Bank Pocztowy

ostrzega o metodach oszustw cyfrowych

Bankowość internetowa jest wygodnym i bezpiecznym sposobem korzystania z produktów bankowych. Wykonując operacje bankowe należy pamiętać o podstawowych zasadach bezpieczeństwa i mieć świadomość o możliwym zagrożeniu.

JAK ROZPOZNAĆ PRÓBĘ CYFROWEGO ATAKU?

! Gdy otrzymasz SMSy rzekomo od Banku, mówiące o:

- zmianie danych osobowych (np. numer telefonu)
- kodzie SMS do autoryzacji operacji w bankowości internetowej

a nie wykonywałeś operacji, o których mowa w SMSie

! Gdy zauważysz na stronie bankowości internetowej, że ostatnie udane logowanie było wykonane w czasie, w którym nie korzystałeś z bankowości internetowej,

! Gdy przeglądarka internetowa żąda instalacji nowych certyfikatów lub strona bankowości internetowej wygląda lub zachowuje się inaczej niż zazwyczaj, np. żąda podania kodu SMS, nr Pesel itp.

JAK REAGOWAĆ?

Niezwłocznie skontaktuj się z Bankiem i poinformuj o niepokojących sygnałach.
Infolinia Banku: **tel. 801 100 500 dla telefonów stacjonarnych, 52 34 99 499 dla telefonów komórkowych oraz stacjonarnych krajowych i zagranicznych**
Pamiętaj, aby:

1. Zablokuj dostęp do bankowości internetowej, by uniemożliwić osobom niepowołanym dostęp do środków.
2. Zweryfikuj wszystkie ostatnio wykonane operacje na rachunkach, a w przypadku niezgodności, zgłoś reklamację.
3. Usuń złośliwe oprogramowanie na wszystkich urządzeniach (komputer/smartfon), najlepiej zwrócić się do serwisu IT. Zwykłe programy antywirusowe mogą nie być wystarczające.
4. Usuń zapisane dane do logowania do serwisu transakcyjnego z przeglądarek internetowych – jeśli korzystasz z zapisywania haseł
5. Zmień hasła lub sposób logowania na innym sprzęcie – gdy Klient korzysta z kont połączonych (np. Gmail), do których automatycznie loguje się na smartfonie lub w przeglądarce internetowej

ŹRÓDŁA INFEKCJI

Złośliwe oprogramowanie najczęściej jest pobierane/instalowane przez nieuwagę, niewiedzę lub przez to, że hacker podszywaj się pod „zaufane" dane lub oprogramowanie. Sposobów jest wiele, np.:

e-Maile wysyłane na skrzynki prywatne lub służbowe:

- napisane niepoprawną polszczyzną, wyglądające jak przetłumaczone przez program komputerowy
- obiecujące zarobki np. zakup złota po okazyjnych cenach
- zawierające załączniki, mogą to być dokumenty (doc, xls, pdf), archiwa (rar, zip), obrazki (jpg, png, bmp, gif).

Nigdy nie otwieraj załączników od nieznanych lub wzbudzających wątpliwości nadawców!

Aplikacje mobilne:

- instalowane z innych stron internetowych niż oficjalne (typu: GooglePlay lub AppStore)
- instalowane ze stron internetowych udających komunikaty programów antywirusowych, które informują o „zagrożeniu" i „bezpłatnej" możliwości przeskanowania urządzenia.

Zapisane dane logowania:

- identyczne hasła do różnych serwisów internetowych,
- łatwe, niezmieniane od lat hasła do serwisów takich jak Gmail – który przechowuje bardzo wiele danych dostępowych (loginy/hasła) i automatycznie jest logowany w przeglądarkach internetowych lub na smartfonach.

Każda z tego typu sytuacji może skutkować zainfekowaniem urządzenia złośliwym oprogramowaniem, które jest w stanie:

- pobierać wszelkie dane wprowadzane na klawiaturze urządzenia
- przesyłać osobom niepowołanym zrzuty z ekranu urządzenia
- przekazywać informacje o odwiedzanych stronach internetowych i danych w nich wpisywanych
- przekazywać informacje o tym kiedy urządzenie jest podłączone do sieci internetowej i kiedy można aktywnie je wykorzystać
- przechwytywać wiadomości SMS przychodzące na smartfon
- podstawiać w bankowości internetowej numer rachunku osób trzecich wbrew temu co jest prezentowane na ekranie.