Seniorze, nie daj się złowić! Czym jest phishing i jak się przed nim bronić?

Podobnie jak wędkarze, oszuści zarzucają na nas przynętę, np. wiadomość e-mail, w której informują o wygranej, nieopłaconej fakturze lub innej sytuacji, która ma nakłonić do kliknięcia w przesłany link lub podjęcia innych - najczęściej szkodliwych dla nas - działań.

Podstawowym oszustwem internetowym jest tzw. phishing - jest to angielskie sformułowanie, które oznacza „łowienie haseł". Nie bez przyczyny oszustwo to jest tak nazwane, gdyż żeby zrozumieć jego mechanizm, najprościej porównać je do wędkowania. W prawdziwym życiu wędkarze łowią ryby w wodzie, natomiast oszuści internetowi próbują złowić twoje dane osobowe i poufne informacje w sieci. Robią to, wysyłając fałszywe e-maile, SMS-y lub komunikaty internetowe, które wyglądają, jakby pochodziły od rzeczywistych firm lub instytucji, takich jak banki, sklepy internetowe czy serwisy społecznościowe.

W fałszywych wiadomościach, które do złudzenia przypominają te prawdziwe, oszuści namawiają do kliknięcia w link, który prowadzi do podrobionej strony logowania. Jeśli podamy tam swoje prywatne dane, przestępcy będą mogli je wykorzystać. A dysponując naszymi danymi, mogą nawet ukraść pieniądze z naszego konta bankowego. Czasami wiadomości mogą zawierać szkodliwe załączniki, za pomocą których dochodzi do zainfekowania naszego urządzenia. Wykorzystując nasze emocje, np. lęk, strach, radość z wygranej, presję czasu (oferta jest aktualna tylko dziś), namawiają nas do podjęcia działań, które w rzeczywistości mogą mieć poważne konsekwencje.

Najpopularniejsze tematy fałszywych wiadomości to:

- niezapłacona faktura;
- problemy z kontem bankowym (np. informacje o zablokowanym koncie lub podejrzanych aktywnościach na koncie);
- wygrane w loterii, zniżki i kupony do popularnych sklepów;
- problemy z wypłaceniem dodatkowych świadczeń.

W jaki sposób możemy rozpoznać taką wiadomość?

- Dokładnie przeczytaj treść wiadomości i sprawdź, czy nie zawiera błędów językowych i stylistycznych, literówek. Nawet jeśli wiadomość wydaje się być prawdziwa, zweryfikuj nadawcę - należy sprawdzić adres e-mail, z którego pochodzi wiadomość. Jeśli informacja pochodzi z banku, a w e-mailu od nadawcy po znaku @ jest inna nazwa niż nazwa banku, to prawdopodobnie jest to oszustwo. Warto samodzielnie zadzwonić do firmy lub instytucji, która się z nami rzekomo kontaktuje i wyjaśnić sprawę telefonicznie lub w najbliższej placówce.
- Uważaj na wiadomości, które wykorzystują Twoje emocje (np. stres, lęk, presję czasu) i namawiają do podjęcia natychmiastowych działań.

- Jeśli coś wydaje się podejrzane lub zbyt dobre, aby było prawdziwe, zachowaj daleko idącą ostrożność i nie działaj na podstawie takich wiadomości.

Jak się chronić przed fałszywymi wiadomościami?

- Nie otwieraj wiadomości e-mail lub wiadomości tekstowych od nieznanych nadawców, osób, których nie znasz.
- Nie klikaj w przesłane do Ciebie linki i nie otwieraj załączników, jeśli nie wiesz, co się w nich znajduje.
- Uważaj na żądania poufnych informacji: oszuści często proszą o podanie hasła, numery kart kredytowych czy dane bankowe. Nie podawaj takich informacji przez e-mail lub wiadomości tekstowe.
- Jeśli korzystasz z poczty elektronicznej, mediów społecznościowych i bankowości elektronicznej - włącz weryfikację dwuetapową na swoich kontach online. Zrób to wszędzie, gdzie jest taka możliwość. To dodatkowa warstwa bezpieczeństwa, która utrudnia dostęp oszustom.
- Stosuj silne, długie i bezpieczne hasła. Pamiętaj, aby Twoja hasła nie zawierały informacji o Tobie ani Twoich bliskich. Do każdej usługi internetowej stosuj inne hasło.
- Zachowaj ostrożność w mediach społecznościowych. Bądź rozważna(-ny) podczas przyjmowania zaproszeń od nieznanych osób na platformach społecznościowych. Unikaj udostępniania poufnych informacji publicznie na swoim profilu.
- Regularnie aktualizuj system operacyjny, przeglądarki internetowe i oprogramowanie antywirusowe, aby być chronionym przed lukami bezpieczeństwa.
- Nie lekceważ komunikatów i alertów bezpieczeństwa, jakie wyświetlają się podczas korzystania z sieci.
- Naucz się rozpoznawać znaki ostrzegawcze wiadomości phishingowych i podziel się tą wiedzą z rodziną i przyjaciółmi.
- Jeśli otrzymasz podejrzaną wiadomość, zgłoś ją do zespołu CERT Polska. Poproś zaufaną osobę, aby pomogła Ci wypełnić formularz i przesłać zgłoszenie. Podejrzane wiadomości SMS możesz przekazywać bezpośrednio na numer 799-448-084.

CERT Polska - zespół ekspertów powołany do reagowania na zdarzenia i incydenty naruszające bezpieczeństwo w internecie oraz oszustwa komputerowe.

Podcast „3 grosze o ekonomii”

W audycji zostały poruszone takie zagadnienia jak phishing, spoofing i rady, jak nie dać się przestępcom oszukać i jak się chronić przed takimi oszustwami w sieci.

Link do audycji: 3 grosze o ekonomii - Nie daj się na metody cyberprzestępców! (google.com)

***

Materiał przygotowany w ramach kampanii pt. *#Halo! Tu cyberbezpieczny Senior*! przygotowanej przez NASK, Centralne Biuro Zwalczania Cyberprzestępczości w Policji oraz Warszawski Instytut Bankowości.

***