Uwaga na fikcyjne komunikaty o „zwrocie podatku”

Zagrożenie phishingiem cały czas rośnie, uważają Polacy. Już niemal 7 na 10 ankietowanych obawia się, że oszuści podszyją się pod jakąś instytucję albo osobę, a oni w dobrej wierze odpowiedzą i przekażą im swoje dane czy dostęp do konta - wynika z realizowanego dla BIK badania „Cyberbezpieczeństwo Polaków”. Okres składania rocznych zeznań podatkowych to dla cyberprzestępców dodatkowa, świetna okazja do nasilenia ataków z wykorzystaniem tej oszukańczej techniki. W tym czasie udają administrację skarbową i robią to na dużą skalę, bo z wyłudzaniem „na PIT” spotkało się w ubiegłym roku aż 15 proc. Polaków.

Wykorzystywanie wizerunku Urzędu Skarbowego to typowy przykład kampanii phishingowej - potwierdza NASK, Państwowy Instytut Badawczy. Ataki z wykorzystaniem tej metody nasilają się zwłaszcza w okresie zbliżającego się terminu rozliczenia rocznych zeznań podatkowych. Dlatego, bardzo ważna jest ostrożność i unikanie podawania swoich danych w reakcji na sms lub telefon o rzekomej nadpłacie lub niedopłacie podatku. Celem cyberprzestępców nie jest pomoc, lecz kradzież pieniędzy.

O co chodzi w phishingu

Z roku na rok oszuści usprawniają swoje metody przestępcze i coraz częściej łączą technologię z socjotechniką. Bez względu jednak na zastosowaną taktykę, schemat jest ten sam. Chodzi o to, by ofiara uwierzyła, że ma do czynienia z prawdziwą instytucją i kliknęła w link bądź ściągnęła sugerowaną aplikację. Niekiedy już nawet część danych wystarczy do podjęcia próby zaciągnięcia kredytu czy podpisania umowy abonamentowej z dostawcą usług telekomunikacyjnych na cudze nazwisko. Drogiego smartfona przestępcy otrzymają za złotówkę i sprzedadzą, a operator będzie oczekiwał, że ofiara przez dwa lata będzie opłacać rachunki.

Technologia - dobrodziejstwo czy przekleństwo

Uproszczone procedury w urzędach, bankach czy u notariusza, możliwość załatwienia coraz większej liczby spraw on-line to dobrodziejstwo naszych czasów - usprawnienie obsługi i ułatwienie dla wielu obywateli.

Według informacji Krajowej Administracji Skarbowej, zaledwie w ciągu trzech pierwszych dni od uruchomienia możliwości składania e-PIT-ów, podatnicy złożyli milion deklaracji. Bez wątpienia, forma elektroniczna jest najwygodniejszym sposobem rozliczenia PIT. Ten sposób złożenia deklaracji pozwala też oczekiwać szybszego otrzymania zwrotu podatku. Na tym właśnie żerują przestępcy. Podstawiają fałszywy komunikat o mniej lub bardziej spodziewanym zwrocie podatku lub koniecznej dopłacie. Ich próby padają na podatny grunt, szczególnie, gdy adresat działa odruchowo. Dodatkowym wabikiem może być informacja, iż niezwłoczne przekazanie im danych sprawi, że przelew z nadpłatą podatku zostanie zlecony jeszcze dziś.

Nasze emocje pomagają złodziejom

Fiskus może przysłać maila z informacją, co i dlaczego powinniśmy zrobić, np. skorygować, dosłać, **ale zalecenia urzędnika należy realizować już na rządowej stronie.** Jednak otrzymując informację, na wszelki wypadek **nie wolno klikać w załączonego w niej linka**, może on bowiem prowadzić do strony łudząco podobnej do rządowej. Nie wolno również otwierać załączników - można w ten sposób zainstalować sobie złośliwe oprogramowanie.

Administracja skarbowa, podobnie jak bank, **nigdy nie żąda podawania danych osobowych poprzez mail czy telefon**. Zasada ta tym bardziej dotyczy loginów czy haseł. Przestępcy jednak wykorzystują socjotechniczne chwyty, abyśmy zapomnieli o tych zasadach.

Technologia umożliwia oszustom podszywanie się pod znane nam numery telefonów urzędów czy instytucji finansowych. Mogą dać się złapać najbardziej zapobiegliwi, którzy pofatygują się, by sprawdzić numer na stronie internetowej urzędu. Pewni, że kontakt pochodzi od zaufanej strony, mogą podać kluczowe dla przestępczej działalności informacje. Z tego powodu najbezpieczniej jest **nie kontynuować rozmowy, nie korzystać z opcji „oddzwoń" w telefonie, ani nie odpowiadać na SMS-y z linkami.** Należy samemu wykonać połączenie na numer podany na oficjalnej stronie internetowej.

W przypadku kontaktu mailowego, trzeba **sprawdzić nadawcę**. Nie tylko nazwę jaka się wyświetla, ale przede wszystkim adres. Żaden urząd ani poważna instytucja nie wysyła informacji z darmowej skrzynki popularnych dostawców usług mailowych, na pewno też nie będzie się posługiwać domenami zarejestrowanymi w egzotycznych krajach. Np. rządowe adresy kończą się na „gov.pl". Banki po @ mają najczęściej swoją domenę, czyli adres swojej strony internetowej.

Dobry patent, by uchronić się przed wyłudzeniem
Co zrobić by uniknąć wyłudzenia? Wystarczy niewiele, bo raptem osobiste zainteresowanie stanem swojej historii kredytowej. Jednak, by zadziałało w praktyce, niezbędny jest nawyk systematycznego sprawdzania swojego Raportu BIK. Przejmując nad nim kontrolę, uda się uniknąć zaskoczenia, że pod naszym nazwiskiem widnieje zobowiązanie, o którym nic nie wiemy.
Można też chronić się przed wyłudzeniami na bieżąco, w czym pomagają Alerty BIK. To ostrzeżenia SMS lub e-mail z informacją o tym, że na przykład ktoś nieuprawniony wykorzystuje nasze dane i się pod nas podszywa. Dzięki temu mamy szansę szybko zareagować i powstrzymać oszusta.

Warto wziąć inicjatywę w swoje ręce. Chodzi przecież o bezpieczeństwo własnych danych i pieniędzy. A nawet najlepsze narzędzia informatyczne nie wystarczą, jeżeli sami nie zadbamy o swoje dane i podstawy bezpiecznego zachowania w sieci.

Oczywiście nad systemami bezpieczeństwa czuwają duże instytucje finansowe, np. banki. Beneficjentem zaawansowanych technologii stosowanych w przedsiębiorstwach jesteśmy my wszyscy. Jednak nie zwalnia to z odpowiedzialności samodzielnego nawyku dbania o swoje dane i kontrolowania własnych finansów.

Źródło: Badanie na zlecenie BIK, pt. „Cyberbezpieczeństwo Polaków", marzec/kwiecień 2023 r., CAWI, Polacy w wieku 18+, N 1057.

***

Biuro Informacji Kredytowej jest inicjatorem programu edukacyjnego Nowoczesne Zarządzanie Biznesem i partnerem w module „Zarządzanie ryzykiem finansowym w biznesie i życiu osobistym".

Więcej: www.nzb.pl oraz www.facebook.com/NowoczesneZarzadzanieBiznesem