Seniorze nie daj się oszukać: Socjotechnika - co to takiego i jak wpływa na Twoje emocje

Cyberprzestępcy kojarzą nam się zwykle z niezwykle zdolnymi hakerami, którzy do perfekcji opanowali technologię i potrafią złamać cyfrowe systemy bezpieczeństwa. Prawda jest inna. Większość cyberprzestępców wykorzystuje nie luki w oprogramowaniu komputerów, ale nieuwagę, brak wiedzy i błędy ludzi. Przydatniejsza od wiedzy informatycznej jest dla nich znajomość inżynierii społecznej, czyli socjotechniki oraz metod manipulowania emocjami.

Specjaliści od cyberbezpieczeństwa wiedzą, że najsłabszym ogniwem wszystkich systemów jest człowiek. Na nic nie zda się najbardziej skomplikowane hasło do logowania, jeśli użytkownik zapisze je na kartce przyczepionej do monitora. Wiedzą o tym również oszuści, którzy na wszelkie sposoby starają się wykorzystać ludzkie słabości do swoich celów.

Cyberataki z zastosowaniem socjotechniki stanowią zwykle przeciwieństwo spamu. Są skierowane do konkretnych osób, a przestępcy potrafią się do nich bardzo dobrze przygotować, zbierając potrzebne informacje. Wiedzą, że jeśli podadzą się za konkretnego członka rodziny (metoda na wnuczka), policjanta czy pracownika banku w którym masz konto to mają duże szanse wzbudzić zaufanie i uśpić twoją czujność. Oszuści mogą kontaktować się telefonicznie, mailowo a nawet przez SMS-y i media społecznościowe. Forma kontaktu ma znaczenie drugorzędne, dlatego w każdym przypadku powinniśmy zachować czujność.

Pośpiech nie jest dobrym doradcą

Przestępcy wiedzą, że gdy działając pod wpływem potencjalnego zagrożenia jesteśmy mniej uważni i nie myślimy w sposób krytyczny. Dlatego próbują wzbudzić w nas silne emocje np. sugerując, że ktoś właśnie włamuje się na nasze konto, albo że bliska nam osoba potrzebuje pomocy. Zwykle okazuje się, że trzeba podjąć określone działanie i to możliwie jak najszybciej. Może chodzić o przelanie pieniędzy na wskazane konto, podanie hasła jednorazowego, kodu BLIK lub danych do logowania. Rzekomy pracownik banku może też nakłaniać do zainstalowania jakiejś aplikacji, aktualizacji czy kliknięcia w link (prawdziwy przedstawiciel banku nigdy nie prosi o takie działanie!). Pamiętaj, że pośpiech jest złym doradcą i zawsze możesz poprosić o czas do namysłu.

Jeżeli zorientujesz się, że działasz pod wpływem emocji, które wywołał u Ciebie rozmówca, najlepiej przerwij rozmowę i rozłącz się. Koniecznie sprawdź, czy to, co zostało ci powiedziane przez telefon, jest prawdą. Zadzwoń do swojego banku, do rodziny, bliskich, albo nawet na policję i zweryfikuj usłyszaną historię. Prawdopodobnie okaże się, że nikt z banku ani z komendy do ciebie nie dzwonił, a twoim bliskim nic złego nie grozi.

W celu weryfikacji warto też korzystać z różnych kanałów komunikacji. Jeśli ktoś pisze do Ciebie przez media społecznościowe, warto do niego zadzwonić, bo może hakerzy przejęli jego konto. Gdy ktoś podszywający się pod bank wysłał ci maila - zadzwoń na infolinię banku.

Pamiętaj, że w starciu z cyberoszustami najlepszą strategią jest zachowanie spokoju.

O socjotechnice i emocjach opowiada Ewa Kasprzyk w filmie kampanii edukacyjnej „Bankowcy dla CyberEdukacji".
Zobacz!: https://youtu.be/exNJCSj4SxI

Program sektorowy „Bankowcy dla Edukacji" to jeden z największych programów edukacji finansowej w Europie. Jest on realizowany od 2016 r. z inicjatywy Związku Banków Polskich przez Warszawski Instytut Bankowości. Jego celem jest edukowanie uczniów, studentów i seniorów w zakresie podstaw praktycznej wiedzy dotyczącej ekonomii, finansów, bankowości, przedsiębiorczości, cyberbezpieczeństwa i obrotu bezgotówkowego.

Zapraszamy na stronę **www.bde.wib.org.pl**

BANKOWCY DLA EDUKACJI
program sektorowy