Nowe metody cyberprzestępców. „Odchodzą od typowych ataków hakerskich”

Trzy czwarte Polaków nie potrafi rozpoznać linku, który powinien wzbudzić podejrzenia. Tymczasem wiedza, wyczulenie na próby manipulacji i odpowiednie zabezpieczenie komputera i swojego urządzenia mobilnego to najskuteczniejsze sposoby na ochronę przed utratą oszczędności bądź danych osobowych.

- *Doświadczenia wielu krajów pokazują, że spowolnienie wzrostu gospodarczego zwykle pociąga za sobą skok liczby wyłudzeń i innego rodzaju oszustw. Spodziewam się, że z podobnym zjawiskiem będziemy mieć do czynienia również w Polsce* - przewiduje Bartosz Wójcicki, dyrektor Biura Usług Antyfraudowych w BIK.
Według niego, w kolejnych kwartałach szczególnie narażone na wzmożoną aktywność przestępców będą zarówno osoby prywatne, jak i małe oraz średnie firmy.

Oszuści podsuwają ofiarom aplikacje. Nie wolno ich pobierać i instalować
Przekierowania na fałszywą stronę internetową banku w celu zalogowania, wysyłanie e-maili i SMS-ów o wygranej czy niezapłaconej fakturze - to działania, których celem jest zwykle skłonienie ofiary do kliknięcia w link umożliwiający kradzież środków lub danych.

Jednak eksperci BIK zwracają uwagę, że coraz popularniejszy wśród cyberprzestępców staje się tzw. vishing. To wszelkiego rodzaju próby manipulacji, podczas których oszuści np. podczas rozmowy telefonicznej podszywają się zarówno pod numer infolinii danej firmy, jak również pod pracownika banku, przedstawiciela firmy inwestycyjnej czy policjanta.

Jednym ze sposobów na oszustwo jest np. skłonienie ofiary do samodzielnego uruchomienia na komputerze bądź smartfonie aplikacji, za pomocą której można obserwować pulpit urządzenia ofiary i z łatwością odczytać loginy i hasła, a nawet przejąć kontrolę nad urządzeniem.

Złudne poczucie bezpieczeństwa. Każdy może paść ofiarą oszustów
- *Aż jedna trzecia Polaków nie obawia się wyłudzenia swoich danych osobowych. Jednak to złudne poczucie bezpieczeństwa może okazać się bardzo kosztowne. Każdy może paść ofiarą złodziei. Nawet świadomość istnienia ryzyka, pilnowanie danych tożsamości czy haseł do logowania nie dają całkowitej pewności, że nie dojdzie do ich wycieku* - podkreśla Andrzej Karpiński, dyrektor ds. Bezpieczeństwa Grupy BIK.

Uwagę zwraca też niewielka wiedza Polaków na temat skutków kradzieży danych. Na pytanie o możliwe konsekwencje takiego zdarzenia 18% respondentów odpowiedziało: „nie wiem”, a 16% posługiwało się ogólnymi stwierdzeniami, jak np.: „dużo złego”.

W specjalnym quizie o cyberbezpieczeństwie 75% ankietowanych nie potrafiło wskazać linku, który powinien wzbudzić niepokój i którego nie należy otwierać. Tymczasem aktywność przestępców nie maleje, a skradzione przez nich dane mogą zostać wykorzystane m.in. podczas próby wyłudzenia kredytu.

Antywirus to za mało. Tak należy chronić siebie i swoje urządzenia:

- Nie instaluj oprogramowania lub aplikacji pod wpływem rozmowy z rzekomym pracownikiem banku czy policjantem,
- Używaj programów antywirusowych i nie wyłączaj ich na prośbę nieznanych ci osób,
- Nie otwieraj linków z niezweryfikowanego źródła,
- Nie ufaj prośbom od znajomego, który za pośrednictwem mediów społecznościowych prosi Cię o pieniądze lub kod BLIK. Najpewniej doszło do włamania na jego profil,
- Stosuj mocne hasła do logowania,
- Jeśli nie możesz zapamiętać haseł, używaj dedykowanego Managera haseł,
- Korzystaj z 2FA (weryfikacji dwuskładnikowej np. za pomocą SMS),
- Miej aktywne Alerty BIK. Dzięki powiadomieniom sms lub e-mail szybko dowiesz się o możliwej próbie wyłudzenia kredytu na Twoje dane.

Źródło: Raport Antyfraudowy BIK 2022 r.

***

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