Im mniej danych podajesz w sieci, tym lepiej

Dane osobowe i kontaktowe w rękach złodziei oznaczają wysokie niebezpieczeństwo. Mogą one zostać wykorzystane przez przestępców do oszustw, wspomaganych poprzez przebiegłe chwyty socjotechniczne, które bazują na ludzkiej naiwności lub nieuwadze, przenoszą ofiarę na fałszywą, ale łudząco podobną stronę naszej siłowni, ulubionej restauracji, firmy kurierskiej, a nawet swojego banku. Wpływ na bezpieczeństwo nas samych oraz naszych pieniędzy mają zachowanie, utrwalone nawyki, rozsądek.

Sposoby wyłudzenia poufnych informacji takich, jak numer dowodu osobistego, czy dane do logowania do konta bankowego to m.in. spoofing – metoda telefoniczna lub mailowa, polegająca na podszywaniu się pod prawdziwe organizacje (w tym banki), phishing – z wykorzystaniem sms lub połączenia telefonicznego, ataki spamowe – rozsyłane linki reklamowe, w które pochopnie klikamy i inne. Łączy je najczęściej efekt zaskoczenia, bazowanie na ludzkiej naiwności czy nieuwadze, często również na automatyzmie, którego sprzymierzeńcem jest pośpiech.

Top 3 socjotechniki cyberprzestępców

Trzy najczęściej wymieniane techniki hackerskie, z jakimi mieli styczność Polacy to:

- phishing – na który wskazało 34 proc. osób, z których styczność miało 21 proc. pośrednio, a 13 proc. bezpośrednio,
- grupa ataków przestępczych, skoncentrowanych wokół **wyłudzeń pieniędzy poprzez maile z informacjami o szybkim zysku i wygranych**, a także o krótkoterminowych ofertach specjalnych na zakupy online. Wskazała na nie niemal co trzecia osoba (29 proc.),
- socjotechnika na **fałszywe inwestycje**. Co piąta osoba (20 proc.) spotkała się z oszukańczymi działaniami w postaci ogłoszeń kuszących łatwym zarobkiem i szybkim zyskiem.

Wszystkie te formy kontaktu mogą wykorzystywać dane pochodzące również z wycieku.

Wyciek danych budzi uzasadnione obawy

Wycieku swoich danych z różnych instytucji obawia się aż 84 proc. Polaków. Tak wynika z ostatniego badania „Cyberbezpieczeństwo Polaków", przeprowadzonego na zlecenie BIK.

Doświadczenie potwierdza, że nikt nie jest w stanie przewidzieć, kiedy i z jakiej instytucji nasze dane mogą się wyciec. Nie ma też sposobów ani narzędzi, które za nas chronią personalia. O to musimy zadbać samodzielnie. Najlepiej zacząć od zmiany dotychczasowych nawyków:

- Uważajmy, gdzie pozostawiamy swoje dane, rozważnie dokonujmy transakcji płatniczych w sieci, dokładnie sprawdzając adresy portali internetowych. Upewnijmy się, czy oddzwaniamy na znany nam numer, nie odpisujmy anonimowym nadawcom;
- Korzystajmy z możliwości doboru grona osób, z którymi się komunikujemy, np. zamiast do wszystkich ograniczmy wiadomość do grup, znajomych albo zachowajmy jako prywatną. Nie udostępniajmy wszystkich informacji jako publicznych;
- Nie dawajmy się zwieść atrakcyjnym ofertom inwestycyjnym pod pozorem szybkiego zarobku (Komenda Główna Policji i FinCERT.pl – Bankowe Centrum Cyberbezpieczeństwa ZBP stale ostrzegają przed próbami oszustw przy inwestowaniu w kryptowaluty oraz na rynku Forex);
- Nigdy nie wiadomo, kiedy i skąd nasze dane zostaną skradzione, dlatego miej włączone Alerty BIK – ostrzeżenia sms, które otrzymasz, gdy ktoś na Twoje dane zaciąga kredyt, pożyczkę, umowę z operatorem telekomunikacyjnym, dokonuje zakupów na raty.