Zasady bezpieczeństwa w bankowości elektronicznej

1. **Nie udostępniaj nikomu loginu i hasła do systemu bankowości elektronicznej, danych kart płatniczych (imię i nazwisko na karcie, numer karty, kod CVV, PIN), kodów BLIK.**
2. **W internetowych płatnościach przy użyciu karty stosuj metodę autoryzacji i identyfikacji posiadacza karty - 3D Secure.**
3. **Zanim zdecydujesz się na zakup w sieci Internet sprawdź opinie o oferencie lub sprzedającym.**
4. **Cyklicznie zmieniaj hasło do logowania w systemie bankowości elektronicznej.**
5. **Nie otwieraj podejrzanych linków w otrzymanych wiadomościach e-mail i SMS, w szczególności informujących Cię o oczekującej przesyłce kurierskiej, zwrocie podatku, braku opłaty za dostawę mediów (energii elektrycznej), wygaśnięciu subskrypcji na usługi sieciowe (np. Netflix).**
6. **Nie odpowiadaj na oszukańcze reklamy w mediach społecznościowych (np. Facebook) zachęcające do inwestowania pieniędzy w różne przedsięwzięcia, rzekomo promowane przez znane osoby.**
7. **Nie odpowiadaj na telefony od oszustów podszywających się pod pracownika banku, kancelarię prawną lub firmę współpracującą z Bankiem, w których oszuści starają się przekonać do przekazania im danych logowania i autoryzacyjnych do bankowości elektronicznej lub nakłaniają do instalacji oprogramowania na komputer lub aplikacji na telefon (np. AnyDesk, TeamViewer, QuickSupport), w celu późniejszego przestępczego przejęcia pieniędzy zgromadzonych na rachunku; Bank nigdy nie wymaga podawania loginu, hasła i kodu sms do bankowości elektronicznej, ani danych kart płatniczych, a pracownik w rozmowie telefonicznej nie poprosi o instalację jakiegokolwiek oprogramowania lub aplikacji na Twoim komputerze lub telefonie.**
8. **Zainstaluj i aktualizuj oprogramowanie antywirusowe, które może uchronić komputer i urządzenia mobilne przed wirusami oraz oprogramowaniem szpiegującym. Na bieżąco aktualizuj system operacyjny urządzenia oraz cyklicznie skanuj każde urządzenie programem antywirusowym.**
9. **Cyklicznie sprawdzaj, czy numery rachunków w przelewach zdefiniowanych nie uległy podmianie.**
10. **Przed potwierdzeniem transakcji zawsze weryfikuj zgodność numeru konta, na które przelewasz środki pieniężne z numerem odbiorcy oraz numerem, który jest w kodzie potwierdzającym transakcję, przekazanym z wykorzystaniem SMS (jeżeli ta funkcjonalność jest udostępniona).**
11. **Na bieżąco przeglądaj historię rachunku i operacji na każdej karcie płatniczej pod kątem podejrzanych transakcji. Jeżeli jest to możliwe, to włącz powiadomienia SMS o każdej wykonywanej transakcji.**
12. **Nie kopiuj numerów rachunków bankowych do przelewów („kopiuj-wklej”), ale wpisuj je samodzielnie i dokładnie weryfikuj.**
13. **Nie korzystaj z bankowości elektronicznej za pośrednictwem niesprawdzonych połączeń (np. publicznej WiFi).**

14. **Zadbaj, aby każde używane oprogramowanie pochodziło z legalnego i zaufanego źródła.**
15. **Jeżeli zaobserwujesz nietypowe lub podejrzane działania, niezwłocznie zgłoś ten fakt do banku, z którego usług korzystasz w ramach bankowości elektronicznej.**

PAMIĘTAJ! Twoje bezpieczeństwo finansowe w sieci zależy w pierwszej kolejności od Ciebie.

Komunikat dla klientów dot. wyłudzania danych przez telefon –„*vishing*”

Bank Spółdzielczy „Mazowsze” w Płocku, ostrzega swych klientów przed przestępczymi próbami wyłudzenia informacji o ich danych osobowych, rachunkach, danych logowania i autoryzujących operacje w kanałach elektronicznych. Oszuści – przestępcy podszywając się pod pracownika banku, kancelarii prawnej lub firmy współpracującej z Bankiem, stosując metody socjotechniczne, starają się przekonać w rozmowie telefonicznej klientów do przekazania im danych logowania (login, hasło) i autoryzujących transakcje – kodów sms lub nakłaniają do instalacji oprogramowania na komputer lub aplikacji na telefon, w celu późniejszego przestępczego przejęcia pieniędzy, zgromadzonych na rachunku, przy wykorzystaniu bankowości elektronicznej. Przestępcy mogą korzystać z techniki tzw. *spoofing`u* numeru telefonu, w taki sposób, by w Waszym telefonie wyświetlił się numer Banku!

W celu obrony przed tego rodzaju zagrożeniami, należy pamiętać, iż:

1) **Bank nigdy nie wymaga podawania loginu, hasła i kodu sms do bankowości elektronicznej;**
2) **Pracownik w rozmowie telefonicznej nie poprosi o instalację jakiegokolwiek oprogramowania lub aplikacji na Twoim komputerze lub telefonie;**
3) **Nigdy nie wolno podawać danych kart płatniczych (nr, PIN, kod CVV) i o dostępie do bankowości elektronicznej przez telefon;**
4) **Każdy przypadek prośby - żądania podania przez telefon jakichkolwiek danych, związanych z posiadanym rachunkiem bankowym, należy zgłaszać niezwłocznie do macierzystego Oddziału Banku;**
5) **Do kontaktów z Bankiem używać tylko nr. telefonów i adresów poczty elektronicznej, wskazanych przez Bank przy zawieraniu umowy o prowadzenie rachunku;**
6) **W każdej nietypowej sytuacji, budzącej wątpliwość lub podejrzanej należy skontaktować się ze swoim doradcą klienta w Banku.**

PAMIĘTAJ! Twoje bezpieczeństwo finansowe w sieci zależy w pierwszej kolejności od Ciebie.