Zasady bezpiecznego korzystania z bankowości elektronicznej

W Pekao24 dbamy o to, aby korzystanie z serwisów było nie tylko wygodne, ale także jak najbezpieczniejsze. Troszczymy się o bezpieczeństwo środków powierzonych naszemu Bankowi, a wszelkie dane dotyczące naszych Klientów są chronione zgodnie z obowiązującymi normami bezpieczeństwa i zachowania poufności. Bezpieczeństwo operacji zależy nie tylko od Banku, ale także od Klientów - istotne jest bowiem przestrzeganie zaleceń i zasad bezpieczeństwa związanych z korzystaniem z bankowości elektronicznej. Prosimy o uważne zapoznanie się z poniższymi zaleceniami oraz o powiadomienie Banku w przypadku zauważenia jakichkolwiek nieprawidłowości w funkcjonowaniu naszych usług, czy podejrzenia, że nastąpiła próba przejęcia dostępu do bankowości elektronicznej przez inne osoby.

Najważniejsze zalecenia bezpieczeństwa:

- **Loguj się wyłącznie osobiście.** Chroń dane do logowania i autoryzacji do Pekao24, dbaj o ich poufność i **nie ujawniaj ich nikomu**, nawet członkom rodziny czy znajomym.
- **Nie zapisuj ww. danych w miejscu łatwo dostępnym i widocznym dla innych osób**. Jeżeli zagubisz dane do logowania / autoryzacji lub podejrzewasz, że inna osoba poznała je, zgłoś to do Banku.
- Pamiętaj, by **nigdy nie podawać pełnego hasła podczas logowania do serwisów bankowości elektronicznej** - Bank zawsze wymaga wpisania tylko niektórych, losowo wybranych znaków.
- **Nie używaj do logowania adresu lub linku podesłanego w wiadomości e-mail.** Zachowaj ostrożność i ograniczone zaufanie w stosunku do wiadomości e-mail pochodzących od nieznanych nadawców. Zalecamy nie odpowiadać na takie e-maile i nie otwierać przesłanych załączników lub linków.
- **Nie podawaj poufnych informacji na stronach przypominających swoim wyglądem strony Banku**. Sprawdź czy strona do logowania serwisu internetowego posiada adres https://www.pekao24.pl/ oraz czy na ekranie widnieje symbol kłódki oznaczający nawiązanie połączenia szyfrowanego (adres zaczyna się wtedy od https, a nie od http).
- **Zawsze sprawdzaj przed zatwierdzeniem szczegóły autoryzowanej operacji** – w przypadku przelewów przede wszystkim pełen numer rachunku odbiorcy. Gdy autoryzujesz operacje kodem SMS zawsze sprawdzaj, czy treść wiadomości z kodem autoryzacyjnym jest zgodna z wykonywaną przez Ciebie operacją.
- **Nie instaluj żadnego dodatkowego oprogramowania na telefonie, aby odbierać kody autoryzacyjne SMS** - Bank tego nie wymaga. Bank nie wysyła również poprzez wiadomość SMS żadnych certyfikatów bezpieczeństwa.
- **Zwracaj uwagę na aplikacje instalowane na swoich urządzeniach mobilnych**. Infekcja telefonu grozi poważnymi skutkami nie tylko w odniesieniu do operacji bankowych. Bank nie rekomenduje pobierania i instalowania jakichkolwiek aplikacji ze źródeł innych niż oficjalne sklepy. Szczególną uwagę zwróć na aplikacje, do których linki otrzymałeś mailem lub SMS-em.
- Aby uniknąć zainfekowania komputera niebezpiecznymi wirusami, **korzystaj z legalnego oprogramowania i regularnie je aktualizuj.** Dbaj również o bezpieczeństwo własnego komputera poprzez stosowanie aktualizowanych na bieżąco programów antywirusowych oraz zapory sieciowej (tzw. firewalla). Jeżeli tylko jest to możliwe, podczas korzystania z bankowości internetowej używaj tylko własnego urządzenia.

  Przestępcy mogą próbować poprzez różnego typu manipulacje wyłudzić dane do logowania, skłonić do akceptacji transakcji lub zainfekować urządzenie złośliwym oprogramowaniem. Zainfekowane urządzenie umożliwia przestępcom śledzenie informacji pojawiających się na ekranie, sczytywanie znaków wprowadzanych na klawiaturze, przekierowanie do fałszywych stron internetowych lub podmianę ich treści (np. szczegółów autoryzowanego przelewu), a nawet pełne przejęcie kontroli nad urządzeniem.

  Do najpopularniejszych technik wyłudzania przez przestępców danych umożliwiających dostęp do bankowości elektronicznej i do składania dyspozycji za jej pośrednictwem należy **phishing**. Polega on na podszywaniu się pod inną osobę lub organizację (np. pod bank) w celu wyłudzenia określonych informacji (danych do logowania i autoryzacji w bankowości internetowej, danych o karcie płatniczej) lub nakłonienia ofiary do realizacji określonych działań. Przestępcy mogą stosować bardzo zróżnicowane metody pozyskania tego typu danych, np. wiadomości e-mail (rzekomo przesyłane przez banki), w których klienci są proszeni o podanie kodów autoryzacyjnych czy danych karty płatniczej (imię i nazwisko posiadacza, data ważności, kod CVV2). Przestępcy przygotowują również odpowiednio spreparowane strony internetowe, komunikaty (np. dotyczące blokady usług banków), formularze rejestracji, które do złudzenia przypominają oryginalne. Celem tego typu ataku jest takie zmanipulowanie ofiary, by nie była świadoma, iż podawane przez nią informacje trafiają do przestępców, a nie do upoważnionej instytucji.

Bank Polska Kasa Opieki Spółka Akcyjna z siedzibą w Warszawie, ul. Grzybowska 53/57, 00-950 Warszawa, wpisany do rejestru przedsiębiorców w Sądzie Rejonowym dla m.st. Warszawy w Warszawie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego, KRS: 0000014843, NIP: 526-00-06-841, REGON: 000010205, wysokość kapitału zakładowego i kapitału wpłaconego: 262 470 034 zł.

Bank Pekao

Coraz powszechniej do ataków na użytkowników bankowości elektronicznej stosowane jest również złośliwe oprogramowanie rozpowszechniane najczęściej jako załącznik do wiadomości e-mail. Treść wiadomości jest bardzo zróżnicowana i może sprawiać wrażenie autentycznej korespondencji i ma przede wszystkim nakłonić do otwarcia dołączonego załącznika lub skorzystania z zawartego w niej linku. Próba otwarcia takiego załącznika lub skorzystanie z linku prowadzi do instalacji złośliwego oprogramowania śledzącego aktywność użytkownika a następnie przejęcia danych do logowania i autoryzacji w bankowości elektronicznej lub modyfikacji danych np. w sposób niewidoczny dla użytkownika zmienić szczegóły przelewu. W przypadku zainstalowania złośliwego oprogramowania na telefonie komórkowym przestępcy mogą uzyskać nad nim pełną kontrolę, w tym przechwycić SMS-y i rozmowy.

- **Informuj** niezwłocznie Bank **o wszelkich podejrzanych sytuacjach**.

Zachęcamy do zapoznania się ze szczegółowymi informacjami dotyczącymi bezpieczeństwa, stanowiącymi rozwinięcie powyższych zasad. Znajdują się one *w Regulaminie Rachunków Bankowych Banku Pekao S.A. dla Osób Fizycznych* oraz na stronach internetowych Banku Pekao S.A. (https://www.pekao.com.pl/, https://www.pekao24.pl/l).

Nieprzestrzeganie powyższych zaleceń może nieść ze sobą następujące ryzyka:

- Utrata środków zgromadzonych na rachunku w Banku w wyniku uzyskania przez osoby nieuprawnione Państwa danych do logowania i autoryzacji, osoby te mogą złożyć zlecenie przelewu z Państwa rachunku na inny rachunek.
- Złożenie przez osoby nieupoważnione innego rodzaju dyspozycji w bankowości elektronicznej – np. zerwanie lokaty, otwarcie innego rachunku, zastrzeżenie karty płatniczej, skasowanie wiadomości w skrzynce odbiorczej w bankowości internetowej czy zmiana układu prezentowanych w niej treści.
- Konsekwencją może być utrata odsetek (przy zerwaniu lokaty), naliczenie opłat za usługi, które zainicjowała osoba nieuprawniona, odmowa realizacji transakcji kartą płatniczą w nieoczekiwanym momencie, czy utrata ważnej wiadomości od Banku ze skrzynki odbiorczej.
- Poznanie przez osoby nieuprawnione danych znajdujących się w bankowości elektronicznej.
- Podszycie się pod Klientów przez osoby trzecie w celu np. założenia konta w innym banku czy wzięcia kredytu w innej instytucji finansowej.
- Niektóre banki umożliwiają otwarcie u siebie pierwszego konta wyłącznie przez internet na podstawie przelewu, bez sprawdzania dokumentu tożsamości. Bank otwierający nowe konto ustala tożsamość klienta na podstawie danych nadawcy przelewu. Taki rachunek otwarty bez wiedzy Klienta, może być następnie wykorzystywany do celów przestępczych, w tym do prania pieniędzy, czy finansowania terroryzmu. Podobny mechanizm jest stosowany przez przestępców w celu wzięcia pożyczki przez internet.
- Udział w działalności przestępczej kierowanej przez inne osoby.

  Przestępcy mogą również nakłaniać Klienta Banku do pośrednictwa w przekazie pieniędzy pochodzących z przestępstw. Przyjęcie pieniędzy na swój rachunek bankowy i przesłanie dalej - np. w bankowości elektronicznej – może pomóc przestępcom w procederze prania pieniędzy (poprzez udział w realizacji łańcucha transakcji mających na celu zamaskowanie rzeczywistych, przestępczych źródeł pochodzenia pieniędzy) czy finansowania terroryzmu.
- Prosimy pamiętać, że dla przestępców równie cenne jak pieniądze mogą być dane osobowe czy informacje o wykonywanych transakcjach i wykorzystanie ich w celach przestępczych.

Nieprzestrzeganie zasad bezpieczeństwa zwiększa ryzyka, na jakie może być narażony użytkownik bankowości elektronicznej. Prosimy, pamiętaj o zaleceniach bezpieczeństwa, zwracaj uwagę na wszelkie niepokojące sytuacje i informuj o nich Bank.

W przypadku jakichkolwiek wątpliwości prosimy o kontakt z konsultantami Pekao24 pod numerem 801 365 365 lub 42 683 82 32 (opłata zgodna z taryfą operatora), którzy poradzą, jak zachować się w danej sytuacji.

Pozdrawiamy
Bank Pekao S.A.