ROZDZIAŁ III. BEZPIECZEŃSTWO FINANSOWE SENIORÓW W CYFROWYM ŚWIECIE

Pani Krystyna dostała SMS-a z informacją o brakującej drobnej kwocie zapłaty za energię elektryczną. Natychmiast kliknęła w podany link. Wiadomość była fałszywa, a w wyniku kliknięcia w link pani Krystyna stała się ofiarą przestępstwa internetowego: mogły zostać wykradzione jej dane osobowe oraz mogła stracić pieniądze.

Z roku na rok coraz więcej płatności i innych operacji finansowych dokonuje się za pośrednictwem komputera i telefonu. Powoduje to nowe zagrożenia dla bezpieczeństwa naszych danych i finansów. Ofiarą takiego ataku może zostać każdy, a skutki mogą być bardzo bolesne: wyłudzenie danych osobowych i utrata pieniędzy. Wyjściem jednak nie jest nieużywanie nowoczesnych technologii i aplikacji w telefonach. Ważne, aby mieć świadomość zagrożeń i wiedzę, jak dbać o swoje bezpieczeństwo w Internecie. Wówczas nie kliknie się pochopnie „zgoda" w otrzymanej wiadomości, nie poda się hasła do swojego konta, rozpozna się i skasuje SMS-a rzekomo od banku lub zakładu energetycznego, który prosi o uregulowanie zaległej faktury, oraz nie zostanie się oszukanym podczas zakupów w Internecie. Natomiast gdy człowiek stanie się już ofiarą przestępstwa, warto wiedzieć, jak się zachować, jak i komu zgłosić to przestępstwo oraz gdzie szukać pomocy.

Na co szczególnie trzeba uważać?

Przestępcy internetowi znajdują wiele różnych pomysłów, żeby pozyskać nasze dane, loginy i hasła, przejąć dostęp do konta lub karty kredytowej, wyłudzić na nasze dane pożyczki lub dokonać zakupów. Poniżej przedstawiamy najczęściej spotykane metody oszustw (opracowane na podstawie infografik przygotowanych przez INPRIS w ramach programu dotyczącego cyberbezpieczeństwa „HAKI na CYBERATAKI" – więcej na naszej stronie internetowej: inpris.pl i na naszym profilu na Facebooku):

1. Oszust podszywa się pod inną osobę lub instytucję w celu wyłudzenia danych albo nakłonienia adresata do wskazanych działań (tzw. phishing), np. wiadomość z „banku" z prośbą o podanie hasła w celu jego weryfikacji lub z linkiem do fałszywej strony logowania czy też e-mail z danymi do zapłaty z fałszywym numerem konta.

Jak się chronić?

- Nigdy nie podawaj poufnych danych (login, hasło, numer karty) w odpowiedzi na SMS-y lub e-maile.
- Nie klikaj w linki zawarte bezpośrednio w treści takich wiadomości.
- Przy logowaniu do banku weryfikuj, czy adres strony WWW zaczyna się od liter „https".

- W razie wątpliwości zawsze możesz skontaktować się z rzekomym nadawcą w celu potwierdzenia autentyczności wiadomości.

2. Oszust podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych danych podczas rozmowy telefonicznej (tzw. vishing). Może to być np. telefon z „banku" z prośbą o podanie loginu czy też telefon od „ubezpieczyciela" z prośbą o podanie numeru PESEL.

Nigdy nie należy podawać przez telefon danych poufnych, takich jak login, hasło, numer karty, kod PIN, kod CVV z karty kredytowej.

Zawsze trzeba weryfikować osobę, z którą się rozmawia, chociażby prosząc o telefon za chwilę w celu zweryfikowania tożsamości dzwoniącego (np. na stronie WWW banku) lub dzwoniąc na oficjalną infolinię banku lub ubezpieczyciela. W razie podejrzenia próby wyciągnięcia informacji trzeba przerwać połączenie i ewentualnie zablokować numer.

3. Oszust (haker) podszywa się pod inne urządzenie lub użytkownika sieci w celu wykradzenia poufnych danych lub zainstalowania złośliwego oprogramowania (tzw. spoofing). Przykłady: podrobienie nagłówka e-maila tak, aby wyglądał jak od konkretnej osoby, manipulacje w celu skierowania użytkownika na podrobione strony internetowe. W tych przypadkach również mogą wyciec poufne dane lub nasz komputer zostanie zainfekowany.

- Nigdy nie podawaj poufnych danych (login, hasło, numer karty) w odpowiedzi na e-maile i SMS-y.
- Sprawdzaj dokładnie, czy adres e-mail nadawcy nie jest podejrzany.
- Zwracaj uwagę, czy strona internetowa lub przeglądarka nie zachowują się dziwnie lub inaczej niż zwykle.
- Warto też korzystać z aktualnych programów antywirusowych.

4. Cyberprzestępca przechwytuje dane przekazywane przez sieć (tzw. sniffing, czyli „podsłuchanie" przez sieć), np. poprzez zainstalowanie na komputerze ofiary programu służącego do „podsłuchiwania" ruchu sieciowego – jest to bardziej zaawansowana technika pozyskiwania poufnych informacji.

Jak możesz się chronić przed takim oszustwem?

- Unikaj używania publicznego i niezabezpieczonego Wi-Fi.
- Nie klikaj w podejrzane linki.
- Korzystaj wyłącznie z bezpiecznych i szyfrowanych komunikatorów i skrzynek pocztowych.
- Korzystaj z aktualnych programów antywirusowych.

Często okazją do prób oszustw finansowych w Internecie są zakupy w sklepach internetowych lub na platformach sprzedażowych.

Stosując proste zasady bezpieczeństwa, możesz się jednak ochronić przed tym zagrożeniem:

- **Uważaj na „wielkie promocje", „wyjątkowe oferty tylko dla ciebie" i „mega okazje, które za chwilę znikną"** – dokładnie sprawdzaj każdy szczegół takich okazji. Niekiedy kryją się za nimi pułapki przygotowane przez cyberprzestępców.
- **Zawsze sprawdzaj adres i stronę internetową sklepu.** Nazwa strony powinna zaczynać się od „https://" i mieć symbol kłódki. Każdy sklep powinien umieścić na stronie regulamin oraz swoje dane.
- **Uważaj na oszustów w serwisach ogłoszeniowych** (np. OLX, Vinted). Udają kupującego lub sprzedającego i wysyłają linki za pomocą wiadomości otrzymanych poprzez serwisy ogłoszeniowe, e-mail, SMS i in., kierujące do fałszywych stron internetowych, które przypominają serwisy ogłoszeniowe lub strony bankowe.
- **Uważaj na oszustów, którzy udają pracowników serwisów zakupowych** (np. Amazon, Shopee). Nie podawaj danych płatniczych przez telefon, nie klikaj w podejrzane linki przesłane np. SMS-em lub Messengerem, nie instaluj podejrzanych aplikacji.
- **Nie zapisuj swoich danych płatniczych.** Nasze urządzenia często podpowiadają opcję zapisywania przy wpisywaniu danych karty płatniczej lub kredytowej. Nie korzystaj z tej funkcji.
- **Ostrożnie z kodami BLIK.** Nie podawaj nikomu kodu BLIK. Zawsze sprawdzaj kwotę podczas akceptacji płatności.
- **Korzystaj z programów antywirusowych na komputerach i telefonach.** Pamiętaj o aktualizacjach.
- **Sprawdzaj opinie o sklepach.** Bądź ostrożny, gdy nie ma wielu opinii lub dużo jest głosów krytycznych.

Jeśli zdarzy Ci się paść ofiarą oszustwa w Internecie, zachowaj spokój, przeanalizuj, jak do tego doszło, zbierz wszystkie dane i zwróć się po pomoc do odpowiednich instytucji.

Gdzie szukać pomocy?

- **Twój bank lub ubezpieczyciel.** Możesz tam zadzwonić lub napisać w każdej niepokojącej sytuacji, gdy chcesz dowiedzieć się, jak postępować. Kontakt znajdziesz na stronie internetowej banku, w aplikacji bankowej lub na karcie kredytowej.
- **Powiatowy rzecznik konsumentów.** Działa w każdym powiecie. Bezpłatnie udziela porad i niekiedy prowadzi sprawy w imieniu konsumentów. Zapytaj o niego w swoim urzędzie powiatowym.
- **Infolinia Konsumencka (tel. 801 440 220).** Uzyskasz poradę i zostaniesz skierowany(-na) do odpowiedniej instytucji.

- **Biuro porad prawnych lub biuro porad obywatelskich.** Działają w każdej gminie w Polsce. Porady są udzielane bezpłatnie. Zapytaj w swoim urzędzie gminy.
- **Rzecznik Finansowy** (www.rf.gov.pl). Wspiera klientów w sporach z instytucjami finansowymi: porady, interwencje oraz postępowania polubowne i sądowe.
- **CERT Polska** (www.cert.pl). Można tu zgłosić incydenty związane z bezpieczeństwem Internetu – są one sprawdzane i wyjaśniane. Na stronie www.cert.pl znajdują się również ostrzeżenia co do domen internetowych prowadzących złośliwą aktywność, a także poradniki i informatory.
- **Policja.** Gdy już wiesz, że padłeś(-łaś) ofiarą przestępstwa, powinieneś/powinnaś jak najszybciej zgłosić sprawę na policję.
- **Adwokat lub radca prawny.** W przypadku ryzyka utraty dużych kwot lub potrzeby występowania w procedurach prawnych warto skontaktować się z adwokatem lub radcą prawnym.