KONRAD POSTAWA

CYBERZAGROŻENIA, PROBLEM WIRTUALNY CZY REALNY?

Erasmus+

O czym dziś porozmawiamy?

- **Analogowe metody oszustw**
  Czyli jak próbuje się nas oszukać na co dzień
- **Cyfrowe metody oszustw**
  Czyli jakie metody stosują złodzieje w sieci
- **Zagrożenia ze strony „wirusów”**
  Co nam grozi ze strony złośliwego oprogramowania
- **Bezpieczeństwo bankomatów i kart płatniczych**
  Czy bankomaty i karty płatnicze są tak bezpieczne jak myślimy
- **Kody QR**
  Czym są kody QR i jakie niosą ze sobą zagrożenie
- **Dane osobowe**
  Ochrona naszych danych oraz prawa i obowiązki z tym związane
- **Bezpieczne hasła**
  Kilka słów o tym jak tworzyć i zapamiętywać bezpieczne hasła
- **Zabezpieczenia smartfonów**
  Czy nasze telefony są tak bezpieczne jak nam się wydaje

Co jest potrzebne do oszustwa?

Może wiedza techniczna i umiejętność programowania?

Nie! Wystarczy maszyna do pisania, pieczątka, dobry pomysł, a do tego sporo cierpliwości i odrobina bezczelności.

Podejście analogowe

Czasem sami podajemy swoje dane

Wystarczy, że złodziej ma ciekawy pomysł

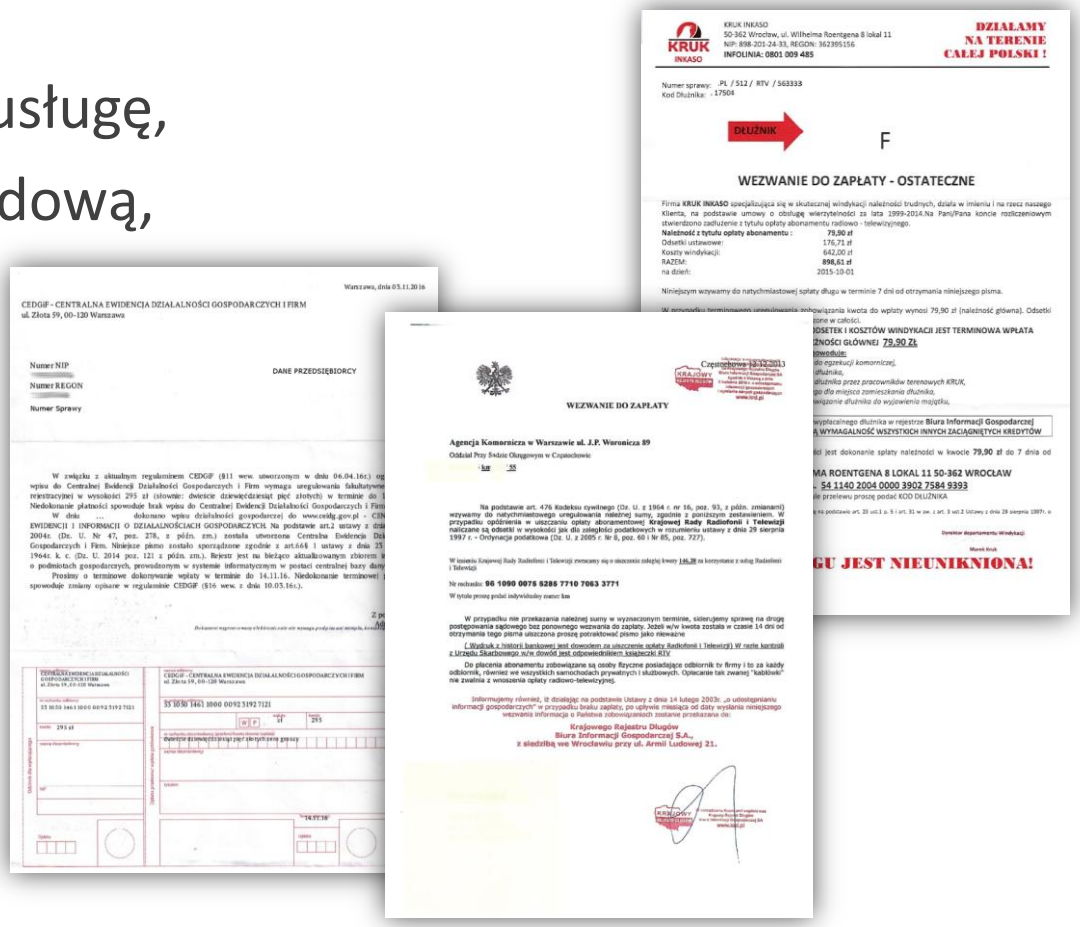
https://www.youtube.com/watch?v=Advj0Zlo5nQ

Metoda „Na pismo urzędowe”

Na czym to polega?

Dostajemy do domu pismo wzywające nas do uiszczenia opłaty:

- za wykonaną usługę,
- jako karę urzędową,
- jako grzywnę,
- itp.



KRUK INKASO
50-362 Wrocław, ul. Wilhelma Roentgena 8 lokal 11
NIP: 898-201-24-33, REGON: 362395156
INFOLINIA: 0801 009 485

DZIAŁAMY NA TERENIE CAŁEJ POLSKI !

Numer sprawy: -PL / 512 / RTV / 563333
Kod Dłużnika: - 17504

DŁUŻNIK F

WEZWANIE DO ZAPŁATY - OSTATECZNE

Firma KRUK INKASO specjalizująca się w skutecznej windykacji należności trudnych, działa w imieniu i na rzecz naszego Klienta, na podstawie umowy o obsługę wierzytelności za lata 1999-2014.Na Pani/Pana koncie rozliczeniowym stwierdzono zadłużenie z tytułu opłaty abonamentu radiowo - telewizyjnego.

Należność z tytułu opłaty abonamentu :	79,90 zł
Odsetki ustawowe:	176,71 zł
Koszty windykacji:	642,00 zł
RAZEM:	898,61 zł
na dzień:	2015-10-01

Niniejszym wzywamy do natychmiastowej spłaty długu w terminie 7 dni od otrzymania niniejszego pisma.

ODSETEK I KOSZTÓW WINDYKACJI JEST TERMINOWA WPŁATA
ŻNOŚCI GŁÓWNEJ 79,90 Zł

MA ROENTGENA 8 LOKAL 11 50-362 WROCŁAW
54 1140 2004 0000 3902 7584 9393

GU JEST NIEUNIKNIONA!

CEDGiF - CENTRALNA EWIDENCJA DZIAŁALNOŚCI GOSPODARCZYCH I FIRM
ul. Złota 59, 00-120 Warszawa

Warszawa, dnia 05.11.2016

Numer NIP
Numer REGON
Numer Sprawy

DANE PRZEDSIĘBIORCY

WEZWANIE DO ZAPŁATY

Agencja Komornicza w Warszawie ul. J.P. Woronicza 89

Na podstawie art. 476 Kodeksu cywilnego (Dz. U. z 1964 r. nr 16, poz. 93, z późn. zmianami) wzywamy do natychmiastowego uregulowania należnej sumy, zgodnie z poniższym zestawieniem. W przypadku opóźnienia w uiszczeniu opłaty abonamentowej Krajowej Rady Radiofonii i Telewizji naliczane są odsetki w wysokości jak dla zaległości podatkowych w rozumieniu ustawy z dnia 29 sierpnia 1997 r. - Ordynacja podatkowa (Dz. U. z 2005 r. Nr 8, poz. 60 i Nr 85, poz. 727).

Nr rachunku: 96 1090 0075 5286 7710 7063 3771

W przypadku nie przekazania należnej sumy w wyznaczonym terminie, skierujemy sprawę na drogę postępowania sądowego bez ponownego wezwania do zapłaty. Jeżeli w/w kwota została w czasie 14 dni od otrzymania tego pisma uiszczona proszę potraktować pismo jako nieważne

(Wydruk z historii bankowej jest dowodem za uiszczenie opłaty Radiofonii i Telewizji) W razie kontroli z Urzędu Skarbowego ma on dowód jest odpowiednikiem książeczki RTV

Do płacenia abonamentu zobowiązane są osoby fizyczne posiadające odbiornik tv firmy i to za każdy odbiornik, również we wszystkich samochodach prywatnych i służbowych. Opłacanie tak zwanej "kablówki" nie zwalnia z wnoszenia opłaty radiowo-telewizyjnej.

Informujemy również, iż działając na podstawie Ustawy z dnia 14 lutego 2003r. o udostępnianiu informacji gospodarczych" w przypadku braku zapłaty, po upływie miesiąca od daty wysłania niniejszego wezwania informacja o Państwa zobowiązaniach zostanie przekazana do:

Krajowego Rejestru Długów
Biura Informacji Gospodarczej S.A.,
z siedzibą we Wrocławiu przy ul. Armii Ludowej 21.

Co jest potrzebne do oszustwa?

W takim razie może trzeba mieć dostęp do komputera ofiary?

Nie! Znów wystarczy dobry pomysł, odrobina bezczelności i umiejętność kopiowania, a ze strony ofiary chwila nieuwagi.

Podejście cyfrowe

Metoda „Na maila”

Najczęściej dotyczy mediów społecznościowych

Dostajemy mail od naszego znajomego, w którym ten informuje nas, że ma nowy ciekawy profil na FB i zachęca nas do obejrzenia. Poniżej przykład takiego maila.

Hej,

Koniecznie musisz zobaczyć mój nowy profil, są tam ekstra zdjęcia z ostatniego wyjazdu.

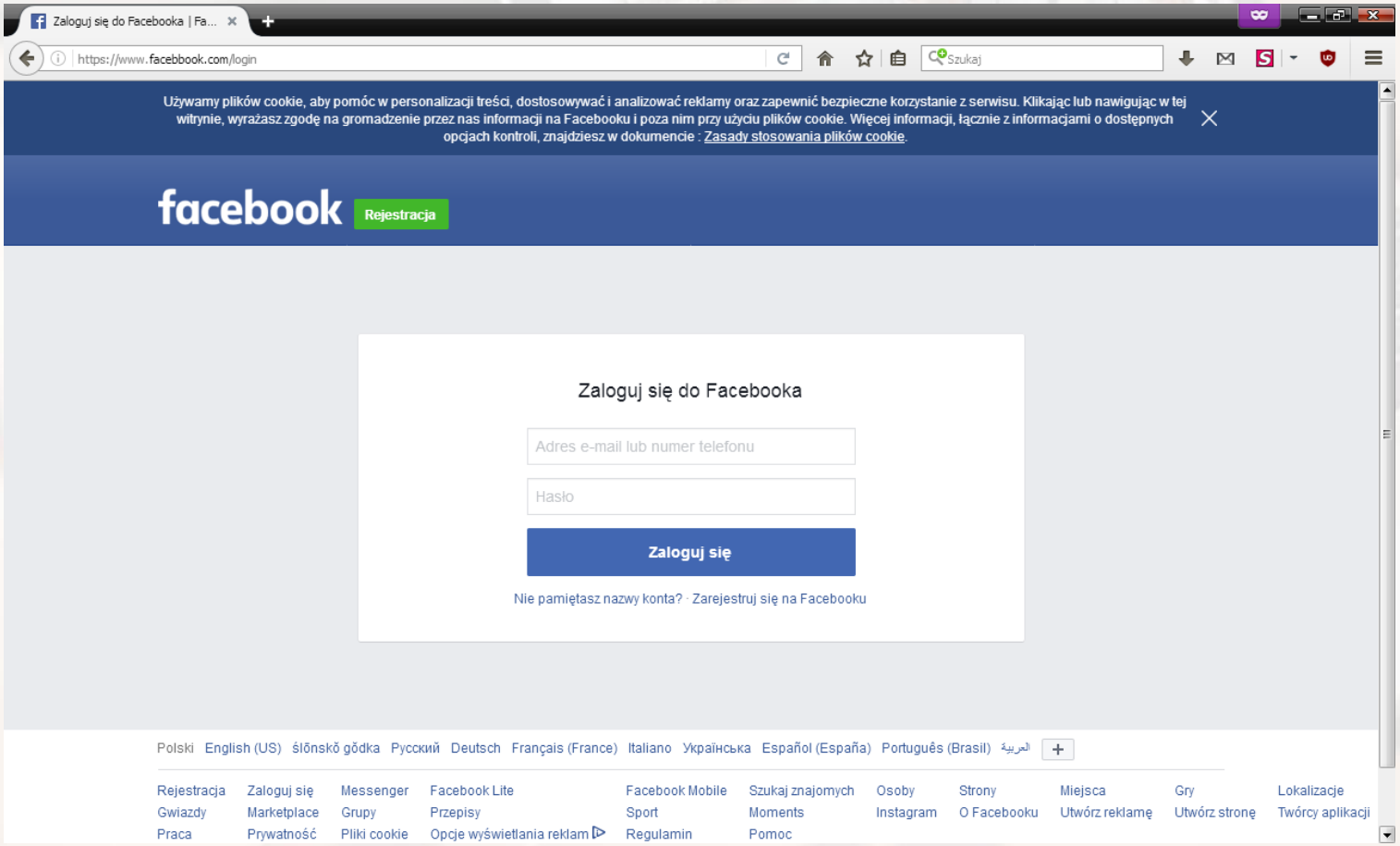
http://facebook.com/jaski-jakis-18857748394/

Pozdrawiam,

Janek

Klikamy na link i jesteśmy…

…no właśnie, gdzie właściwie jesteśmy?



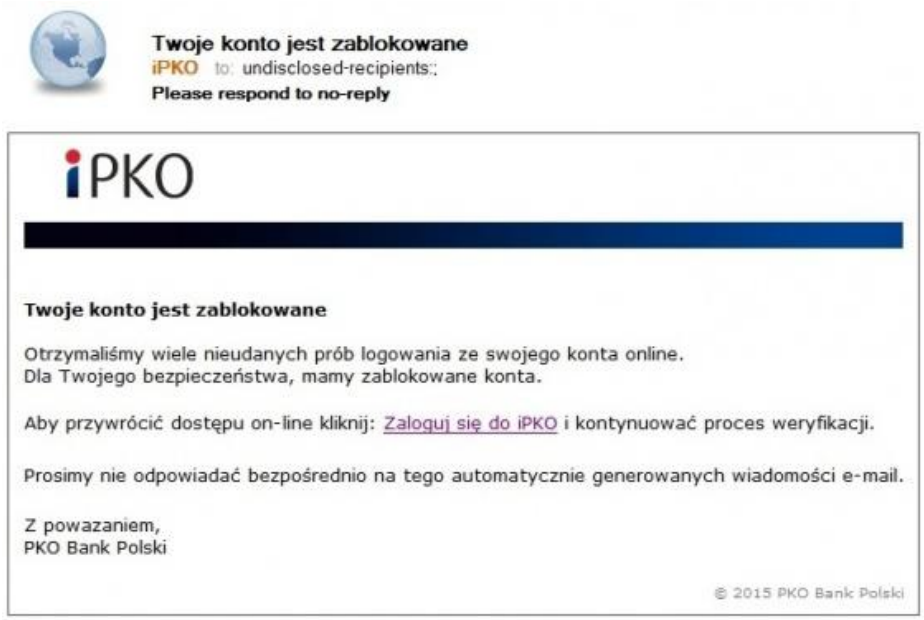
Adres strony brzmi: http://facebbook.com/login - a jak powinien?

Metoda „Na maila”

Może także dotyczyć naszych kont bankowych

W takim przypadku dostajemy najczęściej maila informującego nas, że z powodu problemów technicznych nasz dostęp do baku został zablokowany. Trzeba się zalogować i podać:

- numer naszej karty,
- data ważności karty,
- kod CVC.



Twoje konto jest zablokowane
iPKO to: undisclosed-recipients:;
Please respond to no-reply

iPKO

Twoje konto jest zablokowane

Otrzymaliśmy wiele nieudanych prób logowania ze swojego konta online.
Dla Twojego bezpieczeństwa, mamy zablokowane konta.

Aby przywrócić dostępu on-line kliknij: Zaloguj się do iPKO i kontynuować proces weryfikacji.

Prosimy nie odpowiadać bezpośrednio na tego automatycznie generowanych wiadomości e-mail.

Z powazaniem,
PKO Bank Polski

© 2015 PKO Bank Polski

Wirusy i złośliwe programy

Co jest potrzebne do oszustwa?

A co jeśli haker potrafi się dostać do naszego komputera?

Wtedy warto mieć dobry i aktualny program antywirusowy oraz zachowywać w Internecie podstawowe zasady bezpieczeństwa.

WannaCry – szyfrowanie dysku

Czyli zapłać, albo pożegnaj się z danymi

Jest to złośliwe oprogramowanie typu ransomware, które szyfruje zawartość dysku komputera i żąda zapłaty za przywrócenie dostępu do plików.

Ogromna fala ataków rozpoczęła na początku maja i zainfekowanych zostało wiele komputerów w 99 krajach w tym i w Polsce.

Jeśli padniemy ofiarą ataku mamy trzy dni na zapłatę – w walucie Bitcoin.

Tak wygląda nasz komputer po…

…zainfekowaniu, a właściwie po zaszyfrowaniu

Mamy dwa wyjścia, albo zapłacić, albo skasować dysk i dane.

Zeus i jego pochodne

Co robimy gdy chcemy zrobić przelew online?

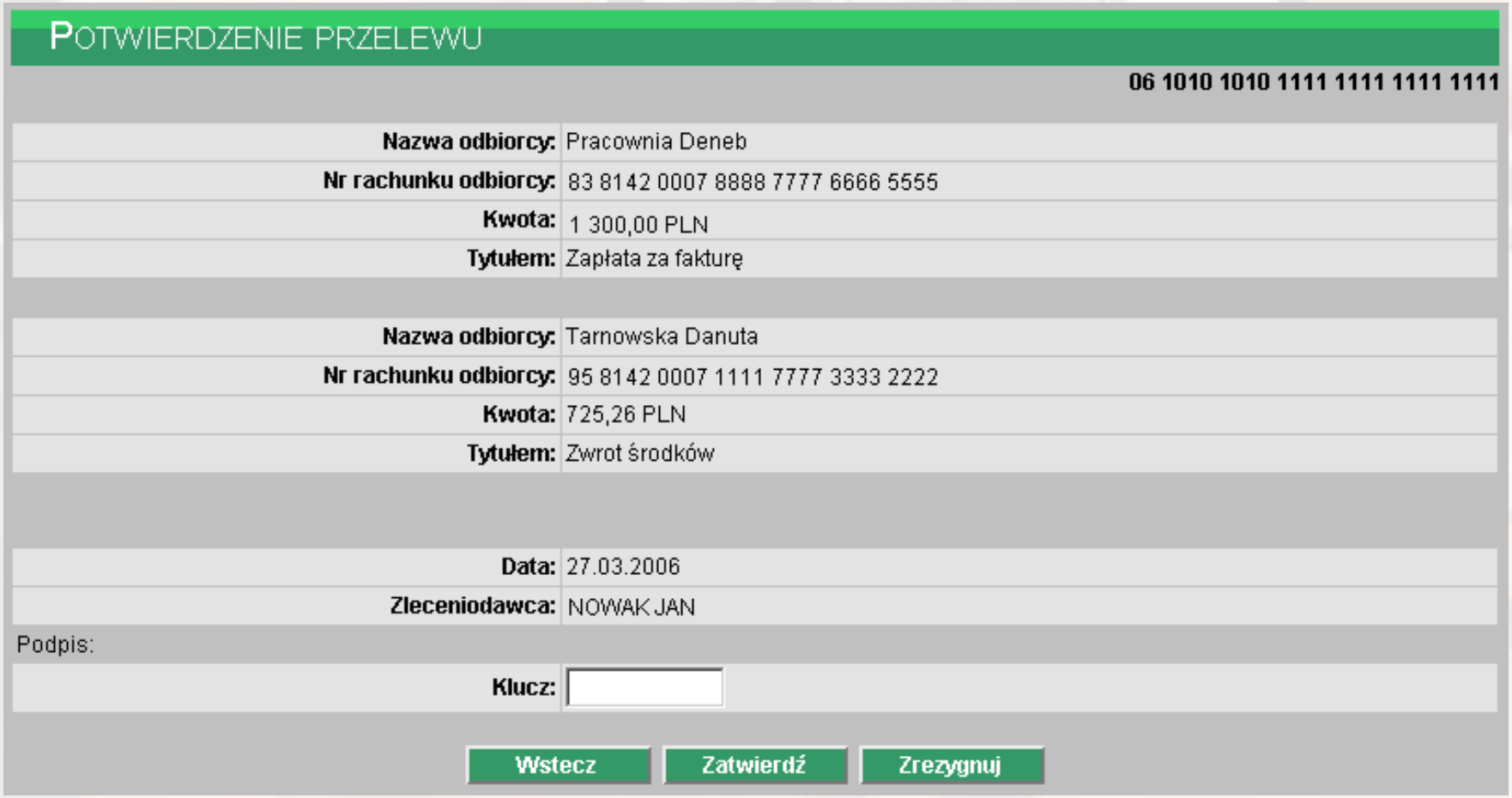
Podajemy kwotę, nazwisko adresata lub nazwę firmy, podajemy także adres oraz tytuł przelewu, ale najważniejsze, że **kopiujemy numer konta.**

No właśnie kopiujemy! No i zwykle nie sprawdzamy, czy skopiowany numer jest tym samym, który się wkleił. Wirus Zeus rozpoznaje skopiowany adres i zamienia go na inny. Legalnie przelewamy pieniądze na konto oszustów.

Nowsza wersja wirusa potrafi oszukać i nasze oczy, bo pokazuje, że wkleiliśmy dobry numer, a podmienia go dopiero podczas zatwierdzania przelewu!

Jak więc uniknąć kłopotu?

Najlepiej sprawdzić numery kont tuż przed podaniem kodu SMS lub kodu ze zdrapki.



POTWIERDZENIE PRZELEWU

06 1010 1010 1111 1111 1111 1111

Nazwa odbiorcy:	Pracownia Deneb
Nr rachunku odbiorcy:	83 8142 0007 8888 7777 6666 5555
Kwota:	1 300,00 PLN
Tytułem:	Zapłata za fakturę

Nazwa odbiorcy:	Tarnowska Danuta
Nr rachunku odbiorcy:	95 8142 0007 1111 7777 3333 2222
Kwota:	725,26 PLN
Tytułem:	Zwrot środków

Data:	27.03.2006
Zleceniodawca:	NOWAK JAN

Podpis:

Klucz:

Wstecz | Zatwierdź | Zrezygnuj

Metoda „Na poczekalnię”

Czyli, co się może zdarzyć, gdy siedzimy i czekamy?

Nie chodzi tu wcale o taką poczekalnie jak na zdjęciu.

Czekać możemy też w innych miejscach…

Metoda „Na poczekalnię” – etap 1

Wchodzimy na stronę banku, podajemy login i hasło, a po chwili pojawia się komunikat.

Trwają prace konserwacyjne, twoje połączenie zostanie wznowione za chwile…

W tym czasie haker, który przejął nasz login i hasło właśnie loguje się do banku i przygotowuje sobie przelew.

Metoda „Na poczekalnię” – etap 2

No to czekami i po minucie dostajemy kolejny komunikat.

Z powodu problemów z bazą danych konieczna jest weryfikacja właściciela rachunku. Podaj otrzymany kod SMS:

WYŚLIJ

Haker już ma przygotowany przelew i czeka tylko, aż podamy mu kod do autoryzacji, by mógł przesłać pieniądze.

Metoda „Na poczekalnię” – etap 3

Znów czekami i otrzymujemy komunikat.

Logowanie do systemu nie jest w tej chwili możliwe.
Prosimy spróbować ponownie za parę minut.

Wydaje się nam, że nic się nie stało, a w rzeczywistości właśnie straciliśmy pieniądze.

Metoda „Na poczekalnię”

W jaki sposób się uchronić?

Po pierwsze powinniśmy zawsze sprawdzać, czy jesteśmy na prawdziwej stronie banku.

Po drugie jeśli widzimy, że coś się dzieje to po prostu wyłączamy przeglądarkę i nie kontynuujemy operacji. Można zadzwonić do banku i spytać w czym jest problem.

Po trzecie warto włączyć powiadomienia SMS, które to zawsze dadzą nam znać jeśli z konta została wypłacona gotówka. Będziemy zawsze wiedzieć, że coś się dzieje.

No i nie czekajmy – działajmy!


Bankomaty, czy to bezpieczne?

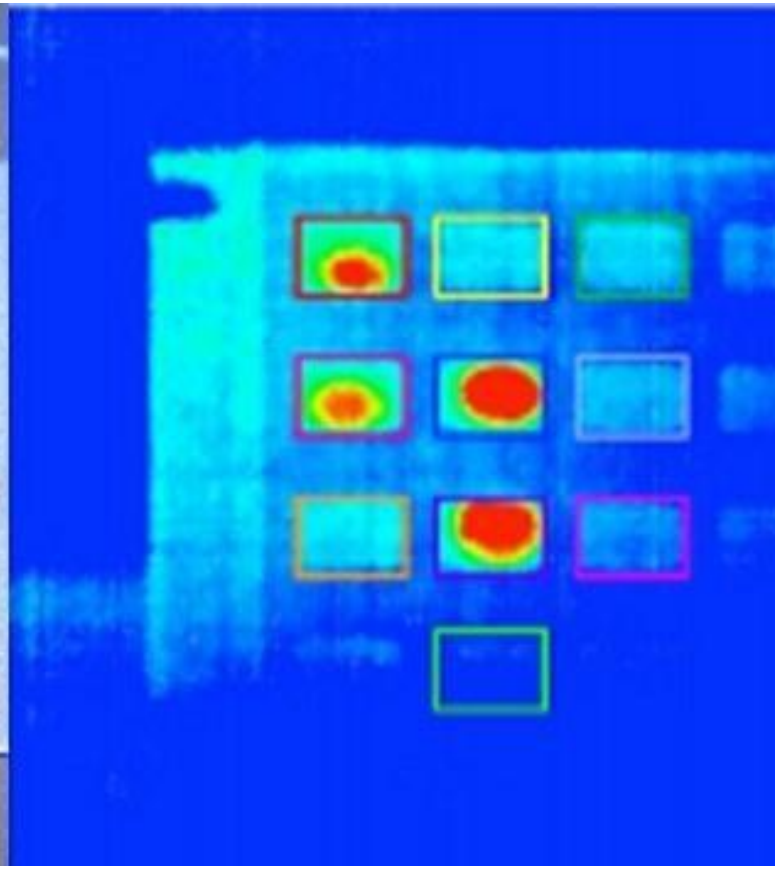
Jeśli komputer nie jest bezpieczny

To może lepiej użyć bankomatu. Przecież tu nic nam nie grozi…

https://www.youtube.com/watch?v=D57HZfrpGkQ

Kamera termowizyjna

Po wypłacie naciśnijmy wszystkie klawisze



Możemy użyć bankomatu inaczej

Można wyciągnąć pieniądze za pomocą telefonu

Pomysł jest bardzo prosty. Za pomocą naszego telefonu zlecamy wypłatę pieniędzy i zamiast PINu podajemy jednorazowy kod SMS.

Możemy użyć do tego kilku aplikacji

Zależy to od naszego banku i rodzaju konta

Cała prawda o kartach płatniczych

Problem polega na tym, że…

…sami ujawniamy dane naszej karty

Na karcie znajduje się jej numer, data ważności i kod CVC. Te trzy informacje wystarczą, by dokonać zakupu w sklepie internetowym.

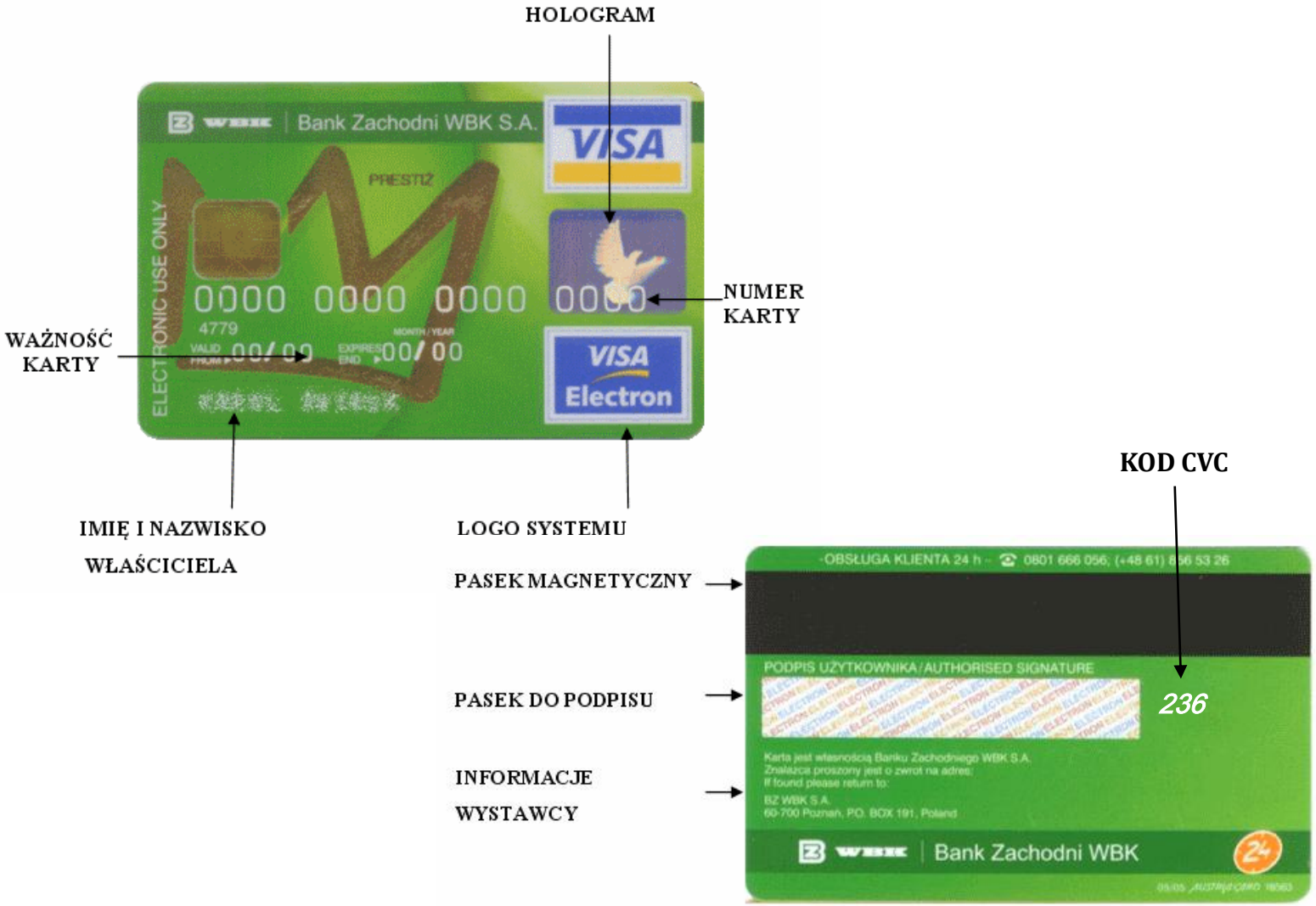
Ale jak to bez PINu? No bez PINu!

Teoretycznie karty mają chip, który uniemożliwia dokonanie takiej transakcji, ale nie zawsze to działa.

W Polsce **83%** kart płatniczych ma chip, przykładowo już w USA tylko **32%**, więc większość sklepów nie sprawdza tego typu zabezpieczenia.

O jakich danych mowa?

Najlepiej będzie użyć ilustracji



Czasem sami się okradamy

Zdjęcia pochodzą z aukcji na Allegro

Czy ktoś mi powie, gdzie jest problem?

Metoda „Na taksówkarza”

Czy karta płatnicza jest bezpieczna?

Metoda ta wygląda następująco:

1. Jedziemy taksówką i po zakończeniu kursu chcemy zapłacić kartą.
2. Taksówkarz wyjmuje terminal, podajemy mu kartę i zostajemy poproszeni o wpisanie PINu i potwierdzenie.
3. Dostajemy paragon, wysiadamy z taksówki i zapominamy o sprawie.

Czy zatem nic się nie stało?

Gdzie został popełniony błąd?

Metoda „Na taksówkarza”

Co się właściwie stało?

Taksówkarz biorąc od nas kartę zapamiętał 3-cyfrowy kod CVC z jej odwrotu. Do tego terminal był fałszywy i zapisał numer naszej karty oraz PIN.

Oczywiście nasze konto nie zostało obciążone, więc mieliśmy przejazd za darmo, ale czy na pewno?

Sprzedawca nie ma prawa prosić nas o podanie karty, więc nie wypuszczajmy jej z rąk. Możemy także zasłonić kod CVC lub wymazać go za pomocą acetonu (zmywacz do paznokci).

Karty zbliżeniowe

Można je odczytać nawet przez portfel

Można jednak się przed tym zabezpieczyć przy użyciu zwykłej folii kuchennej.

Kody QR

Metoda na „Yes Mena”

Czyli zgadzamy się na wszystko - zawsze „TAK”

W jednym z hoteli pojawił się plakat podobny do tego:

Metoda na „Yes Mena”

Co w tym groźnego?

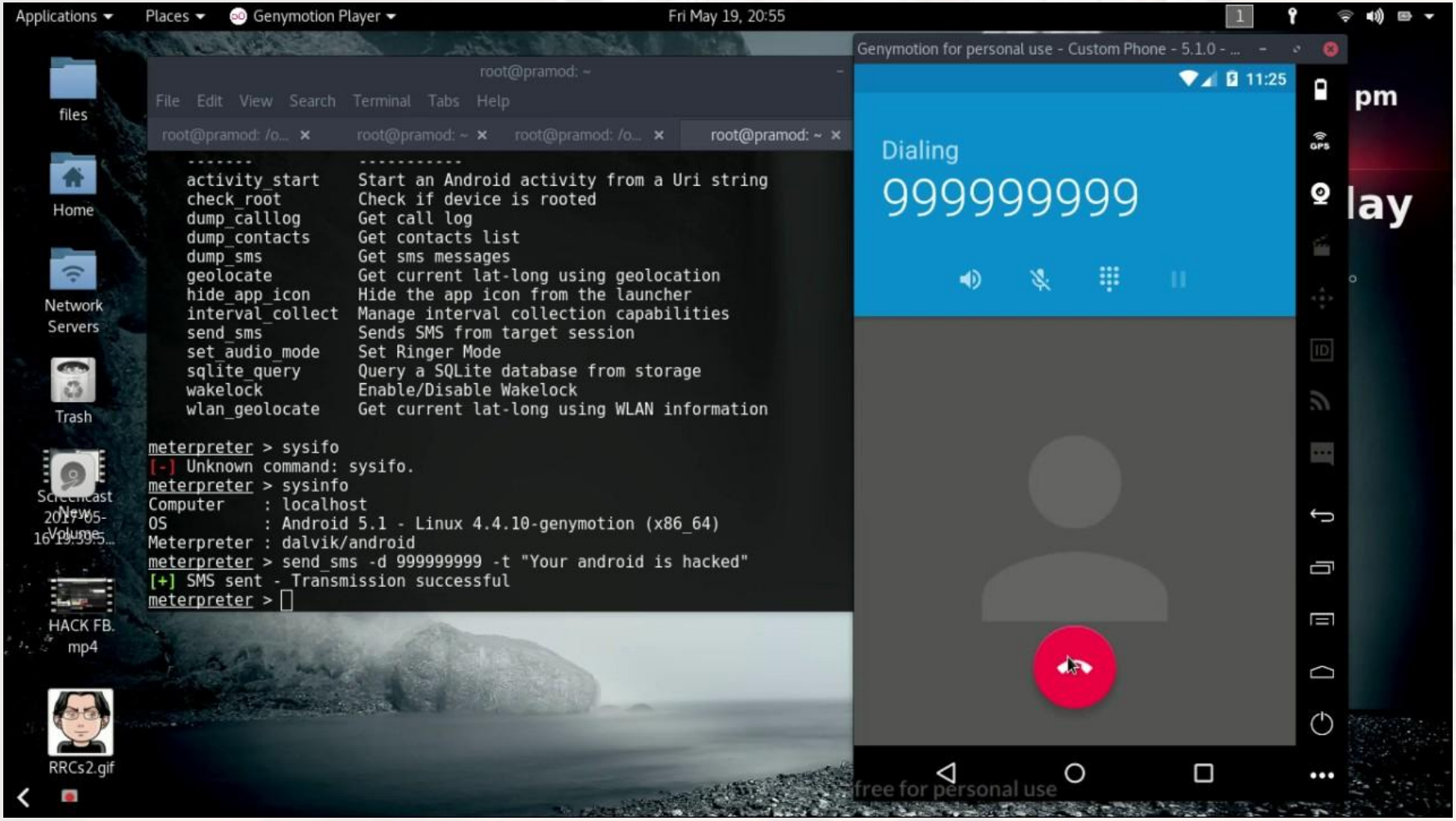
Plakat oferuje nam tańszy dostęp do Internetu. Po stawce $2 zamiast $20 za 10MB danych. Wiele osób chce na wakacjach oszczędzić i skanuje kod.

Co w tym złego?

1. Instalujemy aplikację z nieznanego źródła. Telefon ostrzega, ale zgadzamy się „YES”.
2. Aplikacja pyta o dostęp do naszego telefonu i zgadzamy się „YES”.
3. Telefon sam łączy się z serwerem hakera i zgłasza, że jest gotowy do przesyłania danych.

Co może zrobić haker?

Właściwie to może zrobić co chce!



Metoda na „Yes Mena”

Co się dzieje?

Włamywacz ma dostęp do naszego telefonu, więc może zrobić wszystko to, co robimy mając telefon w ręku.

- może pobrać listę naszych kontaktów
- może pobrać wszystkie SMS-y
- może wysyłać SMS-y i MMS-y
- może dzwonić z naszego telefonu
- może przeglądać zdjęcia, muzykę i dokumenty, które mamy na telefonie
- ma dostęp do mikrofonu i kamery, więc może nas podsłuchać i zobaczyć

Dane osobowe

Co to są dane osobowe?

Według encyklopedii

Dane osobowe – termin prawny, który w prawie polskim został zdefiniowany w ustawie z dnia 29 sierpnia 1997 o ochronie danych osobowych. W rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Dane osobowe to imię, nazwisko, wiek, płeć, adres, PESEL, zawód, ale także numer telefonu, odcisk palca i skan siatkówki oka.

Od niedawna to także nasz login sieciowy, adres email oraz numer rejestracyjne pojazdu.

Jak chronić dane osobowe?

Zasada im mniej tym lepiej

Podczas rejestracji na stronach internetowych, podczas zakładania kart klubowych itp. najlepiej ograniczyć dane tylko do niezbędnego minimum.

Pamiętajmy także o tym, że jeśli firma, urząd czy sklep chce użyć naszych danych osobowych musimy się na to zgodzić.

To, że nasze dane są dostępne publicznie nie znaczy, że można z nimi robić, co się chce! Bez zgody na wykorzystanie danych nie wolno ich użyć!

Tak to wyglądało do tej pory…

…ale już nie będzie. Teraz trzeba jasnej deklaracji TAK lub NIE.

Wyrażam zgodę na przetwarzanie moich danych osobowych, wskazanych w powyższym formularzu przez ABC Sp. z o.o. z siedzibą przy ul. Ulicznej 1, 00-000 Miasto w celu:

- ☐ przesyłania mi bezpłatnych promocyjnych opakowań kosmetyków naturalnych, z oferty sklepu www.stosuj-ziola.pl,
- ☐ przekazania danych osobowych do producentów kosmetyków naturalnych w celu przeprowadzenia badania poziomu satysfakcji z otrzymanych bezpłatnych opakowań,
- ☐ wysyłania na mój adres e-mail informacji handlowych o produktach dostępnych w sklepie: www.stosuj-zioła.pl.

Jakie mamy prawa?

Ochrona danych osobowych działa w dwie strony!

Wyrażenie zgody na przetwarzanie danych jest bezterminowe.

Możemy wystąpić o trwałe usunięcie naszych danych z bazy oraz wszystkich kopii zapasowych.

Co nam daje RODO?

Unijne rozporządzenie dotyczące ochrony danych osobowych

PRAWO PODMIOTU DANYCH
- rozbudowane prawo do informacji, prawo do bycia zapomnianym

KARY FINANSOWE
- do 20 mln euro lub 4% wartości rocznego obrotu

ZGŁASZANIE INCYDENTÓW
- do 72 godzin, wysokie kary za brak zgłoszenia

ZASIĘG GLOBALNY
- wszędzie tam, gdzie przetwarzane są dane osobowe obywateli EU

Bezpieczne hasła

Najpopularniejsze hasła

Ranking z roku 2016

1. 123456
2. 123456789
3. qwerty
4. 12345678
5. 111111
6. 1234567890
7. 1234567
8. password
9. 123123
10. 987654321

Jakieś wnioski?

Jak mocne mamy hasła?

Można to oszacować

Im hasło jest dłuższe i bardziej skomplikowane tym trudniejsze do złamania.

Sprawdźmy to na przykładzie:

haselko – 2 sekundy

Haselko – 26 sekund

Haselk0 – 60 sekund

H@selk0 – 7 minut

H@!sel!k0 – 4 tygodnie

H@!sel!k0. – 5 lat

Jak wygląda mocne hasło?

Powinno spełniać kilka kryteriów:

Duże i małe litery

Cyfry

Znaki specjalne

Długość od 8 do 12 znaków

Wyrazy nie słownikowe

Znaki nie znajdujące się obok siebie

Przykłady dobrych haseł

Mocne hasła, ale łatwe do zapamiętania

Grosz **d**o **g**rosza, **a** **b**ędzie **k**okosza.

gdgabk – to już jest dobre hasło, ale można lepiej.

Gdg@bk – mamy już całkiem mocne hasło, ale za krótkie.

Gdg@bk17 – teraz mamy 8 znaków, małe i duże litery oraz znaki specjalne.

Na **z**łodzieju **c**zapka **g**ore

Nzcg - hasło za krótkie, ale można to poprawić, załóżmy, że to hasło do poczty.

Pocnzcg**Zta** – mamy już dość znaków

B@nzcg**Nk** – lub wariant z hasłem do banku

I jeszcze Smartfony

Pamiętajmy o telefonach

Mamy w nich sporo ważnych informacji

Najgorsze jest to, że wiele osób nie zabezpiecza swojego telefonu, a to wielki błąd.

Smartfon jest dość bezpieczny pod warunkiem, że sami nie damy do niego dostępu.

Możemy zgubić telefon, czy zostawić w pracy lub w innym miejscu. Wtedy obcy mogą przeglądać naszą pocztę, profil na FB, listę kontaktów, prywatne zdjęcia i wiele więcej.

Jak zabezpieczyć telefon?

Jest na to kilka sposobów

PIN – czyli minimum 4-cyfrowy kod zabezpieczający

Wzór – czyli blokowanie za pomocą narysowania symbolu

Odcisk palca – jeśli telefon ma czytniki linii papilarnych

Rozpoznawanie twarzy – odblokuje tylko właściciel

Nie ważne jaka metoda…

…ważne, by zabezpieczyć nasz smartfon


DZIĘKUJĘ ZA UWAGĘ
I DO ZOBACZENIA
ZA TYDZIEŃ
KONIEC