podobnie, nigdy nie udostępniaj swojego numeru ubezpieczenia społecznego, ponieważ może to prowadzić do kradzieży tożsamości

Informacje o Twoich dzieciach

Dzielenie się informacjami o swoich dzieciach może nie tylko narazić Cię na ataki, ale także narazić Twoje dzieci na duże zagrożenie fizyczne. Na przykład zdjęcia twoich dzieci mogą pomóc porywaczowi. Problem może się pogłębić, jeśli obrazy zawierają znacznik czasu i / lub geotagowanie - to znaczy informacje o lokalizacji, w której zdjęcie zostało zrobione. Znaczniki czasu i geotagowanie nie muszą być wykonywane zgodnie z jakąś specyfikacją techniczną, aby stworzyć ryzyko. Jeśli z obrazów jasno wynika, że Twoje dzieci chodzą do szkoły, chodzą na zajęcia pozalekcyjne itd., Możesz narazić je na niebezpieczeństwo. Ponadto odwoływanie się do nazw szkół, obozów, przedszkoli lub innych programów młodzieżowych, do których uczęszczają Twoje dzieci lub ich przyjaciele, może zwiększyć ryzyko skierowania na nich pedofila, porywacza lub innej wrogiej grupy. Taki wpis może również narazić Cię na potencjalnego włamywacza, ponieważ będą wiedzieć, kiedy prawdopodobnie nie będzie Cię w domu. Ryzyko może być znacznie większe, jeśli jasny wzór dotyczący Twojego harmonogramu i / lub Twojego harmonogramu dla dzieci można ekstrapolować na podstawie takich postów. Unikaj też publikowania informacji o wycieczce szkolnej lub obozowej dziecka. Informacje o Twoich zwierzętach. Podobnie jak w przypadku nazwiska panieńskiego matki, udostępnienie imienia obecnego zwierzaka lub imienia pierwszego zwierzaka może narazić Ciebie lub inne znane Ci osoby na ataki socjotechniczne, ponieważ takie informacje są często używane jako odpowiedź na pytania uwierzytelniające.

Informacje o pracy

Szczegółowe informacje o tym, z jakimi technologiami pracujesz w obecnej (lub poprzedniej pracy), mogą pomóc przestępcom zarówno w wyszukiwaniu luk w systemach Twojego pracodawcy, jak i w inżynierii społecznej Twoich współpracowników. Wiele oszustw i oszustw związanych z wirusami stało się wirusowymi - i spowodowało znacznie więcej szkody, niż powinny - ponieważ przestępcy wykorzystują strach ludzi przed cyberatakami i zwiększają prawdopodobieństwo, że wiele osób udostępni posty o cyberzagrożeniach, często bez weryfikacji autentyczności takich postów. Informacje o naruszeniu przepisów dotyczących ruchu drogowego lub mandacie za parkowanie, które otrzymałeś, nie tylko przedstawiają się w mniej niż najlepszym świetle, ale mogą nieumyślnie dostarczyć prokuratorom materiałów potrzebnych do skazania cię za dane przestępstwo. Możesz również dać oszustom możliwość inżynierii społecznej siebie lub innych osób - mogą udawać, że są organami ścigania, sądem lub prawnikiem, kontaktując się z tobą w tej sprawie - być może nawet żądając natychmiastowej zapłaty grzywny, aby uniknąć aresztowania. Oprócz pomocy przestępcom w inżynierii społecznej w sposób podobny do sprawy dotyczącej ruchomego naruszenia, informacje o przestępstwie, które popełniłeś Ty lub ukochana osoba, mogą zaszkodzić Ci zawodowo i osobiście.

Porada medyczna lub prawna

Jeśli oferujesz poradę medyczną lub prawną, ludzie mogą ekstrapolować, że ty lub ktoś bliski cierpi na określony stan chorobowy lub jest zaangażowany w określoną sytuację prawną.

Twoja lokalizacja

Twoja lokalizacja lub zameldowanie w mediach społecznościowych może nie tylko zwiększać ryzyko dla Ciebie i Twoich bliskich fizycznego niebezpieczeństwa, ale może pomóc przestępcom w przeprowadzaniu wirtualnych ataków na porwanie i innych oszustw socjotechnicznych. Wiadomość z okazji urodzin dla każdego może ujawnić datę urodzin tej osoby. Osoby, które ze względów bezpieczeństwa używają fałszywych urodzin w mediach społecznościowych, widziały, jak ich środki ostrożności zostały w taki sposób podważone przez dobrze życzących sobie ludzi. Wszystko, co jest „podobne do grzechu", może prowadzić nie tylko do krzywdy zawodowej lub osobistej, ale także do prób szantażu, a także do inżynierii społecznej siebie lub innych przedstawionych w takich postach lub mediach. Ponadto zdjęcie przedstawiające Ciebie w miejscu odwiedzanym przez osoby o określonych wyznaniach religijnych, seksualnych, politycznych, kulturowych lub innych może prowadzić do ekstrapolacji informacji o tobie przez przestępców, co może prowadzić do różnego rodzaju inżynierii społecznej. Wiadomo na przykład, że przestępcy praktycznie porwali osobę, która była w synagodze i była nieosiągalna w żydowskie święto Jom Kipur. Wiedzieli, kiedy i gdzie będzie szedł w drodze do świątyni, i dzwonili do członków rodziny twierdząc, że porwał osobę. Członkowie rodziny dali się nabrać na oszustwo związane z wirtualnym porwaniem, ponieważ szczegóły były prawidłowe i nie mogli skontaktować się z „ofiarą" telefonicznie w trakcie nabożeństwa w synagodze.

Wyciek danych poprzez udostępnianie informacji w ramach trendów wirusowych

Od czasu do czasu pojawia się wirusowy trend, w którym wiele osób udostępnia podobne treści. Wpisy o wyzwaniu z lodem, twoich ulubionych koncertach i coś o tobie dzisiaj i dziesięć lat temu to przykłady trendów wirusowych. Oczywiście przyszłe trendy wirusowe mogą nie mieć nic wspólnego z wcześniejszymi. Każdy typ posta, który szybko rozprzestrzenia się wśród dużej liczby osób, jest nazywany „wirusem". Chociaż uczestnictwo może wydawać się zabawne - i „co wszyscy robią" - upewnij się, że rozumiesz potencjalne konsekwencje takiego działania. Na przykład dzielenie się informacjami o koncertach, w których uczestniczyłeś i które uważasz za ulubione, może wiele o Tobie ujawnić - zwłaszcza w połączeniu z innymi danymi z profilu - i może narazić Cię na różnego rodzaju ryzyko socjotechniczne.

Rozpoznawanie fałszywych połączeń z mediami społecznościowymi

Media społecznościowe zapewniają swoim użytkownikom wiele korzyści zawodowych i osobistych, ale stwarzają również niesamowite możliwości dla przestępców - wiele osób ma wrodzoną chęć łączenia się z innymi i nadmiernie ufa platformom mediów społecznościowych. Zakładają, że jeśli na przykład Facebook wysyła wiadomość, którą Joseph Steinberg zażądał, aby zostać przyjacielem, to prawdziwy „Joseph Steinberg" o to poprosił - a często tak nie jest. Przestępcy wiedzą na przykład, że łącząc się z Tobą w mediach społecznościowych, mogą uzyskać dostęp do wszelkiego rodzaju informacji o Tobie, członkach Twojej rodziny i współpracownikach - informacje, które często mogą wykorzystać, aby podszyć się pod Ciebie, członka rodziny. lub kolegę w ramach działań przestępczych mających na celu inżynierię społeczną wejście do systemów biznesowych, kradzież pieniędzy lub popełnienie innych przestępstw. Jedną z technik, której często używają przestępcy, aby uzyskać dostęp do „prywatnych" informacji z Facebooka, Instagrama lub LinkedIn, jest tworzenie fałszywych profili - informacje na Facebooku, Instagramie lub LinkedIn, to tworzenie fałszywych profili - profili nieistniejących osób - i prośba o połączenie prawdziwych ludzi, z których wielu prawdopodobnie zaakceptuje odpowiednie prośby o połączenie. Ewentualnie oszuści mogą założyć konta, które podszywają się pod prawdziwe osoby i które mają zdjęcia profilowe i inne materiały pobrane z legalnych kont mediów społecznościowych podszywanej osoby. Jak możesz chronić się przed takimi oszustwami? Poniższe sekcje zawierają porady, jak szybko wykryć fałszywe konta i jak uniknąć możliwych konsekwencji przyjmowania od nich połączeń. Pamiętaj, że żadna ze wskazówek w poniższych sekcjach nie działa w próżni ani nie jest absolutna. Fakt, że profil nie przejdzie pomyślnie testu na przykład pod kątem

określonej reguły, nie oznacza automatycznie, że jest fałszywy. Jednak zastosowanie inteligentnych koncepcji, takich jak te, które wymieniam w następnych sekcjach, powinno pomóc ci zidentyfikować znaczny procent fałszywych kont i uchronić się przed problemami, które mogą ostatecznie wyniknąć z przyjmowania od nich żądań połączenia.

Zdjęcie

Wiele fałszywych kont wykorzystuje zdjęcia atrakcyjnych modelek, czasami skierowanych do mężczyzn, którzy mają konta przedstawiające zdjęcia kobiet i kobiet, których konta zawierają zdjęcia mężczyzn. Obrazy często wydają się być zdjęciami seryjnymi, ale czasami są kradzione prawdziwym użytkownikom.

Jeśli otrzymasz prośbę o połączenie z mediami społecznościowymi od osoby, której nie pamiętasz, by kiedykolwiek się spotkała, a zdjęcie jest tego typu, miej się na baczności. W razie wątpliwości możesz załadować obraz do odwrotnego wyszukiwania grafiki Google i sprawdzić, gdzie jeszcze się pojawia. Możesz także wyszukać imię i nazwisko osoby (i, jeśli to konieczne, na LinkedIn) lub tytuł, aby zobaczyć, czy inne podobne zdjęcia pojawiają się w Internecie. Jednak przebiegły podszywacz może przesyłać obrazy do kilku witryn. Oczywiście każdy profil bez zdjęcia właściciela konta powinien budzić zastrzeżenia. Pamiętaj jednak, że niektórzy ludzie używają emotikonów, karykatur itp. Jako zdjęć profilowych, zwłaszcza w sieciach społecznościowych, które nie są zorientowane zawodowo.

Weryfikacja

Jeśli konto wydaje się reprezentować osobę publiczną, co do której podejrzewasz, że może zostać zweryfikowana (co oznacza, że obok nazwy konta użytkownika znajduje się niebieski znacznik wyboru, który wskazuje, że jest to uzasadnione konto osoby publicznej), ale nie jest zweryfikowany, to prawdopodobny znak, że coś jest nie tak. Podobnie jest mało prawdopodobne, aby zweryfikowane konto na dużej platformie mediów społecznościowych było fałszywe. Zdarzały się jednak sytuacje, w których zweryfikowane konta tego rodzaju zostały tymczasowo przejęte przez hakerów.

Znajomi lub wspólni znajomi

Fałszywi ludzie raczej nie będą mieli z Tobą wielu znajomych lub znajomości, a fałszywi ludzie zwykle nie będą mieli z Tobą nawet wielu drugorzędnych kontaktów (Znajomi znajomych, połączenia drugiego poziomu LinkedIn itd.).

Nie zakładaj, że konto jest wiarygodne tylko dlatego, że ma z Tobą jeden lub dwa połączenia; niektóre z Twoich połączeń mogły zostać oszukane i powiązane z fałszywą osobą, a połączenie Twojego kontaktu z fałszywym kontem może być przede wszystkim sposobem, w jaki przestępca dowiedział się o tobie. Nawet w takim scenariuszu liczba wspólnych połączeń będzie prawdopodobnie stosunkowo niewielka w porównaniu z prawdziwym, wzajemnym połączeniem, a powiązanie między ludźmi, którzy nawiązali kontakt z profilem złoczyńcy, może wydawać się trudne. Znasz swoje połączenia lepiej niż ktokolwiek inny - zachowaj ostrożność, gdy czyjeś wzorce połączeń nie mają sensu. Możesz na przykład pomyśleć dwa razy, jeśli ktoś próbujący nawiązać z tobą kontakt wydaje się nie znać nikogo w branży, w której pracuje, ale zna trzech twoich najbardziej łatwowiernych przyjaciół, którzy mieszkają w trzech różnych krajach i którzy się nie znają .

Odpowiednie posty

Kolejną wielką czerwoną flagą jest sytuacja, gdy konto nie udostępnia materiałów, które powinno udostępniać w oparciu o rzekomą tożsamość właściciela konta. Jeśli ktoś twierdzi, że jest felietonistą,

który obecnie pisze na przykład dla Forbes i próbuje, ale nigdy nie udostępnił żadnych postów artykułów, które napisał dla Forbesa, coś prawdopodobnie jest nie tak.

Liczba połączeń

Prawdopodobnie będzie to osoba na wyższym szczeblu, z wieloletnim doświadczeniem zawodowym masz wiele kontaktów zawodowych, zwłaszcza na LinkedIn. Im mniej połączeń ma konto rzekomo należące do osoby z wyższego szczebla na LinkedIn (im dalej jest od 500 lub więcej), tym bardziej powinieneś być podejrzliwy. Oczywiście każdy profil LinkedIn zaczynał się od zerowych połączeń - tak legalnych, nowe konta LinkedIn mogą wydawać się podejrzane, gdy tak naprawdę nie są - ale w grę wchodzi praktyczna rzeczywistość: ilu prawdziwych osób na wyższym szczeblu, które się z Tobą kontaktują, nie zrobiło tego? do niedawna zakładali swoje konta LinkedIn? Oczywiście niewielka liczba połączeń i nowe konto LinkedIn nie są niczym niezwykłym dla osoby, która właśnie rozpoczęła swoją pierwszą pracę, ani dla osób pracujących w określonych branżach, na określonych stanowiskach i / lub w określonych firmach - tajni agenci CIA nie ” t publikować postępy kariery na swoich profilach LinkedIn - ale jeśli pracujesz w tych branżach, prawdopodobnie już wiesz o tym. Porównaj liczbę połączeń z wiekiem konta i liczbą postów, z którymi wchodził w interakcję lub udostępnił - osoba, która jest na Facebooku od dekady i regularnie publikuje, na przykład, powinna mieć więcej niż jeden lub dwóch przyjaciół.

Przemysł i lokalizacja

Zdrowy rozsądek dotyczy kont, które rzekomo reprezentują osoby mieszkające w określonych lokalizacjach lub pracujące w określonych branżach. Jeśli na przykład pracujesz w technologii i nie masz zwierząt, a otrzymasz prośbę o połączenie z LinkedIn od weterynarza mieszkającego na drugim końcu świata, którego nigdy nie spotkałeś, coś może być nie tak. Podobnie, jeśli otrzymasz zaproszenie do znajomych na Facebooku od kogoś, z kim nie masz nic wspólnego, uważaj. Nie zakładaj, że jakiekolwiek twierdzenia w profilu są z konieczności dokładne i że jeśli masz wiele wspólnych cech, nadawca jest zdecydowanie bezpieczny. Ktoś, do kogo kierujesz reklamy, mógł rozpoznać Twoje zainteresowania na podstawie informacji o Tobie, które są publicznie dostępne w Internecie.

Podobni ludzie

Jeśli otrzymujesz wiele próśb od osób o podobnych tytułach lub twierdzących , że pracujesz dla tej samej firmy, a nie znasz ludzi i nie robisz z nią żadnej umowy, uważaj. Jeśli ci ludzie nie wydają się być powiązani z nikim innym w firmie, o której wiesz, że faktycznie tam pracuje, potraktuj to również jako potencjalną czerwoną flagę. Zawsze możesz zadzwonić, napisać lub wysłać e-mail do prawdziwego kontaktu i zapytać, czy widzi tę osobę na liście pracowników.

Zduplikowany kontakt

Jeśli otrzymasz zaproszenie do znajomych na Facebooku od osoby, która już jest znajomą na Facebooku, potwierdź z tą stroną, że przełącza konta. W wielu przypadkach takie żądania pochodzą od oszustów.

Szczegóły kontaktu

Upewnij się, że dane kontaktowe mają sens. Fałszywi ludzie znacznie rzadziej niż prawdziwi ludzie mają adresy e-mail w prawdziwych firmach i rzadko mają adresy e-mail w dużych korporacjach. Mało prawdopodobne jest, aby mieli fizyczne adresy wskazujące, gdzie mieszkają i pracują, a jeśli takie adresy są wymienione, rzadko odpowiadają faktycznym aktom nieruchomości lub informacjom z książki telefonicznej, które można łatwo sprawdzić online.

Status LinkedIn Premium

Ponieważ LinkedIn pobiera opłaty za swoją usługę Premium, niektórzy eksperci sugerują, że status Premium jest dobrym wskaźnikiem, że konto jest prawdziwe, ponieważ przestępca prawdopodobnie nie zapłaci za konto. Chociaż może być prawdą, że większość fałszywych kont nie ma statusu Premium, niektórzy oszuści inwestują w uzyskanie statusu Premium, aby ich konta wyglądały bardziej realistycznie. W niektórych przypadkach płacą skradzionymi kartami kredytowymi, więc i tak nic ich to nie kosztuje. Dlatego zachowaj czujność, nawet jeśli konto wyświetla ikonę Premium.

Rekomendacje LinkedIn

Fałszywi ludzie nie będą wspierani przez wielu prawdziwych ludzi. A indosantami fałszywych kont mogą być inne fałszywe konta, które również wydają się podejrzane.

Grupowa aktywność

Fałszywe profile rzadziej niż prawdziwi ludzie są członkami zamkniętych grup, które weryfikują członków, kiedy dołączają, i rzadziej uczestniczą w znaczących dyskusjach zarówno w zamkniętych, jak i otwartych grupach na Facebooku lub LinkedIn. Jeśli są członkami zamkniętych grup, mogły zostać utworzone i zarządzane przez oszustów, a także zawierać inne fałszywe profile. Fałszywi ludzie mogą być członkami wielu otwartych grup - grup, do których dołączono, aby uzyskać dostęp do list członków i łączyć się z innymi uczestnikami za pomocą wiadomości typu „Widzę, że jesteśmy członkami tej samej grupy, więc połączmy się". W każdym razie pamiętaj, że na każdej platformie społecznościowej, która ma grupy, bycie członkami tej samej grupy co ktoś inny nie jest w żaden sposób powodem do zaakceptowania połączenia od tej osoby.

Odpowiednie poziomy względnego użycia

Prawdziwi ludzie, którzy używają LinkedIn lub Facebooka na tyle intensywnie, aby dołączyć do wielu grup, są bardziej skłonni do wypełnienia wszystkich informacji profilowych. Żądanie połączenia od osoby, która jest członkiem wielu grup, ale ma mało informacji profilowych, jest podejrzane. Podobnie konto na Instagramie z 20000 obserwujących, ale tylko dwa opublikowane zdjęcia, które mają na celu śledzenie twojego prywatnego konta, jest podejrzane z tego samego powodu.

Działalność człowieka

Wydaje się, że wiele fałszywych kont zawiera w swoich plikach informacje brzmiące jak banale profile, zainteresowania i doświadczenia zawodowe, ale zawierają kilka innych szczegółów, które wydają się przekazywać prawdziwe ludzkie doświadczenia. Oto kilka oznak, że rzeczy mogą nie być takie, na jakie wyglądają:

* Na LinkedIn zalecenia, doświadczenie w wolontariacie i sekcje edukacyjne przedstawiające fałszywą osobę mogą wydawać się niewłaściwe.

* Na Facebooku fałszywy profil może wydawać się narzędziem do usuwania ciasteczek, a posty są na tyle ogólne, że miliony ludzi mogłyby napisać ten sam post.

* Na Twitterze mogą retweetować posty od innych i nigdy nie udostępniać własnych opinii, komentarzy ani innych oryginalnych materiałów.

* Na Instagramie zdjęcia mogą być pobierane z innych kont lub wyglądać na zdjęcia z banku zdjęć - czasami żadne z nich nie zawiera zdjęcia rzeczywistej osoby, która rzekomo jest właścicielem tych kont. Treści w profilu użytkownika w mediach społecznościowych mogą zawierać terminy i wyrażenia, które można wyszukiwać w Google, a także imię i nazwisko osoby, aby pomóc Ci zweryfikować, czy konto

naprawdę należy do człowieka , której tożsamość ma reprezentować profil. Podobnie, jeśli wyszukujesz w Google czyjeś zdjęcia na Instagramie i widzisz, że należą one do innych osób, coś jest nie tak.

Nazwy banalne

W niektórych fałszywych profilach używane są popularne amerykańskie nazwiska, takie jak Sally Smith, które brzmią zbyt amerykańsko i sprawiają, że wyszukiwanie w Google konkretnej osoby jest o wiele trudniejsze niż w przypadku osoby o nietypowym imieniu. Częściej niż w prawdziwym życiu, ale z pewnością nie zawsze, w fałszywych profilach używane są imiona i nazwiska zaczynające się na tę samą literę. Być może oszuści po prostu lubią nazwy lub z jakiegoś powodu je znajdują zabawnymi.

Słabe informacje kontaktowe

Jeśli profil w mediach społecznościowych nie zawiera absolutnie żadnych danych kontaktowych, które można wykorzystać do skontaktowania się z osobą za profilem za pośrednictwem poczty elektronicznej, telefonu lub innej platformy społecznościowej, uważaj.

Zestawy umiejętności

Jeśli umiejętności nie pasują do czyjegoś doświadczenia zawodowego lub życiowego, uważaj. Coś może się wydawać nie tak, jeśli chodzi o fałszywe konta. Na przykład, jeśli ktoś twierdzi, że ukończył studia z języka angielskiego na Ivy, ktoś twierdzi, że ukończył studia z języka angielskiego na uniwersytecie Ivy League, ale popełnia poważne błędy gramatyczne w swoim profilu, coś może być nie tak. Podobnie, jeśli ktoś twierdzi, że ma dwa doktoraty z matematyki, ale twierdzi, że pracuje jako nauczyciel gimnastyki, uważaj.

Pisownia

Błędy ortograficzne są powszechne w mediach społecznościowych. Jednak coś może być nie tak, jeśli ktoś błędnie przeliteruje swoje imię i nazwisko lub nazwę pracodawcy, albo popełnia tego typu błędy na LinkedIn (sieć zorientowana zawodowo).

Podejrzana kariera lub ścieżka życiowa

Osoby, które wydają się być awansowane zbyt często i zbyt szybko lub które zajmowały zbyt wiele różnych wyższych stanowisk, takie jak wiceprezes ds. sprzedaży, następnie dyrektor ds. technologii, a następnie radca prawny, mogą być zbyt piękne, aby mogły być prawdziwe. Oczywiście prawdziwi ludzie szybko awansowali po szczeblach kariery, a niektórzy ludzie (w tym ja) zajmowali różne stanowiska w trakcie swojej kariery, ale oszuści często przesadzają, tworząc dane dotyczące postępów kariery lub różnorodności ról w fałszywym profilu . Ludzie mogą na przykład zmieniać role techniczne na kierownicze, ale niezwykle rzadko zdarza się, aby ktoś pełnił funkcję wiceprezesa ds. Sprzedaży firmy, następnie jej dyrektora ds. Technicznych, a następnie radcy prawnego - ról wymagających różnych umiejętności, wykształcenia, i potencjalnie różne certyfikaty i licencje. Jeśli zauważysz, że mówisz sobie „nie ma mowy", patrząc na czyjąś ścieżkę kariery, możesz mieć rację.

Poziom lub status gwiazdy

Prośby na LinkedIn od osób na znacznie wyższym szczeblu zawodowym niż ty mogą być oznaką, że coś jest nie tak, podobnie jak prośby z Facebooka od celebrytów i innych osób, których prośby o połączenie Ci schlebia. Z pewnością kusi, aby chcieć zaakceptować takie powiązania (co jest oczywiście powodem, dla którego ludzie, którzy tworzą fałszywe konta, często tworzą takie fałszywe konta), ale pomyśl o tym: Jeśli właśnie dostałeś pierwszą pracę po college'u, czy naprawdę myślisz, że dyrektor generalny dużego banku nagle jest zainteresowany połączeniem się z tobą niespodziewanie? Czy naprawdę

myślisz, że pani Universe, której nigdy nie spotkałeś, nagle chce być twoją przyjaciółką? W przypadku Facebooka, Instagrama i Twittera należy pamiętać, że większość kont celebrytów jest weryfikowana. Jeśli prośba pochodzi od znanej osoby, powinieneś być w stanie szybko stwierdzić, czy konto, które ją wysłało, jest prawdziwą okazją.

Korzystanie z fałszywych informacji

Niektórzy eksperci sugerują użycie fałszywych informacji jako odpowiedzi na często zadawane pytania. Ktoś - szczególnie osoba, której matka ma wspólne nazwisko jako nazwisko panieńskie - może ustalić nazwisko panieńskie nowej matki, które będzie używane we wszystkich witrynach, które proszą o takie informacje w ramach procesu uwierzytelniania. Prawdą jest, że takie podejście w pewnym stopniu pomaga zmniejszyć ryzyko inżynierii społecznej. Jednak jeszcze silniej ujawnia, jak kiepskie są pytania stanowiące wyzwanie jako sposób na uwierzytelnienie ludzi. Pytanie o nazwisko panieńskie matki jest w rzeczywistości pytaniem o hasło, a jednocześnie daje wskazówkę, że hasło to nazwisko! Podobnie, ponieważ w dobie mediów społecznościowych i publicznych rejestrów online ustalenie czyichś urodzin jest stosunkowo proste, niektórzy eksperci ds. Bezpieczeństwa zalecają utworzenie drugich fałszywych urodzin do wykorzystania w Internecie. Niektórzy nawet zalecają umieszczanie fałszywych urodzin w mediach społecznościowych, aby zapobiec inżynierii społecznej i utrudnić organizacjom i osobom indywidualnym skorelowanie swojego profilu w mediach społecznościowych i różnych rejestrów publicznych. Chociaż wszystkie te zalecenia mają znaczenie, pamiętaj, że teoretycznie nie ma końca takiej logice, że ustalanie różnych fałszywych urodzin dla każdej witryny, z którą się kontaktujesz, zapewnia silniejszą ochronę prywatności niż na przykład ustanowienie fałszywych urodzin. Ogólnie jednak posiadanie jednej fałszywej daty urodzin, jednego fałszywego nazwiska panieńskiego matki itd. Jest prawdopodobnie opłacalne i nie wymaga dużo dodatkowej siły i dzielenia się umysłami w porównaniu z używaniem tylko prawdziwego. Należy jednak pamiętać, aby nie wprowadzać w błąd witryn, w przypadku których podanie dokładnych informacji jest wymagane przez prawo (na przykład podczas otwierania konta karty kredytowej).

Korzystanie z oprogramowania zabezpieczającego

Oprócz ochrony komputera i telefonu przed włamaniami różne programy zabezpieczające mogą zmniejszyć narażenie na ataki socjotechniczne. Na przykład niektóre programy odfiltrowują wiele ataków phishingowych, podczas gdy inne blokują wiele połączeń telefonicznych ze spamem. Chociaż używanie takiego oprogramowania jest rozsądne, nie polegaj na nim. Istnieje niebezpieczeństwo, że jeśli tylko kilka ataków socjotechnicznych przejdzie przez twoje zabezpieczenia technologiczne, możesz być mniej czujny, gdy ktoś do ciebie dotrze - nie pozwól, aby tak się stało. Podczas gdy dostawcy smartfonów w przeszłości pobierali opłaty za niektóre funkcje bezpieczeństwa, z czasem dostrzegli wartość dla siebie, jaką jest zapewnienie bezpieczeństwa swoim klientom. Obecnie podstawowe wersje oprogramowania zabezpieczającego, w tym technologia ograniczania połączeń spamowych, są często dostarczane bezpłatnie wraz z usługą transmisji danych komórkowych w smartfonie.

Ogólna cyberhigiena może pomóc w zapobieganiu inżynierii społecznej

Ogólnie praktykowanie dobrej cyberhigieny może również pomóc zmniejszyć narażenie na inżynierię społeczną. Jeśli na przykład twoje dzieci mają dostęp do twojego komputera, ale szyfrujesz wszystkie twoje dane, masz oddzielny login i nie zapewniasz im dostępu administratora, twoje dane na komputerze mogą pozostać bezpieczne, nawet jeśli przestępca socjotechniczny zrobi to po swojemu na konto Twojego dziecka. Podobnie, nie odpowiadanie na podejrzane e-maile lub udzielanie informacji potencjalnym oszustom, którzy o to zabiegają, może pomóc w zapobieganiu wszelkiego rodzaju atakom socjotechnicznym i technicznym.