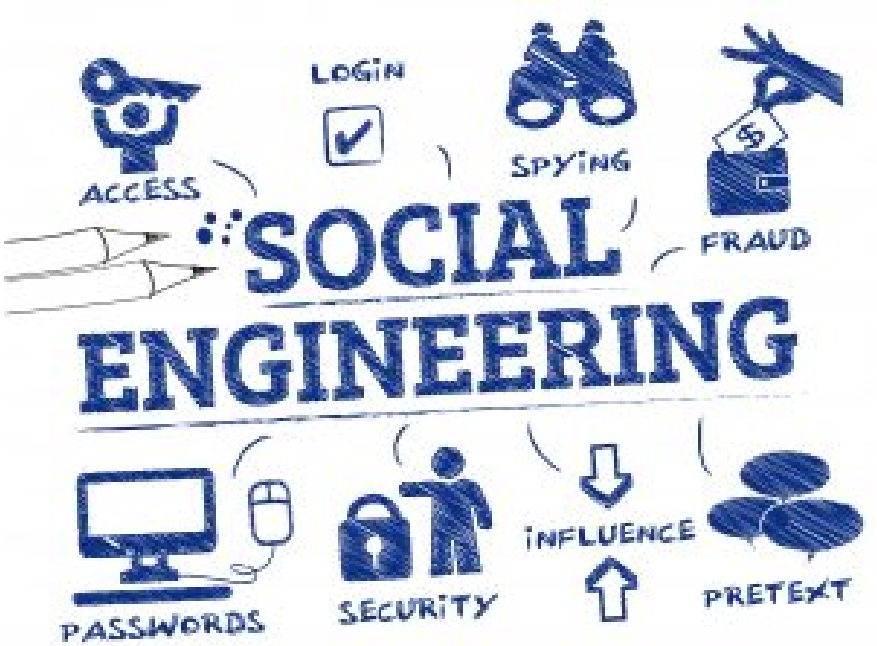
Ostatni numer Cyber Poradnika w 2019 roku poświęcamy socjotechnice, czyli najprostszej pod względem technicznym i zarazem najbardziej skutecznej formie przeprowadzania ataków cybernetycznych.

Kiedy myślimy o ataku cybernetycznych od razu do głowy przychodzą nam wyszukane techniki, zaawansowana znajomość narzędzi czy metod kompromitacji danych oraz szeroka wiedza z zakresu informatyki potencjalnego atakującego. Jednak cyberprzestępcy uciekają się do najprostszych i jednocześnie najskuteczniejszych metod oszustw, a mianowicie działania na naszą podświadomość. W tym celu wykorzystują metody, które określane są mianem socjotechniki. Internetowi oszuści nauczyli się, że łatwiej jest wpłynąć na ofiarę używając technik inżynierii społecznej.

Czym jest socjotechnika?



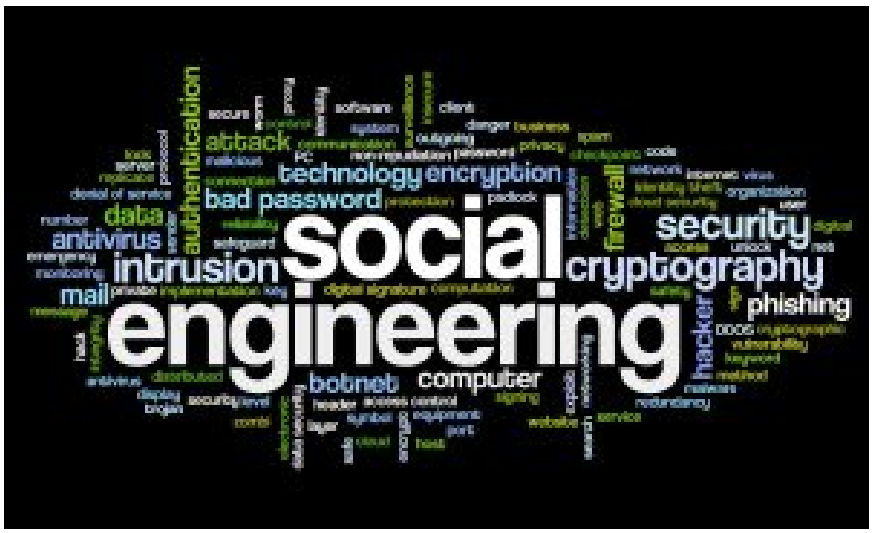
Ale czym dokładnie jest ta socjotechnika? Sam termin odnosi się do kilku dziedzin nauki – politologii, socjologii oraz marketingu i oznacza zespół technik za pomocą, których można dowolnie manipulować społeczeństwem celem osiągnięcia zamierzonych przez manipulatora skutków czy celów. Natomiast ataki cybernetyczne wykorzystujące inżynierię społeczną mają na celu nakłonienie ofiary do wykonania określonych działań. Wykorzystywanie socjotechniki w Internecie jest jednak o tyle skuteczniejsze, że przestępcy mogą mieć realny wpływ

na miliony użytkowników. Na inżynierii społecznej bardzo często bazują ataki phishingowe, które przedstawialiśmy w jednym z poprzednich wydań Cyber Poradnika.

Konstrukcja ataku z wykorzystaniem socjotechniki jest zazwyczaj bardzo podobna. Najczęściej bazując na emocjach, braku zachowania należytej uwagi bądź wytworzeniu przez atakującego wrażenia pilności/konieczności reakcji na kontakt ze strony ofiary,! użytkownik namawiany jest do konkretnych działań. Do najpowszechniejszych wymaganych działań należą:

- kliknięcie w podejrzany link w wiadomości;
- pobranie zainfekowanego pliku;
- przesłanie zainfekowanego pliku/linku dalej;
- wypełnienie formularza na podejrzanej stronie, który najczęściej wymaga podania wrażliwych danych użytkownika (PESEL, numer dowodu, numer klienta bankowości elektronicznej oraz hasło itp.);

Jak wykryć atak?



Najpopularniejszą radą jaką zawsze dajemy naszym klientom i użytkownikom to „Zachowaj zdrowy rozsądek!”. Wam również radzimy przede wszystkim nie dawać ponosić się emocjom podczas korzystania z Internetu. Do tego pamiętajcie również o kilku znakach ostrzegawczych, które mogą pomóc wam w identyfikacji, że macie do czynienia z atakiem z użyciem socjotechniki:

- **Szybko, już, TERAZ!** Jeśli osoba, która się z Tobą kontaktuje próbuje wywrzeć na Tobie jakąkolwiek presję podjęcia natychmiastowej decyzji powinieneś nabrać podejrzeń.
- **Informacja droższa od pieniędzy.** Również żądanie podania obcej osobie informacji, do których nie powinna mieć dostępu powinno wzbudzić Twoją czujność.
- **Loterie, wygrane, miliony za nic…** Umówmy się – jesteśmy dorośli i wiemy jak funkcjonuje współczesny świat. Jeśli ktoś kontaktuje się z Tobą i informuje, że wygrałeś główną nagrodę w loterii, w której nie brałeś nawet udziału na 100% jest to próba oszustwa i zagrania na Twoich emocjach. Pamiętajmy, że dzisiejszych czasach nie ma nic za darmo!

Jak się bronić i zapobiegać?

- **Nie podawaj hasła!** Żadna szanująca się firma czy organizacja nigdy nie poprosi Cię o podanie takich danych jak login czy hasło do Twojego konta na jakimkolwiek portalu/serwisie/usłudze internetowej. Każda taka próba powinna być traktowana jako oszustwo.
- **Uważaj czym się dzielisz.** Pamiętaj, że podczas tworzenia Twojego internetowego wizerunku przestępca przeprowadzając tzw. biały wywiad, czyli zbiera wszystkie leganie dostępne informacje na Twój temat. Wszystko co udostępniasz online za pomocą kont na portalach społecznościowych, forów internetowych czy recenzji produktów może pomóc internetowemu oszustowi na stworzenie pełnego obrazu ciebie, twoich przyzwyczajeń czy upodobań. Dbając o ilość i jakość udostępnianych

informacji na swój temat chronisz swój wizerunek i zmniejszasz ryzyko stania się ofiarom ataku.

- **Sprawdzaj kontakty.** Oczywiście może zdarzyć się tak, że będzie kontaktować się z Tobą osoba odpowiedzialna za prowadzenie usług bankowych, telefonii komórkowej, usług internetowych itd. Spróbuj w takim wypadku ją zidentyfikować. Poproś o podanie danych, numeru telefonu, pod którym możesz się z nią skontaktować. Następnie możesz za pomocą biura obsługi klienta zweryfikować te dane (którego numer znajdziesz na oficjalnej stronie firmy). Przydatne są również aplikacje umożliwiające zidentyfikowanie numeru, za pomocą którego ktoś próbuje się z nami skontaktować. My ze swojej strony polecamy zainstalowanie aplikacji True Caller, która umożliwia identyfikację dzwoniącego (ostrzega przed wyłudzeniami, spamem itp.).

Mamy nadzieję, że teraz wiesz już jak cyberprzestępcy używają socjotechnik, aby oszukać cię w Internecie. Liczymy również, że będziesz w stanie sam rozpoznać takie działania i im zapobiec. Pamiętaj również, że jeśli podejrzewasz, że ktoś próbuje wyłudzić od Ciebie informacje za pomocą inżynierii społecznej natychmiast zaniechaj kontaktu z taką osobą/organizacją! Zachęcamy Cię również do odwiedzenia naszych profili w mediach społecznościowych (Facebook oraz Twitter) , gdzie możemy podyskutować na temat bezpieczeństwa w sieci.

Czytałeś już nasze wcześniejsze numery **Cyber Poradnika**? Jeśli nie to serdecznie zachęcamy Cię do ich lektury i podnoszenia świadomości nt. cyberbezpieczeństwa.

Cyber Poradnik nr 1 – Bezpieczne zakupy

Cyber Poradnik nr 2 – Co zrobić, gdy padniesz ofiarą cyberprzestępcy?

Cyber Poradnik nr 3 – Phishing

Cyber Poradnik nr 4 – Użytkownik w podróży