UKNF | URZĄD KOMISJI NADZORU FINANSOWEGO

Napięta sytuacja geopolityczna stwarza ryzyko pojawienia się wzmożonej aktywności w polskiej cyberprzestrzeni osób próbujących zdestabilizować funkcjonowanie np. poszczególnych podmiotów sektora finansowego.

Rygorystyczne wymogi w zakresie cyberbezpieczeństwa dotyczące tych podmiotów przyczyniły się w ostatnich latach do osiągnięcia i utrzymywania wysokiego poziomu odporności polskiego rynku finansowego na potencjalne cyberataki.

Pamiętaj!

- **W przypadku czasowej niedostępności Twojej bankowości elektronicznej zachowaj spokój i nie ulegaj panice. Taki jest właśnie cel cyberprzestępców, wywołanie paniki, strachu i chaosu. Nie wspieraj ich w tym.**
- **Podmioty rynku finansowego posiadają profesjonalne i wyspecjalizowane zespoły reagowania na tego rodzaju incydenty. Daj im działać.**
- **Nie kieruj się anonimowymi opiniami czy komentarzami np. z mediów społecznościowych czy forów internetowych. Upewnij się, że informacje, które otrzymujesz pochodzą z wiarygodnego źródła, że nie są „fake newsami".**

Kradzież środków z konta bankowego

- **Nigdy nie podawaj nikomu przez internet lub telefon swoich danych osobowych, identyfikatorów, loginów ani haseł.** Oszuści mogą je wykorzystać do kradzieży środków z Twojego konta.
- Nie instaluj oprogramowania i nie ściągaj aplikacji pochodzących z nieznanych źródeł, szczególnie, jeżeli ktoś Cię do tego namawia.

Wiadomości z poleceniem potwierdzenia poświadczeń bezpieczeństwa

- **Zwracaj uwagę na otrzymane wiadomości e-mail oraz SMS** - może się zdarzyć, że otrzymasz SMS z prośbą o potwierdzenie poświadczeń bezpieczeństwa do bankowości elektronicznej lub poczty elektronicznej.
- **Weryfikuj nadawcę e-maila, nawet jeśli znasz jego adres e-mail** - oszuści potrafią podszywać się pod dowolnego nadawcę.
- **Bądź czujny, nawet jeżeli osoba dzwoniąca do Ciebie oznajmia, że jest przedstawicielem banku i zna niektóre Twoje dane (np. imię i nazwisko, numer karty bankomatowej, PESEL, adres zamieszkania)** - oszuści często podszywają się pod pracowników banku.
- **Nie otwieraj przesłanych załączników lub linków przekierowujących do strony, na której będziesz musiał poświadczać swoje hasła.**

Fałszywe strony banków i portali płatniczych

- **Fałszywe strony często zawierają błędy.** Zwracaj uwagę na poprawność językową strony, na której przekazujesz dane karty. W adresach, które widać w oknie przeglądarki często są błędne nazwy. Zwróć uwagę, czy nie została zmieniona kolejność liter lub dodane zostały inne litery lub znaki.