

ZBIÓR NAJWAŻNIEJSZYCH ZASAD BEZPIECZNEGO KORZYSTANIA Z KOMPUTERA I SMARTFONA

Poniżej przedstawiamy Ci kilka najważniejszych zasad, które pomogą uchronić Ci się uchronić w sieci.

I. Urządzenia mobilne:

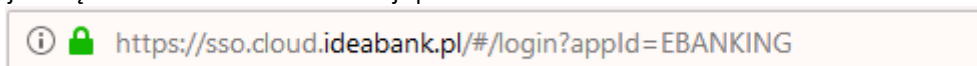
- Nie należy pobierać aplikacji z nieznanymi źródłami.
- Należy stosować zabezpieczenie urządzenia nr PIN lub hasłem.
- Jeśli to możliwe, warto zaszyfrować urządzenie.
- Nie jest zalecane wykorzystywanie automatycznego wypełniania haseł w przeglądarce.
- Należy dokładnie zweryfikować aplikacje pobierane ze sklepu – dokładna nazwa producenta, opinie, liczba pobrań, itp.
- Należy dokonać weryfikacji uprawnień wymaganych przez aplikację – kiedy aplikacja prosi o zgodę na bycie administratorem urządzenia, powinno wzbudzić to podejrzenia, ponieważ oznacza to, że będzie ona mogła dokonywać zmian na urządzeniu bez Twojej wiedzy.
- Należy instalować dostępne aktualizacje systemu i aplikacji.
- Należy reagować na nietypowe zachowanie urządzeń i aplikacji – najlepiej wtedy zmienić hasła do bankowości internetowej z innego bezpiecznego urządzenia, a podejrzaną aplikację oddać do zaufanego serwisu IT.

II. Komputery PC:

- Należy wykorzystywać tylko zaufane urządzenia, zwłaszcza do logowania do bankowości internetowej.
- Należy korzystać z oprogramowania antywirusowego wraz z aktualną bazą wirusów.
- Należy instalować na urządzeniach dostępne poprawki bezpieczeństwa zarówno dla systemu, jak i aplikacji (np. Microsoft Office, Adobe, Java).
- Nie należy instalować aplikacji z nieznanymi źródłami.
- Nie korzystać z niezaufanych sieci internetowych (publiczne hotspoty).
- Należy zabezpieczyć komputer długim, złożonym hasłem i zmieniać je okresowo.
- Należy pracować na komputerze bez uprawnień administratora i korzystać z funkcji Kontrola Uprawnień Użytkownika.
- Nie jest zalecane wykorzystywanie automatycznego wypełniania haseł w przeglądarce.

III. Korzystanie ze stron bankowości internetowej:

Zanim zalogujesz się do bankowości internetowej sprawdź:



- Czy adres strony zawiera protokół https.
- Czy w oknie adresu przeglądarki znajduje się „kłódka”, która oznacza, że połączenie jest szyfrowane. Upewnij się, że po jej kliknięciu pojawi się właściwa informacja o certyfikacie strony.