**Strzeż się inżynierii społecznościowej, to ulubione narzędzie oszustów wykorzystujących scam**

**Inżynieria społecznościowa jest wyjątkowo podstępna, gdyż żeruje na naszej naturalnej chęci bycia uczynnym. Zjawisko to może również grać na ludzkich emocjach, takich jak strach czy współczucie. Oto kilka sztuczek wykorzystywanych w inżynierii społecznościowej w celu zdobycia poufnych danych. Krzysztof Wójtowicz z firmy Check Poit Software Technologies opisuje również metody, które pomagają się bronić przed tymi sztuczkami.**

Jesteś w biurze i nagle zjawia się elektryk, żeby naprawić awarię. Albo dzwoni telefon – Twój dostawca Internetu informuje Cię, że mają jakiś problem z Twoim kontem.

W takich przypadkach naturalnym, ludzkim odruchem jest współpraca, czyż nie? Wpuszczasz elektryka i pozwalasz mu wykonać swoją pracę. Odpowiadasz na pytania zadawane przez pracownika obsługi klienta w celu zweryfikowania Twojej tożsamości. Niestety, w tym przypadku zamiast być uprzejmym i pomocnym, stałeś się ofiarą inżynierii społecznościowej. Elektryk zainstalował właśnie w Twoim biurze ukryte kamery lub router służący do podsłuchu. Fałszywy pracownik działu obsługi klienta poznał Twoje dane osobowe, hasło do Twojego konta, a być może nawet informacje dotyczące karty kredytowej.

Inżynieria społecznościowa odwołuje się do technik stosowanych w celu manipulowania ludźmi i skłaniania ich do wykonania pewnych czynności lub wyjawienia istotnych informacji. Cyberprzestępcy często wykorzystują łatwowierność oraz naturalną ludzką chęć do bycia pomocnym. Scamerzy nie muszą trudzić się i korzystać ze skomplikowanych hakerskich technik, czy też złośliwego oprogramowania omijającego zabezpieczenia – mogą po prostu wysłać email ze szkodliwym załącznikiem i poprosić odbiorcę o jego otwarcie.

Inżynieria społecznościowa nie jest niczym nowym, od zawsze istnieli ludzie zajmujący się sztuką scamu, knując różne spiski i intrygi. Nowością jednak jest to, jak wiele informacji na temat ofiary mogą zdobyć scamerzy zanim jeszcze przystąpią do ataku. Dzięki portalom społecznościowym są w stanie dowiedzieć się naprawdę wiele, np. gdzie dana osoba pracuje, nazwiska znajomych, nazwę szkoły, do której uczęszczała ofiara, a nawet gdzie ostatnio spędzała wakacje. Mogą również poznać strukturę organizacyjną firmy oraz wydedukować, z jakiego oprogramowania korzysta dane przedsiębiorstwo. Te informacje mogą być wykorzystane przeciwko ofierze, gdyż atakujący dzięki nim staje się bardziej wiarygodny.

**Pomagać jest rzeczą ludzką** - DefCon, największy konwent hakerów, co roku organizuje zawody „Capture the Flag” („Zdobyć flagę”) polegające na wykorzystywaniu inżynierii społecznościowej w praktyce. W ubiegłym roku celem były między innymi firmy takie jak Apple oraz Johnson & Johnson. W dniu zawodów, uczestnicy zamykają się w kabinach telefonicznych i dzwonią do osób pracujących w firmach obranych jako cele. Próbują tak prowadzić rozmowę, aby nakłonić pracownika do wyjawienia pewnych informacji („flag”), między innymi o wersji przeglądarki lub rodzaju oprogramowania używanego w firmie. Wielokrotnie uczestnicy udawali kolegów z innego oddziału, których rzekomym zadaniem było zdobycie informacji dla prezesa. Przekonywali, że potrzebują bardzo pilnej pomocy, gdyż są kompletnie przytłoczeni nadmiarem obowiązków. W większości przypadków pracownicy chcieli pomóc i bez problemu dzielili się informacjami.

**Strach jest dochodowy** - scamerzy są doskonali we wzbudzaniu strachu. Popularny przykład: dzwoniący przedstawia się jako reprezentant pomocy technicznej Windows lub podobnego działu Microsoft i informuje ofiarę o wykrytym na ich maszynie problemie. Następnie prosi użytkownika o wpisanie na komputerze kilku standardowych komend i przekonuje, że otrzymany wynik wskazuje na obecność złośliwego oprogramowania lub innego, bardzo poważnego zagrożenia. W tym momencie ofiara myśli, że z jego komputerem dzieje się coś niedobrego i przekazuje „konsultantowi” dane karty kredytowej, aby ten rozwiązał problem.

**Weryfikować, weryfikować i jeszcze raz weryfikować -** jeżeli ktoś dzwoni i przedstawia się jako osoba z pewnej oficjalnej instytucji, warto poprosić o dowód. Zapytać się o numer telefonu, żeby móc oddzwonić. Jeżeli ktoś przedstawia się jako pracownik innego oddziału, należy poprosić o jakiś sposób weryfikacji w celu potwierdzenia tożsamości danej osoby. W przypadku służb porządkowych, poproś o numer odznaki. Jeśli rozmówca nie jest oszustem, bez problemu poda te informacje.

Nie ulegaj presji w stylu „musisz to zrobić w ciągu 20 minut”. Zawsze jest czas na zbadanie i przemyślenie sprawy.

Bądź zawsze sceptyczny w sytuacjach, gdy ktoś proaktywnie kontaktuje się z Tobą odnośnie jakiegoś problemu. Prawdziwa firma nigdy nie zapyta o hasło, organizacje rządowe zawsze wyślą oficjalny list. A gdy nagle otrzymasz telefon od przyjaciela lub znajomego, który twierdzi, że utknął gdzieś zagraniczną i potrzebuje natychmiastowego przelewu, nie ufaj mu tylko ze względu na to, że zna imię Twojego psa oraz nazwiska krewnych.

Bądź świadom tego, co udostępniasz w Internecie i korzystaj z ustawień prywatności. Istnieje kilka rzeczy, których nigdy nie powinieneś publikować online, np. hasła, odpowiedzi na pytania do odzyskiwania haseł (nazwisko panieńskie matki) oraz numeru PESEL.

W dalszym ciągu możesz być uczynny i pomocny, ale zawsze warto przez chwilę zastanowić się i przeanalizować sytuację. Odrobina sceptycyzmu nigdy nie zaszkodzi, a mając do czynienia z cyberprzestępcami - może być bardzo przydatna.

W Polsce dystrybutorami produktów Check Point są firmy Clico Sp. z o.o. ([www.clico.pl](http://www.clico.pl/)), RRC Poland Sp. z o.o. ([www.rrc.pl](http://www.rrc.pl/)) oraz Computerlinks Sp. z o.o. ([www.computerlinks.pl](http://www.computerlinks.pl/)).