

Zasady bezpieczeństwa w bankowości elektronicznej

Urząd Komisji Nadzoru Finansowego kontynuuje kampanię edukacyjną dotyczącą bezpieczeństwa finansowego w bankowości elektronicznej. Przypominamy o podstawowych zasadach bezpieczeństwa w sieci.

- 1) Nie udostępniaj nikomu loginu i hasła do systemu bankowości elektronicznej.
- 2) Cyklicznie zmieniaj hasło do logowania w systemie bankowości elektronicznej.
- 3) Nie otwieraj podejrzanych linków w otrzymanych wiadomościach e-mail i SMS.
- 4) 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.
- 5) Cyklicznie sprawdzaj, czy numery rachunków w przelewach zdefiniowanych nie uległy podmianie.
- 6) 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).
- 7) 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.
- 8) Nie kopiuj numerów rachunków bankowych do przelewów („kopiuj-wklej”), ale wpisuj je samodzielnie i dokładnie weryfikuj.

- 9) Nie korzystaj z bankowości elektronicznej za pośrednictwem niesprawdzonych połączeń (np. publicznej WiFi).
- 10) Zadbaj, aby każde używane oprogramowanie pochodziło z legalnego i zaufanego źródła.
- 11) 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.