Bądź bezpieczny w sieci!

Zasady bezpiecznego korzystania z sieci Internet, w tym z bankowości internetowej 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)

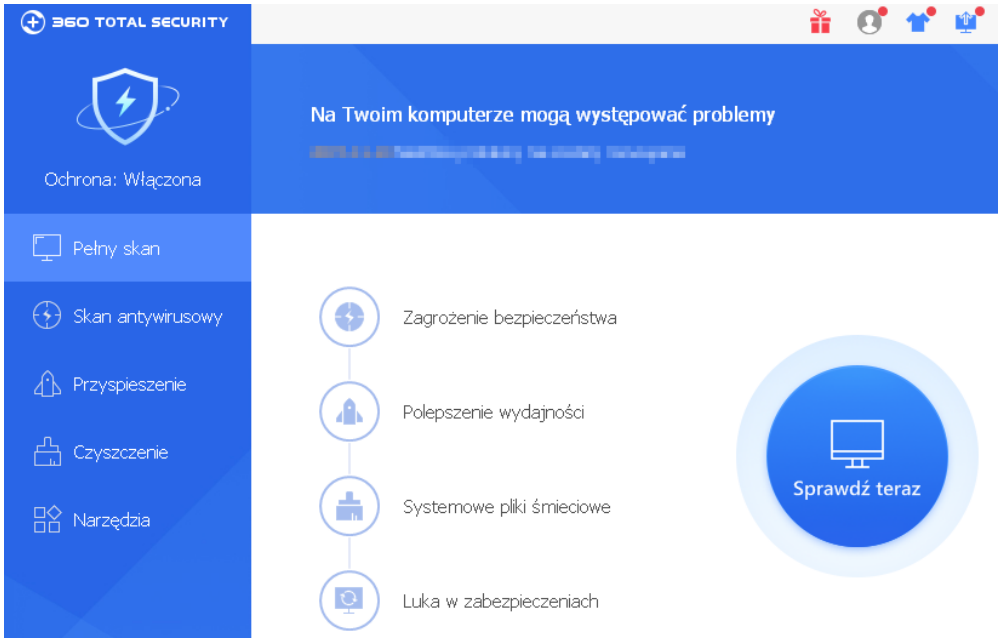
Powinni Państwo posiadać aktualny system operacyjny, który jest na bieżąco aktualizowany przez producenta. Do najpopularniejszych można zaliczyć: Microsoft Windows 10 (komputery), Android 9.x lub nowszy (urządzenia mobilne), Linux Debian / CentOS / RedHat lub inne, z aktywnym wsparciem producenta (bieżące 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/pl/).

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 do użytku prywatnego, również w polskiej 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 „Avast Antywirus" dla systemu Android (https://play.google.com/store/apps/details?id=com.avast.android.mobilesecurity&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). Nie polecamy za każdym razem wyszukiwania strony poprzez wyszukiwarkę google.

Przestępcy często wykupują reklamy stron, do których chcemy dotrzeć i znajdują się one na pierwszych stronach wyników wyszukiwania. Adresy stron wyglądają łudząco podobnie do oryginalnych, stąd istnieje ryzyko, że padniemy ofiarą przestępców i trafimy na „fałszywą" stronę, gdzie następnie przekażemy nasze dane do logowania, a tego na pewno nie chcielibyśmy doświadczyć.

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

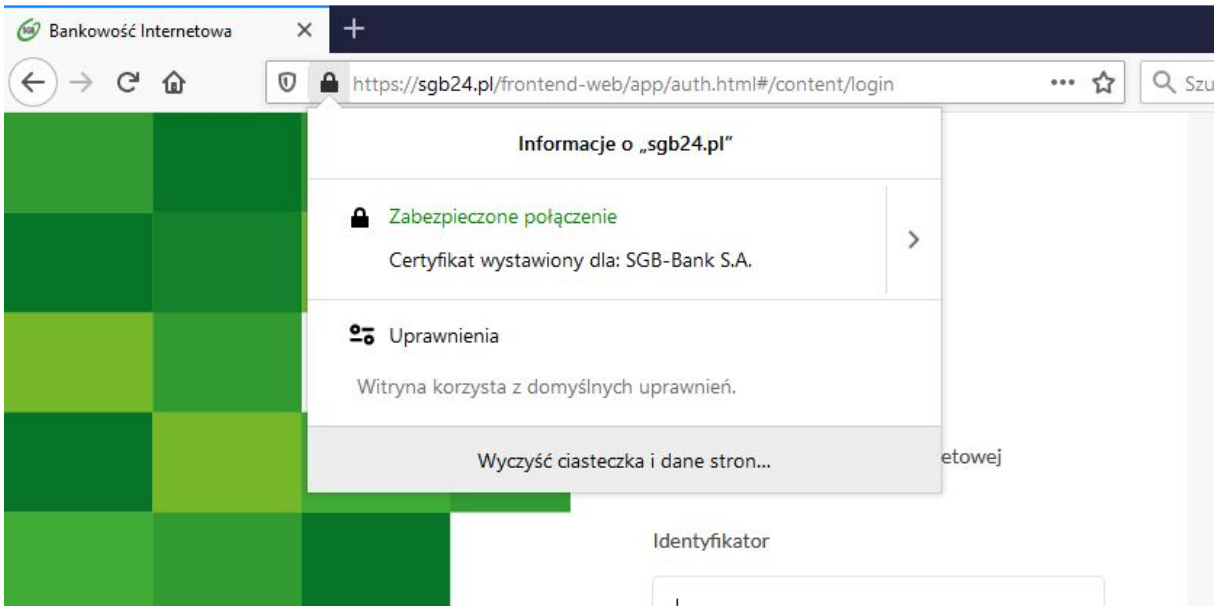
Często złośliwe oprogramowanie – nawet pomimo stosowania oprogramowania antywirusowego – przedostaje się do Państwa urządzeń poprzez świadome otwieranie załączników z poczty elektronicznej, które gdy pochodzą z niewiadomego źródła są najczęściej „zawirusowane". Dlatego nie otwierajmy załączników, nie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

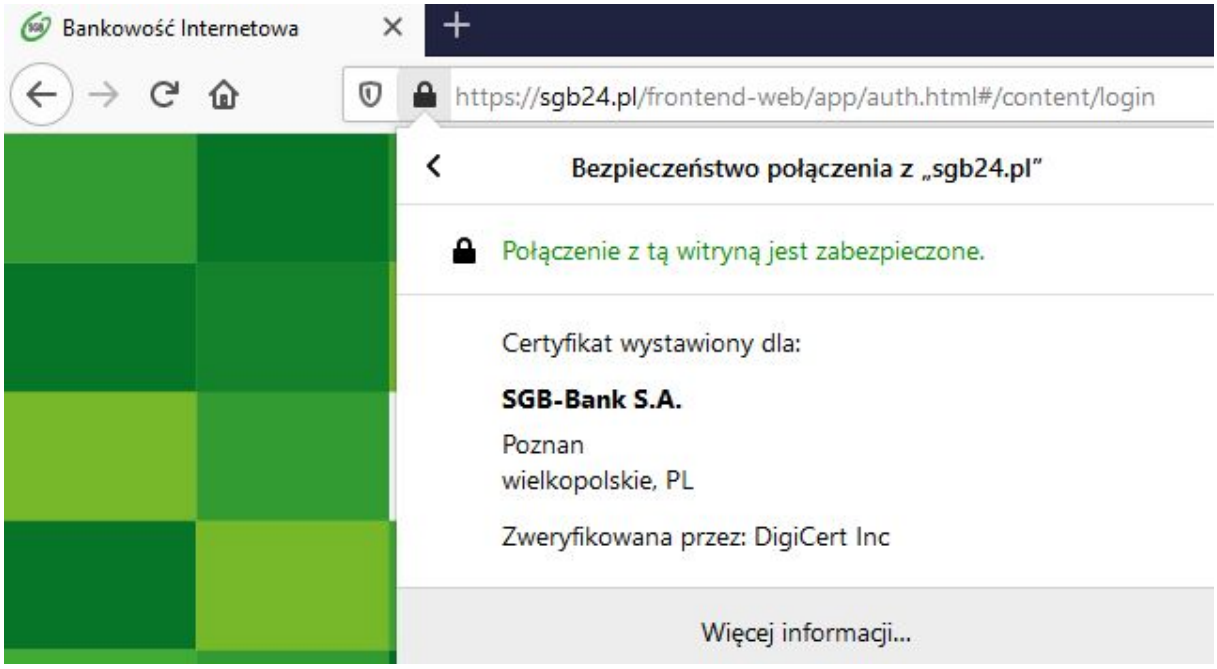
Przestępcy stosują różnego rodzaju ataki socjotechniczne mające na celu wzbudzić w Państwu ufność, stąd często można zauważyć e-maile np. rzekomo wysłane przez firmy spedycyjne lub operatorów sieci komórkowych. Podsumowując: jeśli nie zamawialiśmy żadnej usługi/produktu, tego typu wiadomość od razu usuwajmy.

- Bezpieczne połączenie ze stroną bankowości elektronicznej

Na stronie internetowej bankowości Banku Spółdzielczego w Koronowie (SGB24) oraz każdej innej udostępniającej bankowość internetową powinno być aktywne połączenie szyfrowane https. Należy zwrócić uwagę na początek adresu oraz symbol kłódki.

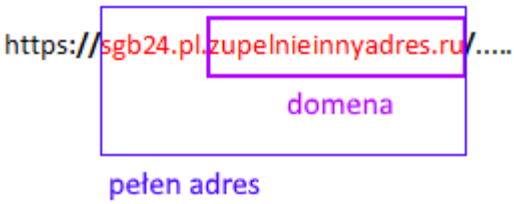
Poniżej przykład dla przeglądarki Firefox z początku 2021 roku, gdzie po wpisaniu adresu bankowości internetowej Banku Spółdzielczego w Koronowie widzimy:





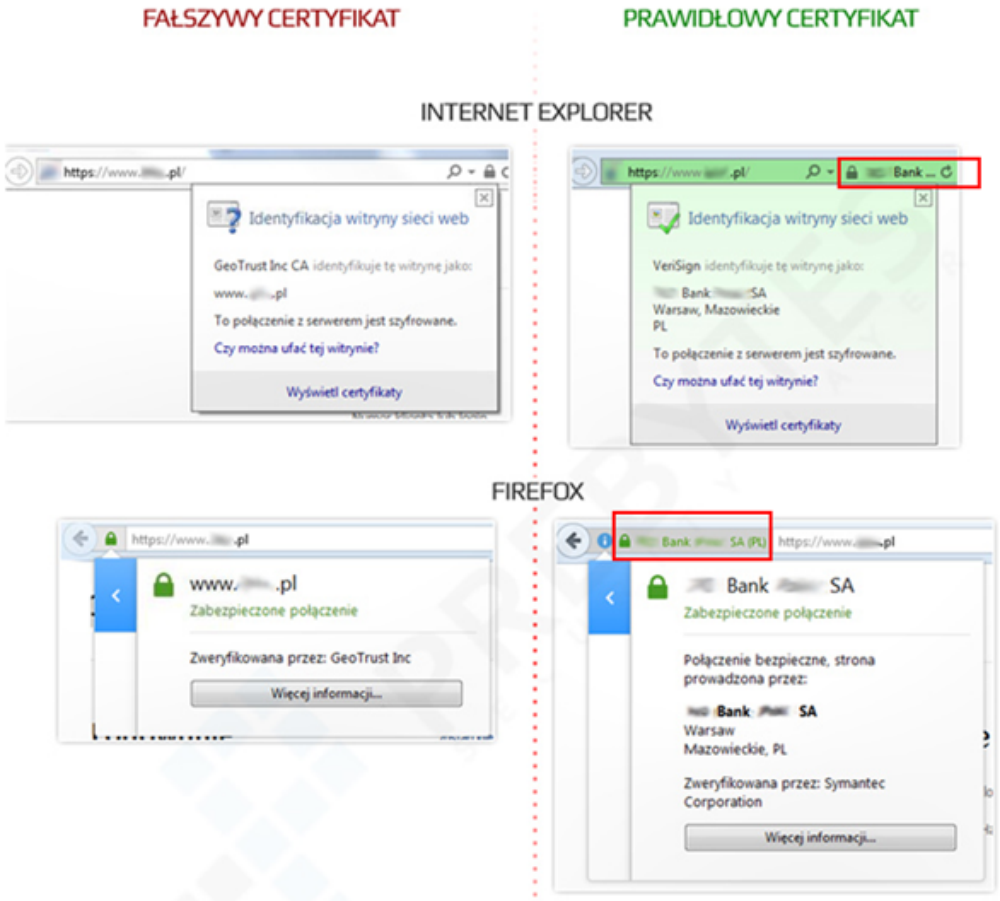
Strona bankowości jest tą „właściwą”, bezpieczną, ponieważ występują WSZYSTKIE poniższe elementy:

- adres rozpoczyna się od **https**
- widoczna jest ikona „kłódki” a po kliknięciu w nią, widoczny jest aktualny certyfikat przypisany do „SGB-Banku S.A.” czyli podmiotu oferującego bankowość
- adres internetowy pomiędzy wystąpieniem znaków **//** a **/** to sgb24.pl
  UWAGA: przestępcy mogą kierować Państwa na swoją stronę łudząco podobną do oryginalnej. Wówczas adres może być zmieniony na sgb24.ru lub sgbb24.pl – wszelkie odstępstwa w nazwie adresu są bardzo istotne. Może też być wykorzystana zupełnie inna domena internetowa (główny adres po **//** i przed pierwszym wystąpieniem znaku **/**) np.



W powyższym przykładzie widać, jak przestępcy manipulują pełnym adresem, wplatając do niego swoją własną domeną poprzedzoną po lewej stronie subdomeną „sgb24.pl”. Są to szczegóły techniczne, niemniej należy być świadomym w zakresie tego typu technik podmiany adresów. Ważne, aby znać dokładny adres strony, na którą chcemy się zalogować, przekazując w formularzu logowania swoje poufne dane.

Dodatkowo: napisano wyżej o wszystkich trzech elementach, które powinny być spełnione, gdy weryfikujemy autentyczność odwiedzanej przez nas strony np. dla bankowości internetowej. Samo słowo w początku adresu „https” i kłódka nie wystarczą. W związku z ostatnio wykrytymi atakami typu PACCA, **wyświetlana kłódka bez dodatkowych informacji nie jest wystarczająca**. Należy zwrócić 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):



- Płatności mobilne (alternatywa dla płatności przez przeglądarkę internetową)

Przy obecnym rozwoju technologii i tzw. płatności mobilnych, bardzo ważny jest aspekt tzw. świadomego bezpieczeństwa i umiejętnego korzystania z tego typu usług. Przykładem jest np. powszechnie dostępne google pay (wystarczy posiadać konto google w domenie @gmail.com lub/i urządzenie z systemem Android 4.x lub nowszym). Ważne zasady:

- gdy nie korzystamy ze smartfona w zakresie płatności mobilnych, **wyłączajmy** NFC
- nie udostępniajmy urządzenia z androidem i aktywnymi płatnościami mobilnymi innym osobom. Ew. odstępstwa należy traktować identycznie, jak udostepnienie karty płatniczej z możliwością płacenia nią przez inne osoby w naszym imieniu!
- nie wolno udostępniać nikomu nr karty płatniczej (ani innych danych z karty np. kodu CVV), kodów dot. płatności (np. blik) itp. Mogą one posłużyć przestępcom do kradzieży.
- smartfon powinien mieć zainstalowane oprogramowanie antywirusowe, a aplikacje należy pobierać tylko z oficjalnych źródeł.

- Zakupy w sklepach internetowych, portalach aukcyjnych/sprzedażowych itp.

Dokonując zakupów przez internet należy przestrzegać następujących zasad:

- zweryfikujmy stronę na której chcemy dokonać zakupu – czy posiada właściwy adres internetowy, szczególnie pierwszy człon pomiędzy znakami **//** oraz **/**

np.

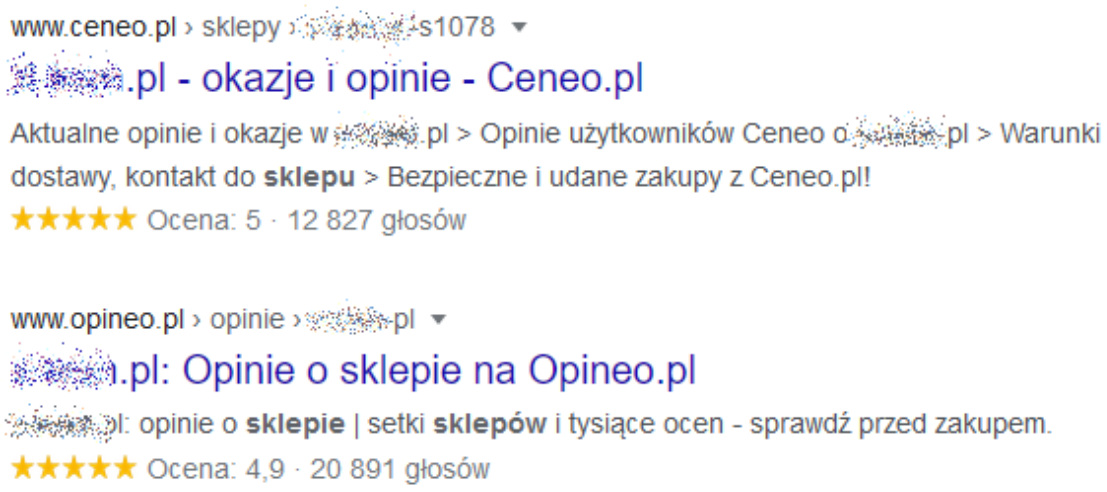
https:**//**www.olx.pl**/**oferty/

nieprawidłowe wersje dla powyższego (jeśli otrzymamy w emailu/sms) to np.

https://www.o1x.pl/

https://www.olx.pl.jakisdziwnyadres.pl/

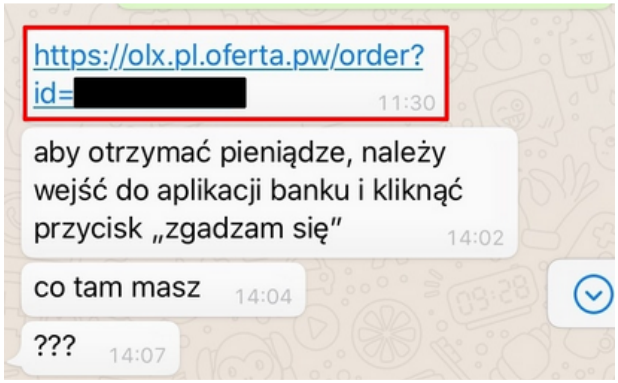
- zanim cokolwiek kupimy i odwiedzamy stronę pierwszy raz, zorientujmy się w internecie (poprzez wyszukiwarkę google), jakie opinie posiada sklep – np. w serwisie ceneo.



Adres przykładowego sklepu jest zamazany na potrzeby niniejszej publikacji

- zapoznajmy się z regulaminem strony lub chociaż z zasadami zakupów – w 99% przypadków zakupy odbywają się bezpośrednio na stronach sklepu / portalu.
  W przypadku portali aukcyjnych, przestępcy często próbują np. w prywatnych wiadomościach do Państwa (udając zainteresowanych kupnem przedmiotu) przysyłać adresy do podejrzanych stron sugerując, że tam będą mogli Państwo np. odebrać od nich pieniądze poprzez szybkie płatności w internecie. To już pierwszy sygnał ostrzegawczy i należy tego typu wiadomości ignorować a najlepiej od razu zgłaszać do właścicieli sklepu / portalu.

Przykład takiej wiadomości np. poprzez aplikację WhatsApp (przestępca – kupujący, pozyskując nr tel z ogłoszenia, wysłał poniższą wiadomość do sprzedawcy sugerując, że wejście na podany w wiadomości adres zagwarantuje otrzymanie pieniędzy.. widać, że adres jest „podstawiony", prawdziwy to https://olx.pl/ a przestępca przysyła niebezpieczny odsyłacz https://olx.pl.**oferta.pw/**



- Komunikacja z bankiem

Należy pamiętać, że Bank komunikuje się z Państwem wyłącznie poprzez kanał elektroniczny (e-mail, sms, publikacja informacji na stronie www/w bankowości elektronicznej), telefoniczny (rozmowa głosowa) i w żadnym z tych kanałów NIE PROSI WPROST O INSTALACJĘ OPROGRAMOWANIA DO OBSŁUGI ZDALNEJ. Przestępcy często próbują podszyć się pod pracownika Banku i pozyskać od Państwa poufne dane (np. dane do logowania do bankowości). Pod żadnym pozorem nie należy przekazywać takich danych podczas rozmowy. Należy ignorować wszelką korespondencję, która po takiej rozmowie często może być przesyłana np. e-mail z linkami (odsyłaczami) do jakiegoś programu. Przestępcy próbują w ten sposób przejąć kontrolę nad Państwa komputerem (dzieje się to zazwyczaj „w tle" od razu po zainstalowaniu programu z niewiadomego źródła).

PODSUMOWANIE:

- korzystając ze stron internetowych, na których logujemy się, przekazujemy nasze dane osobowe np. w formularzach, bezwzględnie sprawdzajmy adres internetowy – czy wpisana w przeglądarce nazwa jest poprawna, czy strona rozpoczyna się od znaków „https”

- otrzymując emaila / sms-a / mms-a lub wiadomość z komunikatora internetowego upewnijmy się, że jest autentyczna, że pochodzi od możliwego do zweryfikowania nadawcy i jeśli nie mamy 100% pewności odnośnie wiarygodności, pod żadnym pozorem nie klikajmy w przesłane adresy / linki, nie otwierajmy załączników!

- dokonując zakupów na portalach aukcyjnych (np. olx, allegro, ebay) korzystajmy z mechanizmów udostępnianych przez sklepy / portale – w żadnym wypadku nie realizujmy transakcji poprzez wiadomości prywatne, które możemy otrzymać od potencjalnego kupca.

- korzystajmy z zaufanych urządzeń z aktualnym systemem operacyjnym, z aktywnym i aktualnym oprogramowaniem antywirusowym. Dobrym nawykiem jest dokonywanie jakichkolwiek logowań do stron wyłącznie na własnych urządzeniach, poprzez własne łącze internetowe. Nie powinno się korzystać z dostępnych publicznie sieci WIFI (takich, które nie wymagają hasła – dostępne są one np. w galeriach handlowych).

- pracownik Banku w rozmowie telefonicznej czy poprzez kontakt drogą elektroniczną (e-mail, sms itd.) nigdy nie prosi o Państwa dane poufne np. dotyczące logowania do bankowości, nigdy nie prosi o instalację programów do pomocy zdalnej!