Bezpieczeństwo w sieci

Cloud

Portale społecznościowe

Zakupy

Internet

mgr Michał Frica

Jedna minuta - czy to dużo ?

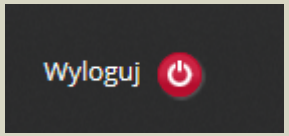
Zagrożenia w Internecie

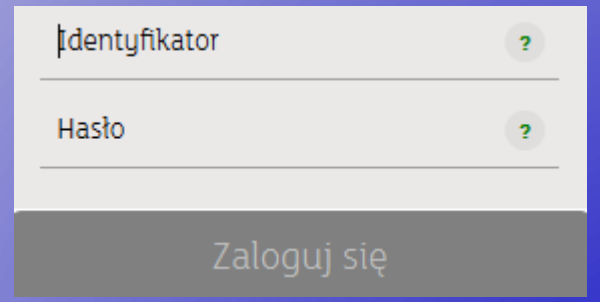
- Fałszywe witryny wyłudzające dane;
- Wiadomości e-mail, których celem jest wyłudzenie informacji;
- Zagrożenie w trakcie korzystania z portali społecznościowych;
- Cloud (Chmura) – dane w sieci;
- Fałszywe oprogramowania;
- Wykradanie danych osobowych;
- Skrócone adresy url, literówka w adresach www;
- Nieaktualne oprogramowanie;
- Fałszywe sklepy internetowe;
- Hot-spot.

Na co zwracać uwagę przy logowaniu się do banku (1/2)

- Kłódka na pasku stanu;
- Protokół https w adresie strony;

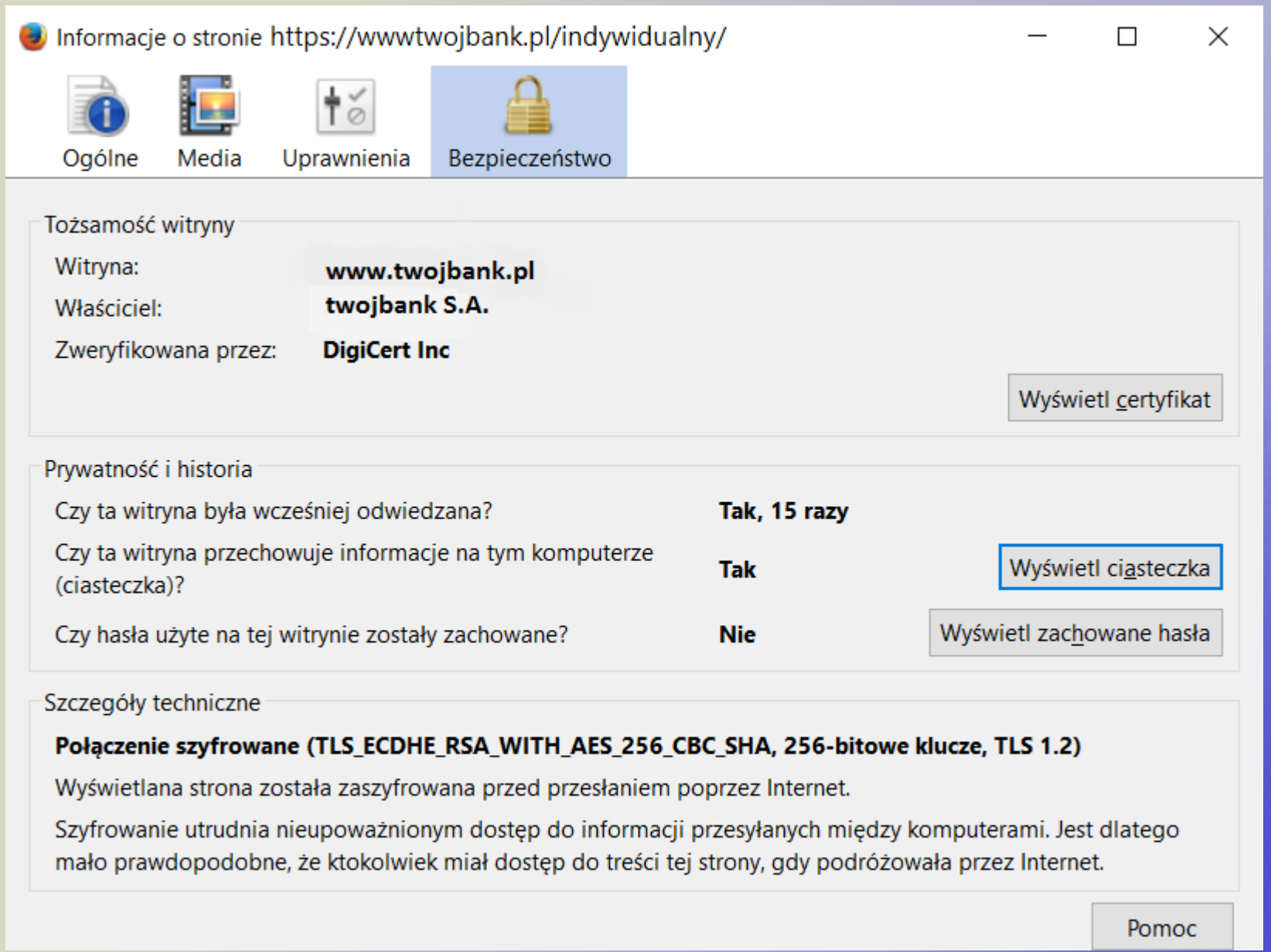
- Numer klienta (login) i hasło;
- Pamiętaj o poprawnym „wyjściu z konta”





- Nazwa i właściciel witryny muszą być zgodne z nazwą banku.

Na co zwracać uwagę przy logowaniu się do banku



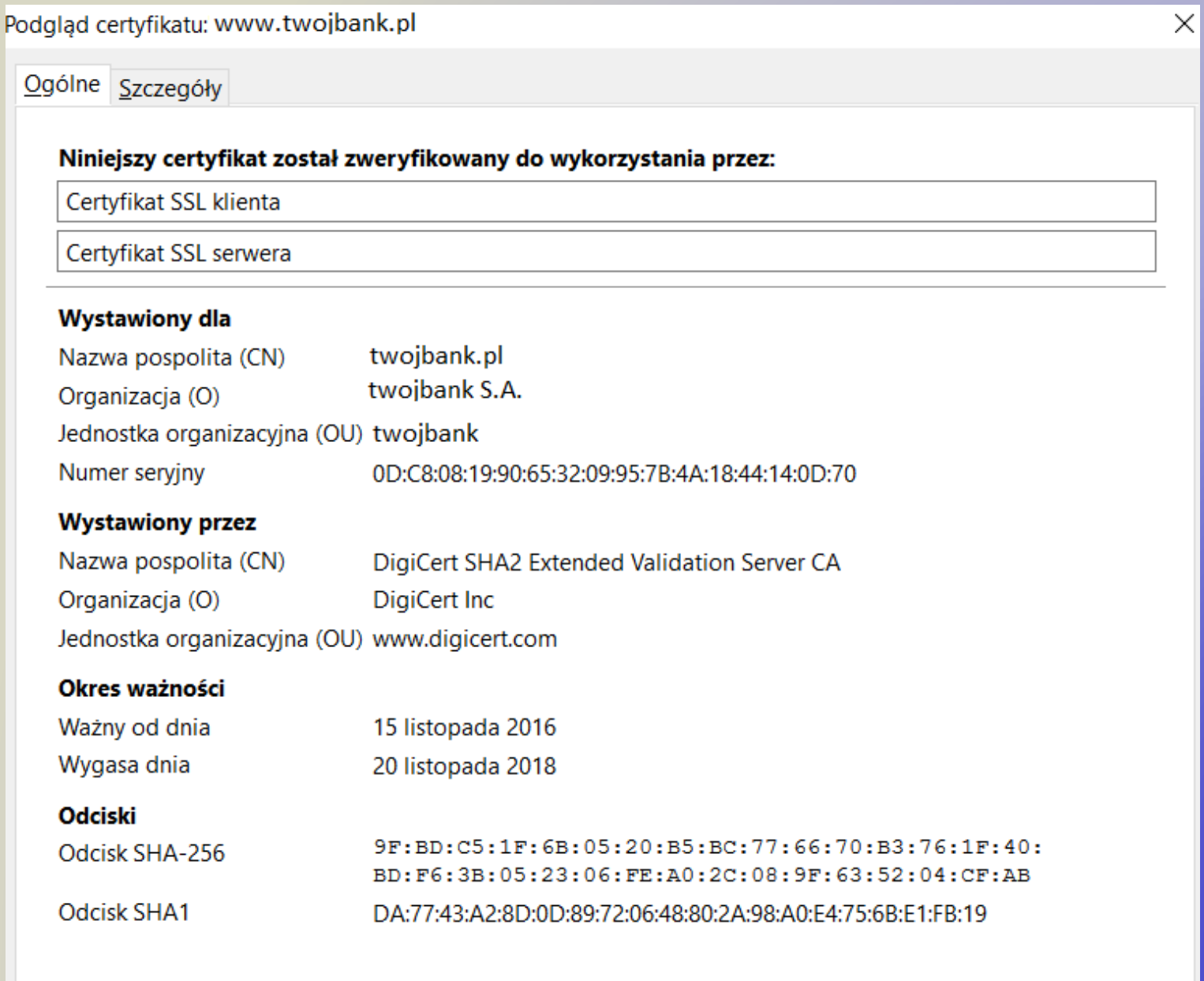
Na co zwracać uwagę przy logowaniu się do banku (2/2)

Sprawdź, czy połączenie jest szyfrowane (SSL)

Rodzaje połączeń SSL:

- Symetryczne –polega na szyfrowaniu i odszyfrowywaniu tym samym tajnym kluczem. Ważne aby bezpiecznie przekazać klucz;
- Asymetryczne – klucz prywatny jest tajny i znany wyłącznie właścicielowi. Klucz publiczny jest znany wszystkim ale jego odczytanie jest możliwe tylko przy wskazaniu odpowiedniego prywatnego klucza.
- Hybrydowe - łączące elementy obu powyższych szyfrowań tak, by się uzupełniały.

Na co zwracać uwagę przy logowaniu się do banku



Fałszywe strony banków - phishing (1/9)

Phishing – wyłudzenie danych osobowych.

Podszywanie się pod bank poprzez:

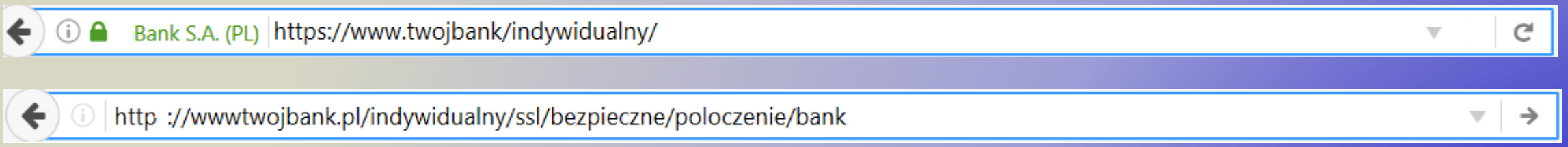
- strony www;
- wiadomości e-mail;
- portal społecznościowy;
- sklepy internetowe.

Oszusta bardzo trudno złapać
ponieważ na ogół strony istnieją kilka godzin.

Fałszywe strony banków - phishing (2/9)

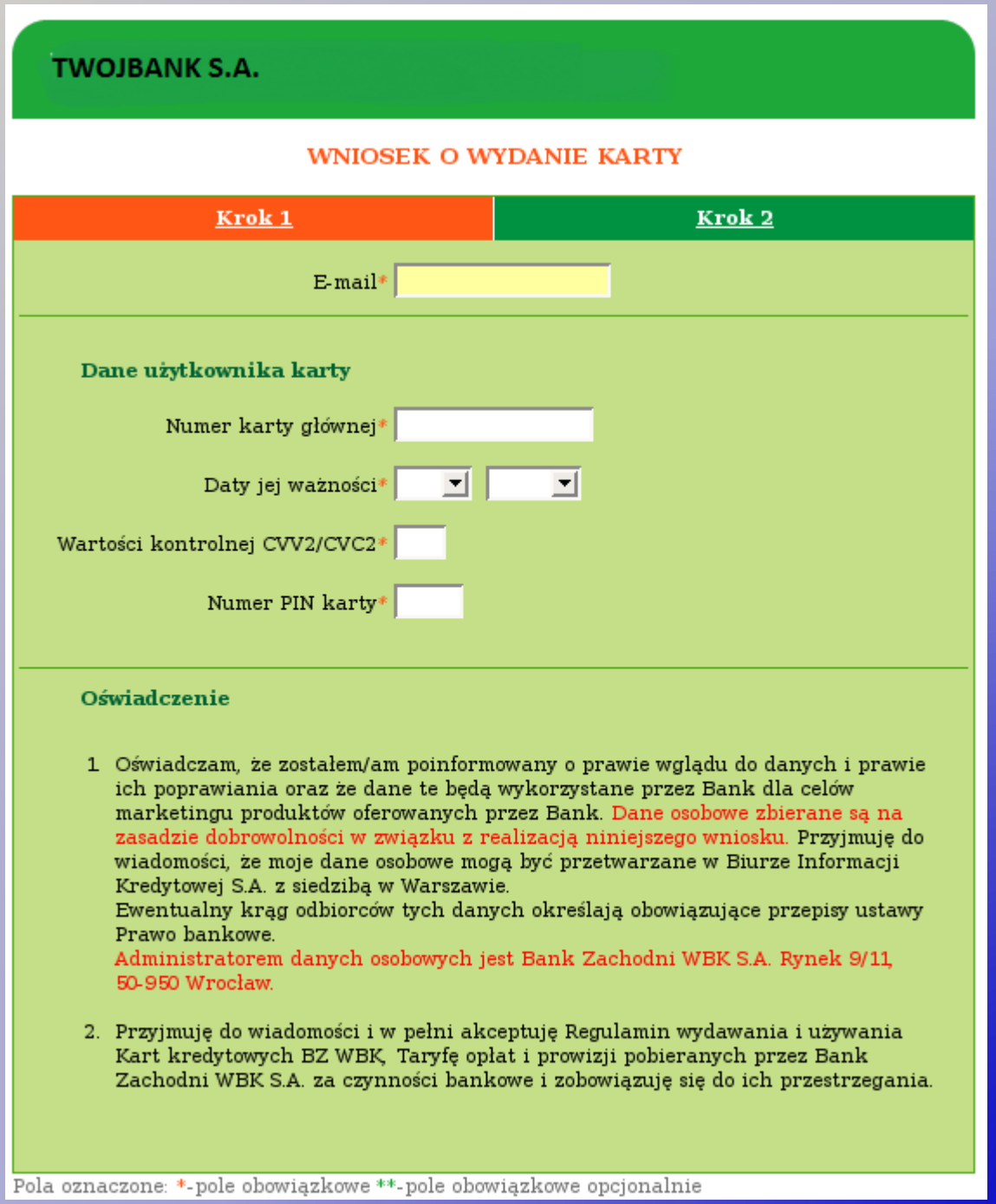
Przestępcy potrafią podrabiać strony w internecie, w tym strony banków.

Przykład fałszywej strony banku – wyłudzenie danych osobowych do wyrobienia karty



- Brak kłódki na pasku stanu
- Brak informacji o banku
- Brak w adresie https

Fałszywe strony banków - phishing



TWOJBANK S.A.

WNIOSEK O WYDANIE KARTY

Krok 1 | Krok 2

E-mail*

Dane użytkownika karty

Numer karty głównej*

Daty jej ważności*

Wartości kontrolnej CVV2/CVC2*

Numer PIN karty*

Oświadczenie

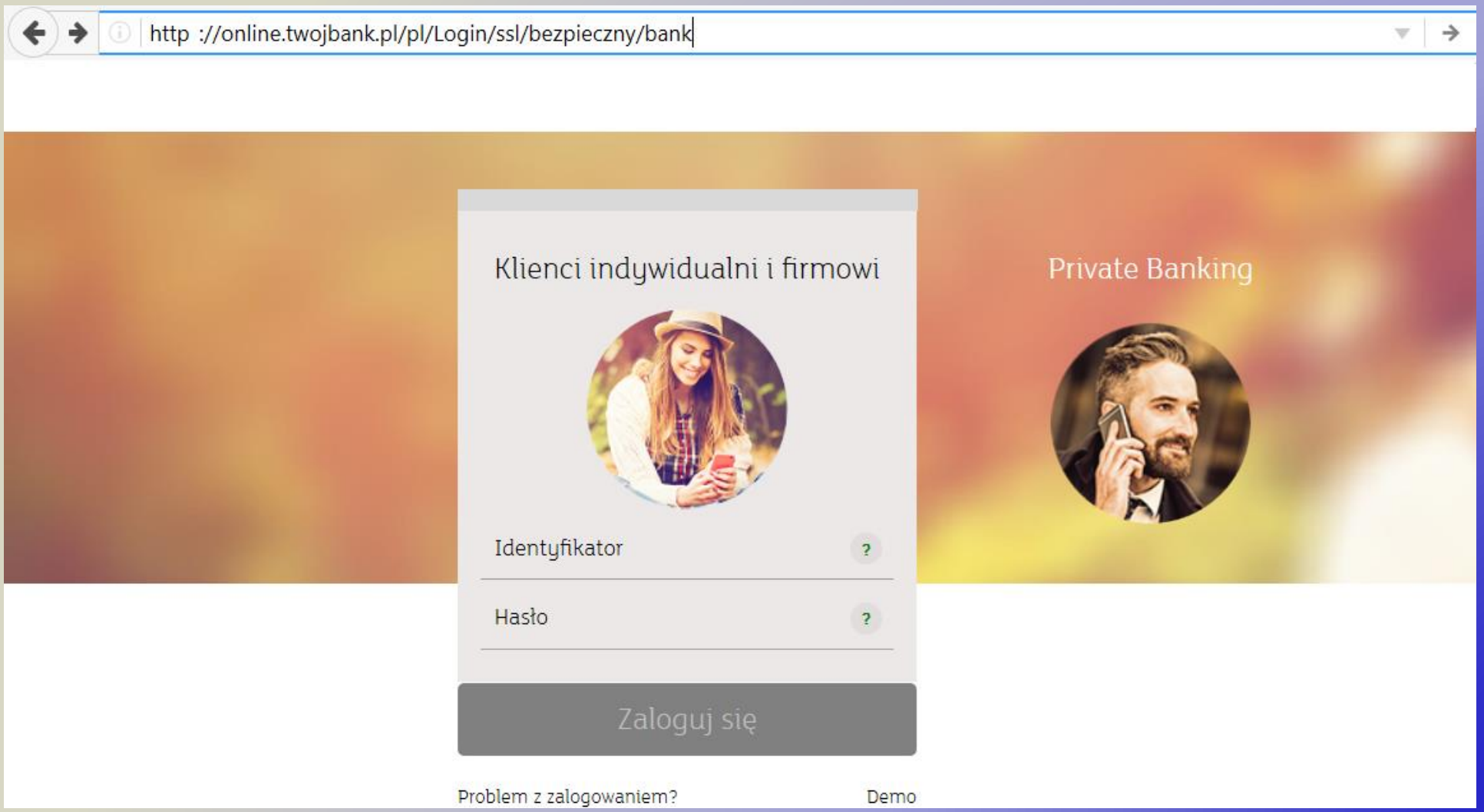
1. Oświadczam, że zostałem/am poinformowany o prawie wglądu do danych i prawie ich poprawiania oraz że dane te będą wykorzystane przez Bank dla celów marketingu produktów oferowanych przez Bank. Dane osobowe zbierane są na zasadzie dobrowolności w związku z realizacją niniejszego wniosku. Przyjmuję do wiadomości, że moje dane osobowe mogą być przetwarzane w Biurze Informacji Kredytowej S.A. z siedzibą w Warszawie.
   Ewentualny krąg odbiorców tych danych określają obowiązujące przepisy ustawy Prawo bankowe.
   Administratorem danych osobowych jest Bank Zachodni WBK S.A. Rynek 9/11, 50-950 Wroclaw.

2. Przyjmuję do wiadomości i w pełni akceptuję Regulamin wydawania i używania Kart kredytowych BZ WBK, Taryfę opłat i prowizji pobieranych przez Bank Zachodni WBK S.A. za czynności bankowe i zobowiązuję się do ich przestrzegania.

Pola oznaczone: *-pole obowiązkowe **-pole obowiązkowe opcjonalnie

Fałszywe strony banków - phishing (3/9)

Przykład fałszywej strony banku – wyłudzenie danych osobowych do logowania się w banku.



Fałszywe strony banków - phishing (4/9)

Nie daj się nabrać twój bank nigdy tego nie robi!

- Nie wysyła informacji o blokadzie konta e-mailem;
- Nie wysyła wiadomości e-mail zawierających link do serwisu bankowości internetowej;
- Nie podaje linków do systemu transakcyjnego w e-mailach lub SMS-ach;
- Nie dzwoni z prośbą o podanie hasła do konta lub numeru karty.

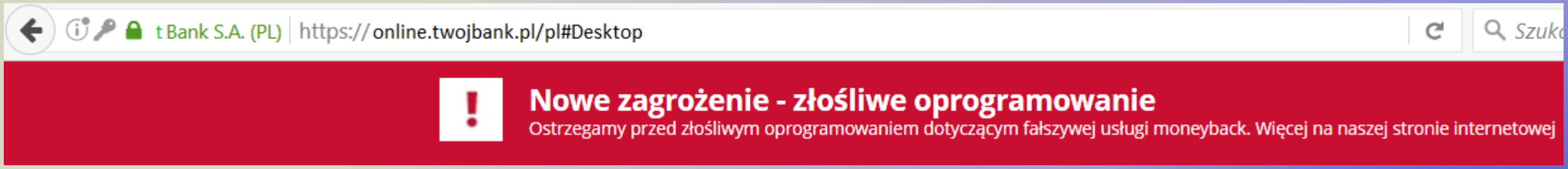
Fałszywe strony banków - phishing (4/9)

Nie daj się nabrać twój bank nigdy tego nie robi!

- **Nie prosi:**
  - o aktywację usług;
  - o zalogowanie do konta w związku ze zwrotem środków;
  - o wykonanie przelewów testowych;
  - o zalogowanie się na stronie „bez kłódki”;
  - o podanie kodu z karty zdrapki;
  - o zainstalowanie programu do otwierania wyciągów z konta;
  - o zainstalowanie antywirusa, aplikacji czy certyfikatów na telefonie;
  - podczas logowania o kod z tokena lub SMS-a, jeśli nie korzystamy z tej usługi;
  - o podanie danych osobowych.

Fałszywe strony banków - phishing (5/9)

Banki informują swoich klientów o zagrożeniach.



Złośliwe oprogramowanie przechwytujące poufne dane i wyłudzające hasła SMS, podszywając się pod usługę moneyback

09-12-2016

Fałszywe strony banków - phishing

Informujemy o kolejnym złośliwym oprogramowaniu zagrażającym klientom korzystającym z bankowości elektronicznej.

W pierwszej kolejności zainfekowany wirusem (złośliwym oprogramowaniem) zostaje komputer. Źródłem infekcji może być otwarcie załącznika do wiadomości e-mail zawierającego wirusa, w którym przestępcy podszywają się m.in. pod notariusza bądź biuro handlowe:

Tytuły: "Faktura Proforma" lub "Płatność".
Treść:
Witam!
Faktura proforma nr 'PF/16/11/27' w załączniku. Bardzo proszę o dokonanie płatności. W przypadku nieuregulowania płatności w terminie 5 dni od dnia otrzymania tej wiadomości, sprawa może zostać skierowana do windykacji.
Z powazaniem,

Po uzyskaniu identyfikatora klienta i hasła przestępcy logują się do serwisu transakcyjnego w jego imieniu, a w przeglądarce klienta pojawia się grafika wskazująca na oczekiwanie na zalogowanie:

Fałszywe strony banków - phishing (6/9)

Banki są jednymi z lepiej zabezpieczonych instytucji.

W związku z tym, celem ataku jest sam użytkownik, którego łatwo oszukać.

Fałszywe strony banków - phishing (7/9)

Co robi bank, by bankowość internetowa była bezpieczna?

- Ściany ogniowe (firewall)
- Przechowywanie kluczowych danych w postaci zaszyfrowanej
- Weryfikowanie i dopasowywanie odpowiednich uprawnień dostępu do danych pracownikom banku
- Ograniczanie do minimum liczby osób, które mają dostęp do poufnych danych klientów banku.
- Tworzenie kopii zapasowych baz danych

Fałszywe strony banków - phishing (8/9)

Inne metody zabezpieczania banków

- Sms-y wysyłane klientom banku potwierdzające transakcje, wskazujące stan konta informujące o zmianie kwoty środków zgromadzonych na rachunku klienta.
- Limity jednorazowych lub dziennych wypłat z kont, przelewów itp. (wszelkich rodzajów transakcji).
- Informatory, poradniki, umożliwiają oglądanie wykładów ekspertów, tworzą fora dyskusyjne i eksperckie.

Fałszywe strony banków - phishing (9/9)

Opisane metody stanowią tylko niewielki procent metod wykorzystywanych przez banki.

Zdecydowana większość zabezpieczeń jest tajna i z uwagi na bezpieczeństwo nie może być przedstawiana publicznie.

Uważaj na wiadomości e-mail (1/4)

Wiadomości:

- Nieodebrana przesyłka pocztowa lub kurierska;
- Egzekucja zajęcia konta bankowego;
- Blokada konta bankowego;
- Od firm, których nie znasz;
- Fałszywe faktury;
- Fałszywe rezerwacje np. hoteli;
- Lokalizacja numerów telefonu;
- Szansa otrzymania wyjątkowej nagrody.

Uważaj na wiadomości e-mail

Szanowny Panie Michale

Pana adres m.frica@najpoczta.pl został wybrany! Prosimy o dokończenie rejestracji w Ankiecie Telewizyjnej.

W ramach podziękowań, dajemy Panu szansę na otrzymanie wyjątkowej nagrody:

2000 zł w gotówce

Kliknij **TUTAJ**

Pozdrawiam serdecznie,

Anna Kowalska z Zespołu Ankieta Telewizyjna

Gratulujemy

Otrzymujesz szansę na wygranie

2000 zł w gotówce

Wypełnij pola, aby wziąć udział. Pozostały 3 nagrody.

Twoje nazwisko

Miejscowość | Kod | Pocztowy

Ulica

Nr budynku | Nr mieszkania

● Abonament ● Karta

Numer telefonu komórkowego

Data urodzenia

DD | MM | RRRR

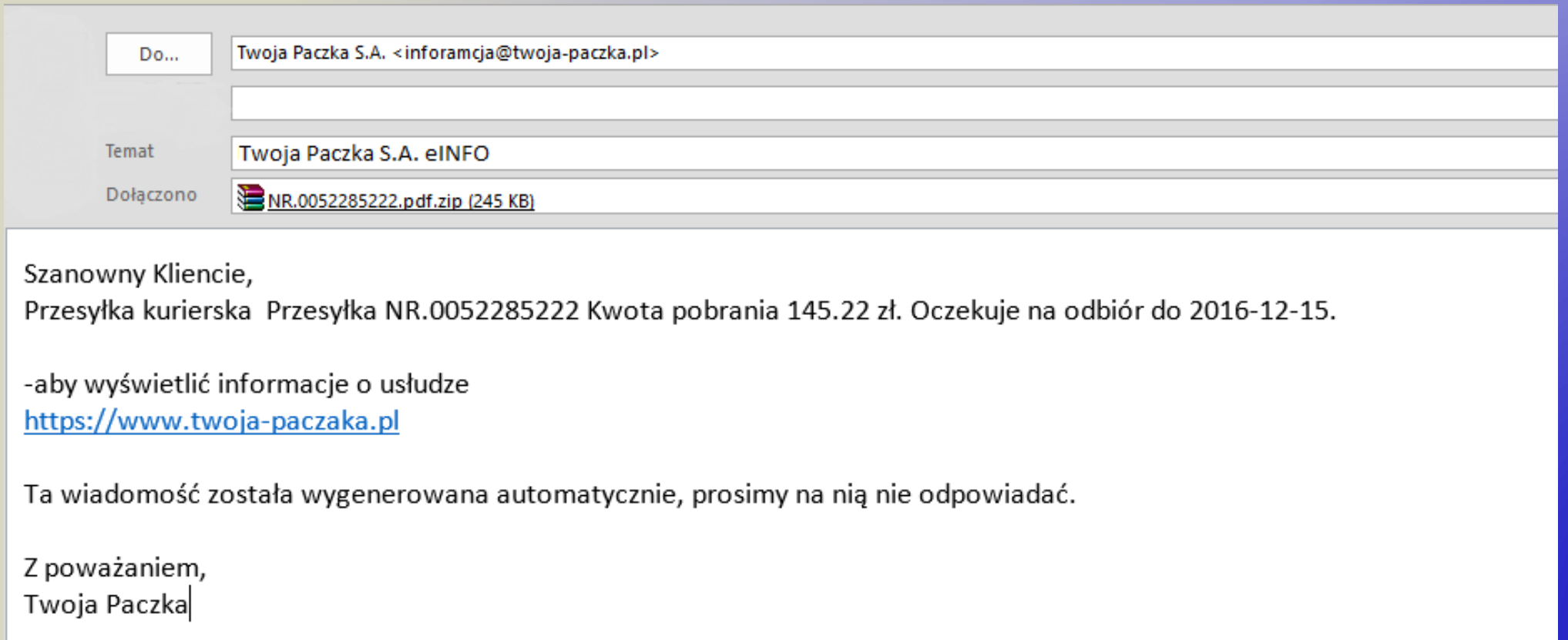
Musisz mieć ukończone 18 lat.

POTWIERDZAM

Uważaj na wiadomości e-mail (3/4)

Uwaga na złośliwe oprogramowania wysłane jako załącznik do wiadomości e-mail – WIRUSY

Pamiętaj w żadnym wypadku nie klikaj na załączony link oraz nie pobieraj złączników ZIP lub PDF.



Uważaj na wiadomości e-mail (4/4)

Jak nie dać się złapać w sidła oszustów:

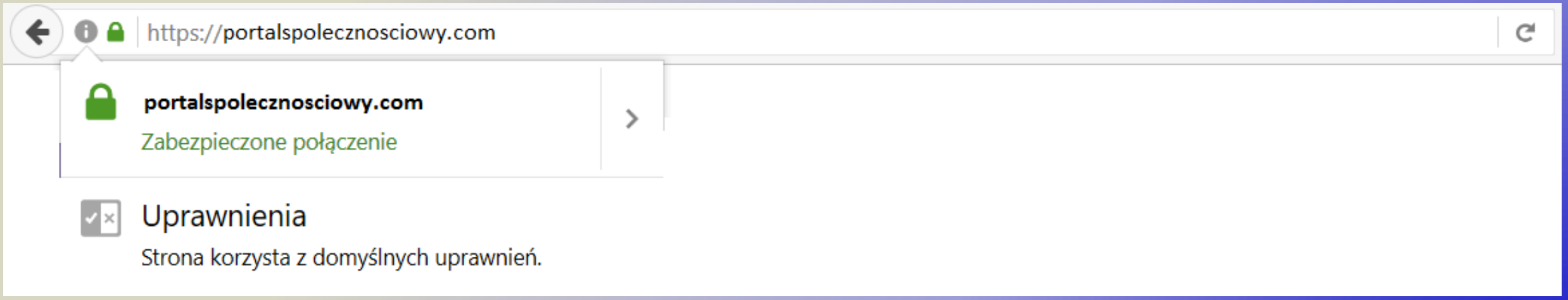
- Nie pobieraj danych z nieznanych źródeł ;
- Nie pobieraj aplikacji z nieznanych źródeł;
- Nie otwieraj wiadomości spam;
- Nie daj się ponieść emocjom związanym np. z szansą wygrania nagrody;
- Nie klikaj w nieznane linki;
- Nie wpisuj swoich danych osobowych.

Zagrożenie w trakcie korzystania z portali społecznościowych (1/4)

- Kradzież tożsamości;
- Przesłanie niebezpiecznego oprogramowania;
- Inwigilacja;
- Wykorzystanie danych przeciwko Tobie;
- Kradzież hasła.

Zagrożenie w trakcie korzystania z portali społecznościowych (2/4)

Portale społecznościowe również mają zabezpieczone połączenia



Zagrożenie w trakcie korzystania z portali społecznościowych (3/4)

Fałszywe reklamy

Zagrożenie w trakcie korzystania z portali społecznościowych

Fałszywe konta

Fałszywe odzyskanie hasła

Zagrożenie w trakcie korzystania z portali społecznościowych (4/4)

Zasady bezpiecznego korzystania z portali społecznościowych:

- Dostosuj do własnych potrzeb ustawienia prywatności swojego konta;
- Unikaj klikania w nieznane linki;
- Dodawaj do listy znajomych wyłącznie osoby, które rzeczywiście znasz i którym ufasz;
- Nie ufaj udostępnianym w serwisie aplikacjom;
- Pamiętaj też o tym, by nie wrzucać do sieci tych danych, których nie chcesz upublicznić;
- Stosuj różne hasła;
- Najsłabszym ogniwem jest zwykle sam użytkownik.

Pamiętaj pliki, zdjęcia pozostają w sieci na wiele lat !!!

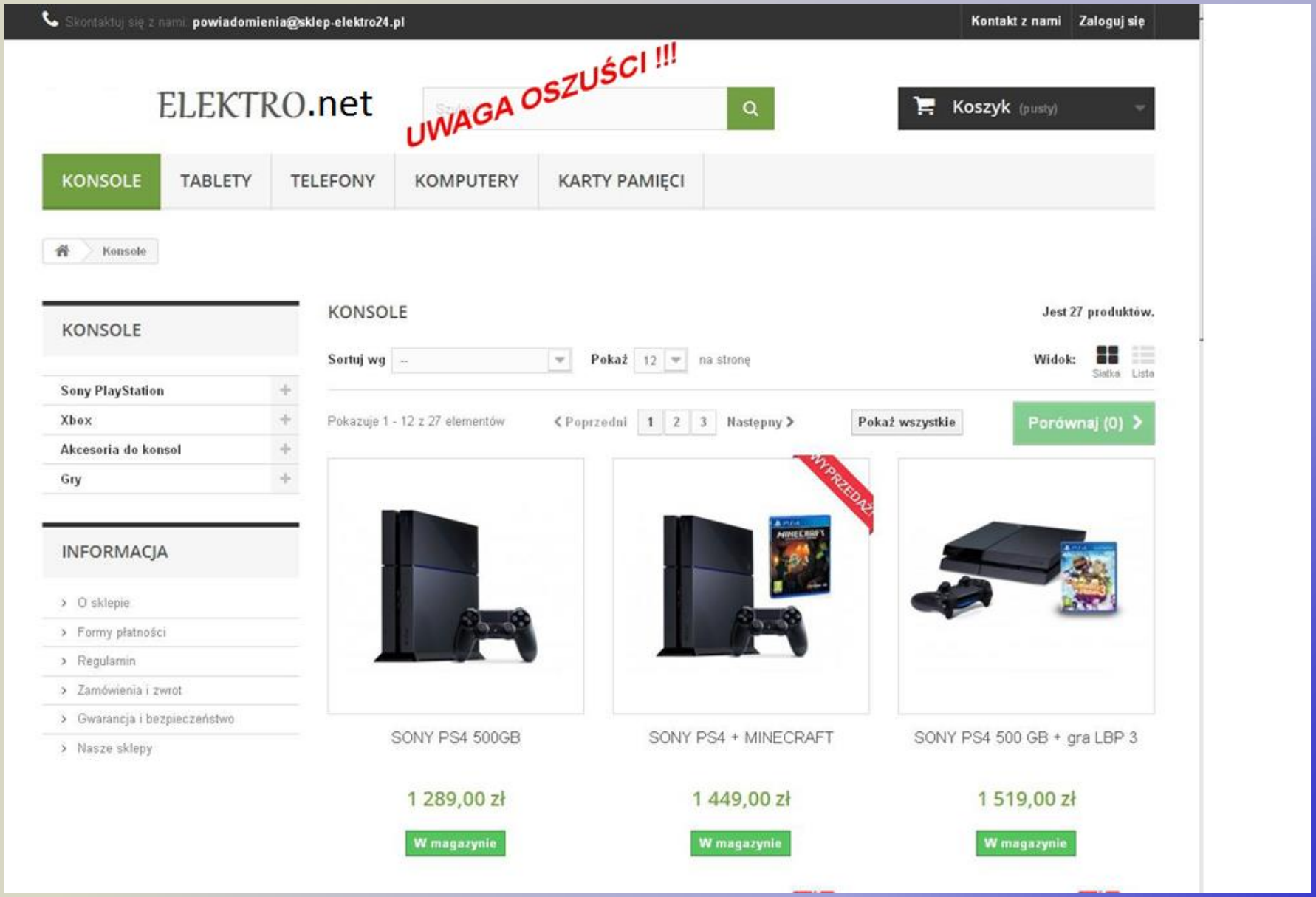
Fałszywe sklepy internatowe

Zanim kupisz sprawdź czy nie masz do czynienia z oszustem !

Jak rozpoznać oszustów:

- Atrakcyjne ceny niższe niż u konkurencji;
- Mało produktów;
- Duża część oferowanych produktów w promocji;
- Brak możliwości płatności przy odbiorze;
- Krótki okres działania sklepu;
- Brak kontaktu telefonicznego;
- Podejrzane dane firmowe;
- Brak opinii lub opinie brzmiące sztucznie.

Fałszywe sklepy internatowe



Sugerowane reklamy - cookies – ciasteczka (1/3)

Pliki cookies są informacją testową wysłaną przez strony internetowe np. sklep internetowy.

Co robią:

- Śledzą ruch użytkownika w internecie;
- Wysyłają reklamy np. produktu, który wcześniej przeglądaliśmy;
- Zapisują się na dysku twardym komputera i przeglądarkach internetowych.

Najczęściej są zapisywane ostatnie wizyty na stronach oraz czas w którym plik ma zostać usunięty automatycznie.

Sugerowane reklamy - cookies – ciasteczka (2/3)

Pliki cookies to niestety również niebezpieczeństwo .

Mogą przechowywać:

- Login.
- Zaszyfrowane hasło.

W takim przypadku istnieje możliwość, że odpowiednio przygotowany wirus będzie wykradał nasze osobiste dane.

Dzieje się tak kiedy ciasteczka zostają zapisane na naszym komputerze dłużej niż okres trwania zamknięcia przeglądarki.

Sugerowane reklamy cookies – ciasteczka (3/3)

Jak pozbyć się ciasteczek?

- **Firefox** - Narzędzia > Historia > Wyczyść historię przeglądania (zaznaczamy "ciasteczka") i wyczyść teraz;
- **Internet Explorer** - Narzędzia > Bezpieczeństwo > Usuń historię przeglądania (zaznaczamy "ciasteczka") i usuń;
- **Google Chrome** - Narzędzia > Historia > Wyczyść dane przeglądarki > zaznaczamy pole: Usuń pliki cookie oraz inne dane witryn i wtyczek naciskamy Wyczyść dane przeglądarki.

Dane w sieci – Cloud (Chmura) (1/3)

Chmura to usługa przechowywania danych dostarczana przez zewnętrznego dostawcę

Dostawca posiada serwery połączone ze sobą, dzięki czemu może zaoferować przechowywanie danych

ZALETY

- Dostępne w każdym miejscu, gdzie jest zasięg internetu;
- Obniżenie kosztów związanych z infrastrukturą;
- Zabezpiecza dane przed fizyczną kradzieżą oraz awarią sprzętu.

WADY

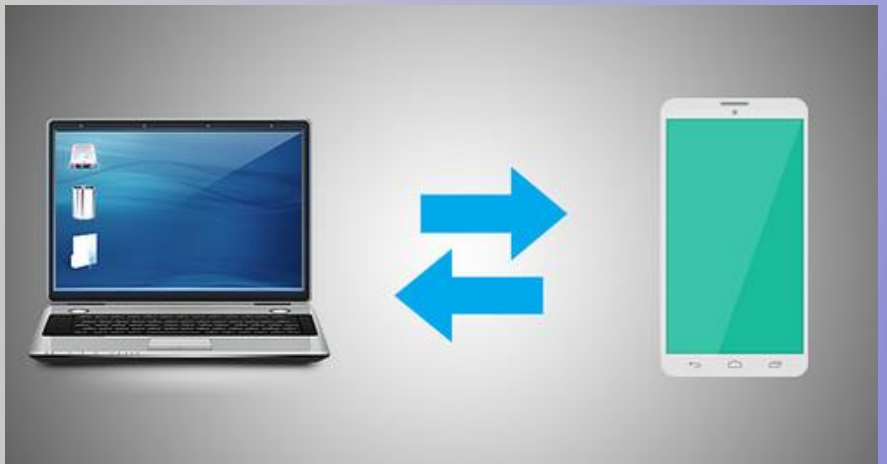
- Mniejsza kontrola nad danymi;
- Serwery ulokowane w krajach o różnych systemach prawnych;
- Możliwy nieuczciwy dostawca lub personel.

Dane w sieci – Cloud (Chmura)(2/3)

W chmurze można przechowywać:

- Wszystkie rodzaje dokumentów np. tekstowe, arkuszowe, prezentacje;
- Zdjęcia z telefonu, tableta, komputera;
- Dane kontaktowe np. z telefonu;

Chmura pozwala synchronizować dane w różnych urządzeniach np. między telefonem, tabletem, komputerem



Dane w sieci – Cloud (Chmura)(3/3)

Najczęściej używane konta w chmurze

Hotspot na co uważać (1/2)

➢Cafe Internet zagrożenia:

- Nie wiemy co jest zainstalowane na komputerach;
- Inni użytkownicy komputerów;
- Dane mogą być przechowywane – ktoś może z nich skorzystać;
- Loginy i hasła mogą być przejęte.

➢Hot-spot zagrożenia:

- Takie same jak przy Cafe internet;
- Cyberprzestępcy tworzą własne hot-spoty podszywając się pod inne;
- Infekcja komputera, tableta, telefonu.

Hotspot na co uważać (2/2)

Jeżeli musimy skorzystać z Cafe internetu lub Hot-spota pamiętajmy, aby nigdy nie korzystać z operacji związanych z logowaniem do konta bankowego, poczty czy też portali społecznościowych

Dbaj o swój komputer jak o samochód (1/7)

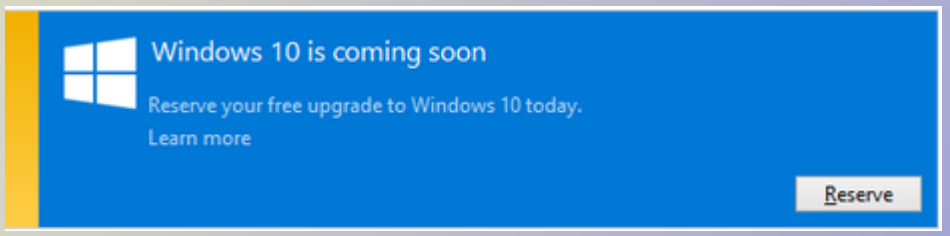
Bezpieczeństwo danych zaczyna się od Twojego sprzętu.

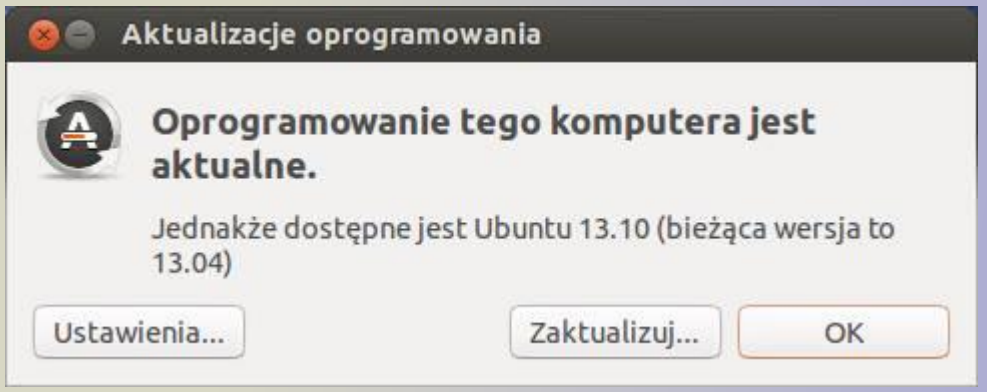
- Używaj legalnego systemu;
- Aktualizuj system;
- Serwisuj komputer;
- Zainstaluj i aktualizuj program antywirusowy;
- Skanuj programem antywirusowym pliki z nieznanego źródła przed ich otwarciem;
- Aktualizuj przeglądarkę internetową;
- Zabezpiecz komputer hasłem;
- Nie dawaj osobom niezaufanym dostępu do swojego komputera.

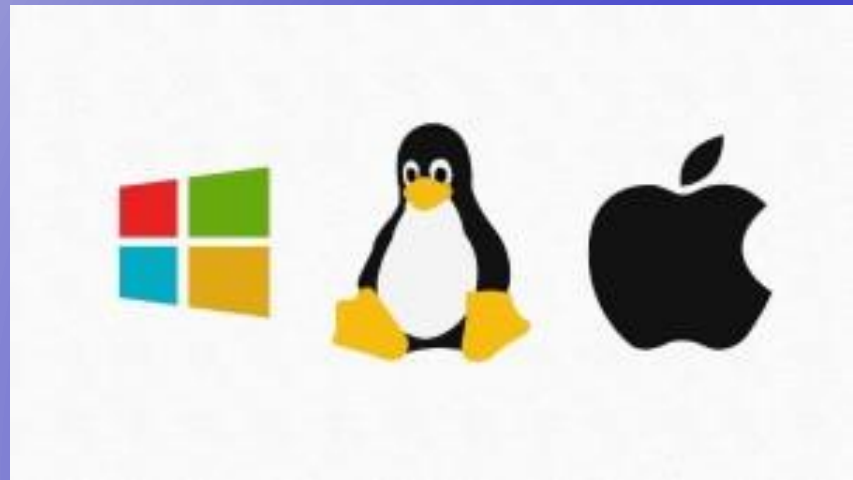
Dbaj o swój komputer jak o samochód (2/7)

Najczęściej używane systemy operacyjne :

- Windows;
- IOS;
- Linux.



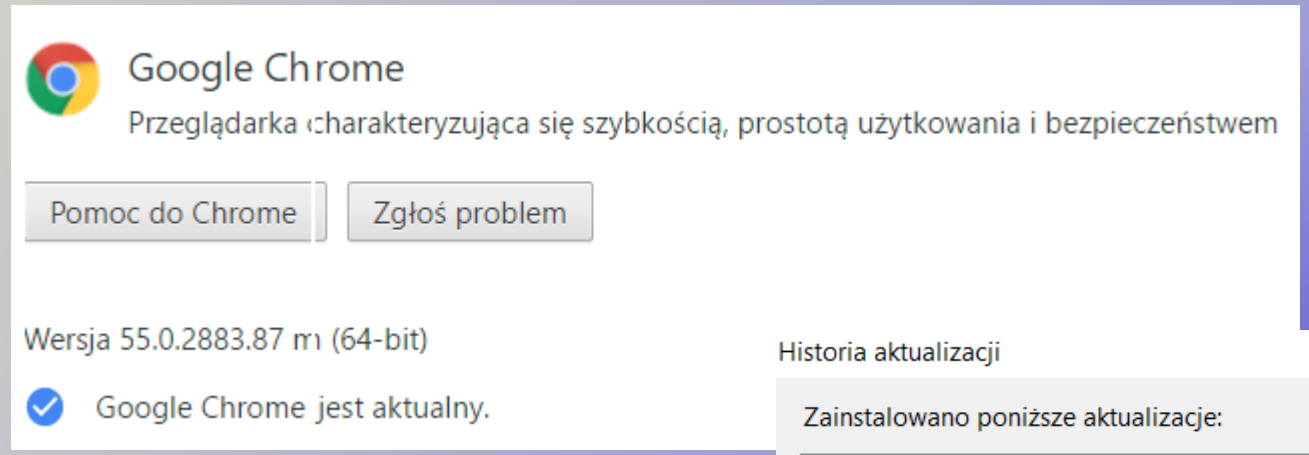


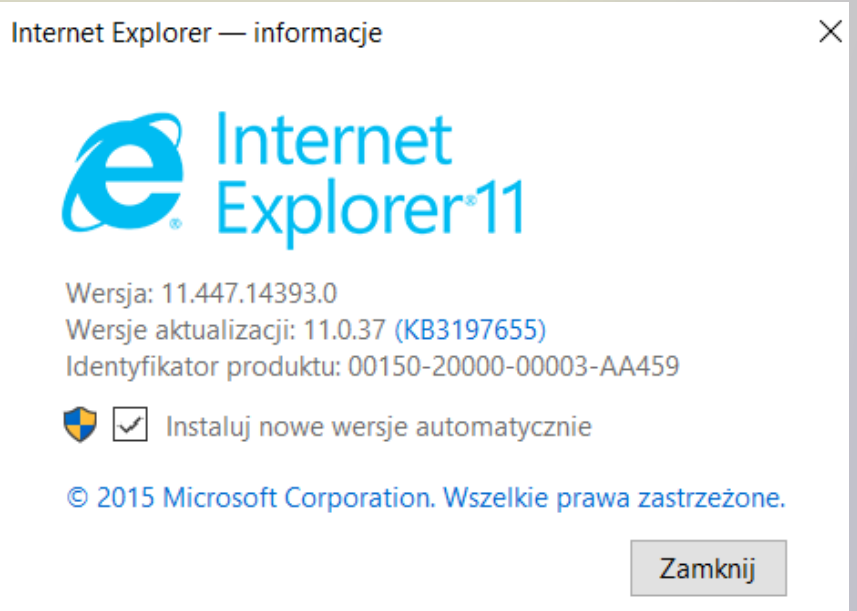


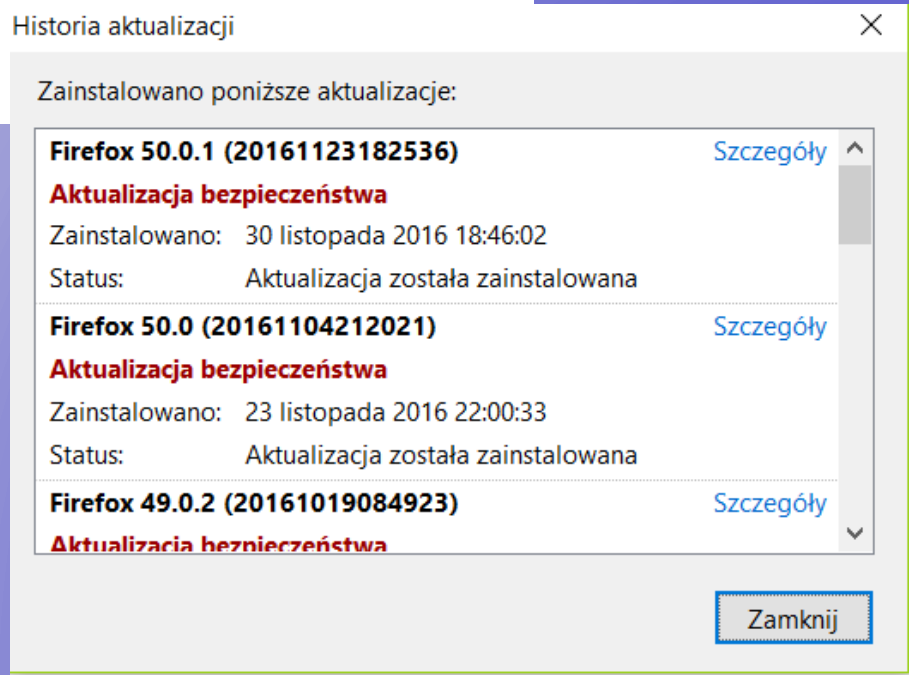
Dbaj o swój komputer, jak o samochód (3/7)

Najczęściej używane przeglądarki internetowe - aktualizacja:

- Chrome;
- Firefox;
- Internet Explorer;
- Safari.







Dbaj o swój komputer jak o samochód (4/7)

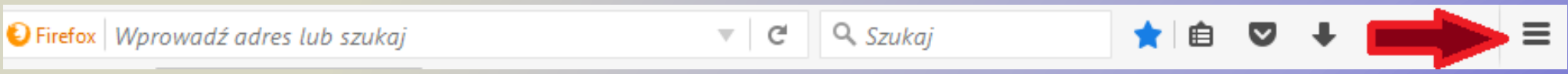
Uwaga na przeglądarki internetowe ! W nich mogą być zapisane nasze hasła.

Pamiętaj by zmieniać hasła co jakiś czas.

Dbaj o swój komputer jak o samochód

Jak pozbyć się hasła z przeglądarki?

- **Firefox** - Narzędzia > Opcje > Bezpieczeństwo > Zachowane dane logowania;



- **Internet Explorer** - Narzędzia > Bezpieczeństwo > Usuwanie historii przeglądarki > Hasła;

- **Google Chrome** - Narzędzia > Ustawienia > Pokaż ustawienia zaawansowane > Zarządzaj hasłami.

Dbaj o swój komputer jak o samochód (5/7)

Oprogramowanie antywirusowe ma za zadanie wykryć, zwalczyć i usunąć złośliwe programy.

- Avast;
- AVG;
- ESET;
- Kaspersky;
- Symantec.

Dbaj o swój komputer jak o samochód (6/7)

Co robią wirusy:

- Przyjmują dane;
- Uszkadzają system;
- Niszczą dane;
- Uniemożliwiają prace na komputerze;
- Ukrywają zdarzenia przed użytkownikiem;
- Wyświetlają niechciane programy, grafiki.

Dbaj o swój komputer jak o samochód (7/7)

Jakie są wirusy

- Koń trojański;
- Makrowirusy;
- Wirusy plikowe;
- Wirusy BIOS-owe;
- Bomby logiczne;
- Robaki.

Powszechne urządzenie Smartfony i Tablety (1/4)

Korzystając z mobilnych urządzeń wykonujemy:

- Logowanie do banku;
- Wysyłamy zdjęcia;
- Przeglądamy internet;
- Korzystamy z portali społecznościowych;
- Robimy zakupy.

Powszechne urządzenie Smartfony i Tablety (2/4)

O co zadbać aby korzystać bezpiecznie z naszych urządzeń mobilnych?

- Aktualizować urządzenie;
- Zainstalować i aktualizować program antywirusowy;
- Nie korzystać w miejscach publicznych z logowania np. do konta bankowego;
- Omijać darmowe Hot-spoty;
- Korzystać z internetu oferowanego przez twojego operatora sieci;

Powszechne urządzenie Smartfony i Tablety (3/4)

O co zadbać aby korzystać bezpiecznie z naszych urządzeń mobilnych?

- Blokadę ekranu zabezpieczyć hasłem;
- Korzystać wyłącznie z zaufanych aplikacji;
- Nie odwiedzać „dziwnych” stron internetowych;
- Uważajmy na ważne sms-y od banku, np. polecenie zainstalowania najnowszej wersji aplikacji mobilnej;
- **Po zmianie lub utracie telefonu poinformować bank**.

Powszechne urządzenie Smartfony i Tablety (3/4)

Najczęściej używane systemy w urządzeniach mobilnych:

- IOS;
- Android;
- Windows Phone.

Życzę Wesołych Świąt oraz

bezpiecznych i przyjemnych

zakupów przez internet.

Dziękuje za uwagę

Michał Frica