Bądź bezpieczny w sieci!

Zasady bezpiecznego korzystania z bankowości internetowej Centrum Usług Internetowych oferowanej przez Bank Spółdzielczy w Koronowie

Aby zminimalizować ryzyko ew. ataku na Państwa komputer bądź urządzenie mobilne (np. zainfekowanie złośliwym oprogramowaniem) należy mieć na uwadze poniższe wytyczne:

- Oryginalna wersja systemu operacyjnego z wykupionym wsparciem (aktualizacje)

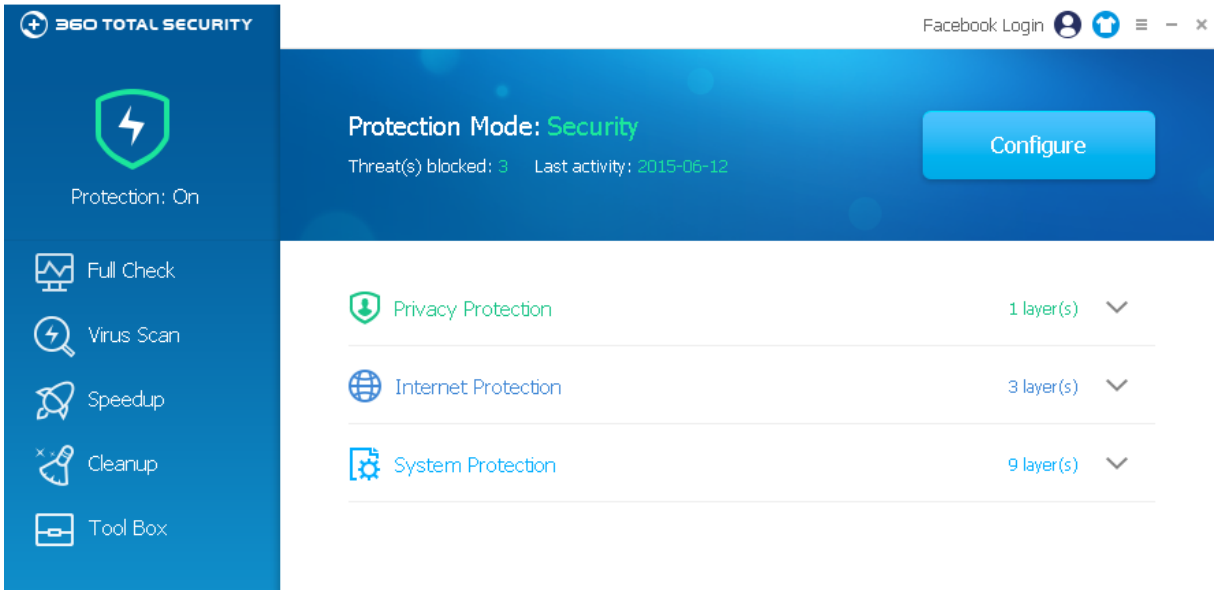
Powinni Państwo posiadać aktualny system operacyjny, który jest na bieżąco aktualizowany przez producenta. Do najpopularniejszych można zaliczyć: Microsoft Windows 7 / 8 / 10 (komputery), Android 5.x lub nowszy (urządzenia mobilne), Linux Debian / CentOS / RedHat lub inne, z aktywnym wsparciem producenta (bieżące aktualizacje gwarantują eliminację dotąd poznanych luk w zabezpieczeniach).

- Zainstalowane oprogramowanie antywirusowe wraz z aktywną aktualizacją sygnatur

Do użytku domowego dla komputerów polecamy darmowy program antywirusowy „360 Total Security" (https://www.360totalsecurity.com/en/download-free-antivirus/360-total-security/?offline=1).

Jego zaletą jest wbudowana "ściana ogniowa" (firewall), czyli dodatkowe zabezpieczenie monitorujące ruch sieciowy i potrafiące działać na zasadzie reguł automatycznych, bądź manualnych (blokowanie wybranych aplikacji itp.).

Oprogramowanie dostępne w angielskiej wersji językowej.



Istnieje na rynku szereg komercyjnych, płatnych antywirusów – dlatego jeśli nie posiadacie Państwo żadnego oprogramowania tego typu z aktualnymi, automatycznymi aktualizacjami bazy sygnatur, należy jak najszybciej zainstalować tego typu program.

Dla urządzeń mobilnych (smartfony, tablety) proponujemy aplikację „Zoner Antivirus" dla systemu Android (https://play.google.com/store/apps/details?id=com.zoner.android.antivirus&hl=pl) lub inny program antywirusowy, który potrafi działać „w tle".

- Korzystanie z bezpiecznej, najnowszej przeglądarki internetowej podczas przeglądania stron www

Zalecamy korzystanie z tych przeglądarek internetowych, które są na bieżąco aktualizowane (włączona opcja automatycznych aktualizacji). Dodatkowo warto pamiętać, aby ważniejsze strony internetowe, szczególnie związane z bankowością internetową zapisywać w zakładce „Ulubione" i w ten sposób korzystać ze stron lub logować się do systemów bankowości poprzez oficjalne strony banku (w żadnym przypadku poprzez odebrany email).

- Rozważne korzystanie z poczty elektronicznej (te same zasady dotyczą stron internetowych)

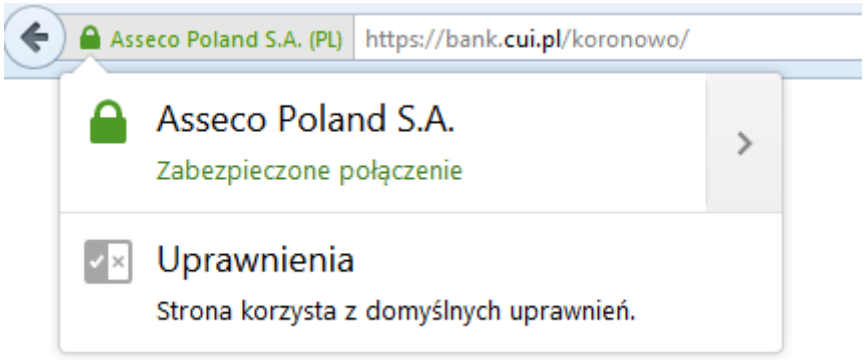
Często złośliwe oprogramowanie – nawet pomimo stosowania oprogramowania antywirusowego – przedostaje się do Państwa urządzeń poprzez świadome otwieranie załączników z poczty elektronicznej, które gdy pochodzą z niewiadomego źródła są najczęściej „zawirusowane". Dlatego nie otwierajmy załączników, nie naciskajmy na odsyłacze (adresy www) w poczcie internetowej lub na stronach internetowych, co do których pochodzenia nie jesteśmy pewni.

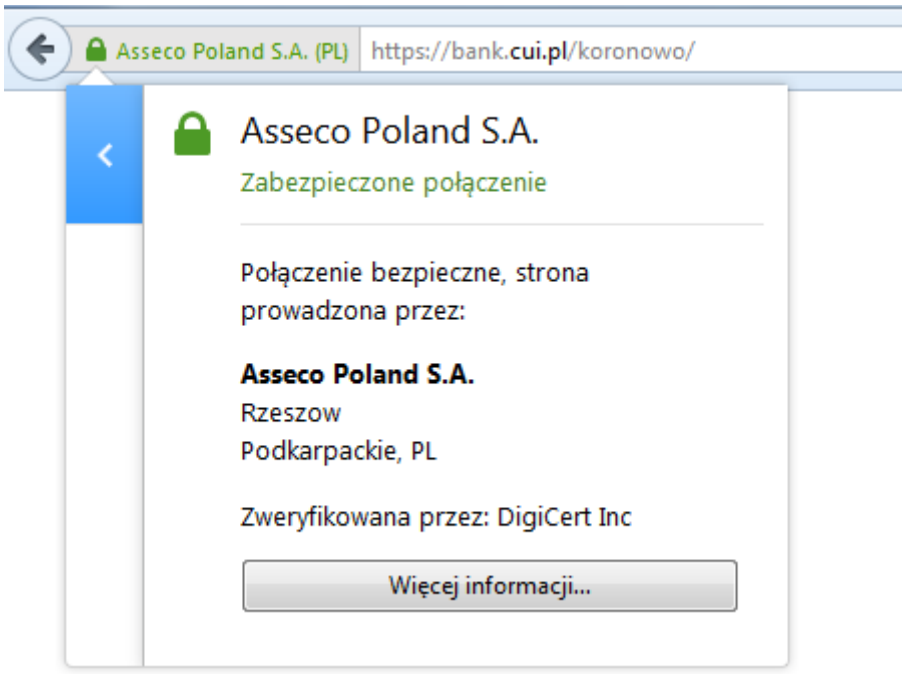
Przestępcy stosują różnego rodzaju ataki socjotechniczne mające na celu wzbudzić w Państwu ufność, stąd często można zauważyć e-maile np. rzekomo wysłane przez firmy spedycyjne lub operatorów sieci komórkowych. Podsumowując: jeśli nie zamawialiśmy żadnej usługi/produktu, tego typu wiadomość od razu usuwajmy.

- Bezpieczne połączenie ze stroną bankowości elektronicznej

Na stronie internetowej CUI oraz każdej innej udostępniającej bankowość internetową powinno być aktywne połączenie szyfrowane https. Należy zwrócić uwagę na początek adresu oraz symbol kłódki.

Poniżej przykład dla przeglądarki Firefox.



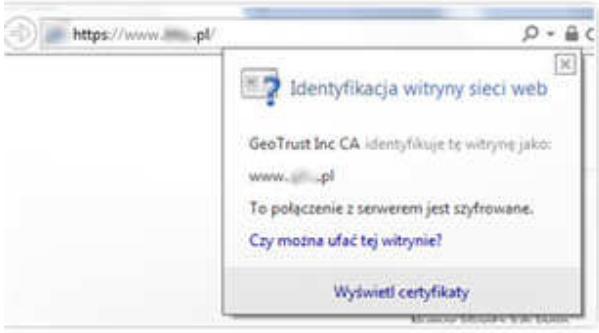


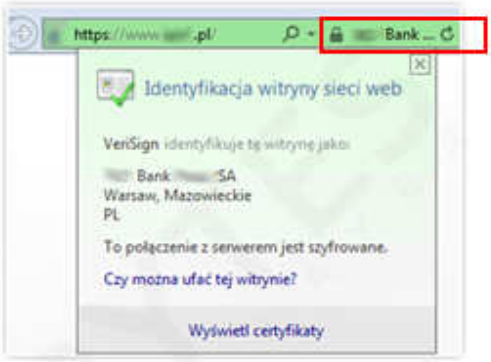
W związku z ostatnio wykrytymi atakami typu PACCA, **wyświetlana kłódka bez dodatkowych informacji nie jest wystarczająca**. Należy zwrócić dodatkowo uwagę na informację dotyczącą wystawcy certyfikatu oraz nazwy banku, która wyświetlana jest na wysokości kłódki (przykłady poprawnej informacji przedstawiono na kolejnej stronie na prawo, zaznaczone w czerwonym, prostokątnym obramowaniu):

FAŁSZYWY CERTYFIKAT

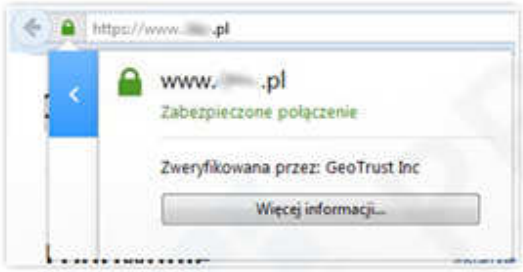
PRAWIDŁOWY CERTYFIKAT

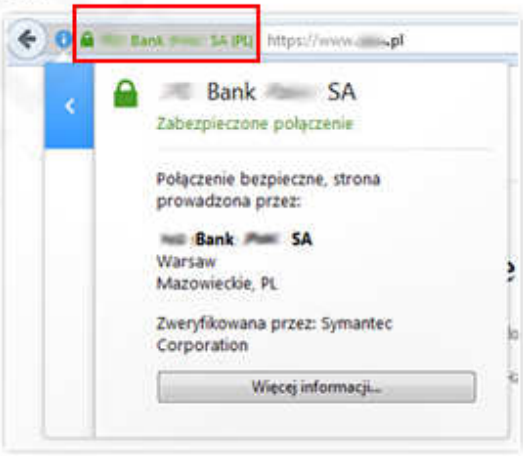
INTERNET EXPLORER





FIREFOX





CHROME