

Bezpieczeństwo w sieci



Jedna minuta - czy to dużo ?

20 ofiar
kradzieży
tożsamości

kradzież
własności
intelektualnych
na 2 mln
dolarów

168 mln
wysłanych
zdjęć

500 tys komentarzy
zamieszczonych na
portalu
społecznościowym
Facebook

Minuta
w
Inter necie

12 stron
przyjętych
przez
hakerów

232 komputery
zainfekowane
wirusami

570 nowych
stron

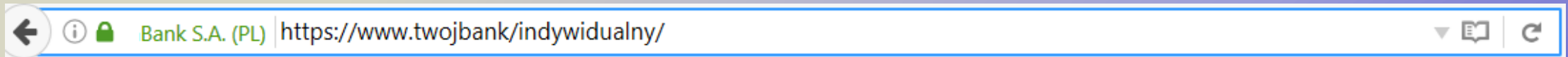
2 mln pytań
wpisanych w
wyszukiwarkę
Google

Zagrożenia w Internecie

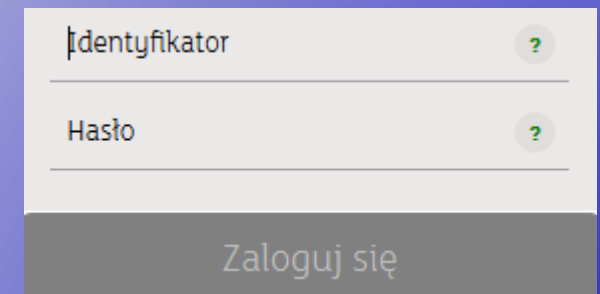
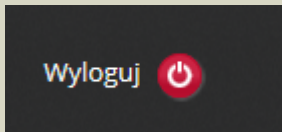
- Fałszywe witryny wyłudzające dane;
- Wiadomości e-mail, których celem jest wyłudzenie informacji;
- Zagrożenie w trakcie korzystania z portali społecznościowych;
- Cloud (Chmura) – dane w sieci;
- Fałszywe oprogramowania;
- Wykradanie danych osobowych;
- Skrócone adresy url, literówka w adresach www;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

A login form with two input fields. The first field is labeled "Identyfikator" and the second "Hasło". Both fields have a green question mark icon to their right. Below the fields is a grey button labeled "Zaloguj się".

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

Na co zwracać uwagę przy logowaniu się do banku

Informacje o stronie <https://www.twojbank.pl/indywidualny/>

Ogólne Media Uprawnienia **Bezpieczeństwo**

Tożsamość witryny

Witryna: **www.twojbank.pl**
Właściciel: **twojbank S.A.**
Zweryfikowana przez: **DigiCert Inc**

Wyświetl certyfikat

Prywatność i historia

Czy ta witryna była wcześniej odwiedzana?	Tak, 15 razy	
Czy ta witryna przechowuje informacje na tym komputerze (ciasteczka)?	Tak	Wyświetl ciasteczka
Czy hasła użyte na tej witrynie zostały zachowane?	Nie	Wyświetl zachowane hasła

Szczegóły techniczne

Połączenie szyfrowane (TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, 256-bitowe klucze, TLS 1.2)

Wyświetlana strona została zaszyfrowana przed przesłaniem poprzez Internet.

Szyfrowanie utrudnia nieupoważnionym dostęp do informacji przesyłanych między komputerami. Jest dlatego mało prawdopodobne, że ktokolwiek miał dostęp do treści tej strony, gdy podróżowała przez Internet.

Pomoc

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

Podgląd certyfikatu: www.twojbank.pl

Ogólne Szczegóły

Niniejszy certyfikat został zweryfikowany do wykorzystania przez:

Certyfikat SSL klienta

Certyfikat SSL serwera

Wystawiony dla

Nazwa pospolita (CN)	twojbank.pl
Organizacja (O)	twojbank S.A.
Jednostka organizacyjna (OU)	twojbank
Numer seryjny	0D:C8:08:19:90:65:32:09:95:7B:4A:18:44:14:0D:70

Wystawiony przez

Nazwa pospolita (CN)	DigiCert SHA2 Extended Validation Server CA
Organizacja (O)	DigiCert Inc
Jednostka organizacyjna (OU)	www.digicert.com

Okres ważności

Ważny od dnia	15 listopada 2016
Wygasa dnia	20 listopada 2018

Odciski

Odcisk SHA-256	9F:BD:C5:1F:6B:05:20:B5:BC:77:66:70:B3:76:1F:40:BD:F6:3B:05:23:06:FE:A0:2C:08:9F:63:52:04:CF:AB
Odcisk SHA1	DA:77:43:A2:8D:0D:89:72:06:48:80:2A:98:A0:E4:75:6B:E1:FB:19

Fałszywe strony banków - phishing (1/9)

Phishing – wyłudzenie danych osobowych.

Podszywanie się pod bank poprzez:

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

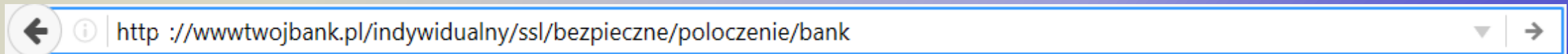
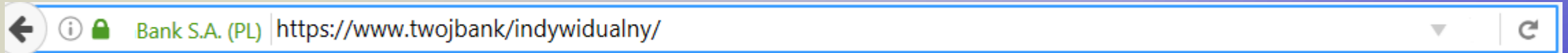


**Oszusta bardzo trudno złapać
ponieważ na ogół strony istnieją kilka godzin.**

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*

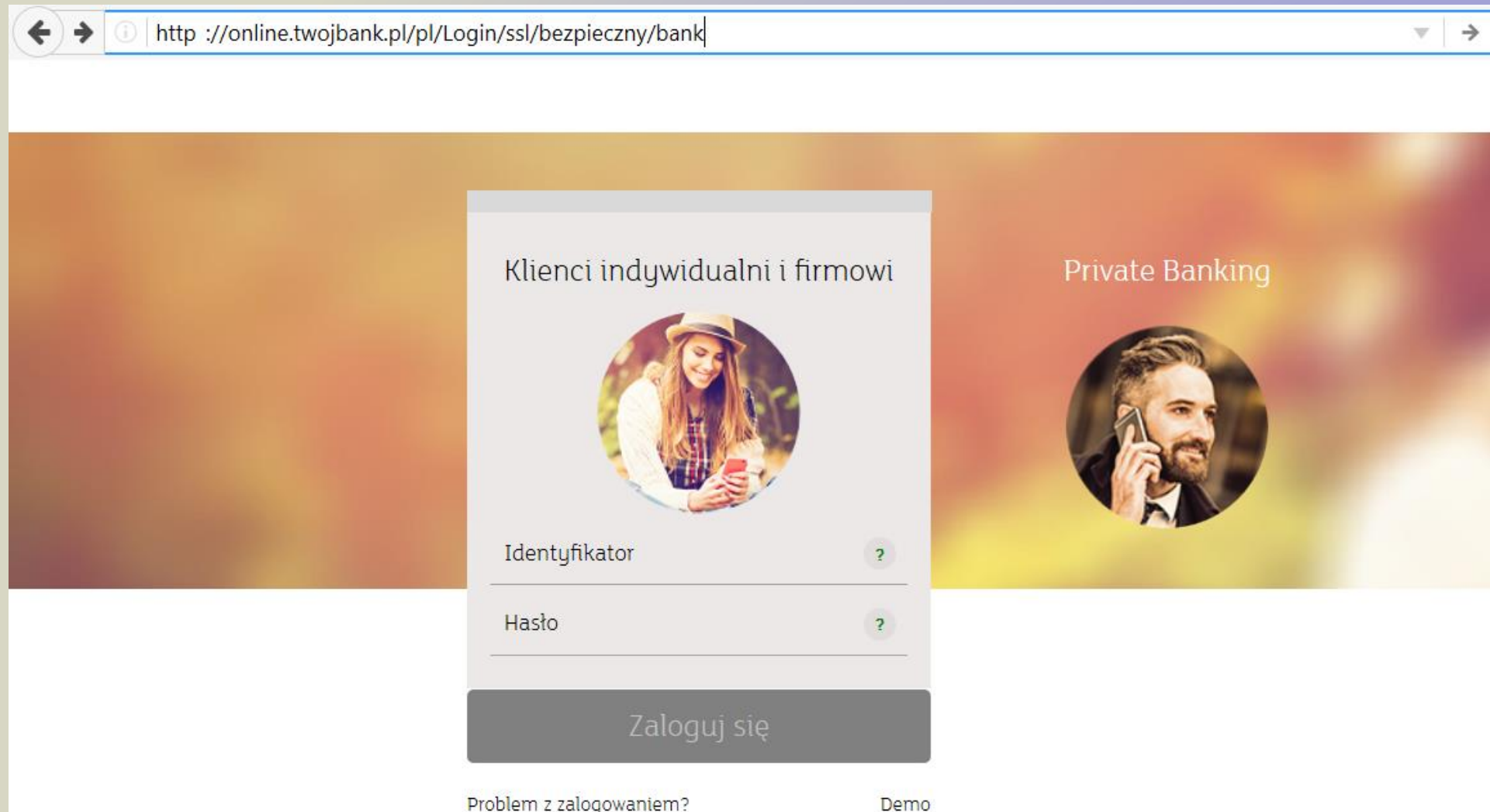
Oświadczenie

- 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 Wrocław.
- 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.



The image shows a browser window with the address bar containing the URL `http://online.twojbank.pl/pl/Login/ssl/bezpieczny/bank`. The main content area features a login form with the following elements:

- Header: "Klienci indywidualni i firmowi" (Individual and corporate clients) with a circular image of a woman using a smartphone.
- Header: "Private Banking" with a circular image of a man on a phone.
- Input field: "Identyfikator" (Identifier) with a green question mark icon.
- Input field: "Hasło" (Password) with a green question mark icon.
- Button: "Zaloguj się" (Log in).
- Footer: "Problem z zalogowaniem?" (Problem with login?) and "Demo".

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)

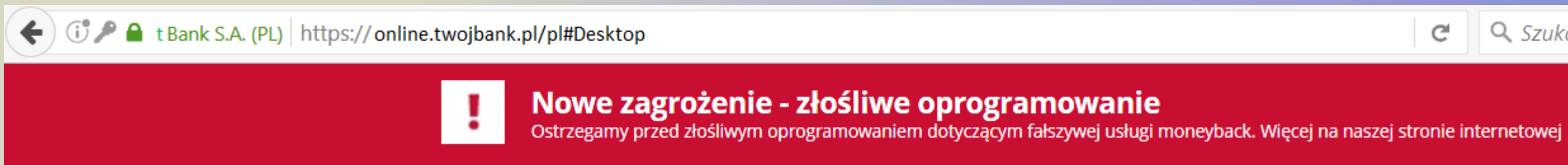
Nie daj się nabrać twój bank nigdy tego nie robi!

➤ 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 przechwytyjące poufne dane i
wyłudzające hasła SMS, podszywając się pod usługę
moneyback**

09-12-2016

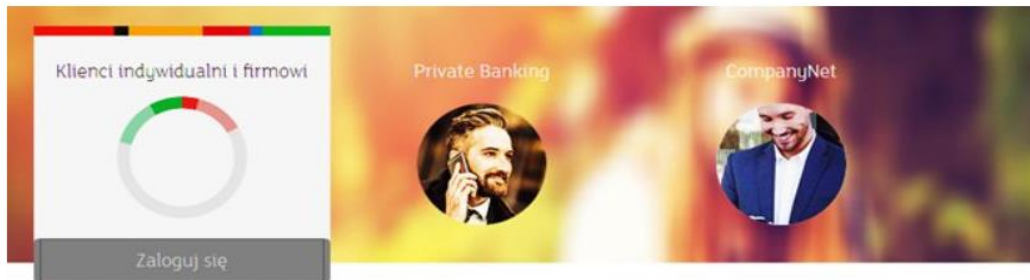
Fałszywe strony banków - phishing

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:



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.



LOKALIZATOR
Zlokalizuj dowolny telefon w sieci komórkowej
Z naszych usług skorzystało już **1 053 603** osób!

Strona główna Produkty Jak to działa? Abonament Dodatki Kontakt

Idealne narzędzie pozwalające na:

- ✓ Śledzenie niewiernych żon, mężów oraz partnerów biznesowych
- ✓ Namierzanie wartościowych przesyłek
- ✓ Śledzenie osób
- ✓ Ochronę pracowników w terenie
- ✓ Monitorowanie bezpieczeństwa dzieci i osób starszych

Lokalizator numerów telefonów komórkowych

Szybki system i algorytm pozwala na dyskretne użytkowanie oraz prowadzenie nadzoru pozostając niezauważonym.

Wygodny dostęp online lub za pomocą SMS do danych zebranych przez system zwiększa komfort użytkowania.

Numer do zlokalizowania **NAMIERZ**

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

Otrzymałeś tego maila ponieważ zapisałeś się do programu lojalnościowego ~~Neocraft~~ Neocraft Sp. z o.o. lub jego partnera. W każdej chwili możesz się wypisać klikając w ten link i zrezygnować z możliwości otrzymywania atrakcyjnych ofert, zniżek oraz kuponów rabatowych.

Gratulujemy

Otrzymujesz szansę na wygranie

2000 zł w gotówce



Wypełnij pola, aby wziąć udział. Pozostały 3 nagrody.

Abonament

Karta

Data urodzenia


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 załączników ZIP lub PDF.

Do...	Twoja Paczka S.A. <inforamcja@twoja-paczka.pl>
Temat	Twoja Paczka S.A. eINFO
Dołączono	 NR.0052285222.pdf.zip (245 KB)

Szanowny Kliencie,
Przesyłka kurierska Przesyłka NR.0052285222 Kwota pobrania 145.22 zł. Oczekuje na odbiór do 2016-12-15.

-aby wyświetlić informacje o usłudze
<https://www.twoja-paczka.pl>

Ta wiadomość została wygenerowana automatycznie, prosimy na nią nie odpowiadać.

Z poważaniem,
Twoja Paczka|

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.



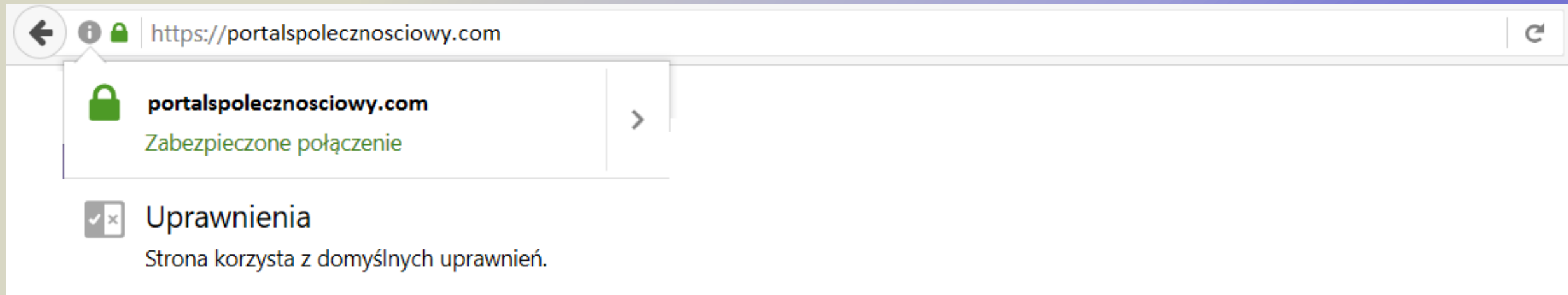
Zagrożenie w trakcie korzystania z portali społecznościowych (1/4)

- 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

Dwa dni temu doszedł mi nowy super telefon wygrany w konkursie, niby wygrywa co 3 osoba. Po wypełnieniu formularza zadzwonili do mnie po 30 minutach i poinformowali, że udało mi się wygrać, poprosili jeszcze adres do wysyłki. Doszedł po dwóch dniach! łapcie link do konkursu:



Konkurs ! Wygraj Super telefon

Ogłaszamy konkurs w którym do wygrania jest

GRATULACJE! MASZ WIELKĄ SZANSĘ NA WYGRANIE KARTY PODARUNKOWEJ DO SUPER ODZIEŻY

Jeszcze tylko musisz zeweryfikować swoją tożsamość.

PROSIMY WYŚLAĆ 2X SMS O TREŚCI: [REDACTED] POD NUMER: [REDACTED]

Następnie wpisz otrzymane kody poniżej:

Otrzymany kod nr. 1

Otrzymany kod nr. 2

Zatwierdź

Zagrożenie w trakcie korzystania z portali społecznościowych

Fałszywe konta

Mam dla Was Świąteczny Prezent.

Bony Wartości 1500zł, Zapraszam do odbierania.



AŻ 1000 BONÓW

PROMOCJA!

CZEKA 1500ZŁ W BONACH

H&M ZARA
CROPP
sinsay

PROMOCJA OGRANICZONA
CZASOWO

LINK POWYŻEJ

Fałszywe odzyskanie hasła

← → ↻ www.odzyskiwanie.ps/

Portal społecznościowy

Adres e-mail lub numer telefonu Hasło

Nie wylogowuj mnie Nie pamiętasz hasła?

Twoje Hasło Zostało Zmienione

Ktoś Próbował Włamać się Na Twoje Konto w Serwisie Portal społecznościowy
Dlatego Hasło zostało automatycznie zmienion
Aby odzyskać swoje konto pobierz i uruchom generator n
Generator Przeprowadzi Cię poprzez proces generowania i.....

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;
- Najślabszym ogniwem jest zwykle sam użytkownik.



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

Fałszywe sklepy internetowe

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 internetowe

Skontaktuj się z nami powiadomienia@sklep-elektro24.pl Kontakt z nami Zaloguj się

ELEKTRO.net

Koszyk (pusty)

KONSOLE TABLETY TELEFONY KOMPUTERY KARTY PAMIĘCI

Konsole




KONSOLE

Jest 27 produktów.

Sortuj wg -- Pokaż 12 na stronę Widok: Siatka Lista

Pokazuje 1 - 12 z 27 elementów < Poprzedni 1 2 3 Następny > Pokaż wszystkie Porównaj (0)

WYPRZEDAŻ

		
SONY PS4 500GB	SONY PS4 + MINECRAFT	SONY PS4 500 GB + gra LBP 3
1 289,00 zł	1 449,00 zł	1 519,00 zł
<input type="button" value="W magazynie"/>	<input type="button" value="W magazynie"/>	<input type="button" value="W magazynie"/>

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.
- Zaszifrowane 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



IOS



ANDROID



WINDOWS PHONE

SYNCHRONIZACJA Z KOMPUTEREM PRZEZ INTERNET (WYGODNA)



PRZEZ ICLOUD

Bezpłatną usługę chmurową Apple'a konfigurujemy w ustawieniach iPhone-a/iPada. Przechowuje ona multimedia, kontakty i wpisy w terminarzu



PRZEZ GOOGLE

Każdy użytkownik sklepu Play ma konto w usłudze Gmail. Umożliwia ona wygodne zarządzanie danymi kontaktowymi i terminarzem



PRZEZ OUTLOOK.COM

Użytkownicy telefonów z Windows Phone posiadający konto w usługach Microsoftu mogą zapisywać kontakty i terminy w serwisie Outlook.com

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-spotu 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)

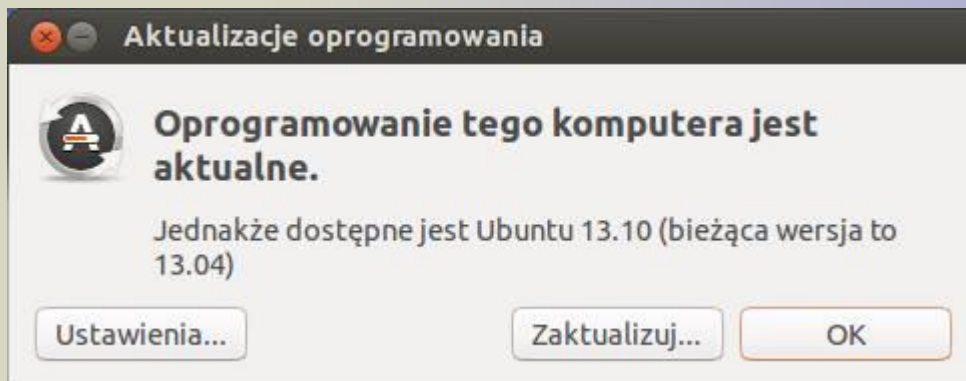
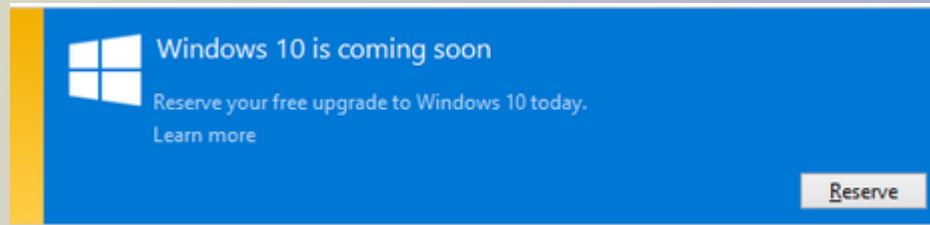
Bezpieczeństwo danych zaczyna się od Twojego sprzętu.

- 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 :

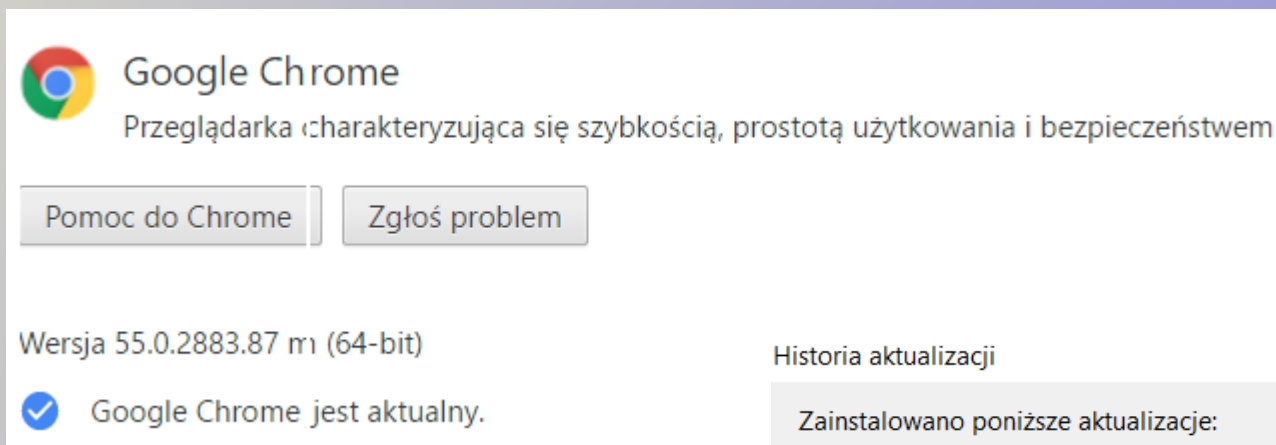
- Windows;
- IOS;
- Linux.



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

Najczęściej używane przeglądarki internetowe - aktualizacja:

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



Google Chrome
Przeglądarka charakteryzująca się szybkością, prostotą użytkowania i bezpieczeństwem

Pomoc do Chrome Zgłoś problem

Wersja 55.0.2883.87 m (64-bit)

Google Chrome jest aktualny.



Internet Explorer — informacje



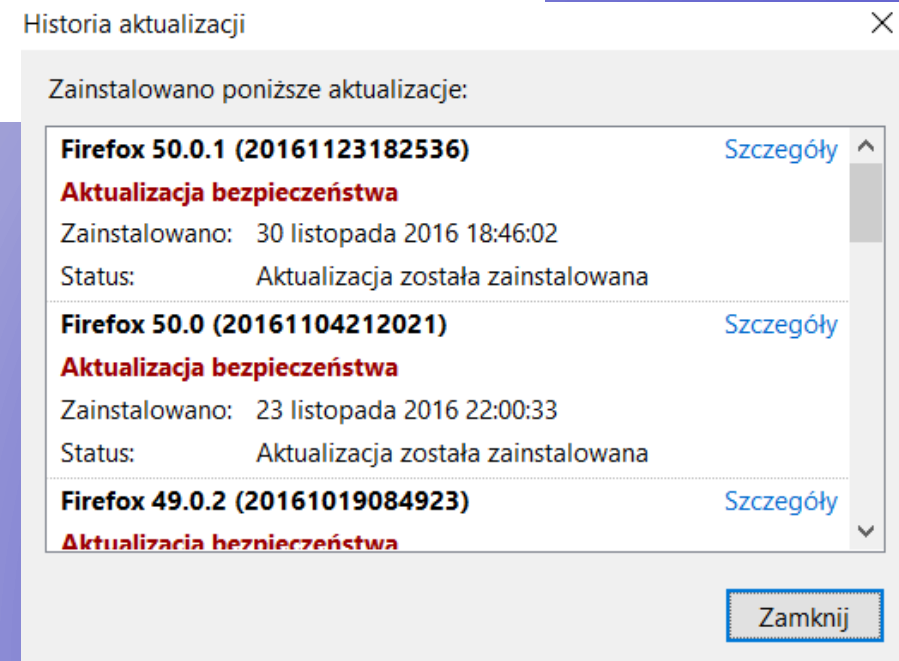
Internet Explorer®11

Wersja: 11.447.14393.0
Wersje aktualizacji: 11.0.37 (KB3197655)
Identyfikator produktu: 00150-20000-00003-AA459

Instaluj nowe wersje automatycznie

© 2015 Microsoft Corporation. Wszelkie prawa zastrzeżone.

Zamknij



Historia aktualizacji

Zainstalowano poniższe aktualizacje:

Firefox 50.0.1 (20161123182536) Aktualizacja bezpieczeństwa Zainstalowano: 30 listopada 2016 18:46:02 Status: Aktualizacja została zainstalowana	Szczegóły
Firefox 50.0 (20161104212021) Aktualizacja bezpieczeństwa Zainstalowano: 23 listopada 2016 22:00:33 Status: Aktualizacja została zainstalowana	Szczegóły
Firefox 49.0.2 (20161019084923) Aktualizacja bezpieczeństwa	Szczegóły

Zamknij

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.**



Dziękuję za uwagę

Michał Frica