



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 ofercie lub sprzedającym. Dokonuj zakupów na renomowanych platformach sprzedażowych.
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, przekazany 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.**