

Jak ustrzec się przed kradzieżą danych osobowych?

Każdy z nas ma praktycznie nieograniczony dostęp do informacji, aż 95 proc. osób korzysta z internetu każdego dnia. To zasługa rozwoju technologii informatycznych, które zmieniły sposób komunikowania się zarówno ludzi między sobą, jak również instytucji i firm. Pozytywne aspekty cyfryzacji praktycznie wszystkim użytkownikom sieci zakłóca cyberprzestępczość zagrażająca bezpieczeństwu osobistych danych. Wyłudzenia na skradzione dane boi się 54 proc. Polaków, a aż 84 proc. obawia się wykorzystania swoich personaliów w wyniku wycieku - i nie bez powodu - bo najnowsze raporty donoszą, że oszuści średnio 21 razy na dobę próbują wykraść nasze dane.



Imię i nazwisko oraz numer PESEL to dla potencjalnych złodziei danych cenne informacje. Znajdują się one nie tylko na naszych dokumentach (paszporcie, dowodzie osobistym, prawie jazdy). Są one także w sieci internetowej, w rejestrach, umowach czy dokumentach. O ile o bezpieczeństwo fizycznych dokumentów możemy w pełni zadbać sami, tak na pozostałe źródła naszych danych, nie zawsze mamy wpływ.

Gdy nasze dane osobiste wpadną w ręce oszustów, mogą im posłużyć do zaciągnięcia kredytu lub pożyczki, zawarcia umowy z firmą telekomunikacyjną, wynajmu samochodu, założenia firmy na skradzione dane itp.

Top 3 socjotechnik cyberprzestępców

W opinii osób, które wzięły udział w badaniu „Cyberbezpieczeństwo Polaków”, przeprowadzonym na zlecenie Biura Informacji Kredytowej na koniec marca tego roku, pierwsze miejsce na podium działań hackerskich zajął **phishing**.

Z tą metodą wyłudzenia miało styczność 34 proc. osób (21 proc. pośrednio, 13 proc. bezpośrednio). To socjotechnika, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji takich, jak numer dowodu osobistego, czy dane do logowania do konta bankowego.

Zaraz po phishingu plasuje się grupa ataków przestępczych, skoncentrowanych wokół wyłudzeń pieniędzy poprzez maile sprzedażowe, **informacje o szybkim zysku i wygranych**, a także o krótkoterminowych ofertach specjalnych na zakupy online. Wskazała na nie niemal co trzecia osoba (29 proc.).

Na trzecim miejscu niechlubnej trójki przestępstw znalazła się socjotechnika na **falszywe inwestycje**. Co piąty badany (20 proc.) spotkał się z oszukańczymi działaniami w postaci ogłoszeń kuszących łatwym zarobkiem i szybkim zyskiem.

Ostrożności nigdy za wiele, ale trzeba wiedzieć, jak się chronić

Choć powszechnie znane są zagrożenia związane z kradzieżą danych osobowych, to wciąż słaba jest wiedza na temat sposobów reagowania na takie zdarzenia. Niewiele osób wie, że można zabezpieczyć się przed szkodą, zamiast szukać rozwiązań dopiero po fakcie.

Zabezpieczyć się na przyszłość to korzystać z ostrzeżenia przed wyłudzeniami. Alerty BIK to usługa, która zapewnia szeroką ochronę przed wyłudzeniem 24 godziny na dobę. SMSy z BIK ostrzegają o próbie wykorzystania naszych danych. Ostrzeżenia przychodzą w momencie, gdy oszust próbuje zaciągnąć kredyt na nasze dane. W Alercie podana jest data oraz nazwa instytucji, w której składany jest wniosek. Alert zawiera także numer infolinii BIK - na wypadek, gdyby potrzebne było wsparcie w wyjaśnieniu sprawy.

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

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