# Bezpieczeństwo Bankowości Internetowej i Telefonicznej

Aby bezpiecznie korzystać z **Bankowości Internetowej oraz Bankowości Telefonicznej**, pamiętaj o kilku podstawowych zasadach.

## Bankowość Telefoniczna:

- nie podawaj nikomu nadanego telekodu
- w przypadku podejrzenia dostania się telekodu w ręce osoby trzeciej natychmiast skontaktuj się z telefonicznym Centrum Obsługi Klienta w celu zmiany telekodu.

## Bankowość Internetowa:

1. **Korzystaj z najnowszych wersji przeglądarek internetowych.**
   **Zalecane przeglądarki w wersji desktopowej to:**
   - Firefox: http://www.mozilla.org/pl/firefox/new/
   - Chrome: http://www.google.pl/intl/pl/chrome/
   - Internet Explorer: http://windows.microsoft.com/pl-pl/internet-explorer/download-ie

   **Zalecane przeglądarki w wersji mobilnej (dla urządzeń typu smartfon, tablet itp.) to:**
   - natywna przeglądarka systemu Android (oznaczona ikoną Internet) lub Google Chrome – urządzenia z systemem Android
   - Safari – urządzenia z systemem iOS
   - Internet Explorer – urządzenia z systemem Windows Phone

2. **Stosuj dobre praktyki bezpieczeństwa:**
   - zwracaj uwagę na komunikaty przeglądarki
   - chroń swój identyfikator i hasło przed niepowołanymi osobami
   - podczas wpisywania loginu i hasła / PINu zwracaj uwagę, czy nikt nie podgląda wpisywanych danych
   - używaj funkcji *wyloguj się* zawsze po zakończeniu pracy
   - zamykaj wszystkie okna przeglądarki przed odejściem od komputera
   - nie korzystaj z funkcji:
     - autouzupełniania formularzy,
     - zapamiętywania haseł,
     - zapamiętywania sesji przeglądarki

     logując się do Bankowości Internetowej. Rozwiązania te są praktyczne, jednak niosą za sobą ryzyko dostępu do Twojego rachunku przez innych użytkowników komputera bez Twojej wiedzy.
   - sprawdzaj poprawność adresu URL – prawidłowy adres to: https://online.eurobank.pl

3. **Używając Tokena GSM / Aplikacji mobilnej:**
   - pobieraj aplikację tylko za pośrednictwem oficjalnych kanałów dystrybucji (App Store, Sklep Play, Sklep Windows Phone)
   - ustaw PIN do tokena / aplikacji mobilnej inny niż PIN do telefonu
   - zawsze sprawdzaj czy informacje o transakcji wyświetlone przez token / aplikację są zgodne z operacją, jaką zamierzasz wykonać
   - nie udostępniaj nikomu tokena / aplikacji mobilnej / danych karty do „płatności mobilnych Visa”
   - nie odblokowuj systemu operacyjnego swojego urządzenia mobilnego (tzn. rooting, jailbreak)
   - w wypadku utraty – niezwłocznie zgłoś to w placówce lub telefoniczne
   - nie korzystaj z funkcji logowania za pomocą odcisku palca, gdy na urządzeniu masz zarejestrowane odciski palców innych osób
   - jeżeli korzystasz z funkcji logowania za pomocą odcisku palca (aplikacja na system iOS) ustaw skomplikowany kod urządzenia. Jeżeli, ktoś pozna Twój kod urządzenia, będzie mógł dodać nowy odcisk palca i mieć dostęp do Twojej aplikacji mobilnej. Skomplikowany kod ustawisz w Ustawieniach urządzenia (wybierz opcję „Touch ID i kod”, a następnie odznacz „Prosty kod”). Pamiętaj aby chronić swój kod urządzenia.

4. **Używając Haseł SMS:**
   - zawsze sprawdzaj czy informacje o transakcji przesłane w treści SMS są zgodne z operacją, jaką zamierzasz wykonać
   - nie instaluj na telefonie komórkowym żadnego dodatkowego oprogramowania czy certyfikatów bezpieczeństwa, które miałoby podnosić poziom bezpieczeństwa wykonywanych transakcji lub dostępu do serwisu eurobank online
   - w wypadku utraty telefonu, na który wysyłane są Hasła SMS – niezwłocznie zgłoś ten fakt w placówce lub telefonicznie

5. **Regularnie aktualizuj swój system operacyjny i używane oprogramowanie.**
   Każdy system operacyjny, w tym również dla urządzeń mobilnych, wymaga regularnej instalacji aktualizacji, które usuwają błędy w oprogramowaniu. Niezałatane luki mogą zostać wykorzystane przez osoby trzecie do przejęcia danych poufnych. Bezwzględnie unikaj korzystania z systemów, dla których producent nie zapewnia wsparcia w postaci aktualizacji bezpieczeństwa, m. in. Windows XP, Me, 2000, 98, 95, Mac OS X 10.4 i starsze. Informacji o cyklu wsparcia dla swojego systemu operacyjnego szukaj bezpośrednio na stronie producenta.

6. **Korzystaj z programów antywirusowych zarówno na komputerze, jak i urządzeniach mobilnych (smartfon, tablet).**
   Dbaj o to, aby oprogramowanie to było zawsze aktualne i włączone. Systematycznie wykonuj skanowania całego komputera.

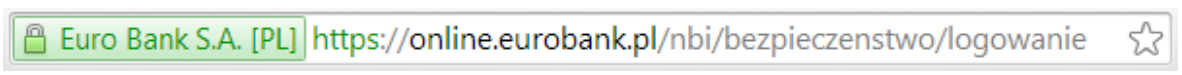
7. **Wykorzystuj jedynie legalne oprogramowanie.**
   Instaluj jedynie programy, do których masz zaufanie. Unikaj programów pochodzących z nielegalnych lub niepewnych źródeł – mogę one być zainfekowane szkodliwym oprogramowaniem szpiegującym użytkownika.

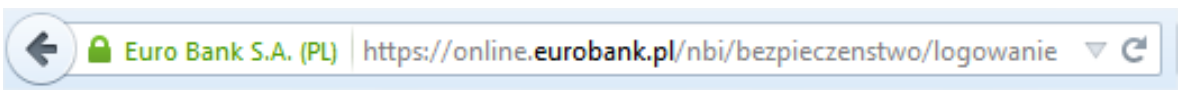
8. **Nie otwieraj załączników poczty e-mail, których nie oczekiwałeś.**
   Bardzo często szkodliwe oprogramowanie wykorzystuje do infekcji kolejnych komputerów pocztę e-mail. Zawsze ostrożnie podchodź do załączników od nieznanych osób lub takich, których nie oczekiwałeś otrzymać.

9. **Używaj osobistej zapory firewall.**
   Zapora firewall pełni funkcję strażnika, który kontroluje każdy ruch na styku komputera z Internetem, ograniczając przychodzące i wychodzące połączenia sieciowe. Na rynku dostępnych jest wiele różnych zapór firewall. W Windows Vista, 7 i 8 oraz Mac OS X firewall znajduje się już w systemie operacyjnym – wystarczy upewnić się, że jest włączony.

10. **Dbaj o bezpieczeństwo połączenia.**
    Komunikacja między komputerem użytkownika a serwerem banku szyfrowana jest protokołem SSL. Potwierdzeniem bezpiecznego (szyfrowanego) połączenia jest:
    - adres URL rozpoczynający się od **https** (zamiast standardowego http), gdzie „s” oznacza „secure” – bezpieczny
    - ikona kłódki na dolnym pasku przeglądarki lub pasku adresowym (miejsce zależy od rodzaju i wersji przeglądarki),

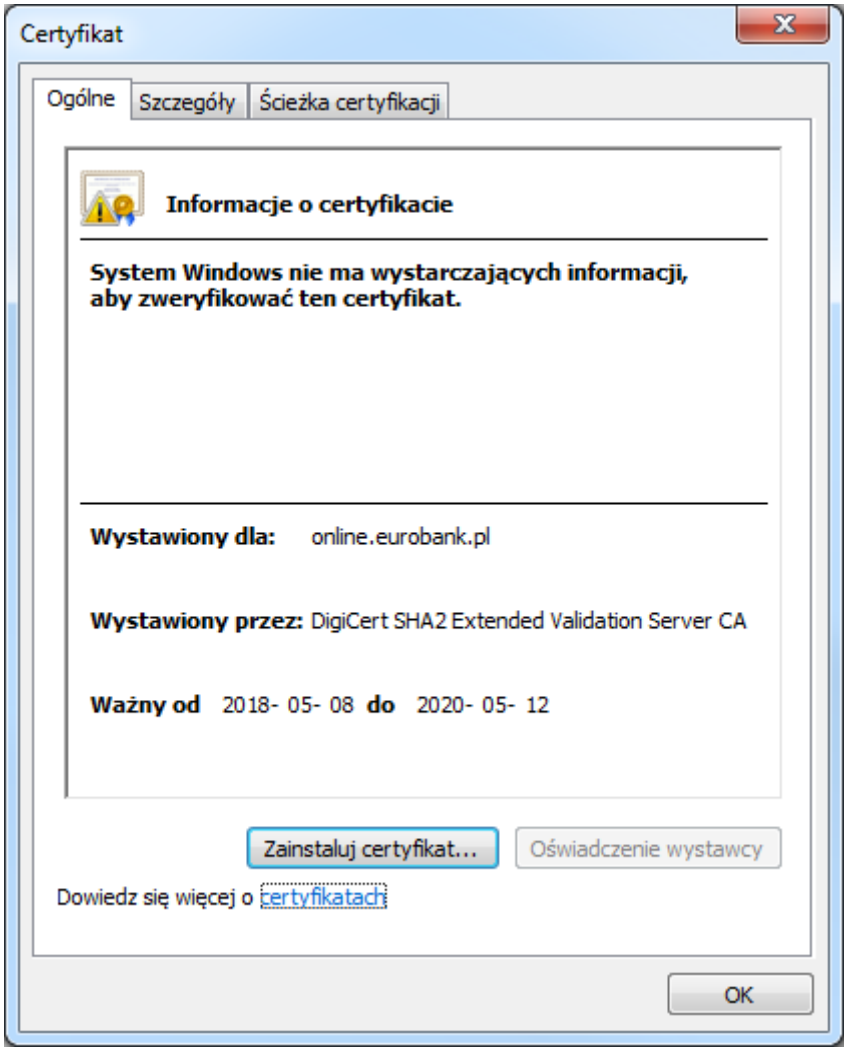
    Dodatkowo najnowsze przeglądarki obok paska adresu wyświetlają informacje o instytucji, dla której został wystawiony certyfikat, w tym przypadku: Euro Bank S.A. Poniżej przykład baneru w przeglądarkach Internet Explorer, Chrome i Firefox:

Certyfikat SSL służy do poświadczania autentyczności serwera, z którym komunikuje się dany komputer. Sprawdzenie szczegółów certyfikatu **przed zalogowaniem do serwisu** pozwala się upewnić, że strona, z którą nawiązane jest połączenie, to rzeczywiście strona eurobanku.

**Prawidłowy certyfikat Euro Bank S.A. powinien zawierać informacje:**
**- wystawiony dla: online.eurobank.pl**
**- wystawiony przez: DigiCert SHA2 Extended Validation Server CA**
**- ważny od: 08 maja 2018**
**- ważny do: 12 maja 2020**
**- numer seryjny: 04 d1 da 75 d5 56 0a 3d 99 6e e7 93 94 fc 5a 70**
**- odcisk palca: cd 20 91 ec d1 7b ae bf 67 85 8f df 37 42 09 ad 2f da 13 55**




**Uwaga!** Jeśli przy wejściu na stronę serwisu eurobank online przeglądarka wyświetli jakikolwiek komunikat ostrzegawczy dotyczący certyfikatu, skontaktuj się telefonicznie z eurobankiem pod numerem 19 000 (koszt wg taryfy operatora).

## 11. Zabezpiecz się przed atakami złośliwego oprogramowania i phishingiem.

Zainstaluj na Swoim komputerze i skorzystaj z programu **IBM®Security Trusteer Rapport™**, którego celem jest pomoc w zapobieganiu atakom złośliwego oprogramowania oraz incydentom wyłudzania poufnych danych przekazywanych drogą elektroniczną (phishing), będących punktem wyjścia do większości oszustw finansowych.
Dzięki współpracy eurobanku z firmą IBM, połączenie z internetowym serwisem transakcyjnym eurobank online zostanie objęte automatyczną ochroną programu Trusteer Rapport, który blokuje wszelkie próby nieuprawnionego dostępu do Twojego konta podejmowane przez złośliwe oprogramowanie. Ponadto program Trusteer Rapport jest zintegrowany z bankowymi procesami przeciwdziałania oszustwom finansowym.

Trusteer Rapport pomaga w zapobieganiu atakom złośliwego oprogramowania, ale korzystanie z tego programu nie zwalnia użytkownika z przestrzegania opisanych powyżej podstawowych zasad bezpieczeństwa.
Więcej informacji o programie oraz link do jego pobrania znajdziesz na http://www.eurobank.pl/trusteer-rapport

## 12. Uważaj na phishing.

Phishing jest szczególną formą przestępstwa informatycznego polegającego na skłonieniu użytkowników komputerów do ujawnienia swoich danych (nazwa użytkownika, hasło, numer PIN lub inne informacje o dostępach), a następnie wykorzystaniu tych informacji. Phishing jest szczególnie groźny dla użytkowników bankowości internetowej. Wiadomości phishingowe wysyłane do potencjalnych ofiar kierują na strony, które to podszywają się pod stronę bankowości internetowej.
Typowe sposoby poławiania poufnych informacji to:

- informowanie o rzekomym dezaktywowaniu konta i konieczności ponownej aktywacji – z podaniem wszelkich poufnych informacji; strona przechwytująca informacje jest wówczas łudząco podobna do prawdziwej
- informowaniu o potrzebie podania kolejnych wskazań tokena / Haseł SMS wymaganych do zalogowania się do serwisu (np. w celu synchronizacji tokena z Bankowością Internetową),
- tworzenie fałszywych stron serwisów z adresami bardzo przypominającymi oryginalne, a więc łatwymi do przeoczenia dla osób niedoświadczonych w obsłudze przeglądarki internetowej.

**Pamiętaj! Wszystkie wiadomości e-mail zawierające prośbę o podanie jakichkolwiek informacji lub zalogowanie się są podejrzane!**

Euro Bank S.A. nigdy nie poprosi Klientów o potwierdzenie loginu lub hasła pocztą elektroniczną ani nie podaje w wiadomościach e-mail odsyłaczy do strony logowania.
Jedynie na stronie serwisu www.eurobank.pl mogą znajdować się odsyłacze do logowania do serwisu eurobank online. W wypadku jakichkolwiek podejrzeń, co do autentyczności strony, przed zalogowaniem prosimy o kontakt telefoniczny pod numer **19 000** (koszt wg taryfy operatora).
Również w przypadku wykrycia potencjalnych transakcji oszukańczych lub podejrzanych zdarzeń prosimy o kontakt telefoniczny pod numerem **19 000** (koszt wg taryfy operatora). Wszystkie takie zgłoszenia będą rozpatrywane przez bank w trybie i terminach wskazanych dla zgłoszeń reklamacyjnych, opisanym w Regulaminie świadczenia Usług Bankowości Elektronicznej.

## 13. Widget / aktywny kafelek w aplikacji eurobank mobile.

Jeżeli korzystasz z widgetu (na urządzeniach z systemem Android lub iOS) lub aktywnego kafelka (na urządzeniach z systemem Windows Phone), rekomendujemy zabezpieczenie dostępu do Twojego telefonu czy tabletu za pomocą symbolu graficznego (łączenie punktów dla urządzeń z systemem Android) lub hasła. Dodatkowo, w przypadku systemu iOS, zalecamy wyłączenie dostępu do prezentacji widoku „Dzisiaj” przy blokadzie ekranu.
Tego typu zabezpieczenia można skonfigurować w Ustawieniach Twojego urządzenia:

- system Android - opcje: Blokada ekranu lub Bezpieczeństwo,
- system iOS - opcje: Kod lub TouchID i kod,
- system Windows Phone - opcja: ekran blokady.

Jeżeli korzystasz z widgetu w formie aplikacji na Apple Watch, rekomendujemy ustawienie kodu zabezpieczającego do zegarka, który uniemożliwi podgląd danych dotyczących Twoich finansów osobom trzecim.
Kod zabezpieczający włączysz w Ustawieniach zegarka Apple Watch, wybierając opcję Kod, a następnie Włącz kod.

## 14. Informowanie o zagrożeniach

Bank będzie informował Klientów o zagrożeniach związanych z korzystaniem z bankowości internetowej poprzez umieszczenie odpowiedniej informacji na stronie internetowej www.eurobank.pl, stronie logowania do serwisu eurobank online lub poprzez wysłanie wiadomości w serwisie eurobank online.
Bank będzie powiadamiał Klienta po potencjalnych transakcjach oszukańczych i podejrzanych zdarzeniach na rachunkach Klienta telefonicznie lub poprzez wysłanie wiadomości w serwisie eurobank online.

**Pamiętaj! Wszystkie wiadomości e-mail zawierające prośbę o podanie jakichkolwiek informacji lub zalogowanie się są podejrzane! Ponadto Bank nie przekazuje informacji na temat poprawnego i bezpiecznego korzystania z usług bankowości i płatności internetowych innymi kanałami niż wskazane w tym dokumencie.**