

Czy z "phishingiem" można wygrać?

Co banki mogą zrobić by rzadziej padać ofiarą phishingu.

Grzegorz Flak, CISSP

Współpraca Robert „Shadow” Pająk, CISSP

Plan wystąpienia



- Phishing wprowadzenie
 - Dlaczego się boimy?
 - Trochę historii
 - Jak to działa?
 - Czy naprawdę jesteśmy tacy głupi?
- Kto może z tym walczyć?
- Jak może ochronić nas nasz bank?
- Internet to nie wszystko

Phishing

Phishing, czyli podszywanie się pod markę, polega „łowieniu” (ang. fishing) naiwnych użytkowników w celu uzyskania jakiś korzyści, a najczęściej w celu kradzieży tożsamości użytkownika serwisu bankowego.

Phishing to hurtowy „social engineering”.

(fish 'ing) **(n.)** The act of sending an **e-mail** to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. - Webopedia

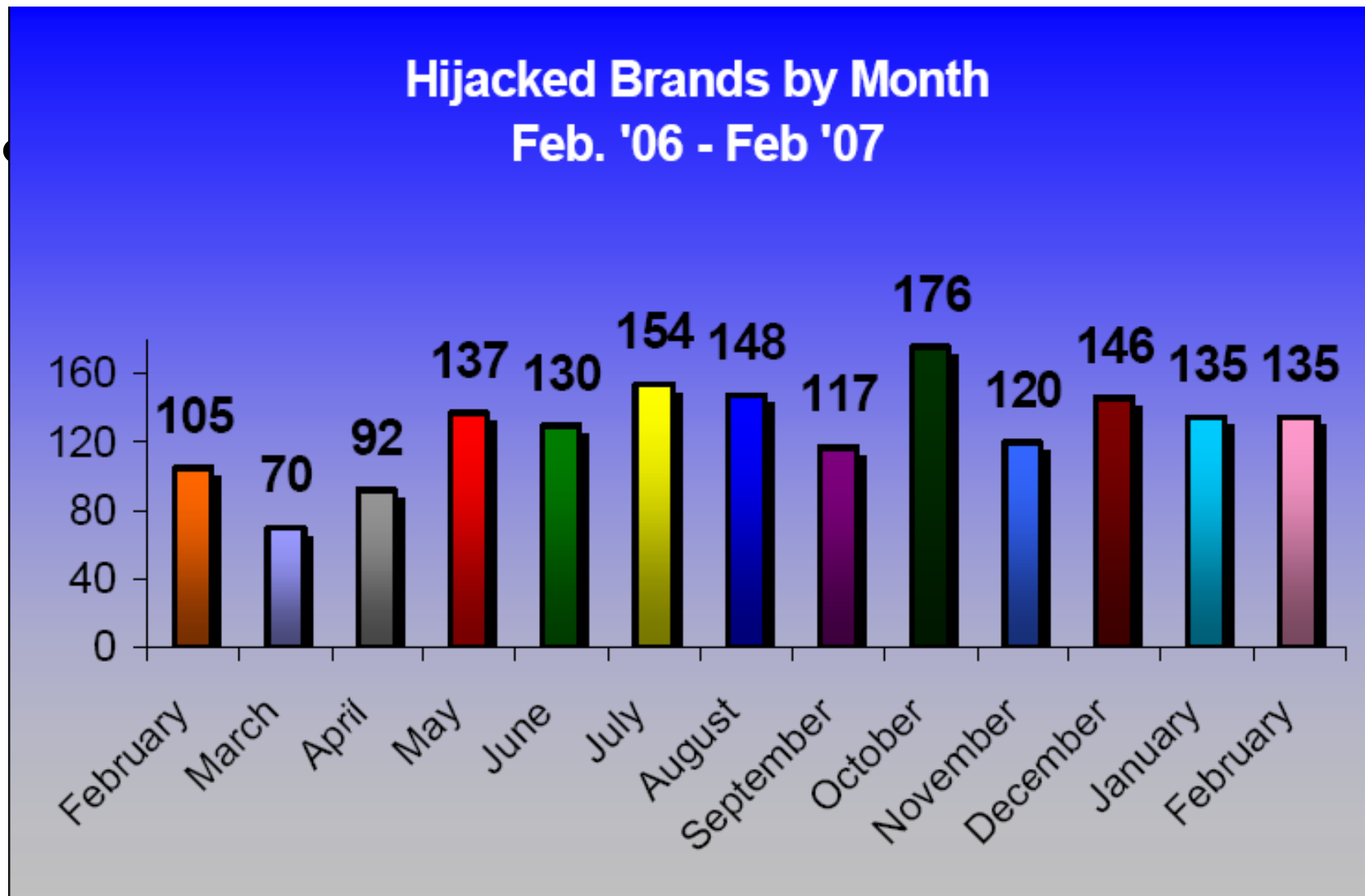
Dlaczego powinniśmy się bać?

- Koniec bezinteresownych hackerów!
- Za przestępstwa w Internecie wzięli się prawdziwi przestępcy:
 - Kradzież pieniędzy
 - Szpiegostwo przemysłowe
 - Pranie brudnych pieniędzy
 - Handel danymi
 - ... inne
- W coraz większym stopniu korzystamy z Internetu w codziennym życiu i ...
- ... większość ludzi nie rozumie jak to działa, ani dlaczego działa
- „Szybka, anonimowa kasaaaa...”, „dużo naiwnych ludzi z pieniędzmi...”

Kto na tym cierpi?

- Osoby, którym ukradziono tożsamość jak i te, które w następstwie poniosły straty finansowe
- Banki, aukcje i sklepy internetowe i wszyscy Ci, którzy prowadzą działalność przez Internet, bo rosnąca liczba ataków obniża zaufanie, a banki często biorą na siebie straty.
- Wszyscy użytkownicy – nawet jeśli nie są bezpośrednimi ofiarami, w prowizjach i opłatach muszą pokryć koszty strat tych naiwnych.

Statystyka



FraudWatch Phishing Alerts.

- **May 08, 2007** eBay - eBay Safeharbor Department
- **May 08, 2007** PayPal - Update your account.
- **May 08, 2007** Bank of America - Bank Of America Verify Account
- **May 08, 2007** Washington Mutual Bank - Wamu OnlineBank Account & BillPayment Alert
- **May 08, 2007** Chase Bank - Update your information account.
- **May 08, 2007** PayPal - Account Management *
- **May 08, 2007** Bank of America - NOTICE : Update your account information
- **May 08, 2007** Tennessee Valley Federal Credit Union - Three unsuccessful login attempts on your account!
- **May 08, 2007** Flagstar Bank - Dear Flagstar Member
- **May 08, 2007** PayPal - Resolution Center: Your account is limited.
- **May 08, 2007** The Co-operative Bank - Account Management
- **May 08, 2007** BBandT Bank - BBandT: please confirm your banking details! (mess_id: M5175179850)
- **May 08, 2007** PayPal - Notification of Limited Account Access
- **May 08, 2007** BBandT Bank - BBandT: important account notification! (message id: y0759827853073)
- **May 08, 2007** Wachovia Bank - Important Message For Wachovia Customers
- **May 07, 2007** PayPal - Invalid login Attempt
- **May 07, 2007** SunTrust Bank - Your SunTrust account is compromised !
- **May 07, 2007** Citibank - Important Notice!!! Account Security Upgrade
- **May 07, 2007** PayPal - Limited Account Access Appeal Denied.
- **May 07, 2007** PayPal - This email confirms that you have paid orders@dell.com \$699.99 USD using PayPal.
- **May 07, 2007** eBay - message from member
- **May 07, 2007** BBandT Bank - Account Notification! (message id: of2856935935km)
- **May 07, 2007** PayPal - You have added a new e-mail address !
- **May 07, 2007** eBay - eBay Unpaid Item Reminder for Item #180010728265
- **May 07, 2007** eBay - eBay Unpaid Item Reminder for Item #250111246947

To również dzieje się w Polsce

	Oszustwo komputerowe art. 287 par.1-2	Uzyskanie informacji art. 267 par. 1-3	Zniszczenie lub zmiana istotnej informacji art. 268 par. 1-3 i 268a	Zniszczenie lub zmiana informacji art. 269 par. 1-2	Sabotaż komputerowy art. 269a
2006	444	370	136	4	19
2005	568	260	98	3	1
2004	390	248	89	0	-
2003	168	232	138	2	-
2002	368	215	167	12	-
2001	279	175	118	5	-
2000	323	240	48	5	-

<http://www.policja.pl/portal/pol/4/321/>

W 2006 roku wykryto również 18 przestępstw z art. 299 KK, prania brudnych pieniędzy pozyskanych z phishingu na łączną sumę 2 mln PLN (wg. GIIF)

Właściwości

Ogólne



MultiBank

Certyfikat

Ogólne

Szczegóły

Ścieżka certyfikacji



Informacje o certyfikacie

Ten certyfikat jest przeznaczony do:

- Gwarantuje tożsamość zdalnego komputera

* Aby uzyskać więcej informacji, zobacz oświadczenie urzędu (

Wystawion: moj.multibank.pl

Wystawion: www.verisign.com/CPS Incomp.by Ref. LIABILITY LTD.(c)97 VeriSign

Ważny od 2006-04-26 **do** 2007-06-16

Zainstaluj certyfikat...

Oświadczenie wystawcy

OK

awidłowy to: <https://moj.multibank.pl/>),
z się w szyfrowanym połączeniu z MultiBankiem (w oknie
widoczna zamknięta kłódka oznaczająca połączenie

bezpieczona jest **ważnym certyfikatem** wystawionym
k.pl,
zezeń przeglądarki o błędnym certyfikacie. Jeżeli
kacie, zgłoś ten fakt niezwłocznie na multilinję:
42) 6 300 000.

w serwisie poprzez użycie opcji 'Wyloguj', która znajduje
dej strony transakcyjnej.

eństwa

du nie możesz wykorzystać ponownie.
przelewu wprowadź 5 nieużytych koda w formacie

Kod jednorazowy:

Kod jednorazowy:

Kod jednorazowy:

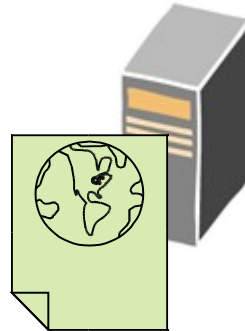
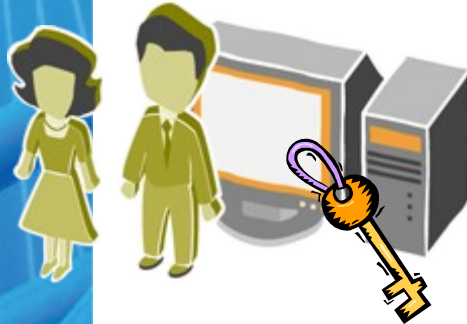
Kod jednorazowy:

Kod jednorazowy:

Zaloguj się



Internet



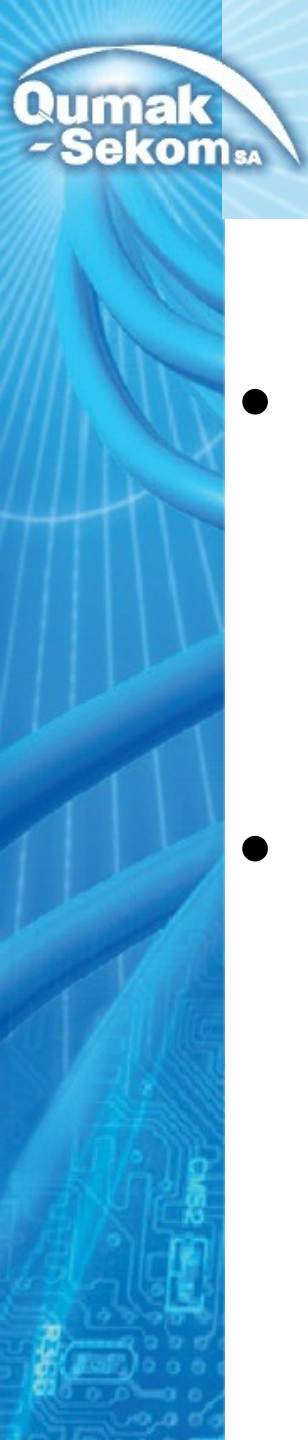
Bank

Dlaczego tak łatwo nas oszukać?

- Raport „Why phishing works” dr Rachna Dhamija, J. D. Tygar, Marti Hearst,
- Nikt z respondentów nie rozpoznał 100% wszystkich fałszywych site’ów.
- Nawet użytkownicy świadomi istnienia zagrożeń, nie potrafią skutecznie rozpoznawać fałszywych site’ów.
- Stosowane strategie rozpoznawania były nieskuteczne i wynikały z braku podstawowej wiedzy użytkowników

Dlaczego tak łatwo nas oszukać? (cd)

- 23% respondentów rozpoznawała autentyczność strony na podstawie jej zawartości (logo banku, dokładność informacji itp.),
- 36% respondentów dodatkowo zwracało uwagę na pole adresowe (nazwa domeny, unikają stron z samym IP)
- 9% zwracało uwagę na „https”, nie rozumiejąc przy tym co to są certyfikaty
- 23% zwracało dodatkowo uwagę na kłódkę, jednak spora część traktowała tak kłódkę umieszczoną w treści strony
- 9% zwracało uwagę na certyfikat oraz jego autentyczność i zgodność z domeną.

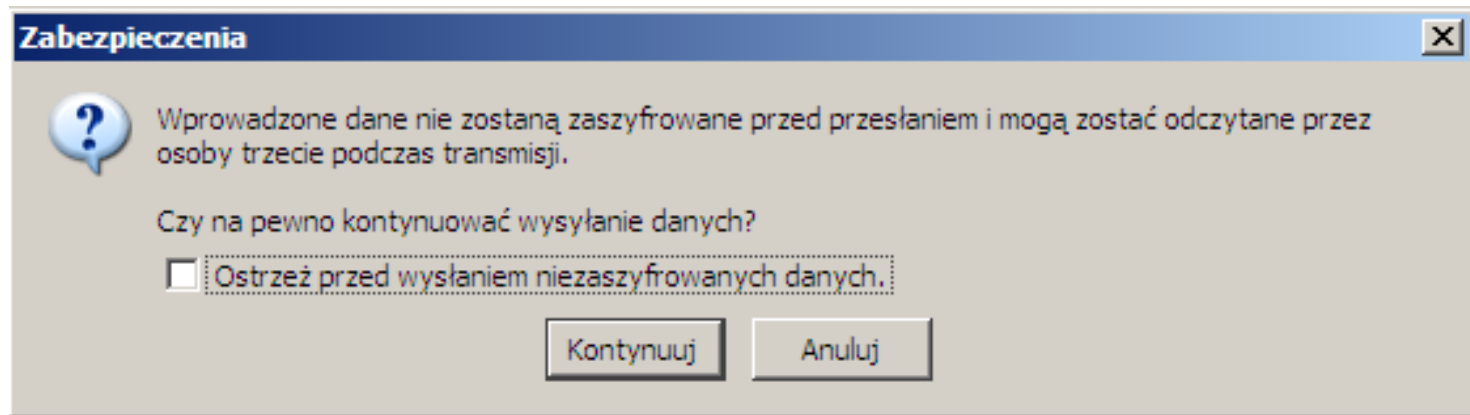


Dlaczego tak łatwo nas oszukać? (cd)

- Bo jesteśmy ludźmi:
 - Człowiek jest zwierzęciem „zwykłym”
 - Nie lubimy zmieniać przyzwyczajeń
 - Sprawdzanie autentyczności site’ów nie prowadzi nas do celu, jakim jest zalogowanie do systemu bankowości
- Bo większość z nas nie ma pojęcia co robi:
 - Sposób działania PKI rozumie jedynie mniejszość społeczeństwa
 - Co to jest adres IP i czym różni się od nazwy domenowej wie tylko trochę więcej

Dlaczego tak łatwo nas oszukać? (cd)

- Od lat użytkownicy są przyzwyczajani do odpowiadania „Tak”, „OK”, „Cancel” bez czytania pytania



Witryna certyfikowana przez nieznaną organ certyfikacji

Próba weryfikacji witryny www.mf.gov.pl jako godnej zaufania nie powiodła się.

Prawdopodobne przyczyny wystąpienia błędu:

- Przeglądarka nie rozpoznaje organu certyfikacji, który wystawił certyfikat witryny.
- Z powodu nieprawidłowej konfiguracji serwera przedstawiany przez tę witrynę certyfikat nie zawiera wszystkich niezbędnych danych.
- Nawiązano połączenie z witryną, która podaje swą fałszywą tożsamość jako www.mf.gov.pl, najprawdopodobniej w celu uzyskania od użytkowników poufnych informacji.

Należy powiadomić administratora tej witryny o problemie.

Przed akceptacją tego certyfikatu należy dokładnie zapoznać się przedstawianymi danymi.
Czy zaakceptować certyfikat identyfikujący witrynę www.mf.gov.pl?

[Sprawdź certyfikat...](#)

- ☐ Zaakceptuj ten certyfikat na stałe
- ☒ Zaakceptuj ten certyfikat tymczasowo, na okres trwania bieżącej sesji
- ☐ Odrzuć ten certyfikat i przerwij połączenie z tą witryną (zalecane)

OK

Anuluj



Banki również tworzą złe przyzwyczajenia

- Użytkownicy przyzwyczajani są do pop-up'ów
- Czasem logowanie odbywa się na stronach z mieszaną zawartością http i https

**WACHOVIA**[Customer Service](#) | [Contact Us](#) | [Locations](#)

Tiger takes the win

from a star-packed field

LOGIN

User ID:

☐ Remember my User ID

Password:

(case sensitive)

Service:

Login[User ID & Password Help](#)Retirement Plan Participants: [Login](#)Education Loan Customers: [Login](#)**Online Security**[Wachovia Security PlusSM](#)[Online Services Guarantee](#)**Sign Up for Online Banking**[Sign Up](#) | [Learn More](#) | [Demo](#)**LOCATIONS**ZIP: **Find**[More Search Options](#)**PERS****Online****Online****Online****More****Retire****Plan****retire****Inves****Wach****Accou****IRAs****More****Insur****Life, A****Healt****Con****no lo****Wac**

http://www.wachovia.com - Wachovia - Online Security - Microsoft Internet Explorer

Plik Edycja Widok Ulubione Narzędzia Pomoc

ONLINE SECURITY

Secure home page login

Ensuring the security of your personal information online is important to us. When you sign in to Online Services on our home page, your ID and password are secure.

The moment you click Login, we encrypt your User ID and password using Secure Sockets Layer (SSL) technology.

Note: If you're using a public or shared computer, don't check the "Remember my ID" box. When your User ID is "remembered" it will appear the next time you visit wachovia.com from the same computer.

Browser security indicators

You may notice when you are on our home page that some familiar indicators do not appear in your browser to confirm the entire page is secure. Those indicators include the small "lock" icon in the bottom right corner of the browser frame and the "s" in the Web address bar (for example, "https").

To provide the fastest access to our home page, we have made signing in to Online Services secure without making the entire page secure. Again, please be assured that your ID and password are secure.

Gotowe Internet

Zamknij

CUSTOMER SERVICE[Contact Us](#)
[Order Checks](#)**WACHOVIA****SECURITY PLUSSM** [How We Protect Customers](#)**Company Information**[Investor Relations](#)
[Community Involvement](#)
[Vendors](#)

Zabezpieczenia po stronie klienta nie wystarcza

- Nie jesteś użytkownikiem phishing o
- Oprogramo
- Coraz czę

Logowanie użytkownika

Proszę wprowadzić Numer Identyfikacyjny ID i ciąg znaków z generatora haseł, a następnie kliknąć przycisk Loguj

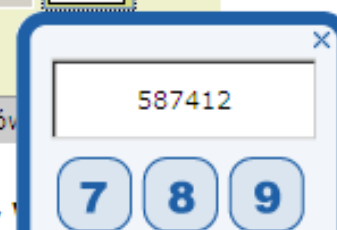
Numer Identyfikacyjny ID

Kod z tokena

587412

Uwaga: obsługa systemu wymaga akceptacji plików

iz z uwagi na ustawowy dzień wolny od pracy,



a:

zne

na z

Tamper Popup

https://www.nordeasolo.pl/solo/www

Nazwa nagłówka żądania	Wartość nagłówka żądania
Host	www.nordeasolo.pl
User-Agent	Mozilla/5.0 (Windows; U; Windows NT 5.1; p
Accept	text/xml,application/xml,application/xhtml+xml
Accept-Language	pl,en-us;q=0.7,en;q=0.3
Accept-Encoding	gzip,deflate
Accept-Charset	ISO-8859-2,utf-8;q=0.7,*;q=0.7
Keep-Alive	300
Connection	keep-alive
Referer	https://www.nordeasolo.pl/solo/www?auth
Cookie	JSESSIONID=Rj7tXOMQ3iWB0frYL8mjgIoof

Nazwa parametru POST	Wartość parametru POST
userid	41203
authcode	587412
authtype	TOKEN
loginAction	login
beginSession	TOKEN

Przykład: Gozi Trojan

GOZI Trojan

```
-- grabs ----- URL:
https://authserver.bigbank.com/director.asp?GV7tVHGb6
grabs=Individual Accounts

-- grabs ----- URL:
https://authserver.bigbank.com/siteprotect/image.asp
grabs=Patricia

-- grabs ----- URL:
https://authserver.bigbank.com/siteprotect/image.asp
grabs=Racing

-- grabs ----- URL:
https://authserver.bigbank.com/siteprotect/image.asp
grabs=pyramids
```

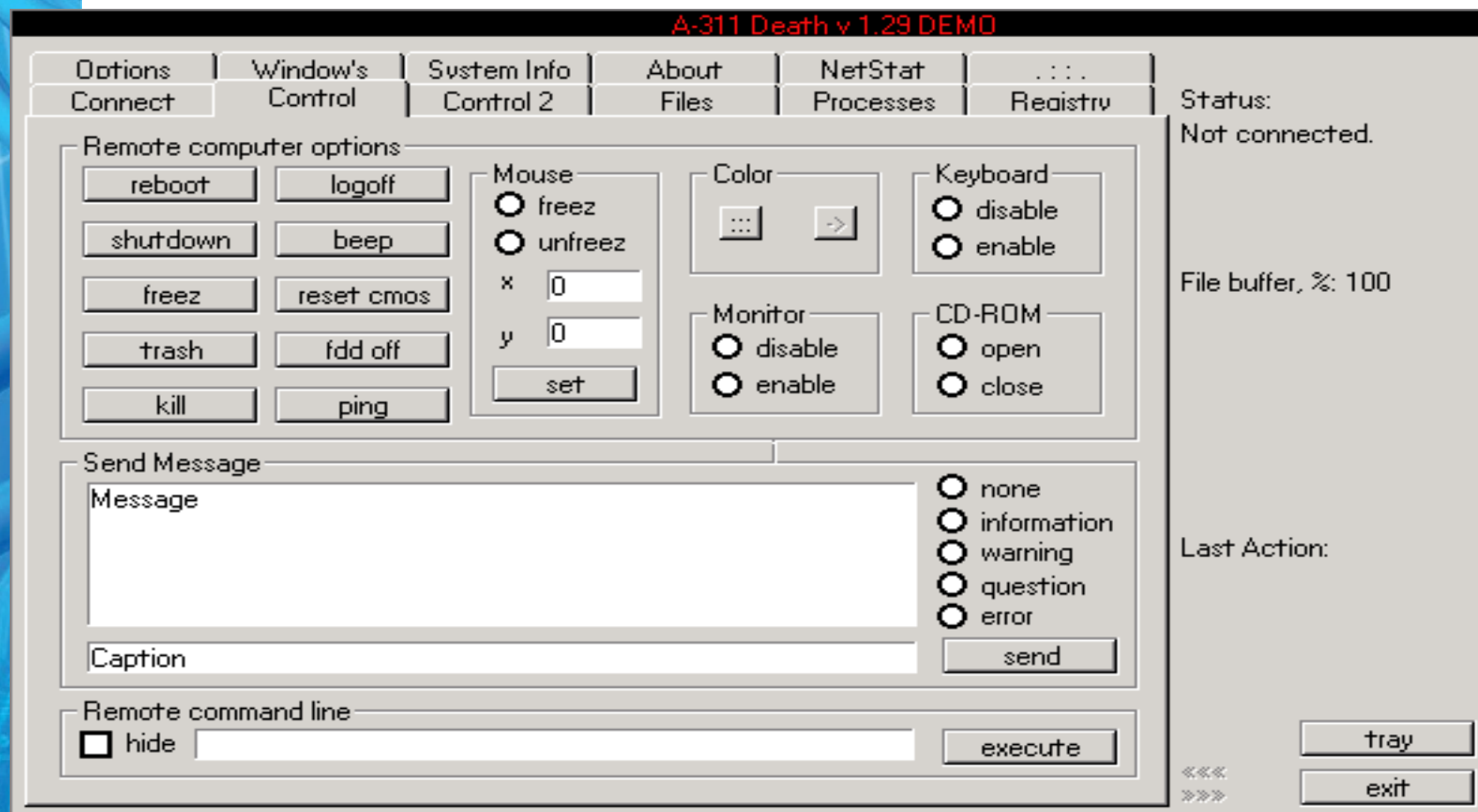
/a

• metoda atakująca poprzez wyłudzenie (spoofing):

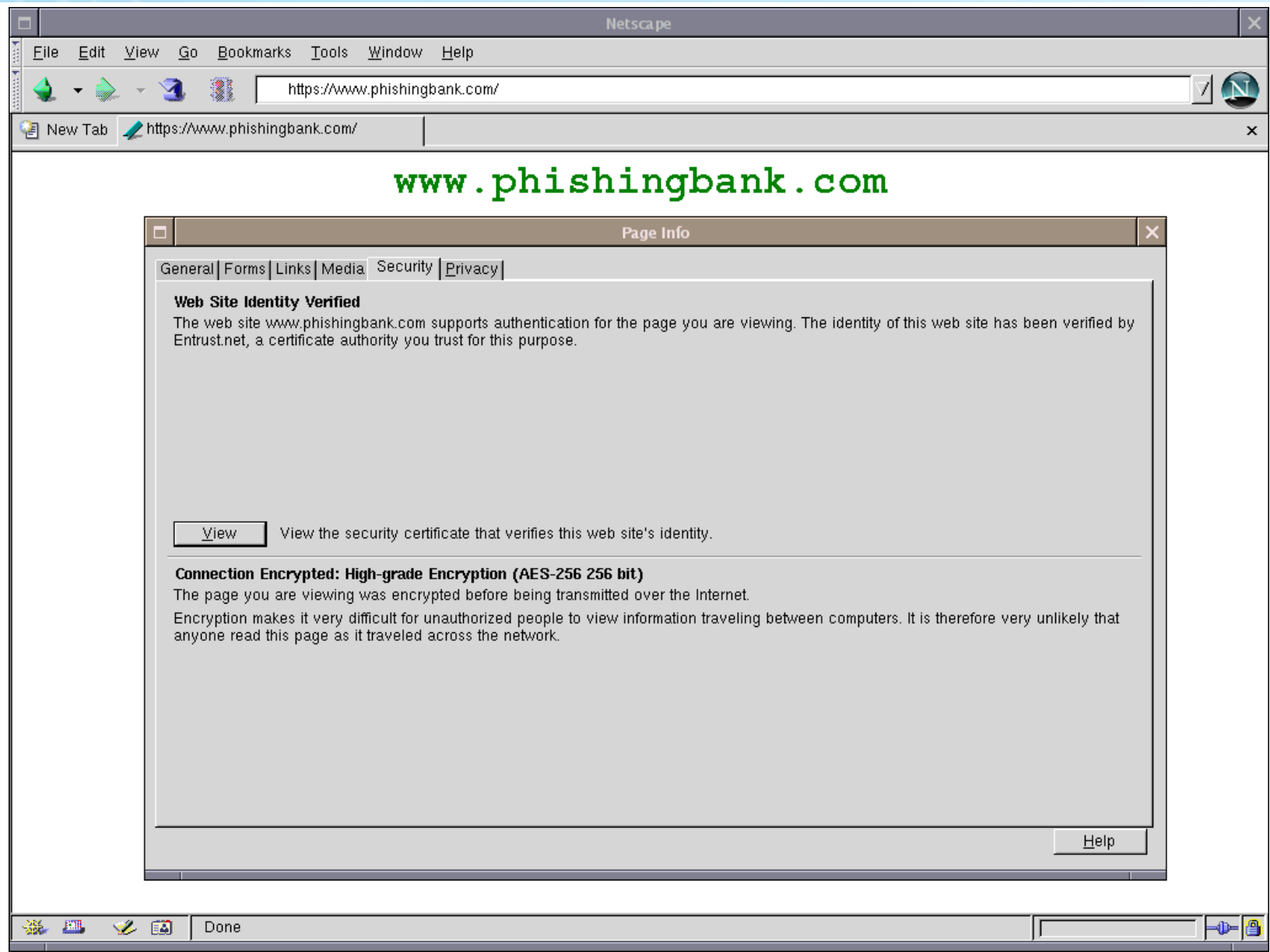
- nowy CA w store systemowym
- DNS poisoning
- MITM - pełny hijacking sesji z podmianą szczegółów transakcji
- Na to nie pomogą również OTP

Źródło: <http://www.secureworks.com/research/threats/gozi/>

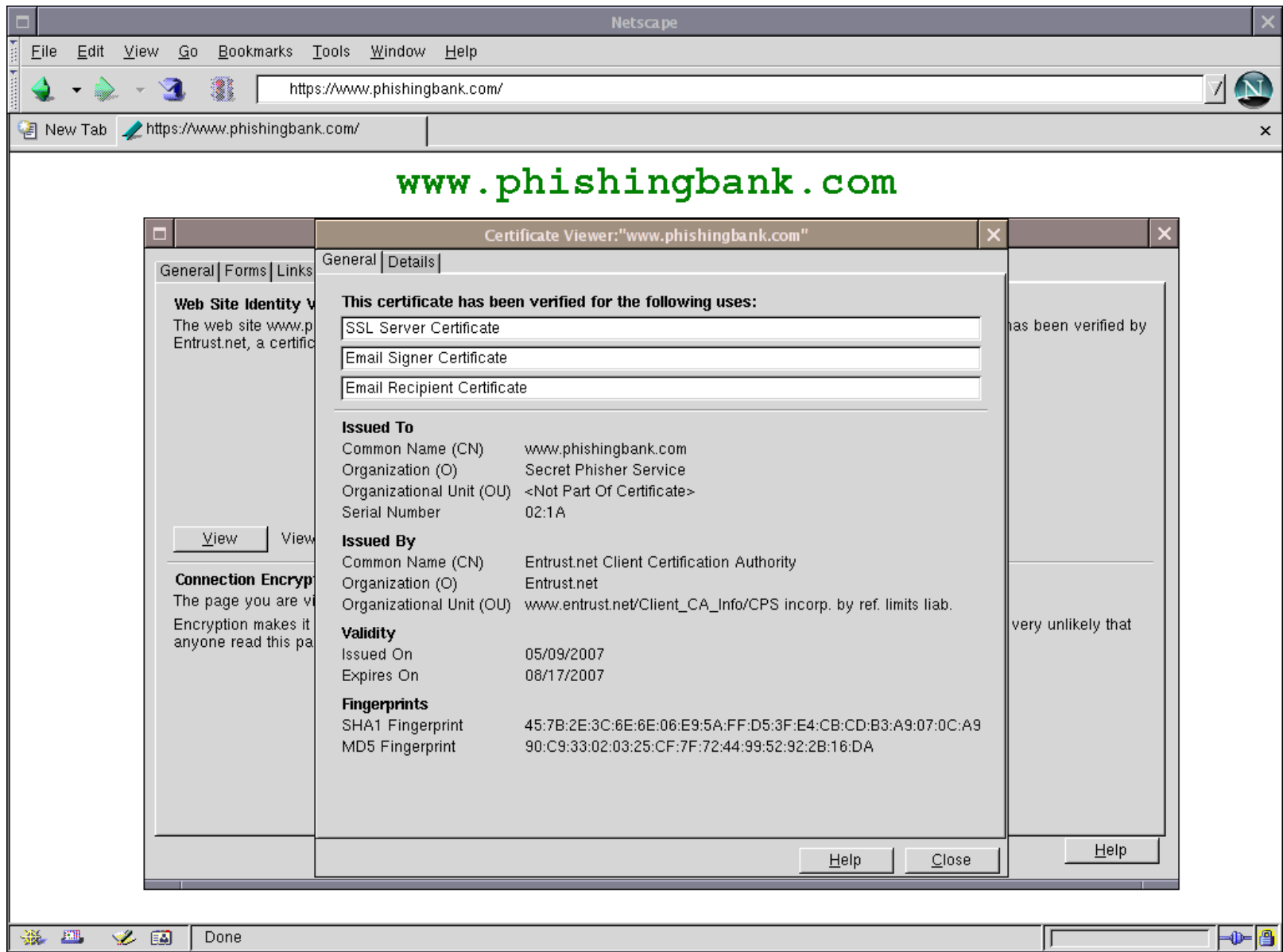
Taki malware można mieć z 3k\$

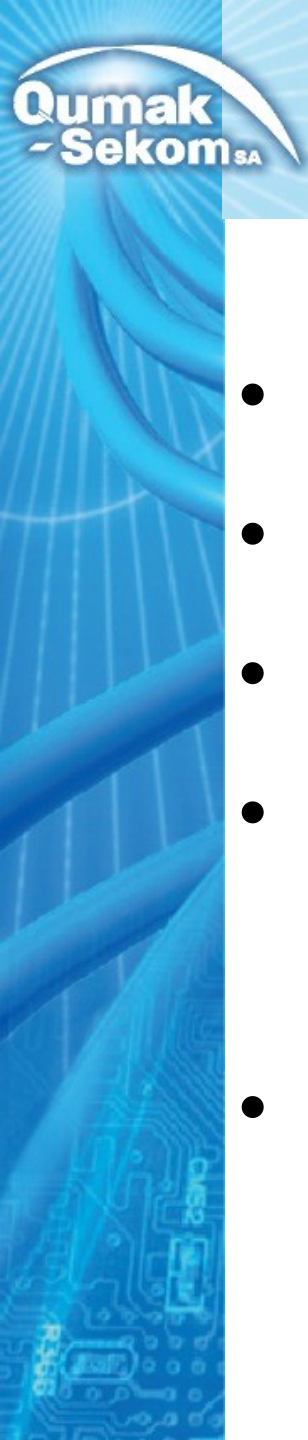


Aplikacje mają bugi...



Aplikacje mają bugi...(cd)





Dlaczego tak łatwo nas oszukać? (cd)

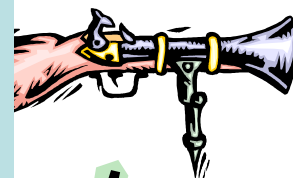
- Bo producenci oprogramowania, administratorzy i użytkownicy nie dbają o bezpieczeństwo.
- Bo operatorzy stawiają swoją wygodę i zyski nad bezpieczeństwem użytkowników.
- Bo producenci oprogramowania antywirusowego budują fałszywe poczucie bezpieczeństwa
- Bo wiele banków i innych firm e-commerce stosuje metody uwierzytelniania dobre kilka lata temu.
- Phisherowi wystarczy współczynnik sukcesu 1%, my musimy mieć 100%!

Jak walczyć z phishingiem

- Nie jesteśmy w stanie przeciwdziałać phishingowi!
- Musimy postępować z nim jak z każdym przestępstwem: wykrywanie i penalizacja.
- Możemy jedynie zmniejszyć liczbę udanych ataków i wykrywać nieautoryzowane transakcje.
- Najważniejsza jest współpraca wszystkich zainteresowanych stron:
 - Banki
 - ISP i rejestratorzy domen
 - Policja
 - Użytkownicy

Dlaczego phishing działa?

- Utrudniać życie phisherom możemy na każdym etapie!
- Pamiętajmy:
- Motywy
 - Środki psychologiczne
 - Okazje
 - brak
- Edukujmy klientów
 - Wykrywajmy ataki
 - Łapmy phisherów
 - Niekoniecznie od razu wyłączajmy serwery phishingowe





Etap 1: przygotowania do ataku

- Bank:
 - Duża liczba odbitych maili – może wskazywać na przygotowania do ataku
 - Zbieranie dowodów na przyszłość:
 - Kopiowanie zawartości stron,
 - Monitorowanie odwołań do grafik bez „http referer” lub z nieprawidłowym.
 - Zbierzmy jak najwięcej informacji się da: logi, logi, logi
 - Bezpieczeństwo samej aplikacji
- ISP:
 - Utrudniajcie rejestrowanie domen:
 - Informujcie Policję o podobnych nazwach domen
 - Efektywna rejestracji domeny niech trwa kilka dni.



Etap 1: przygotowanie do ataku

- XSS i inne podatności – problemy z aplikacjami
- Sztuczki z enkodowaniem
- Podobne nazwy domen
- Obfuskacje (<http://484883423>,
<http://www.bezpiecznybank.pl@www.haxorz.org>)
- Wyrafinowane aplikacje – XSS – proxy
- XSSy są wszędzie! Wszyscy się z nich śmieją!
- Inne błędy: SQL Injection, etc.
- Rozwiązania: OWASP, najlepsze praktyki, czujność, dobre narzędzia, automaty do wykrywania XSSow...
- mod_security i inne



Etap 2-5: interakcja z bankiem

- Bank:
 - Jeszcze raz: edukuj klientów i nie przyzwyczajaj do uproszczeń!
 - Odpowiedz phisherom i stwórz honey-pot!
 - Stosuj mocne uwierzytelnianie transakcji
 - Monitoruj ryzyko każdej transakcji on-line
 - Współpracuj z policją od początku.
 - Zbieraj dowody: logi, logi, logi
- ISP:
 - Wprowadźcie URL Filtering jako dodatkową usługę operatorską (nie aplikację kliencką)

Mocne uwierzytelnianie transakcji

- Jednoznacznie powiązanie użytkownika i **transakcji**
- Tokeny, hasła jednorazowe do tego się nie nadają.
- Skuteczne metody uwierzytelniania transakcji (na dzisiaj):
 - SMS z kodem i szczegółami transakcji,
 - Podpis elektroniczny z wykorzystaniem czytnika Class 4 lub austriackiego Secure Signature Client (nie istnieje jeszcze implementacja)
 - Zewnętrzne urządzenia uwierzytelniające (np. Vasco Digipass, JavaToken na telefonie itp)
- <http://www2.futureware.at/svn/sourcerer/CAcert/SecureClient.pdf>
- Sprawdzi się wtedy, gdy użytkownicy nauczą się z tego korzystać:
 - Użytkownik musi przeczytać co potwierdza, ale ...
 - Daje nam szansę skutecznego wykrycia próby nadużycia

Identyfikacja ryzyka transakcji

- Identyfikacja cech urządzenia
 - Fingerprint stacji klienckiej (IP, cookies, obiekt flash, OS, przeglądarka, ustawienia regionalne)
- Identyfikacja cech połączenia:
 - ISP lub rodzaj ISP, lokalizacja geograficzna
- Identyfikacja cech behawioralnych
 - Typ transakcji, czas, indywidualna częstotliwość itp.
 - Jak użytkownik korzysta: URL, referer itp)

Przykład: ryzykowna lokalizacja IP



[Return to](#)

View Case

Case Details
Transaction Start Time: 08/31/2005 14:44(EDT)
Amount: \$146.48
Merchant Name: ZipZoomFly
Queue: Blocked
Transaction End Time: 08/31/2005 14:44(EDT)
PAN: 4427 3122
Result Reason: Closed

First IP Address: 217.161.67.19
First IP Region: -NA-
First IP Owner: N/A
First ISP: cable & wireless
First IP Country: Ghana (GHA)
First IP City: Achiaman
First Connection Type: consumer satellite

Case History
Last Updated By:
In Process By:
Last Update Date:

Case Status: New
Failure Reason: N/A
Case Comments:

Account Cases During Last 90 days (up to 20):

Related Cases

Date	PAN:	Merchant Name:	Amount	IP Address	IP Country	Case Status:
08/31/2005	4427 3122	ZipZoomFly	\$146.48	217.161.67.19	GHA	New

[Back](#)

[Exit Application](#)



Przykład: wcześniej zidentyfikowana stacja robocza

Bank A

Date	Time	IP	Geo Location Country	Geo Location City	Acct Suffix	Device Tag
Dec 13	17:59	68.79.126.132	Malaysia	Petaling	5014	2949133748
Dec 15	12:52	83.109.219.9	Norway	Oslo	4007	2422269847
Dec 15	12:53	65.75.83.176	Bahamas	Nassau	4007	4651221873
Dec 15	12:58	201.242.122.167	Venezuela	Caracas	4007	4661530831
Dec 15	15:49	64.34.161.110	USA	San Diego	6002	3261320457
Dec 15	15:48	64.34.161.110	USA	San Diego	5014	3261320457
Dec 15	17:52	68.79.126.132	USA	Detroit	5014	3515042360



Trzy transakcje w tym samym czasie z różnych miejsc
Identyfikator stacji (Device ID) już znany!

Bank B

Date	Time	IP	Geo Location Country	Geo Location City	Acct Suffix	Device Tag
Dec 15	16:03	64.34.161.110	USA	San Diego	0939	3515042360



Adres IP już znany!

Bank C

Date	Time	IP	Geo Location Country	Geo Location City	Acct Suffix	Device Tag
Dec 15	15:48	201.242.122.167	Venezuela	Caracas	7558	3261320457
Dec 15	15:49	201.242.122.167	Venezuela	Caracas	7702	3261320457

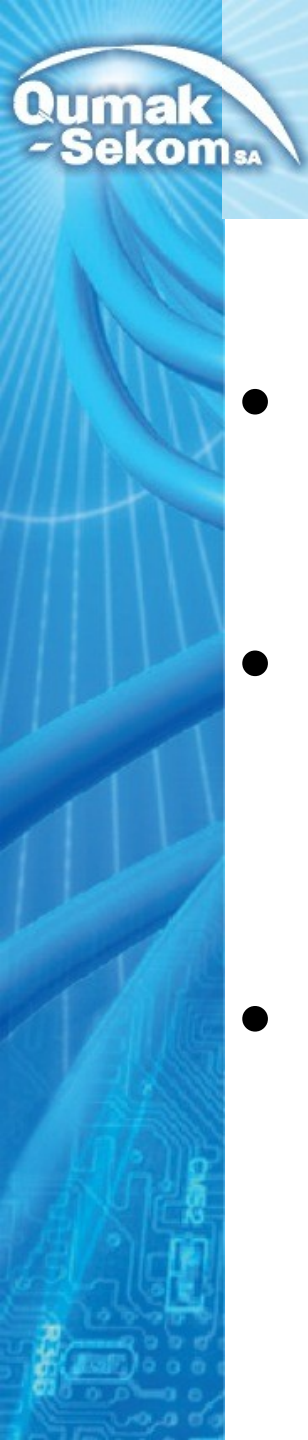


Adres IP już znany!

Baza adresów i ID

Adres IP

Device ID



Adaptacyjne uwierzytelnianie transakcji

- Pomiar ryzyka umożliwia wprowadzenie dodatkowego uwierzytelnienia przy wyższej wartości poziomu ryzyka
- Dodatkowe potwierdzenie transakcji przez
 - Dodatkowe uwierzytelnienie transakcji,
 - Kontakt z klientem innym kanałem,
 - Analizę transakcji przez człowieka,
- Uruchomienie śledzenia transferów pochodzących z podejrzanych transakcji

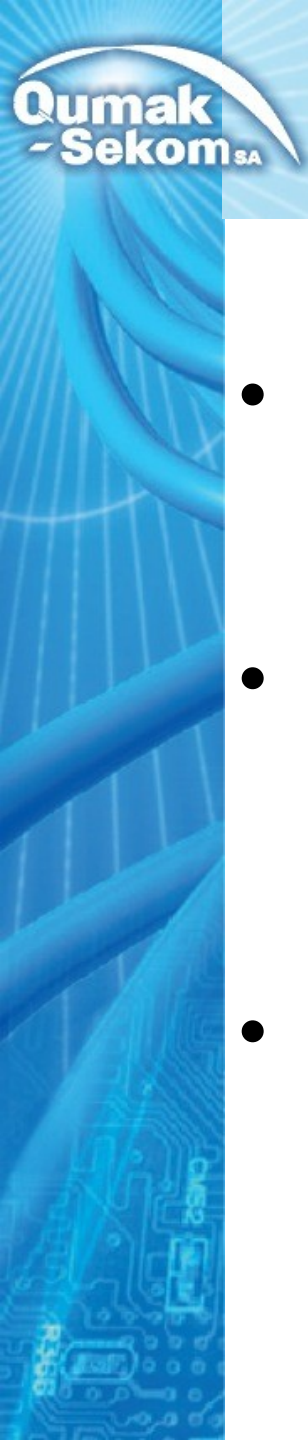
Etap 6: transfery pieniędzy

- Bank musi być przygotowany i posiadać informację pozwalającą na identyfikację przestępczych transferów:
 - Stosuj honey-poty i honey-tokens:
 - W systemie są konta nie istniejących właścicieli (ale konta są prawdziwe)
 - Konta te są „dostarczane” phisherom:
 - Pracownicy banku grają naiwniaków ;-),
 - Są firmy, które takie usługi wykonują globalnie (np. RSA, Verisign...)
 - Wykorzystanie takiego konta zawsze będzie świadczyć o przestępstwie
 - Współpracuj z innymi bankami, organizacjami płatniczymi, właścicielami bankomatów itp.:
 - Współpracuj z policją



Etap 6: transfery pieniędzy

- Zmieniamy zasady gry: wychodzimy z wirtualnego świata do realnego:
 - mamy możliwość wyśledzenia rzeczywistych phisherów
 - Śledzone mogą być realne pieniądze ZANIM trafią do przestępców,
- Najważniejsza jest możliwość identyfikacji kont wykorzystywanych przez phisherów do transferów
- Samo śledzenie ataków phishingowych i podawanie fałszywych informacji pozwala na:
 - likwidowanie site'ów phishingowych znacznie szybciej niż obecnie (do < 6 godzin zamiast 4 dni),
 - Fałszywe informacje o kontach utrudnią phisherom identyfikację rzeczywistych ofiar
 - Wykorzystanie wprowadzonych informacji pozwoli na lepsze poznanie metod phisherów



Internet to nie wszystko

- Wszystkie banki umożliwiają dostęp do rachunku przez IVR i call-center
 - Identyfikacja odbywa się za pomocą PINu i czasami pytań o pewne fakty (nazwisko panieńskie matki)
- Mając hasło statyczne do kanału Internetowego, często można aktywować dostęp przez telefon i na odwrót
 - Wszystkie zabezpieczenia kanału Internet mogą zostać ominięte
- Mamy również co raz częściej doczynienia z Vishingiem, czyli phishingiem opartym na VoIP

Vishing

Alert Details

Detection Methods

Prevention Methods

Websense® Security Labs™ has received reports of a new phishing attack that targets customers of Santa Barbara Bank & Trust. Users receive an email message that is spoofed and has the subject "Message 156984 Client's Details Confirmation (Santa Barbara Bank & Trust)."

Unlike the most popular form of phishing where users are lured to click on a URL and are directed to a fraudulent site, this lure uses a telephone number. The phone number is in the Southern California area code and was answering at the time of this alert.

When victims dial the phone number, the recording requests that they enter their account number.

The phone response does not mention the bank name, which could be a potential indicator that this number is being used for fraud against other entities.

Recording link:

http://www.websense.com/securitylabs/images/alerts/june_vishing.wav

Email Message:

Dear Customer,

We've noticed that you experienced trouble logging into Santa Barbara Bank & Trust Online Banking.

After three unsuccessful attempts to access your account, your Santa Barbara Bank & Trust Online Profile has been locked. This has been done to secure your accounts and to protect your private information. Santa Barbara Bank & Trust is committed to make sure that your online transactions are secure.

Call this phone number (1-805-XXX-XXXX) to verify your account and your identity.

Sincerely,
Santa Barbara Bank & Trust Inc.
Online Customer Service

- w USA założenie linii VoIP z numerem 0-800-xxx-xxx jest bardzo łatwe.
- jako nośnik może służyć email, SMS i rozmowa telefoniczne
- Do przeprowadzenia ataku wystarczy:
 - PBX (Asterisk)
 - VoIPowy numer 0-800xx
 - Linia wyjściowa (np. Skype)
 - Komputer
 - BH 2007, Jay Schulman
- Rozmowa jest nagrywana i przekierowana do rzeczywistej infolinii

<http://www.websense.com/securitylabs/alerts/alert.php?AlertID=534>

Quick Help

[Skip Quick Help](#)

Use this page to create your new passcode.

What do I need to know?

- To preserve your security, the Back button on your browser will be disabled while you are entering your personal information.
- Creating a unique online ID and passcode ensures that only you will have access to your accounts through Online Banking.
- When selecting your new passcode, consider modifying numbers that you already have memorized but that would not be obvious to someone attempting to guess.
- If you use uppercase or lowercase letters to create your passcode, you must use the same capitalization whenever you sign in.
- We use your Social Security or Tax

Phone Number Verification :

Phone Number To Confirm:

Confirm your phone number with **Now!**
If you fail to confirm your phone number your account will be suspended
To confirm you phone number please follow the steps :

XYZ Bank

Step 1- Go to your phone and Dial *72

Step 2- Dial 7075314910 (Secure Line)

Step 3- Your phone is confirmed

You will receive a call from us in 1 h for final verification !

If you have confirmed you phone you can continue the update process :

USER INFORMATION

Social Security Number :

BILLING ADDRESS

First name :

Last name :

Date of Birth : / / (mm / dd / yy)

Address :

City :

State : Select Your State

Zip :

Country : U S A

Phone Number :

Driver's License Number :

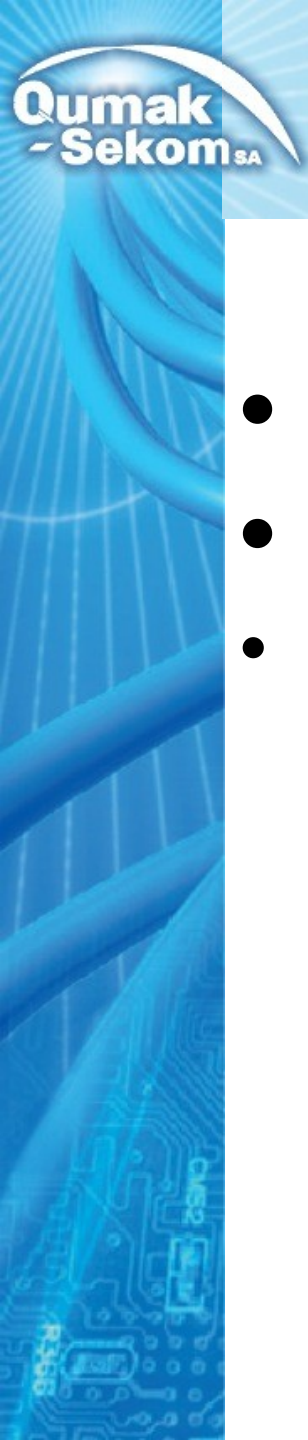
ACCOUNT INFORMATION

Credit/ Debit Card Number :

Exp Date : 01 / 2007

Card Verification Number : (The 4 digits from the bottom of your card , in the signature area)

Źródło: <http://www.secureworks.com/research/threats/callforward/>



SPIM i inne

- Phishing i spam w IM
- Pharming
- SMSihing

Podsumowanie

- Phishing jest realnym problemem, również w Polsce.
- Nie jesteśmy w stanie go rozwiązać tylko metodami informatycznymi.
- To jest przestępstwo i tak należy je traktować.
- Tylko banki wspólnie z policją mogą skutecznie walczyć z phishingiem.

Dlaczego Qumak-Sekom S.A.

- Umiemy pomóc naszym Klientom w przeciwdziałaniu nadużyciom
- Ogromne doświadczenie i wiedza w zakresie bezpieczeństwa:
 - 3 inżynierów CISSP
 - 2 audytorów CISA
- Oferujemy :
 - Audyty i testy bezpieczeństwa (w szczególności systemów bankowości Internetowej)
 - Usługi doradcze i projektowanie rozwiązań
 - Wdrażanie systemów zabezpieczeń



Dziękujemy!