

OSTRZEŻENIE PRZED NOWYM RODZAJEM CYBERATAKÓW NA KLIENTÓW!

Bank zidentyfikował nowy sposób działania przestępców próbujących wykraść środki Klientów. Przestępcy, podszywając się pod numery infolinii, dzwonią do Klientów z prośbą o podanie kodów jednorazowych otrzymanych SMS-em.

Jak bronić się przed przestępcami:

- 1) Pamiętaj, NIE PODAWAJ NIKOMU haseł do bankowości ani kodów jednorazowych, które otrzymujesz w momencie dokonywania transakcji w bankowości.
- 2) Bank NIGDY nie prosi o podanie haseł jednorazowych ani haseł do bankowości.
- 3) Bank NIGDY nie prosi też o podanie całego hasła do kontaktu telefonicznego, a jedynie o wskazane znaki z hasła.
- 4) NIGDY nie otwieraj podejrzanych załączników. Przestępcy bardzo często wysyłają wiadomości z informacją o zaległych fakturach, podszywają się np. pod urząd skarbowy itp. Otwarcie załącznika (najczęściej .pdf, .doc, .exe, .xls, .zip) skutkuje zainfekowaniem komputera i wykradzeniem informacji.
- 5) Jeśli otworzyłeś podejrzany e-mail lub załącznik, NIE BAGATELIZUJ tego błędu – niezwłocznie oddaj komputer do wyczyszczenia przez specjalistów, zaloguj się do bankowości z innego urządzenia i zmień hasło, w razie pytań skontaktuj się z infolinią Banku.
- 6) Pobierz i zainstaluj system IBM Trusteer (dostępny na stronie logowania do bankowości Idea Cloud).

Jeżeli zadzwoni do Ciebie osoba przedstawiająca się jako pracownik Banku i poprosi Cię o podanie wymienionych wyżej danych uwierzytelniających, rozłącz się i niezwłocznie skontaktuj się z infolinią Banku.

Aby uzyskać więcej informacji o bezpieczeństwie, zajrzyj na stronę www.ideabank.pl/bezpieczenstwo.

W przypadku pytań pozostajemy do dyspozycji pod numerem telefonu 22 101 10 10 oraz 801 999 111 (infolinia czynna jest codziennie w godzinach od 8.00 do 20.00; koszt połączenia zgodny ze stawką operatora). Zachęcamy również do kontaktu poprzez bankowość internetową lub do wizyty w oddziale Banku. Lista oddziałów udostępniona jest pod adresem: www.ideabank.pl/oddzialy.