Bezpieczeństwo
Sieci Komputerowych

Część 6.
Sieciowe zagrożenia bezpieczeństwa danych

Praktyczny Pedagog

Bezpieczeństwo Systemów Komputerowych

PROGRAM ZAJĘĆ

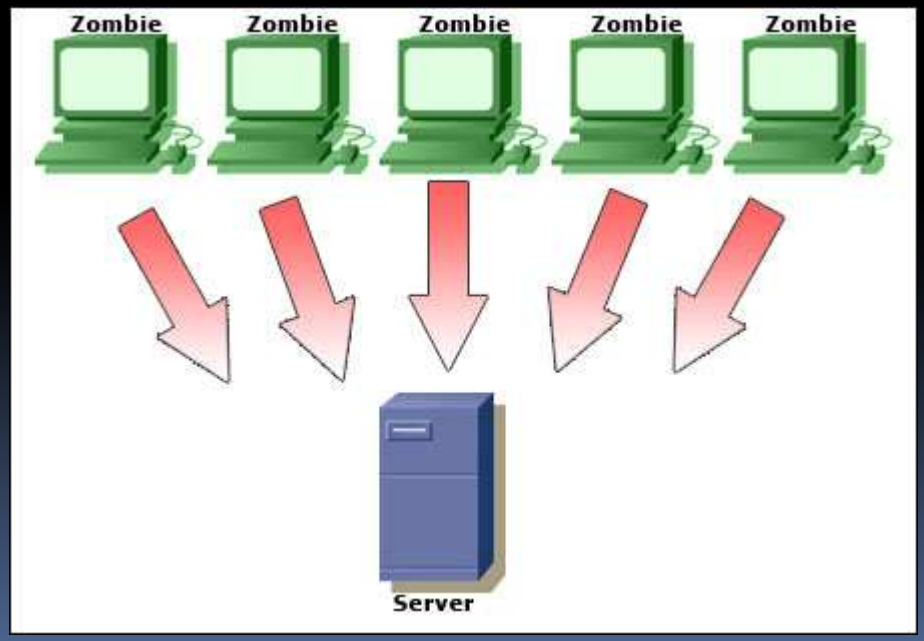
Rodzaje zagrożeń.
Hakerzy i włamania
Socjotechnika.
Oszustwa sieciowe.
Złośliwe oprogramowanie.
Zagrożenia dla sieci WiFi.

Rodzaje zagrożeń

Zagrożenia to zjawiska wywołane działaniem człowieka (umyślnym bądź nieumyślnym) lub sił wyższych (przyrody, środków trwałych itp.), które powodują, że poczucie bezpieczeństwa maleje bądź zupełnie zanika. Mogą one obejmować osoby (np. krakerzy czy szpiedzy), rzeczy (np. wadliwe urządzenie), czy zdarzenia (np. powódź).

Rodzaje zagrożeń

Zagrożenia są zawsze obecne, nie można ich wyeliminować a jedynie przewidywać i chronić się przed nimi. Dlatego należy stale przeprowadzać ich analizę (czyli szacować, np. ich wielkość, typ), która pozwoli ocenić ich wpływ na zasoby (systemy) oraz oszacować potencjalne straty w wyniku ich wystąpienia (pojawienia się incydentu), czyli naruszenia lub zniszczenia zasobów (np. nieuprawnione ujawnienie, modyfikację, zniszczenie lub uniemożliwienie przetwarzania informacji).



Rodzaje zagrożeń

Ocena ryzyka ich wystąpienia pozwoli natomiast zastosować odpowiednie zabezpieczenia chroniące zasoby przed tymi zagrożeniami, które zminimalizują prawdopodobieństwo ich wystąpienia.

Zagrożenia zależne od człowieka

Rozmyślne

Przede wszystkim rozmyślna działalność sieciowa (zazwyczaj przestępcza), która związana jest z atakami i włamaniami hakerskimi do zasobów komputerowych przy użyciu różnych technik i metod (np. przy użyciu złośliwych programów, rozsyłania spamu), często ataki są zautomatyzowane. Działania te mogą powodować utratę poufności (np. ujawnienie informacji), integralności (np. modyfikacja informacji) czy dostępności zasobów (np. brak dostępu do informacji czy systemu dla uprawnionych użytkowników).

Także mogą to być działania fizyczne, czyli związane z dostępem fizycznym (bezpośrednia obserwacja - podsłuch czy powodujące kradzież zasobów).

Takie działania są przeprowadzane często przez samych pracowników – przed takimi najtrudniej ochronić system.

Zagrożenia zależne od człowieka

Przypadkowe

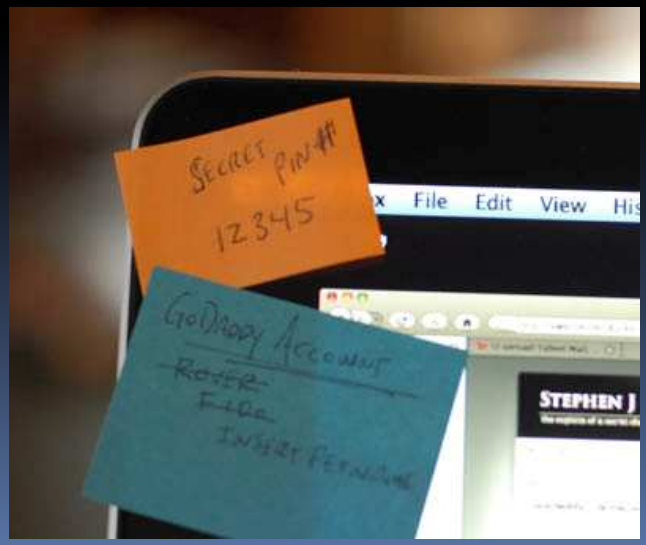
Pomyłki, pominięcia czy wypadki fizyczne. Mogą one wynikać z:

problemów technicznych (z wad sprzętu i oprogramowania) – np. wady oprogramowania (podatność), awarie sprzętu, przerwy i zakłócenia w sieci energetycznej itp.), problemów organizacyjnych (ze złej organizacji pracy) – brak odpowiednich procedur, brak organizacji infrastruktury informatycznej, brak dostatecznej wiedzy, brak właściwych zasobów, niewystarczające monitorowanie zabezpieczeń (np. nieprzeglądane listy kontrolne, dzienniki zdarzeń), brak lub niewłaściwe utrzymanie zasobów itp.)...

Zagrożenia zależne od człowieka

Przypadkowe

...lub być bezpośrednim **błędem ludzkim** (nieprzestrzeganie podstawowych zasad bezpieczeństwa, nie przeszkolony personel bez świadomości zagrożeń bezpieczeństwa (np. podatny na metody socjotechniczne, zapisywanie haseł na karteczkach przyczepionych do komputera), zniszczenie urządzenia na skutek niedbalstwa (np. zalanie urządzenia kawą, pomyłkowe skasowanie danych), złe obchodzenie się z informacjami (np. przesłanie pliku tajnego pocztą elektroniczną czy skierowanie do wydruku), złe administrowanie systemem (np. nie wyłączone usługi, które nie są używane, ustawione domyślnie, nie zamknięte konta itp.)



Zagrożenia niezależne od człowieka - środowiskowe

Takie jak: trzęsienie ziemi, pożar, powódź, piorun (powodujące rozległe uszkodzenia fizyczne – zalanie wodą, pożary itp.).

Ataki sieciowe

W wirtualnym świecie (cyberprzestrzeni), podobnie jak w realnym, też grasują włamywacze, złodzieje, wyzyskiwacze czy szpiedzy, używający tylko trochę innych narzędzi czy metod do czynienia szkód. Dlatego stanowią oni zagrożenie dla zasobów komputerowych i innych użytkowników internetu.

Włamywacze ci (krakerzy, często myleni z hakerami), czyli złośliwi intruzi (cyberprzestępcy), próbują uzyskać dostęp do systemu komputerowego bez zgody i wiedzy jego właściciela w celu zniszczenia, skopiowania poufnych danych, przejęcia i często wykorzystania go jako źródła kolejnego ataku wymierzonego w innego użytkownika. Przykładowa niepożądana aktywność z przejętej maszyny to rozsyłanie spamu. Aby przejąć kontrolę nad systemem włamywacze wykorzystują luki w systemie posługując się przy tym różnymi metodami i technikami, np. używają złośliwego programu (exploita, trojana) czy metod socjotechnicznych.

Ataki sieciowe

haker (*hacker*) - to osoba posiadająca dogłębną wiedzę na temat systemów operacyjnych, aplikacji sieciowych oraz działania sieci komputerowych. Dla hackerów największym wyzwaniem jest poszukiwanie nowych możliwości przełamywania zabezpieczeń systemów informatycznych, zaś celem jest odkrywanie i wykorzystywanie luk w bezpieczeństwie dla satysfakcji oraz samej wiedzy. Hackerzy wbrew obiegowym opiniom nie czynią ze swych odkryć złego użytku. W potocznym języku słowo hacker jest mylnie kojarzone z osobą, którą określamy mianem krakera.

Ataki sieciowe

kraker (*cracker*) to osoba, która celowo chce dokonać jak największych zniszczeń poprzez celowe rozsyłanie wirusów, włamywanie się i kasowanie danych. Można również spotkać określenie *script-kiddies* - przypisywane tym, którzy korzystają z gotowych zestawów narzędzi służących do przełamywania zabezpieczeń, a nie posiadających zbyt dużej wiedzy z dziedziny zabezpieczeń sieci komputerowych.

Ataki sieciowe

Atak sieciowy (hakerski, komputerowy, cyberatak) to jakiekolwiek rozmyślne działanie przeprowadzane bez autoryzacji, które ma na celu zakłócenie funkcjonalności systemu teleinformatycznego (wraz z przetwarzaną w nim informacją), ograniczenie dostępu do niego, kradzież lub zniszczenie danych w nim znajdujących się itp. Obecnie ataki hakerskie mają najczęściej charakter hybrydowy, tzn. atak przeprowadzany jest z wykorzystaniem różnych technik i metod.

Ataki sieciowe

Ogólnie proces ataku na system teleinformatyczny można podzielić na klika etapów:

- **etap wstępny** (przygotowanie ataku/zbieranie informacji o systemie - rozpoznanie systemu, czyli tzw. rekonesans),
- **etap główny** (wykorzystanie podatności/wejście do sytemu/uzyskanie niezbędnych uprawnień w systemie oraz wykorzystanie go),
- **etap końcowy** (opuszczenie systemu/zacieranie śladów).

Rodzaje ataków

Ataki komputerowe można dzielić na różne kategorie. Atak może mieć charakter:

- **fizyczny** (polegający na fizycznej obecności intruza i np. kradzieży zasobów komputerowych), **techniczny** (wykorzystujący środki i techniki informatyczne, np. złośliwe oprogramowanie),

- **społeczny** (polegający na wyciąganiu informacji bezpośrednio od ludzi, czyli wykorzystujący socjotechniki).

Rodzaje ataków

Ze względu na miejsce skąd jest przeprowadzany atak może być on:

- lokalny/**bezpośredni** (intruz ma fizyczny dostęp do atakowanego komputera)
- z sieci/**zdalny** (zarówno z sieci lokalnej lub zewnętrznej, czyli z Internetu).

Rodzaje ataków

Ataki przeprowadzane z systemu, który znajduje się w atakowanej sieci nazywane są **wewnętrznymi** (zwykle są one przeprowadzane przez pracowników firm), zaś przeprowadzane z systemu znajdującego się poza atakowaną siecią nazywane są **zewnętrznymi**.

Inny podział ataków to np. ze względu na zamiar ataku: zamierzony lub niezamierzony, czy ze względu na skutek ataku: aktywny (w wyniku ataku zostaje naruszona integralność czy poufność zasobu komputerowego) lub pasywny (w wyniku ataku następuje jedynie kradzież zasobu, np. poufnych danych).

Rodzaje ataków

Zazwyczaj jednak ataki występujące w sieci mają postać złożoną (hybrydową), czyli są przeprowadzane jako tzw. ataki kombinowane. Oznacza to, że intruz (cyberprzestępca), aby osiągnąć swój cel musi skorzystać z połączenia różnych metod i technik hakerskich, np. socjotechnicznych, złośliwych programów czy ataków DoS. Przy tym mogą mieć one charakter mniej lub bardziej zautomatyzowany (lub jego poszczególne etapy).

Rodzaje ataków

Ogólnie można powiedzieć, że czym bardziej atak jest zautomatyzowany, tym na większą skalę występuje w sieci (np. zautomatyzowane ataki przy użyciu złośliwych programów jakimi są robaki czy trojany). Z tego powodu w cyberprzestrzeni (w sieci) bez względu na podjęte lub niepodjęte działania jesteśmy stale narażeni na ataki złośliwych automatów, które raz uruchomione działają niezależnie od woli właścicieli komputerów (które wcześniej zostały przejęte).

Przykłady ataków często występujących w sieci to: atak złośliwego kodu (np. robaki automatycznie rozprzestrzeniające się), atak spamowy (zalewanie niechcianymi wiadomościami zasoby komputerowe), phishingowy (rozsyłanie fałszywych wiadomości nakłaniających do podania poufnych danych).

Rodzaje ataków

Często, aby przeprowadzić skuteczny atak na system komputerowy cyberprzestępcy wykorzystują **metody socjotechniczne**. Metody te są często wykorzystywane przez cyberprzestępców, gdyż człowiek jest najsłabszym ogniwem systemu ochronnego zasobów komputerowych i okazują się skuteczne nawet wtedy, gdy obiekt atakowany jest silnie zabezpieczony. Hakerzy posługując się tymi metodami oddziaływują na emocje ofiary i wykorzystują jej naiwność oraz niewiedzę, manipulują nią tak, by wyjawniła im informacje, które chcą pozyskać (zwykle ułatwiające atak). Jedną z najbardziej typowych metod działań socjotechnicznych jest podszywanie się (np. w rozmowie telefonicznej pod kogoś ze współpracowników czy przedstawiciela jakiejś firmy).

Skutki ataków

Ataki i włamania hakerskie mogą stanowić poważne niebezpieczeństwo zarówno dla Twoich zasobów komputerowych jak i dla samego Ciebie. Mogą one być mniej lub bardziej niebezpieczne w zależności od skutków jakie wywołują. Począwszy od zakłócenia funkcjonowania systemu zaatakowanego (np. spowolnienie jego pracy na skutek "zalania" spamem), poprzez spowodowanie braku dostępu do zaatakowanego systemu i informacji w nim znajdujących się (np. na skutek ataku DoS), a kończąc na modyfikacji czy wykradnięciu poufnych danych znajdujących się w zaatakowanym systemie (np. przy pomocy trojana), wykorzystaniu go do dalszych nieuprawnionych działań (np. rozsyłania spamu) czy nawet dużych strat finansowych w firmie (np. spowodowanych brakiem działania systemu w wyniku ataku DoS).

Skutki ataków

Obecnie celem ataków hakerów są nie tylko potężne serwery przechowujące cenne informacje, ale zwykłe domowe komputery. W sieci niemal cały czas funkcjonują automatyczne skanery przeszukujące całe podsieci w celu znalezienia maszyn podatnych na atak. Celem tych ataków jest przejęcie komputera i wykorzystanie go do dalszych nieuprawnionych działań. **Przejęty komputer (tzw. zombie) może zostać wykorzystany m. in. do rozsyłania spamu, ataków DoS, rozpowszechniania danych chronionych prawem własności intelektualnej (prawem autorskim, np. pirackich kopii filmów czy gier) i innych nielegalnych materiałów i treści (np. pornografii dziecięcej, szkodliwych programów), hostowania podrobionej strony internetowej, za pomocą której cyberprzestępca wyłudza poufne dane itp.**

Oszustwa internetowe

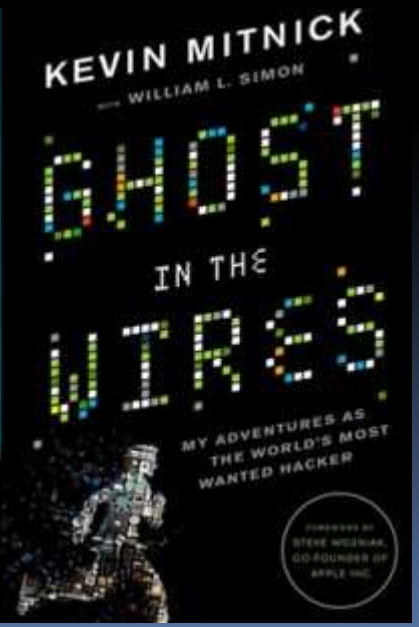
Oszustwa sieciowe bazują głównie na zjawisku **socjotechniki**. Cyberprzestępcy stosujący jej metody wchodzą w posiadanie informacji, których nie powinien znać nikt poza nami.

„Socjotechnika - jest to umiejętność skutecznego oddziaływania na ludzi (na społeczeństwo).” (*źródło: Gostkowski Zygmunt, Wybrane zagadnienia socjologii, Łódź 2005, ISBN 83-920189-3-1*)

Oszustwa internetowe

Jeden z najsłynniejszych hakerów, **Kevin Mitnick**, wszystkie uprawnienia jakie zdobył i dzięki którym zinfiltrował różne organizacje, otrzymał od ludzi, pracowników firmy. Najzwyczajniej w świecie o nie prosił… Wiele ze swoich trików opisał w dwóch książkach: „Sztuka podstępu" oraz „Sztuka infiltracji".

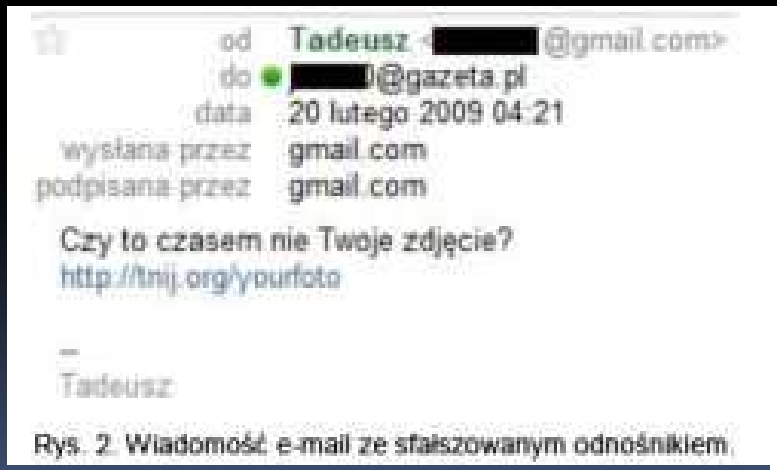
„Szpiedzy przemysłowi lub hakerzy czasami próbują fizycznie dostać się na teren firmy. Zamiast łomu socjotechnik korzysta ze swojej umiejętności manipulacji i przekonuje osobę po drugiej stronie, aby otworzyła mu drzwi".



Oszustwa internetowe

Spam i phishing - ulubione narzędzia socjotechnika

Przykładem manipulowania w sieci jest spam. Codziennie wielu użytkowników boryka się z problemem niechcianych wiadomości. Spam to nic innego jak nachalna reklama lub jedna z możliwości zainfekowania komputerów. Niejednokrotnie aby wzbudzić ciekawość i zachęcić do kliknięcia odnośnika korzysta się z tego co najbardziej przykuwa w dzisiejszych czasach uwagę - treści dla dorosłych. Jest to również sposób wpływania na nasze zachowanie i decyzje. Nie od dzisiaj wiadomo, że kontrowersyjne tematy, zwłaszcza jeżeli dotyczą znanych osób, są chodliwym tematem.



Rys. 2. Wiadomość e-mail ze sfałszowanym odnośnikiem.

Rys. 1. Spam zachęcający do kliknięcia odnośnika prowadzącego do programu szpiegującego.

Oszustwa internetowe

Spam to niezamawiana i niechciana przez odbiorcę wiadomość elektroniczna, rozpowszechniana zazwyczaj masowo, najczęściej za pomocą poczty elektronicznej. Tego typu wiadomości są najczęściej rozsyłane anonimowo z wyłudzonych lub przechwyconych adresów nadawcy (z fałszywymi nagłówkami listu).

Oszustwa internetowe

Przyjmuje się, że wiadomość uznawana jest za spam gdy:

- **odbiorca jej nie zamawiał,** czyli nie wyraził uprzedniej zgody na jej otrzymanie w sposób świadomy, weryfikowalny i możliwy do odwołania
- **treść i kontekst są niezależne od tożsamości odbiorcy** (czyli wiadomość może być przesyłana do wielu niezależnych odbiorców)
- **treść daje podstawy do przypuszczeń, że wysyłający odniósł niewspółmierną korzyść z faktu wysłania wiadomości w stosunku do korzyści, jaką odniósł odbiorca w związku z jej odebraniem**

Spam zazwyczaj posiada charakter komercyjny, przesyłane za jego pomocą treści reklamują produkty lub usługi.

Oszustwa internetowe

Ze względu na charakter treści wiadomości spam można podzielić na dwie kategorie:

- **wiadomość o charakterze komercyjnym, tzw. niezamawiany komercyjny email (ang. Unsolicited Commercial Email - UCE)**, przesyłane za jego pomocą treści reklamują produkty lub usługi. Ta kategoria jest najczęstszym przypadkiem spamu

- **wiadomość o charakterze często niekomercyjnym, to tzw. niezamawiany wielokrotny email (ang. Unsolicited Bulk Email - UBE)**, np: "spam polityczny", czyli masowo rozsyłane e-maile mające przekonać lub zniechęcić odbiorców do jakiejś idei czy partii politycznej, apele pochodzące rzekomo od instytucji społecznych czy charytatywnych, fikcyjne ostrzeżenia, np o wirusach komputerowych, łańcuszki szczęścia, oszustwa finansowe (tzw. scam) itp.

Oszustwa internetowe

Ze względu na platformę komunikacyjną można wyróżnić spam:

- **korespondencyjny** - najczęściej przesyłany pocztą elektroniczną, ale również m. in. faksem, telefonem, telefonem komórkowym (SMS, MMS), przez komunikatory internetowe (np. Gadu Gadu) i czaty (IRC)
- **na stronach WWW** - spam na stronach internetowych związany jest z zaśmiecaniem i przeciążaniem stron internetowych, np. bannerami, "wyskakującymi" okienkami reklamowymi (tzw. pop-up), czy innymi agresywnymi reklamami
- **inna forma spamu** to np. tzw DNS Pollution (spam DNS' owy) związany z tworzeniem niehierarchicznych, rozbudowanych nazw hostów internetowych

Oszustwa internetowe

Techniki i metody rozsyłania spamu

Przykładowe techniki i metody rozsyłania spamu to m. in.:

- **bezpośrednie wysyłanie wiadomości**
- **wykorzystanie serwerów**, np. open relay, open proxy
- **wykorzystanie przejętych (zainfekowanych) komputerów (tzw. zombie) lub sieci zainfekowanych komputerów (botnety).** Na przejętym komputerze (którego właściciel jest nieświadomy zagrożenia), nazywanym również "spam zombie" spamerzy instalują ukryte oprogramowanie, które przekształca komputer w serwer pocztowy lub tzw. serwer proxy. Za pośrednictwem przejętego komputera spamerzy masowo wysyłają korespondencję elektroniczną, maskując jednocześnie prawdziwe źródło jej pochodzenia

Oszustwa internetowe

Obecnie do masowego rozsyłania spamu często wykorzystywane są specjalne programy, które mogą m. in. wysyłać pocztę przez różne kanały komunikacyjne (w tym również poprzez specjalnie spreparowaną stronę internetową hostowaną zazwyczaj na przejętym komputerze), śledzić aktualność baz adresów, tworzyć dynamicznie tekst wiadomości. Spamerzy wyszukują coraz to nowsze sposoby rozsyłania spamu celem wysłania jak największej liczby wiadomości jak najmniejszym kosztem (czasu i pieniędzy).

Oszustwa internetowe

Kim są spamerzy i jak zdobywają adresy?

Spamerzy, czyli podmioty rozsyłające spam to często osoby prywatne mające różne motywacje (najczęściej zarobkowe), a także firmy reklamowe. Spamerzy wchodzą w posiadanie baz adresów najczęściej w wyniku:

- zbierania adresów e-mail na publicznych zasobach (np. stron WWW, grup dyskusyjnych) zazwyczaj poprzez ich automatyczne skanowanie - programy używane do tego celu nazywane są harvesterami (żniwiarkami) oraz za pomocą łańcuszków

- kradzieży baz adresów (np. zbierając wszystko, co pasuje do wzorca *użytkownik@domena*, lub poprzez kradzież osobistych danych użytkowników przy użyciu złośliwego programu, zazwyczaj trojana)

- kupna baz adresów

Oszustwa internetowe

Dlaczego łańcuszki należy ignorować?

Łańcuszki mają dwa główne cele:

- zbieranie adresów mailowych dla spamerów – kiedy rozsyłamy łańcuszek do wielu znajomych, pozostaje ślad nie tylko naszych, ale i ich kont pocztowych; większość osób po prostu dodaje adresy znajomych korzystając z opcji „prześlij dalej", dzięki czemu w łańcuszku gromadzi się całkiem pokaźny ich zbiór.

- bezpośrednie spamowanie – ma to miejsce wówczas, gdy w treści łańcuszka pojawia się informacja o konkretnym produkcie czy usłudze, a osoby rozsyłające po prostu same robią za nadawcę spamu reklamowego.

Oszustwa internetowe

Dlaczego łańcuszki należy ignorować?

Łańcuszki wykorzystują naszą chęć pomocy i dzielenia się informacjami. Niezależnie od tego, czy w treści jest prośba o wsparcie dla nieistniejącego chorego dziecka, czy ostrzeżenie przed wirusem, czy też śmieszna albo straszna historyjka – twórcom chodzi o to, żeby zainteresować nas na tyle, abyśmy chcieli się tym podzielić ze znajomymi. I wysłali łańcuszek dalej.

Oszustwa internetowe

Sprawdź, czy masz do czynienia z łańcuszkiem – atrapa.net

Serwis atrapa.net kolekcjonuje łańcuszki, jest więc świetnym sposobem sprawdzenia, czy otrzymana mailem wiadomość jest prawdziwa, czy też jest to kolejny spam. Większość listów-łańcuszków krąży w Internecie już od kilku lat – można więc porównać sobie kolejne wersje dowiedzieć się, kiedy były one aktywne.

Zanim więc roześlemy kolejną ściskającą za serce prośbę o „wsparcie dla umierającego syna koleżanki przyjaciółki" lub „ostrzeżenie znajomych przed groźnym wirusem" – wejdźmy na atrapa.net i poszukajmy tego konkretnego łańcuszka. Unikniemy w ten sposób spamowania znajomych, udostępnienia swojego adresu mailowego, no i odciążymy nieco serwery poczty.

Oszustwa internetowe

Szkodliwość spamu - czyli dlaczego spam jest zły?

Spam ze względu na masowy charakter stanowi obecnie jeden z większych problemów internetu. Według wielu źródeł szacuje się, że ilość wiadomości wysyłanych jako spam przerosła ilość pożądanej korespondencji. Powoduje to wymierne straty zarówno dla dostawców usług jak i końcowych użytkowników m. in. poprzez:

Oszustwa internetowe

Ponadto rozsyłanie spamu może skutkować m. in.:

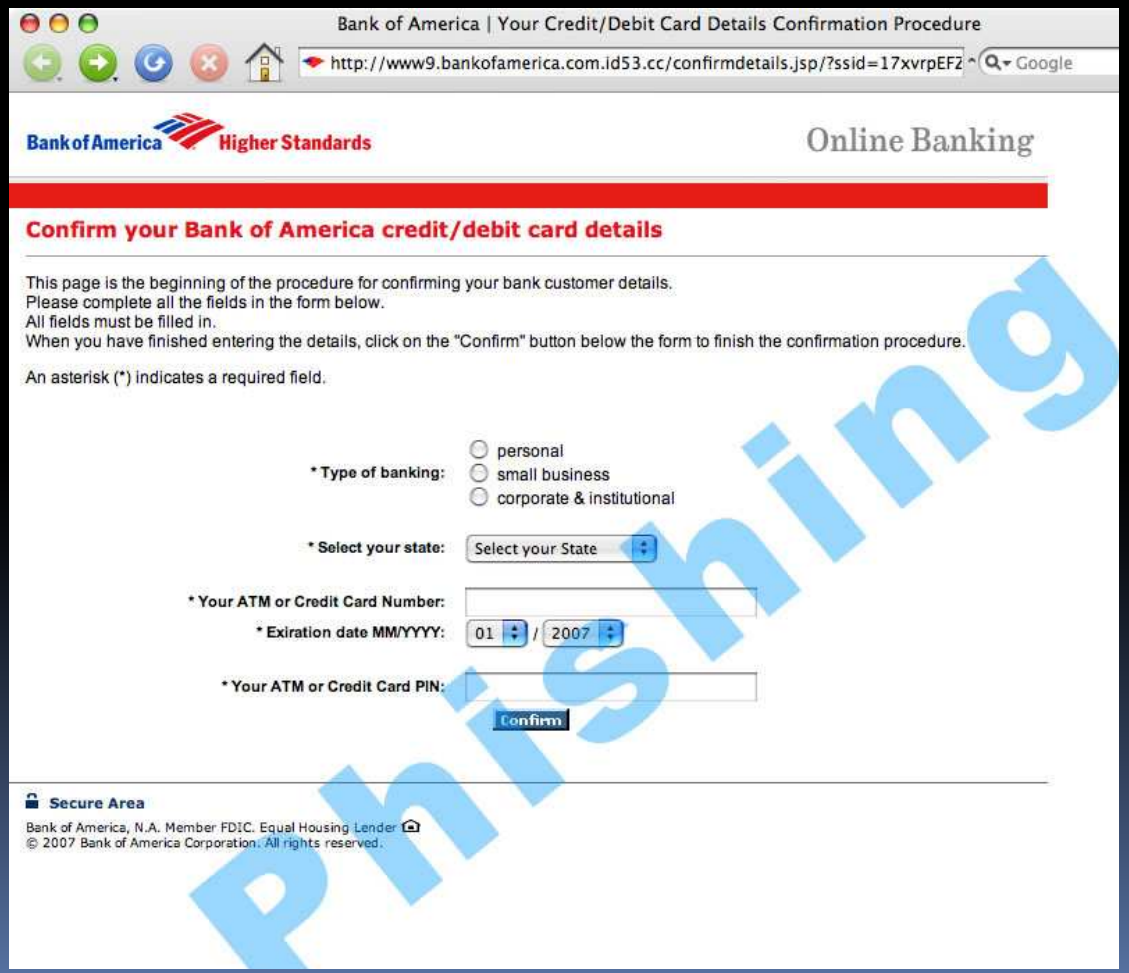
- **ograniczeniem dostępu do niektórych adresatów poczty elektronicznej,** np. poprzez umieszczenie adresów IP przydzielonych do usługi na tzw. czarnych listach (blacklists, z których korzystają administratorzy wielu serwerów pocztowych. Bezpośrednim wynikiem umieszczenia na takiej liście jest brak możliwości wysyłania poczty elektronicznej do wielu adresatów
- **sankcjami zgodnie z regulacjami prawnymi (w tym także z regulaminem świadczenia usługi)**

Oszustwa internetowe

Phishing to rodzaj oszustwa internetowego mającego na celu kradzież tożsamości, czyli poufnych danych osobistych, np. numerów kart kredytowych, haseł do systemów bankowych, czy haseł do portali aukcji internetowych. Termin ten często tłumaczony jest z ang. *password harvesting fishing* jako łowienie haseł.

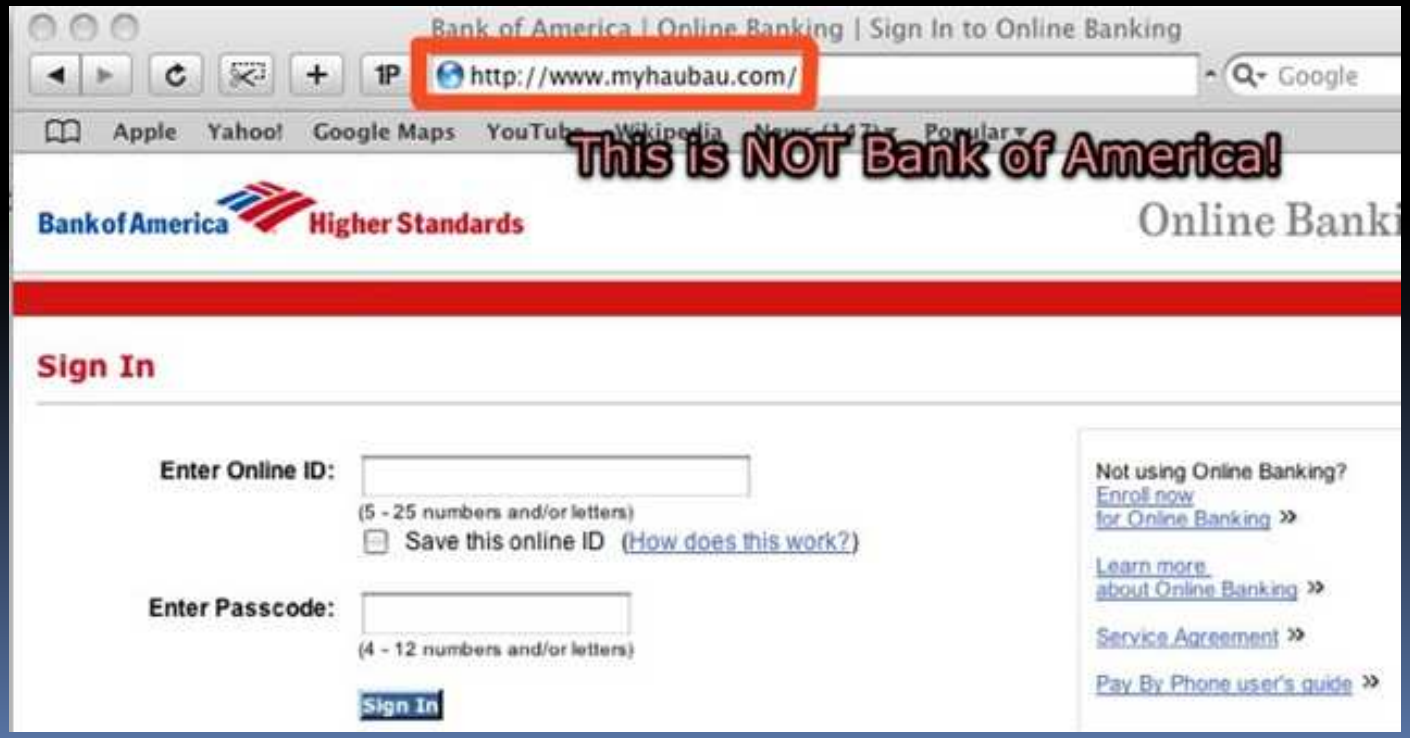
Oszustwa internetowe

Metoda phishingu może przebiegać w różny sposób, ale najczęściej polega na nakłonieniu użytkownika do samodzielnego wpisania poufnych danych na specjalnie przygotowanej stronie internetowej mającej imitować oryginalną stronę instytucji (np. banku internetowego, serwisu aukcyjnego, internetowego systemu płatności), pod którą podszywają się oszuści (cyberoszuści).



Oszustwa internetowe

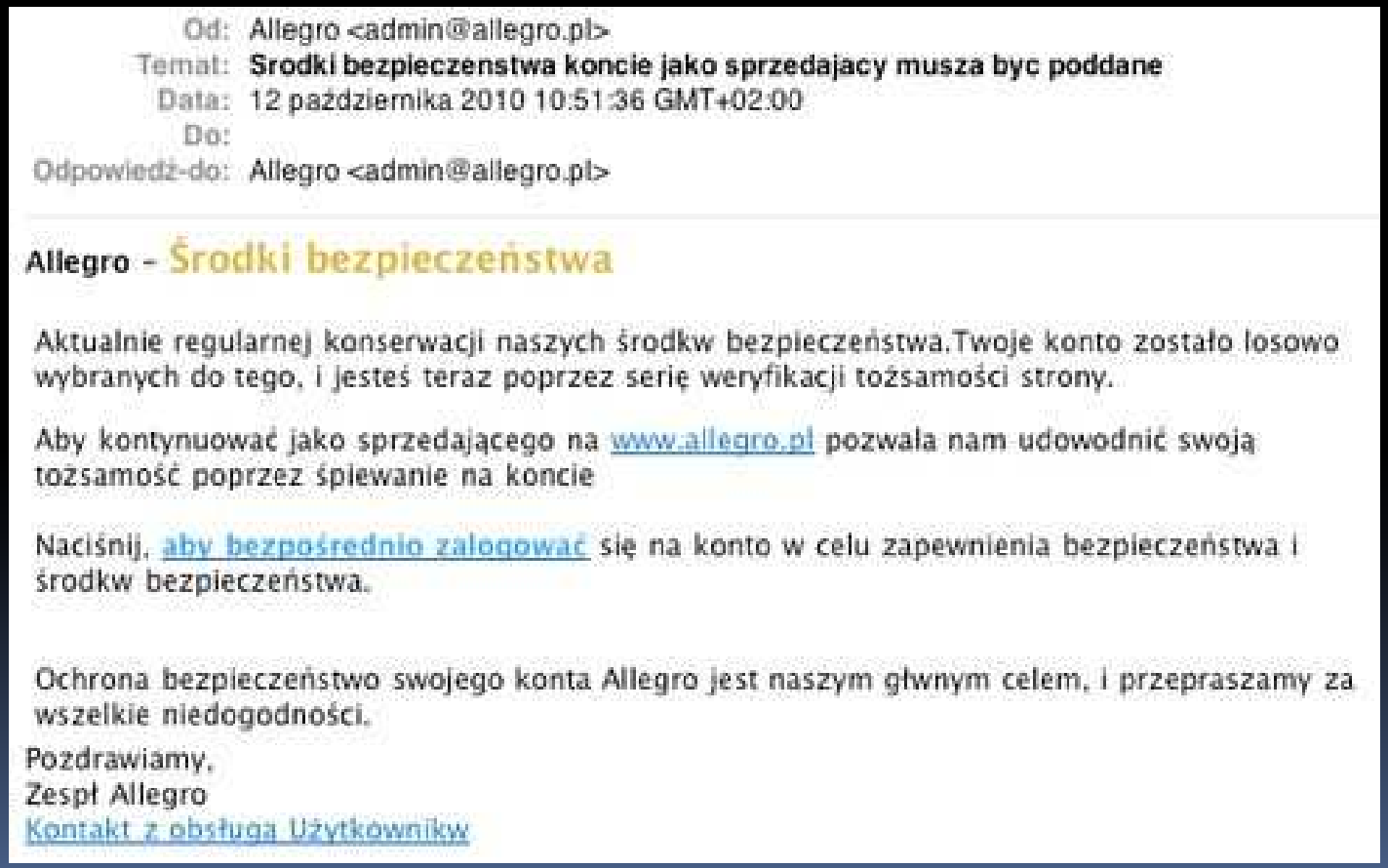
Zazwyczaj stosowaną techniką przez phisherów jest wysyłanie spreparowanego listu elektronicznego, który rzekomo pochodzi np. z banku. Treść e-maila zwykle zawiera link prowadzący do sfałszowanej strony. Adres jest tak podrobiony, aby ofiara myślała, że to prawdziwa strona instytucji, z którą chcemy się połączyć. W tym celu wykorzystywane są błędy w przeglądarkach lub proste triki, np. adres strony zawiera cyfrę 1 zamiast litery l.



Oszustwa internetowe

Przykładowy phishing danych logowania do konta Allegro*

Sfałszowane wiadomości e-mail zawierają odsyłacz prowadzący do strony logowania podstawionej przez cyberprzestępców.



Od: Allegro <admin@allegro.pl>
Temat: **Srodki bezpieczenstwa koncie jako sprzedajacy musza byc poddane**
Data: 12 października 2010 10:51:36 GMT+02:00
Do:
Odpowiedź-do: Allegro <admin@allegro.pl>

Allegro - Środki bezpieczeństwa

Aktualnie regularnej konserwacji naszych środkw bezpieczeństwa.Twoje konto zostało losowo wybranych do tego, i jesteś teraz poprzez serię weryfikacji tożsamości strony.

Aby kontynuować jako sprzedającego na www.allegro.pl pozwala nam udowodnić swoją tożsamość poprzez śpiewanie na koncie

Naciśnij, aby bezpośrednio zalogować się na konto w celu zapewnienia bezpieczeństwa i środkw bezpieczeństwa.

Ochrona bezpieczeństwo swojego konta Allegro jest naszym głwnym celem, i przepraszamy za wszelkie niedogodności.

Pozdrawiamy,
Zespł Allegro
Kontakt z obsługą Użytkownikw

*wg http://tech.wp.pl/kat,1009785,title,Phishing-z-Allegro-w-tle-uwaga-na-falszywe-wiadomosci-e-mail,wid,12750115,wiadomosc.html?ticaid=1d499

Oszustwa internetowe

Przykładowy phishing danych logowania do konta Allegro

Jak widać, treść wiadomości jest napisana niezwykle niedbale i wygląda na przetłumaczoną przy użyciu internetowego translatora. Jest to typowa cecha phishingu, który często jest organizowany na skalę globalną. Odsyłacz znajdujący się w wiadomości prowadzi do sfałszowanej strony logowania, która jest łudząco podobna do oryginalnej strony Allegro.pl.

Oszustwa internetowe

Przykładowy phishing danych logowania do konta Allegro

Można zauważyć, że strona (następny slajd) różni się od oryginału wyłącznie adresem URL oraz brakiem ważnego certyfikatu. Nawet doświadczony internauta może paść ofiarą takiego ataku. Dane wprowadzone w sfałszowanym formularzu trafią do cyberprzestępcy, który będzie miał do dyspozycji konto oszukanego użytkownika w serwisie Allegro.pl.

Oszustwa internetowe

Przykładowy phishing danych logowania do konta Allegro

Oszustwa internetowe

Przykładowy phishing danych logowania do konta Allegro

Właściciel serwisu Allegro.pl nie ma nic wspólnego z wysyłką tych wiadomości e-mail. Jest to typowy atak phishingowy mający na celu wyłudzenie informacji. Cyberprzestępca nielegalnie wykorzystał wizerunek Allegro.pl.

Oszustwa internetowe

PandaLabs, laboratorium antywirusowe firmy Panda Security, przygotowało w 2010 r. ranking najpopularniejszych oszustw z ostatnich kilku lat. Wszystkie te sztuczki wykorzystujące zaufanie ofiary mają ten sam cel: wyłudzenie od użytkowników pieniędzy. Ukradzione kwoty wynoszą od 500 do 1000 dolarów.*

*wg http://www.egospodarka.pl/58060,Najpopularniejsze-oszustwa-internetowe,1,12,1.html

Oszustwa internetowe

Takie oszustwa wpisują się zwykle w podobny schemat: pierwszym krokiem jest nawiązanie kontaktu przez e-mail lub sieci społecznościowe, w którym ofiara proszona jest o odpowiedź za pomocą poczty elektronicznej, telefonu czy faksu. Gdy użytkownik chwyci przynętę, przestępcy będą starali się zdobyć jego zaufanie, prosząc w końcu o jakąś sumę pieniędzy pod tym czy innym pretekstem.

Luis Corrons, dyrektor techniczny laboratorium PandaLabs stwierdził: „Podobnie jak w przypadku klasycznych oszustw sprzed ery Internetu, wielu użytkowników, którzy stają się ofiarami oszustwa on-line i tracą pieniądze, nie zgłasza przestępstwa. Już dawniej odzyskanie straconych pieniędzy było trudne, a teraz jest to jeszcze trudniejsze, gdyż ślady przestępców giną w sieci. Najlepszą ochroną jest wiedza o tym, jak rozpoznawać takie oszustwa i nie dać się nabrać”.

Oszustwa internetowe

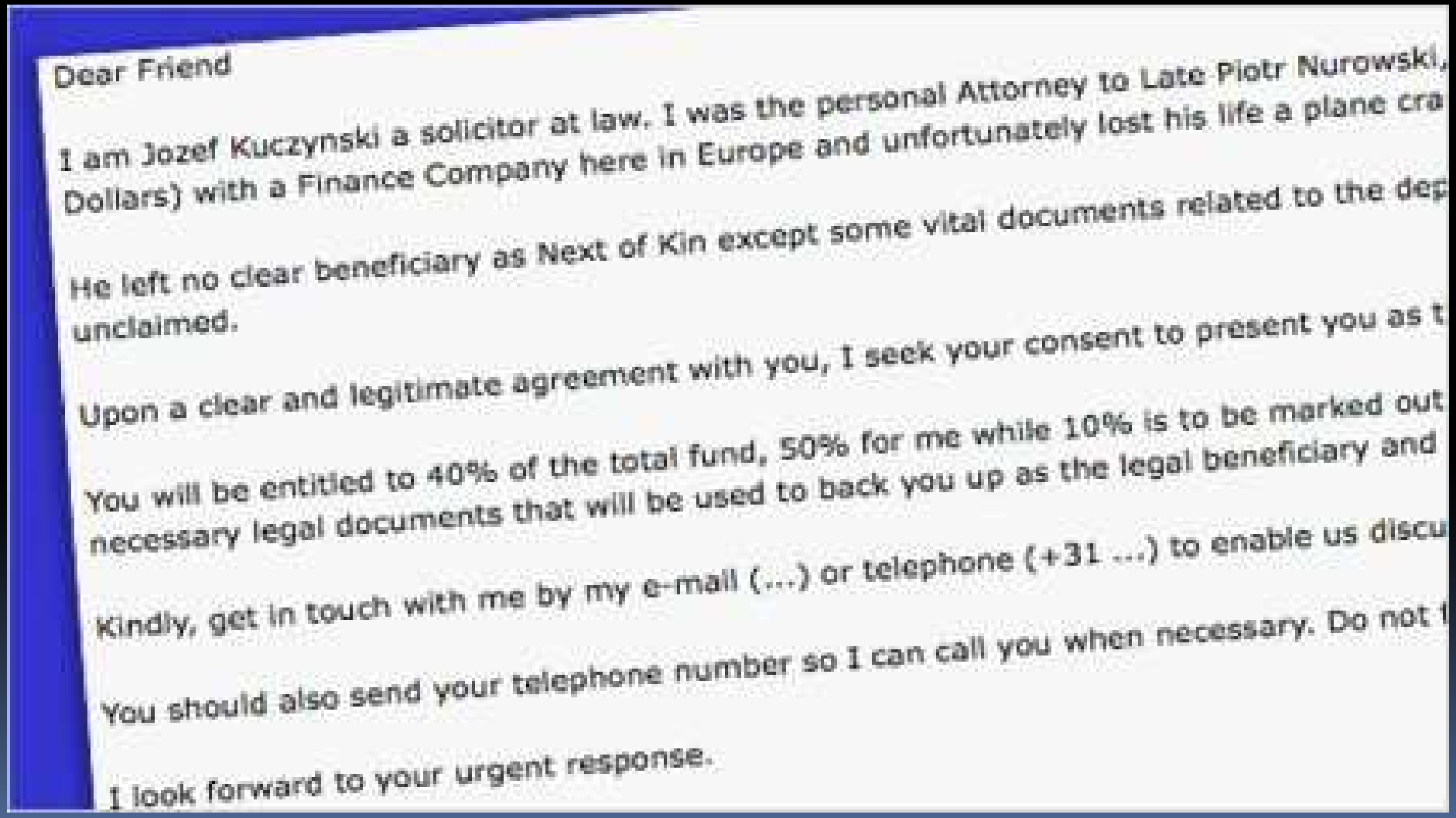
Oszustwo nigeryjskie: To pierwszy typ oszustwa, jaki pojawił się w Internecie, często stosowany przez cyberprzestępców, aż do dzisiaj. Najczęściej ma formę e-maila, rzekomo od osoby, która musi odzyskać dużą sumę pieniędzy od jakiegoś kraju (zwykle jest to Nigeria, stąd nazwa). Za pomoc obiecuje wysoką nagrodę. Użytkownicy, którzy w to uwierzą, są proszeni o przelanie pewnej sumy na pokrycie opłat bankowych (często około 1000 dolarów). Po zapłaceniu kwoty kontakt zanika, a pieniądze przepadają.

Nigeryjski przekręt bazuje na bardzo starej metodzie oszustwa, którą wykorzystywano już w latach 1904-1911 (chodziło o pomoc w wykupieniu rzekomego rosyjskiego więźnia z hiszpańskiego więzienia). Warto zatem wiedzieć, że droga elektroniczna nie tyle umożliwia prowadzenie "nigeryjskich przekrętów", ale znacząco ułatwia ten stary jak świat proceder.*

*http://www.komputerswiat.pl/jak-to-dziala/2008/11/oszustwa-w-internecie.aspx

Oszustwa internetowe

Oszustwo nigeryjskie, przykład 1.



Dear Friend

I am Jozef Kuczynski a solicitor at law. I was the personal Attorney to Late Piotr Nurowski,
Dollars) with a Finance Company here in Europe and unfortunately lost his life a plane cra

He left no clear beneficiary as Next of Kin except some vital documents related to the dec
unclaimed.

Upon a clear and legitimate agreement with you, I seek your consent to present you as t

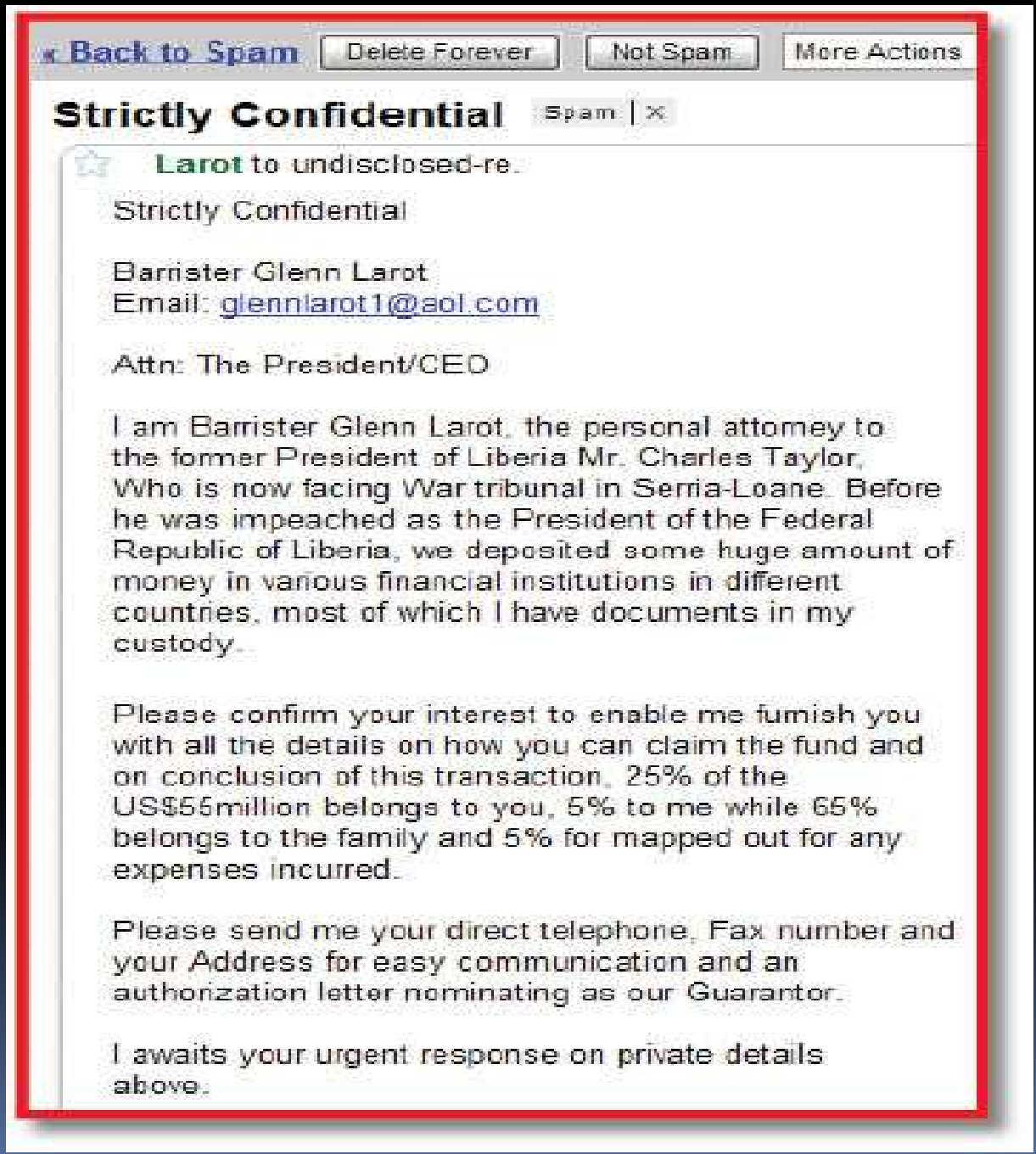
You will be entitled to 40% of the total fund, 50% for me while 10% is to be marked out
necessary legal documents that will be used to back you up as the legal beneficiary and

Kindly, get in touch with me by my e-mail (...) or telephone (+31 ...) to enable us discu

You should also send your telephone number so I can call you when necessary. Do not f

I look forward to your urgent response.

Oszustwo nigeryjskie, przykład 2.



« Back to Spam | Delete Forever | Not Spam | More Actions

Strictly Confidential Spam | X

Larot to undisclosed-re.

Strictly Confidential

Barrister Glenn Larot
Email: glennlarot1@aol.com

Attn: The President/CEO

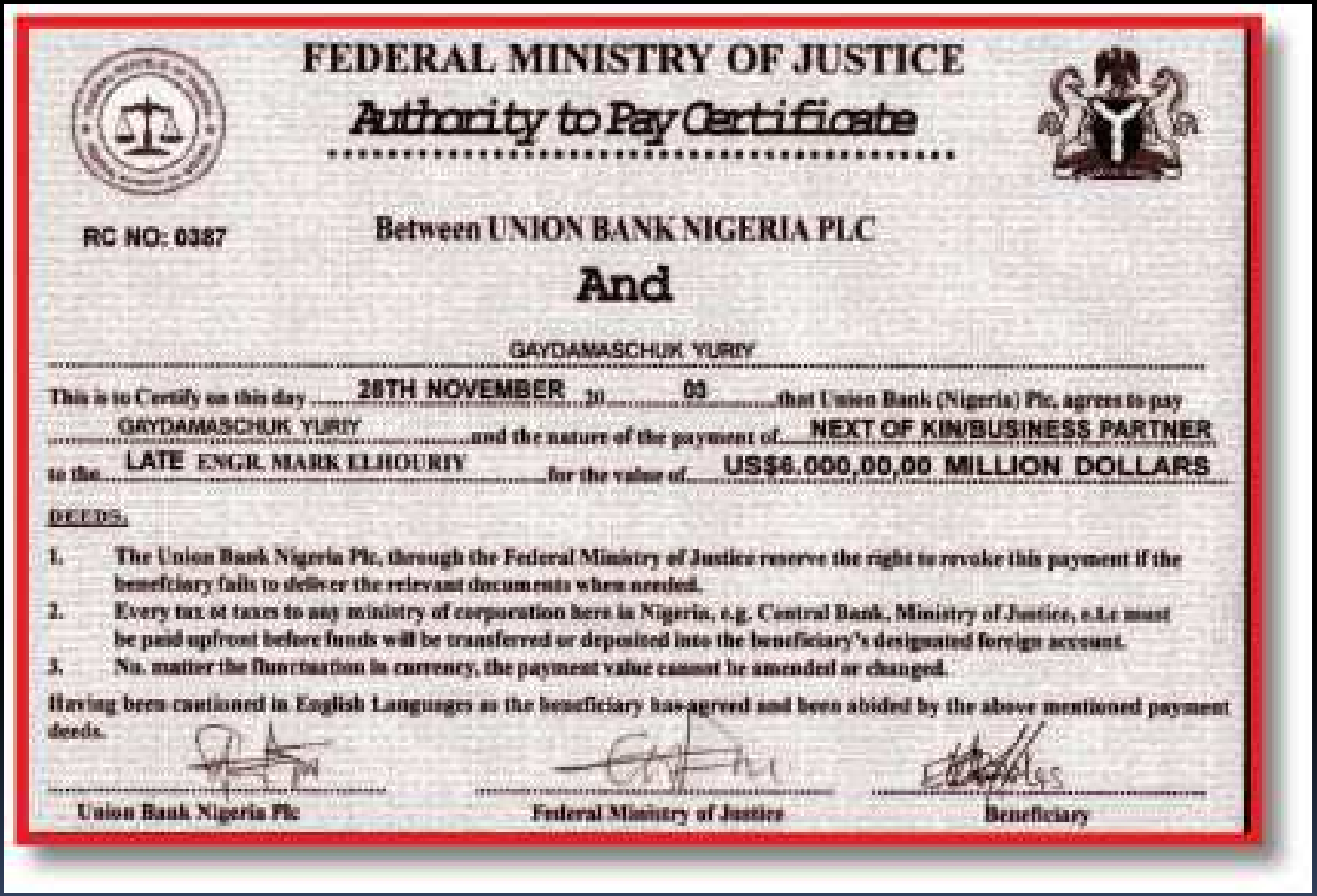
I am Barrister Glenn Larot, the personal attorney to the former President of Liberia Mr. Charles Taylor, Who is now facing War tribunal in Serria-Loane. Before he was impeached as the President of the Federal Republic of Liberia, we deposited some huge amount of money in various financial institutions in different countries, most of which I have documents in my custody.

Please confirm your interest to enable me furnish you with all the details on how you can claim the fund and on conclusion of this transaction, 25% of the US$55million belongs to you, 5% to me while 65% belongs to the family and 5% for mapped out for any expenses incurred.

Please send me your direct telephone, Fax number and your Address for easy communication and an authorization letter nominating as our Guarantor.

I awaits your urgent response on private details above.

Oszustwo nigeryjskie



FEDERAL MINISTRY OF JUSTICE

Authority to Pay Certificate

RC NO: 0387

Between UNION BANK NIGERIA PLC

And

GAYDAMASCHUK YURIY

This is to Certify on this day 28TH NOVEMBER 20 09 that Union Bank (Nigeria) Plc, agrees to pay GAYDAMASCHUK YURIY and the nature of the payment of NEXT OF KIN/BUSINESS PARTNER to the LATE ENGR. MARK ELHOURIY for the value of US$6.000,00,00 MILLION DOLLARS

DEEDS;

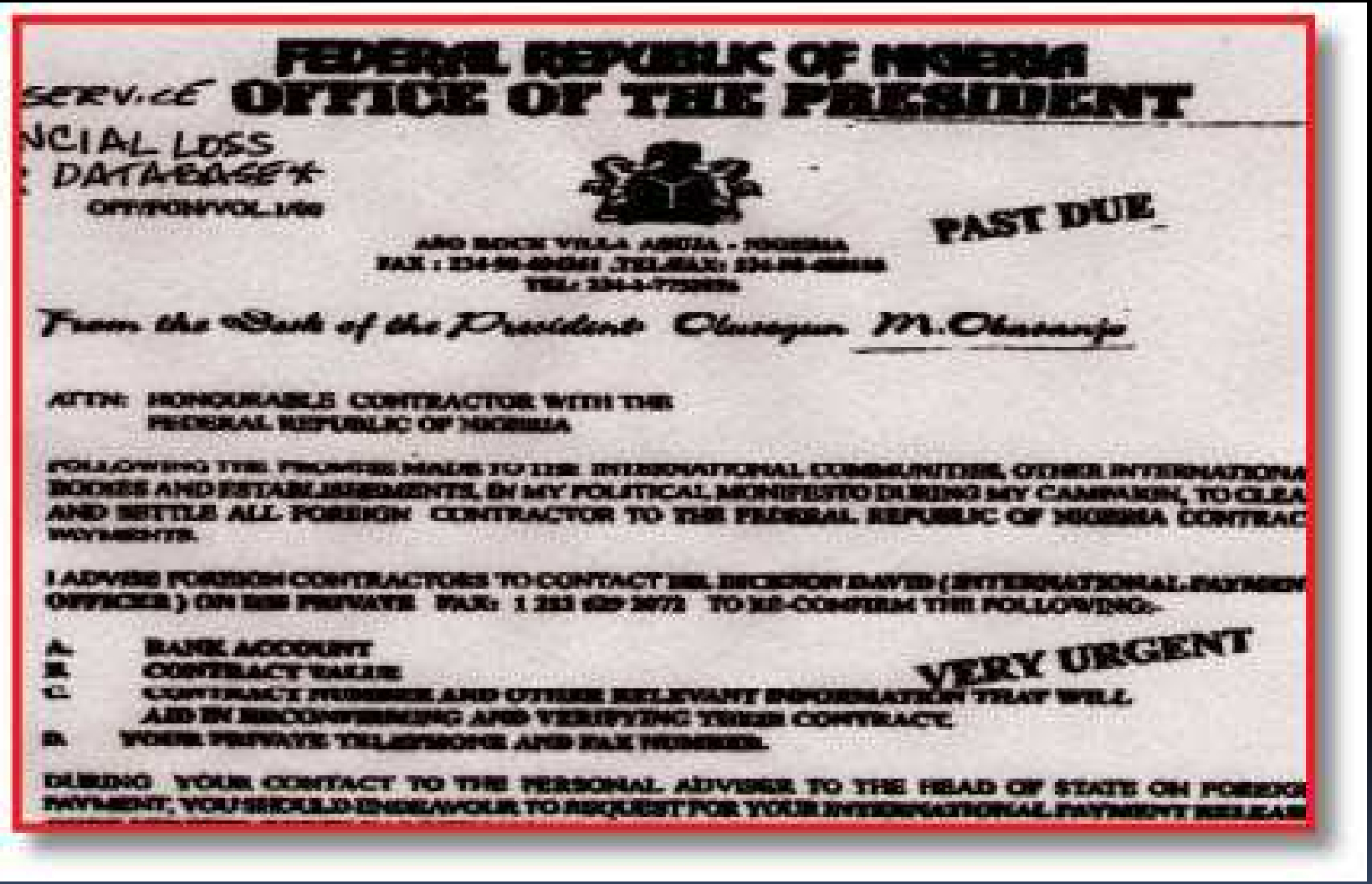
1. The Union Bank Nigeria Plc, through the Federal Ministry of Justice reserve the right to revoke this payment if the beneficiary fails to deliver the relevant documents when needed.
2. Every tax or taxes to any ministry of corporation here in Nigeria, e.g. Central Bank, Ministry of Justice, e.t.c must be paid upfront before funds will be transferred or deposited into the beneficiary's designated foreign account.
3. No. matter the fluctuation in currency, the payment value cannot be amended or changed.

Having been cautioned in English Languages as the beneficiary has agreed and been abided by the above mentioned payment deeds.

Union Bank Nigeria Plc | Federal Ministry of Justice | Beneficiary

Naiwnych kuszą czeki z Ministerstwa Sprawiedliwości Nigerii.

Oszustwo nigeryjskie



FEDERAL REPUBLIC OF NIGERIA

OFFICE OF THE PRESIDENT

NCIAL LOSS
DATABASE

PAST DUE

From the Desk of the President Olusegun M.Obasanjo

ATTN: HONOURABLE CONTRACTOR WITH THE
FEDERAL REPUBLIC OF NIGERIA

VERY URGENT

Oszuści preparują dokumenty, które mają przekonywać ofiary. Listy wyposażone są w stosowne pieczęcie.

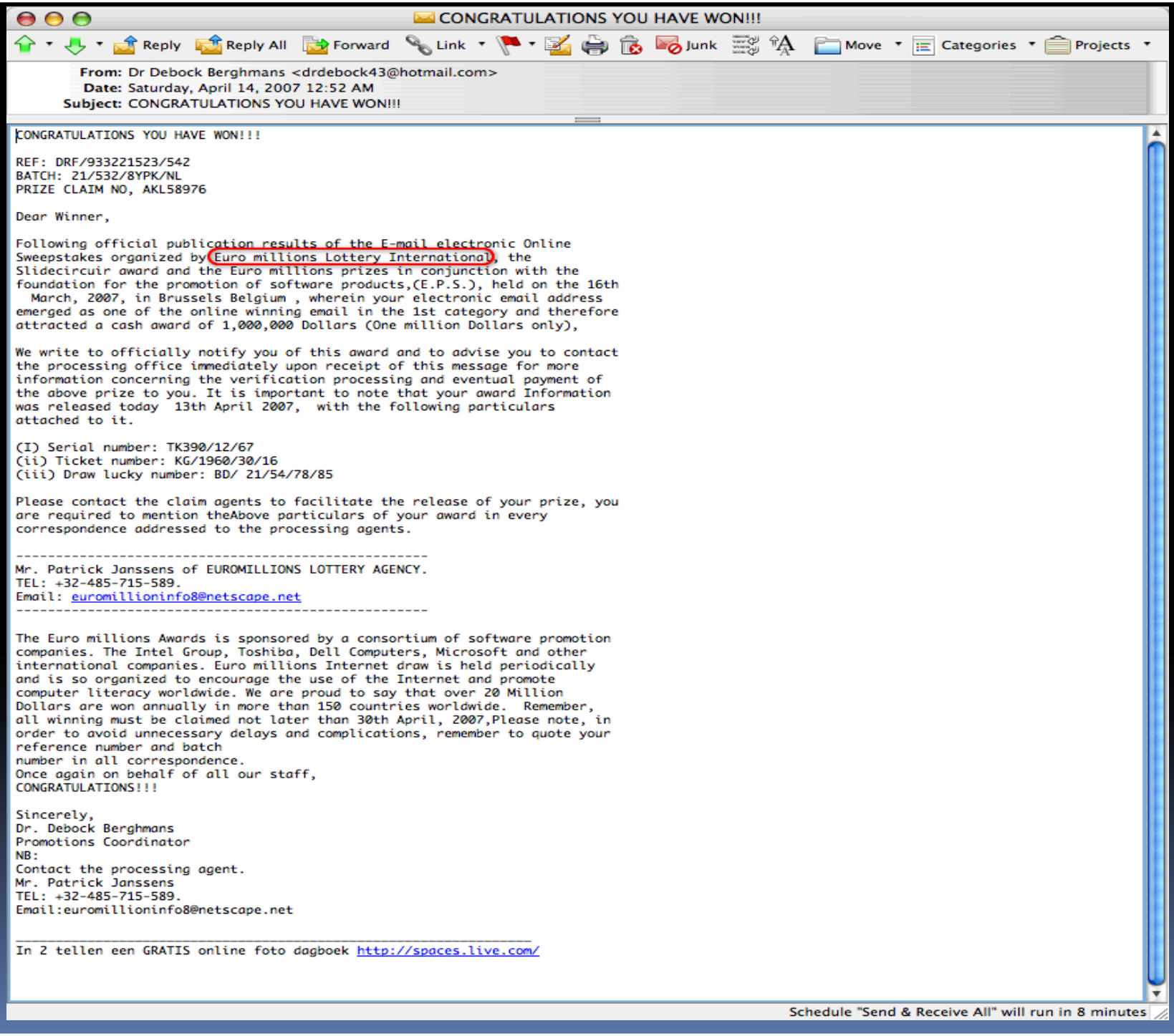
Oszustwo nigeryjskie

Czasami internauci kontratakują. Oszust musiał ponieść wysokie koszty przesyłki, cła i podatku, a dostał wykonany z kartonu „notebook". Należy jednak zadbać, by zachować anonimowość - wśród oszustów zdarzają się zarówno naciągacze, jak i doświadczeni, groźni przestępcy.

Oszustwa internetowe

Loterie: Podobne do oszustwa nigeryjskiego. Użytkownik otrzymuje informację o rzekomej wygranej w loterii i prośbą o dane osobowe w celu przekazania zwycięzcy wysokiej nagrody. Tak jak w przypadku poprzedniego oszustwa - ofiary proszone są o wysłanie płatnego SMS albo np. zaliczkę w wysokości około 1000 dolarów na pokrycie opłat bankowych itp.

Loterie



CONGRATULATIONS YOU HAVE WON!!!

Reply | Reply All | Forward | Link | Junk | Move | Categories | Projects

From: Dr Debock Berghmans <drdebock43@hotmail.com>
Date: Saturday, April 14, 2007 12:52 AM
Subject: CONGRATULATIONS YOU HAVE WON!!!

CONGRATULATIONS YOU HAVE WON!!!

REF: DRF/933221523/542
BATCH: 21/532/8YPK/NL
PRIZE CLAIM NO, AKL58976

Dear Winner,

Following official publication results of the E-mail electronic Online Sweepstakes organized by Euro millions Lottery International, the Slidecircuir award and the Euro millions prizes in conjunction with the foundation for the promotion of software products,(E.P.S.), held on the 16th March, 2007, in Brussels Belgium , wherein your electronic email address emerged as one of the online winning email in the 1st category and therefore attracted a cash award of 1,000,000 Dollars (One million Dollars only),

We write to officially notify you of this award and to advise you to contact the processing office immediately upon receipt of this message for more information concerning the verification processing and eventual payment of the above prize to you. It is important to note that your award Information was released today 13th April 2007, with the following particulars attached to it.

(I) Serial number: TK390/12/67
(ii) Ticket number: KG/1960/30/16
(iii) Draw lucky number: BD/ 21/54/78/85

Please contact the claim agents to facilitate the release of your prize, you are required to mention theAbove particulars of your award in every correspondence addressed to the processing agents.

Mr. Patrick Janssens of EUROMILLIONS LOTTERY AGENCY.
TEL: +32-485-715-589.
Email: euromillioninfo8@netscape.net

The Euro millions Awards is sponsored by a consortium of software promotion companies. The Intel Group, Toshiba, Dell Computers, Microsoft and other international companies. Euro millions Internet draw is held periodically and is so organized to encourage the use of the Internet and promote computer literacy worldwide. We are proud to say that over 20 Million Dollars are won annually in more than 150 countries worldwide. Remember, all winning must be claimed not later than 30th April, 2007,Please note, in order to avoid unnecessary delays and complications, remember to quote your reference number and batch
number in all correspondence.
Once again on behalf of all our staff,
CONGRATULATIONS!!!

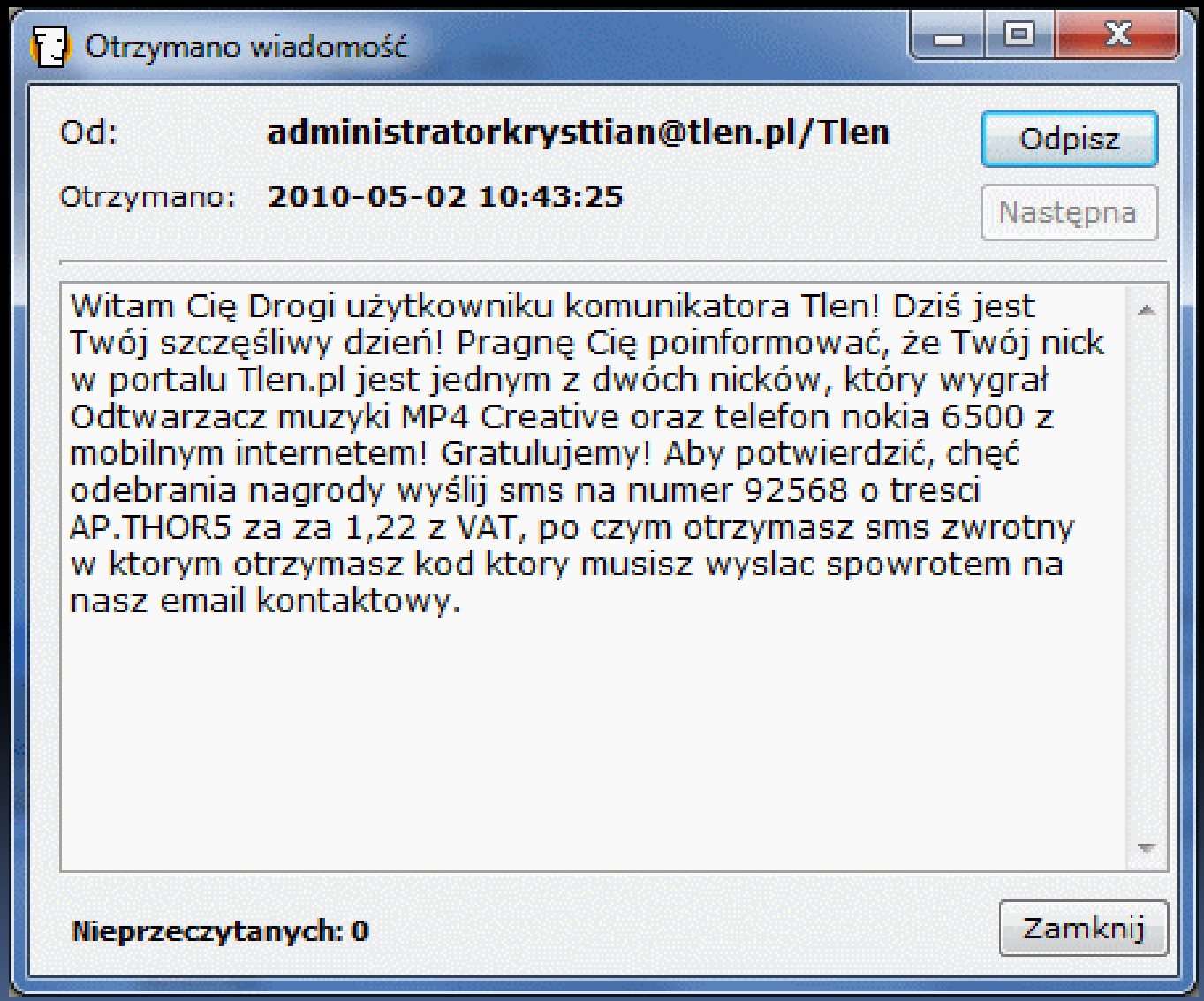
Sincerely,
Dr. Debock Berghmans
Promotions Coordinator
NB:
Contact the processing agent.
Mr. Patrick Janssens
TEL: +32-485-715-589.
Email:euromillioninfo8@netscape.net

In 2 tellen een GRATIS online foto dagboek http://spaces.live.com/

Schedule "Send & Receive All" will run in 8 minutes

Oszustwa internetowe

Loterie

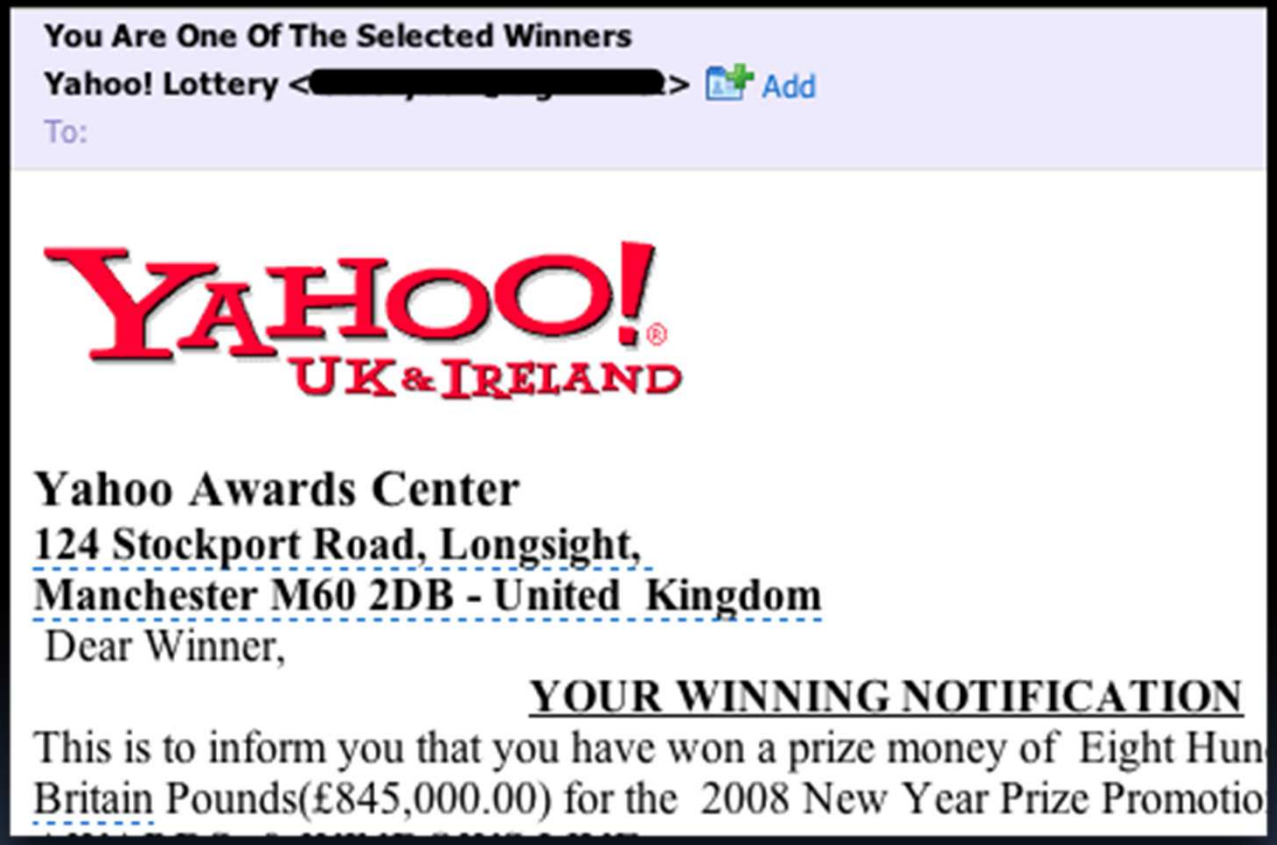


Oszustwa internetowe

Loterie

Oszustwa internetowe

Loterie


You Are One Of The Selected Winners

Yahoo! Lottery <[redacted]> Add

To:

YAHOO! UK & IRELAND

Yahoo Awards Center
124 Stockport Road, Longsight,
Manchester M60 2DB - United Kingdom

Dear Winner,

YOUR WINNING NOTIFICATION

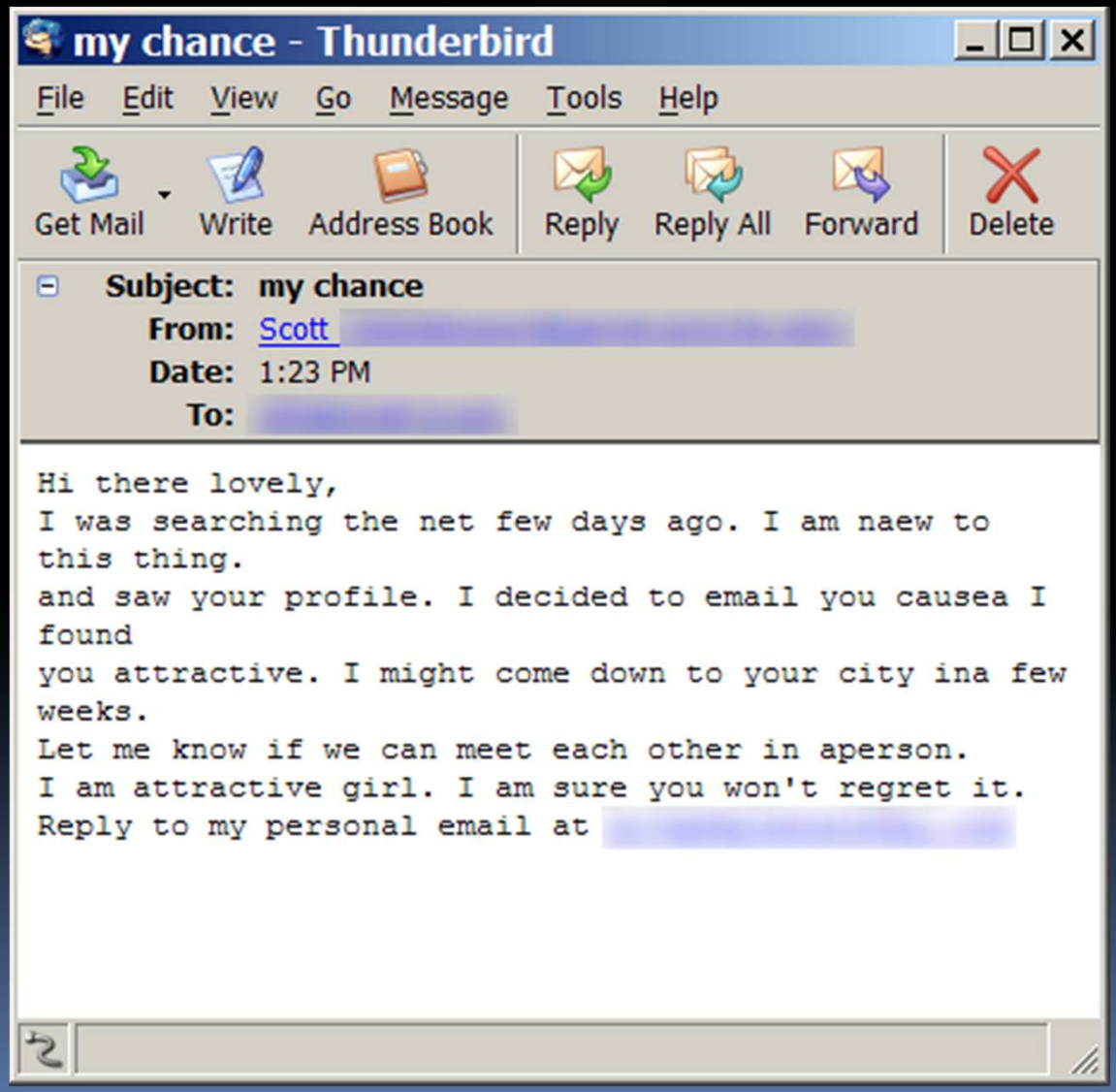
This is to inform you that you have won a prize money of Eight Hun
Britain Pounds(£845,000.00) for the 2008 New Year Prize Promotio

Oszustwa internetowe

Dziewczyny: Piękna dziewczyna, zwykle Rosjanka, znajduje adres e-mail użytkownika, którego chce poznać. Jest młoda i marzy o przyjeździe do kraju ofiary i spotkaniu, ponieważ jest po uszy zakochana. Chce przyjechać natychmiast, lecz w ostatniej chwili pojawia się problem i okazuje się, że nie posiada wystarczających środków finansowych na podróż. Prosi, więc o gotówkę (i w tym przypadku jest to około 1000 dolarów) na opłacenie biletów lotniczych, wizy itp. Łatwo zgadnąć, że pieniądze i dziewczyna przepadają.

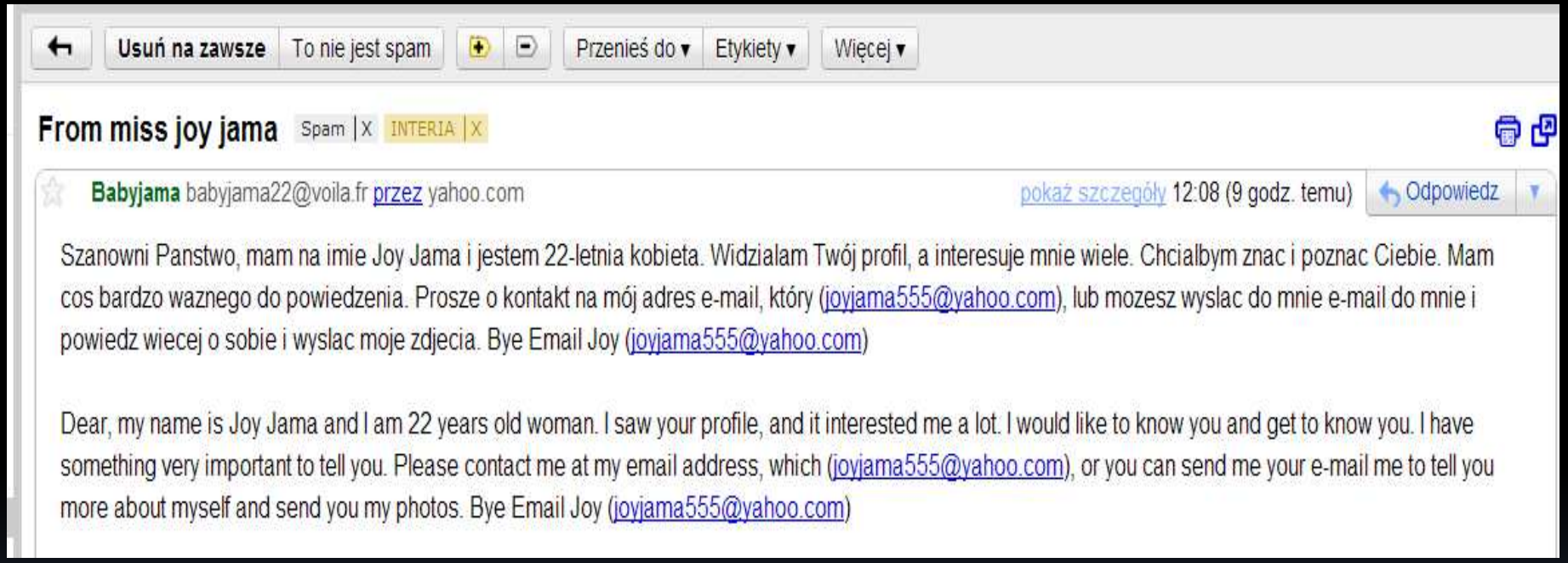
Oszustwa internetowe

Dziewczyny



Oszustwa internetowe

Dziewczyny



Oszustwa internetowe

Oferty pracy: Tym razem użytkownik otrzymuje wiadomość od zagranicznej firmy poszukującej agentów finansowych w jego kraju. Praca jest łatwa – można ją wykonywać w domu – i pozwala zarobić do 3000 dolarów przy 3-4 godzinach pracy dziennie. Jeśli ofiara się zgodzi, zostaje poproszona o dane bankowe. Użytkownik jest wykorzystywany do kradzieży pieniędzy z kont bankowych osób, których dane zostały wcześniej skradzione przez cyberprzestępców. Pieniądze są przelewane bezpośrednio na konto ofiary, która jest proszona o przesłanie sumy przez Western Union. Ofiara staje się tzw. „słupem", a w policyjnym śledztwie w sprawie kradzieży uznawana jest za współsprawcę. Mimo, że praktyka ta jest często określana jako scam, czyli wyłudzenie, rożni się od innych oszustw tego typu tym, że „słup" również może czerpać korzyści, choć nieświadomie popełnia przestępstwo.

Oszustwa internetowe

Oferta pracy

New position in a large bank

1 message

[redacted] **26 May 2011 13:31**

Reply-To: [redacted]

To: Rebekah Hah

Good day Rebekah Hah Your resume was found at one of the {vacancies|job offering} sites. Here is a description of an interesting position. We are one of the many charity organizations that have appeared lately as a result of the last events in Japan. I am talking about a vacancy in the new Department of beneficence of a big japanese bank. Thousands of persons all over the world desire to participate in the helping programs for the victims. If are one of them, please study our offer. Qualification demands: PC user Permanent internet access Telephone connection: mobile and fixed Responsibility Reliability Attentiveness Main functions: - Business correspondence - Conducting transactions from corporate and physical persons interested in giving help anonymously transfer from a sponsor - Conducting transactions to the funds or private individual or his/her legal representative by the bank order or Western Union or MoneyGram International system s - Accounting Work schedule: From Monday to Friday, during the regular work day. This job will not take more than 2 hours a day. Salary From 600 to 3000 GBP monthly. To receive more details|please write that you are interested in this position. Marianne Houston

Oszustwa internetowe

Oferta pracy

From: "{1kk}" <gqwym@bonia.com.my> **To:** [redacted]
Subject: Sichere Arbeitsplaetze

Zdravstvuyte!

Ya predstavitel' krupnoy ukrainskoy firmy, kotoraya zanimaetsya razrabotkoy programmnogo obespecheniya!
V dannyy moment nam trebuyutsya regional'nye predstaviteli. Horoshaya oplata, gibkie usloviya raboty.
Esli vy zaineteresovanny - pojaluysta vyshlite vashe rezyume na email morgankerbsdt841@gmail.com i v pis'me ukajite
kakie yazyki znaete i kontaktnii telefon. Nashi menedjery svyajutsya s vami v blijayshee vremya.

Hello!

I am the representative of the large Ukrainian firm, which is engaged in software development.
At the moment regional representatives are required to us. Good payment, flexible operating conditions. If you are interested to work with us ,
please send your resume to e-mail morgankerbsdt841@gmail.com and in the letter specify what languages
you know(German,Russian,English). Our managers will contact you in the nearest time.

Sehr geehrte Dammen und Herren,
Ich bin der Vertreter der grossen ukrainischen Firme,
die sich auf der Erarbeitung der Software spezialisiert.
Im Moment brauchen wir den Regional Manager. Gute Bezahlung und flexible Arbeitsbedienung sind garantiert.
Wenn Sie dazu Interesse haben, schiecken Sie uns bitte Ihre Bewerbung auf die Email: morgankerbsdt841@gmail.com , und schreiben Sie bitte uns welche Sprache Sie kennen.
Unsere Manager werden sich mit Ihnen in die allernaechste Zeit verbinden.

Oszustwa internetowe

Pilna pomoc: Przestępcy uzyskują dane dostępowe do Facebooka, NK, e-mail lub komunikatora. Następnie mogą zmienić dane do logowania, tak by prawdziwy użytkownik nie mógł korzystać z konta. Oszuści wysyłają do wszystkich kontaktów wiadomość o tym, że użytkownik wyjechał na wakacje (często do Londynu) i został obrabowany tuż przed powrotem do domu. Wciąż posiada on bilety lotnicze, ale potrzebuje około 500-1000 dolarów na hotel.

Oszustwa internetowe

Pilna pomoc

Date: Tue, Jun 21, 2011 at 1:39 PM
Subject: Help!!!!!!!!!!
To:

I'm writing this with tears in my eyes,my family and I came down here to Valencia,Spain for
a short vacation unfortunately we were mugged at the park of the hotel where we stayed all
cash,credit card and Phone were stolen off from us luckily for us we still have our passports with us.

We've been to the Embassy and the Police here they're not helping issues at all but we're
having problems settling the hotel bills and the hotel manager won't let us leave until we
settle the bills,I'm freaked out at the moment...

--

Oszustwa internetowe

Odszkodowanie: Stosunkowo nowy rodzaj wyłudzenia, bazujący na oszustwie nigeryjskim. Użytkownik otrzymuje e-mail informujący o rzekomym utworzeniu funduszu wypłacającego odszkodowania ofiarom oszustwa nigeryjskiego. Ofiara może otrzymać odszkodowanie (często około 1 miliona dolarów), ale tak jak w przypadku pierwotnego oszustwa, musi oczywiście wpłacić zaliczkę w wysokości około 1000 dolarów.

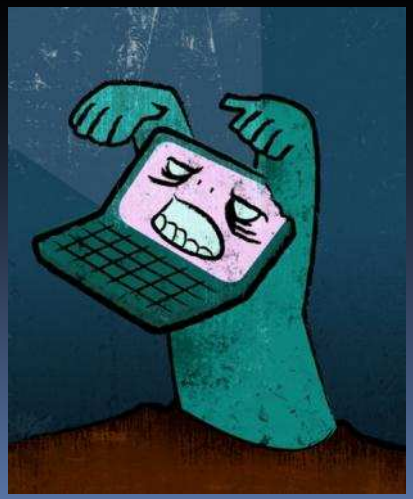
Oszustwa internetowe

Pomyłka: Bardzo popularny rodzaj oszustwa w ostatnich miesiącach, być może związany w kryzysem finansowym i trudnościami w sprzedaży towarów i domów. Oszuści kontaktują się z osobą, która zamieściła ogłoszenie o sprzedaży domu, samochodu itp. Z wielkim entuzjazmem zgadzają się kupić oferowany towar i wkrótce przysyłają czek, ale na niewłaściwą sumę (zawsze wyższą od uzgodnionej). Sprzedawca jest proszony o zwrócenie różnicy. Czeku nie można zrealizować, dom pozostaje niesprzedany, a ofiara traci przelane pieniądze.

Oszustwa internetowe

Phishing stanowi poważne zagrożenie nie tylko dla Twoich zasobów komputerowych ale i samego Ciebie.

W wyniku ataku phishingowego **następuje kradzież Twojej tożsamości, czyli Twoich poufnych danych osobistych** (np. hasła dostępu do stron banku internetowego, nr karty kredytowej), co zazwyczaj prowadzi do utraty przez Ciebie środków finansowych oraz wystąpienia innych problemów związanych z dokonywaniem oszustw sieciowych z udziałem Twoich danych osobowych. Ponadto w związku z oszustwem phishingowym **możesz otrzymywać spam oraz Twój komputer może zostać wykorzystany do hostowania podrobionej strony internetowej** (co oprócz zagrożenia dla Ciebie, w tym Twoich zasobów komputerowych, stanowi zagrożenie dla innych).



Oszustwa internetowe

Inną formą dotarcia przestępców do ofiar ataków i kradzieży ich poufnych danych to m. in. poprzez telefon (tzw. **vishing**), wiadomość SMS (**SMiShing**), komunikator internetowy, faks, czy nawet poprzez przejęcie (podszycie się pod domenę strony, tzw. **pharming**) stron internetowych instytucji finansowych i innych, które stają się celem ataku phishingowego.

Oszustwa internetowe

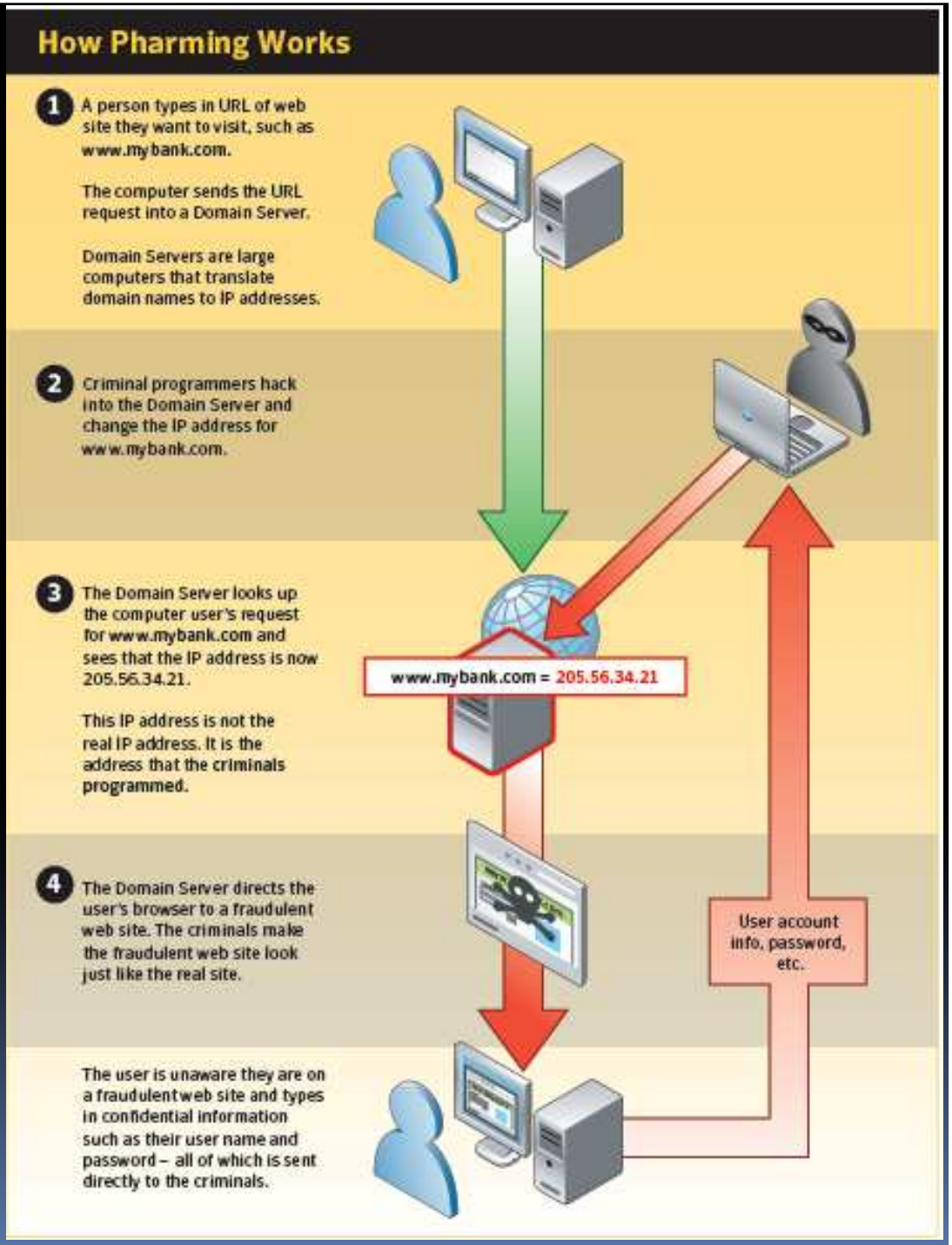
Pharming to bardziej zaawansowana i niebezpieczna dla użytkownika odmiana phishingu.

Cel jest ten sam, czyli wyłudzenie poufnych danych osobistych. Różnica jest taka, że nie jest wysyłana informacja nakłaniająca użytkownika do podania swoich poufnych informacji, natomiast w momencie odwiedzania przez użytkownika witryny internetowej następuje przekierowanie połączenia (bez jego wiedzy i udziału) do fałszywej strony cyberoszusta, zamiast na właściwą stronę, mimo wpisania poprawnego adresu strony.

W tym celu oszust najpierw atakuje serwer nazw domenowych (DNS), który tłumaczy dla nas nazwy domen na adresy IP. W efekcie serwer DNS, zamiast adresu prawdziwej instytucji, podaje przeglądarce użytkownika adres IP strony spreparowanej przez oszusta. W tym przypadku atak następuje poza Twoim komputerem.

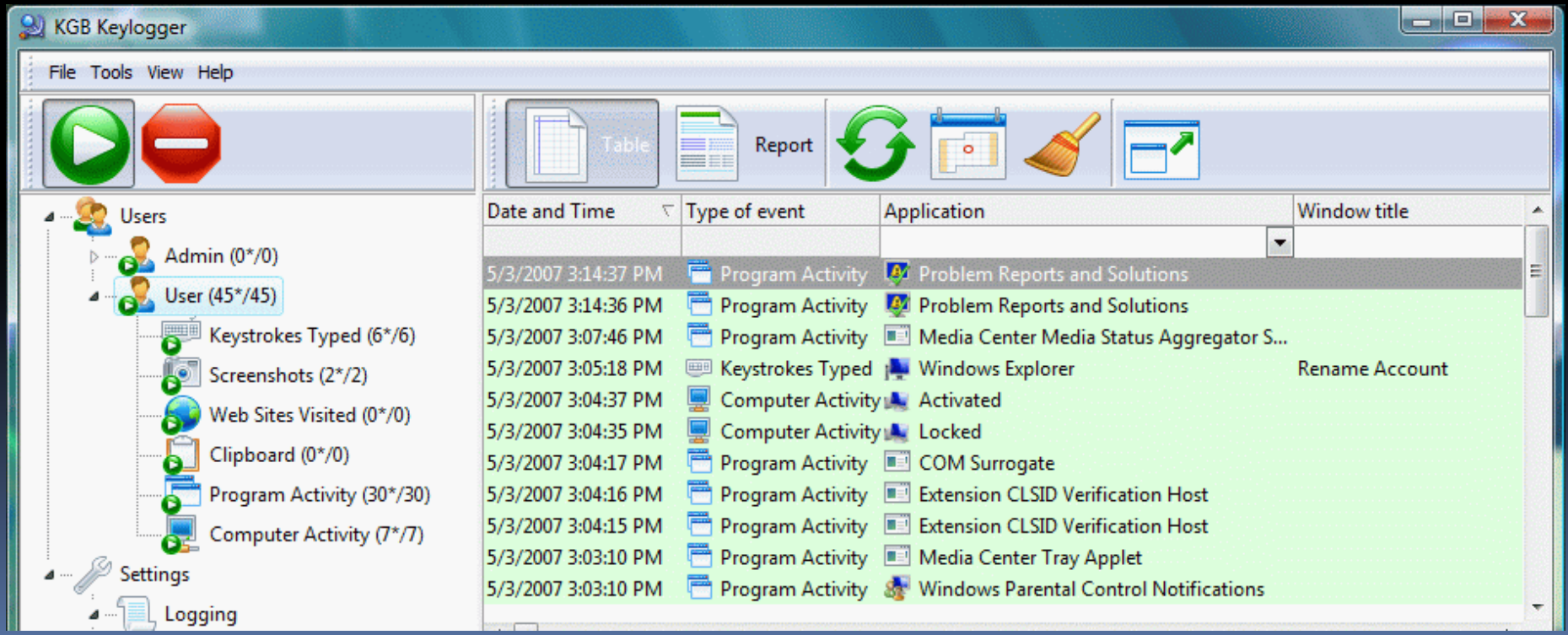
Oszustwa internetowe

Podobny efekt można również osiągnąć poprzez atak na Twój komputer i modyfikację Twojej przeglądarki (pliku na twardym dysku związanego z przekształcaniem nazw domen na adresy IP), np. za pomocą złośliwego oprogramowania.



Inne sposoby kradzieży i oszustw

Twoje poufne dane osobiste mogą zostać ujawnione oszustom na wiele innych sposobów. Przykładowo oszust może poznać Twoje dane (nr klienta i hasło dostępu na strony banku internetowego) poprzez obserwację Ciebie, gdy logujesz się w nieodpowiednim miejscu. Innym sposobem może być zainstalowanie na komputerze przez oszusta złośliwego programu, np. tzw. **keyloggera**, który będzie rejestrował znaki wprowadzane przez Ciebie z klawiatury.



Inne sposoby kradzieży i oszustw

Skimming

Przestępcy uprawiający ten proceder działają zawsze w podobny sposób. Miniaturowy skaner jest najczęściej nakładany na wlot służący do wprowadzania karty do bankomatu. Podczas wkładania karty do bankomatu pasek magnetyczny zostaje sczytany i zapisany. Kod PIN przestępcy poznają dzięki miniaturowej kamerze, która rejestruje jego wprowadzenie.

Dane z kamery i czytnika są przekazywane drogą radiową do znajdującego się w pobliżu samochodu przestępców, gdzie są zapisywane na przenośnym komputerze.

Inne sposoby kradzieży i oszustw

Skimming

Alternatywną metodą poznania kodu PIN jest nałożenie na oryginalną klawiaturę bankomatu jej dokładnie wykonanej kopii.

Klient wpisuje PIN nie na klawiaturze oryginalnej, lecz na kopii, która zapamiętuje wprowadzony kod.

Nakładka jest wykonana w taki sposób, że naciskając jej przyciski jednocześnie naciskane są oryginalne klawisze maszyny, w związku z tym klient nie dostrzega jakiejkolwiek różnicy w funkcjonowaniu bankomatu.

Inne sposoby kradzieży i oszustw

Skimming

Równie groźne jak skimming bankomatowy może stać się klonowanie kart w punkcie handlowym. Do tego przestępstwa wykorzystywane są miniaturowe skanery, sczytujące zawartość paska magnetycznego karty. Obecna technika pozwala na tworzenie skanerów tak małych, że w całości mogą zmieścić się w dłoni. Takie urządzenie może służyć do zeskanowania karty nawet na oczach nieświadomej niczego ofiary. Inną stosowana metodą jest umieszczenie skanera w blacie stołu tak, że pasek magnetyczny jest sczytywany podczas przesuwania kartą po stole. Ogólnoświatowa tendencja wskazuje, że przestępcy kopiujący karty stają się coraz bardziej zuchwali.

Inne sposoby kradzieży i oszustw

9 zasad bezpiecznego korzystania z kart:

O ile to możliwe, korzystaj ze znanych Ci bankomatów. Będzie Ci wtedy łatwiej zauważyć ewentualne zmiany, jakie zaszły w wyglądzie urządzania. Jeśli zauważysz podejrzane zmiany, informuj bank lub Policję.

Dokładnie sprawdzaj, czy do bankomatu nie są dołączone od zewnątrz żadne urządzenia. Jeśli zauważysz podejrzanie wyglądający element, zrezygnuj w wypłaty i zgłoś swoje obawy do banku.

Dokładnie przyglądaj się otoczeniu bankomatu, jeśli zobaczysz coś podejrzanego, zrezygnuj z wypłaty.

Nigdy nie korzystaj przy bankomacie z pomocy nieznanych Ci osób.

Inne sposoby kradzieży i oszustw

9 zasad bezpiecznego korzystania z kart:

Kiedy wprowadzasz kod PIN, zawsze zasłaniaj klawiaturę ręką, i to w taki sposób by nie można go było podejrzeć z żadnej strony. Naucz się wprowadzać PIN automatycznie, bez patrzenia na klawisze numeryczne. Jest wielce prawdopodobne, że jeśli Ty widzisz wprowadzany przez siebie PIN, mogą go też zobaczyć przestępcy.

Kiedy płacisz kartą w sklepie, nigdy nie trać jej z oczu.

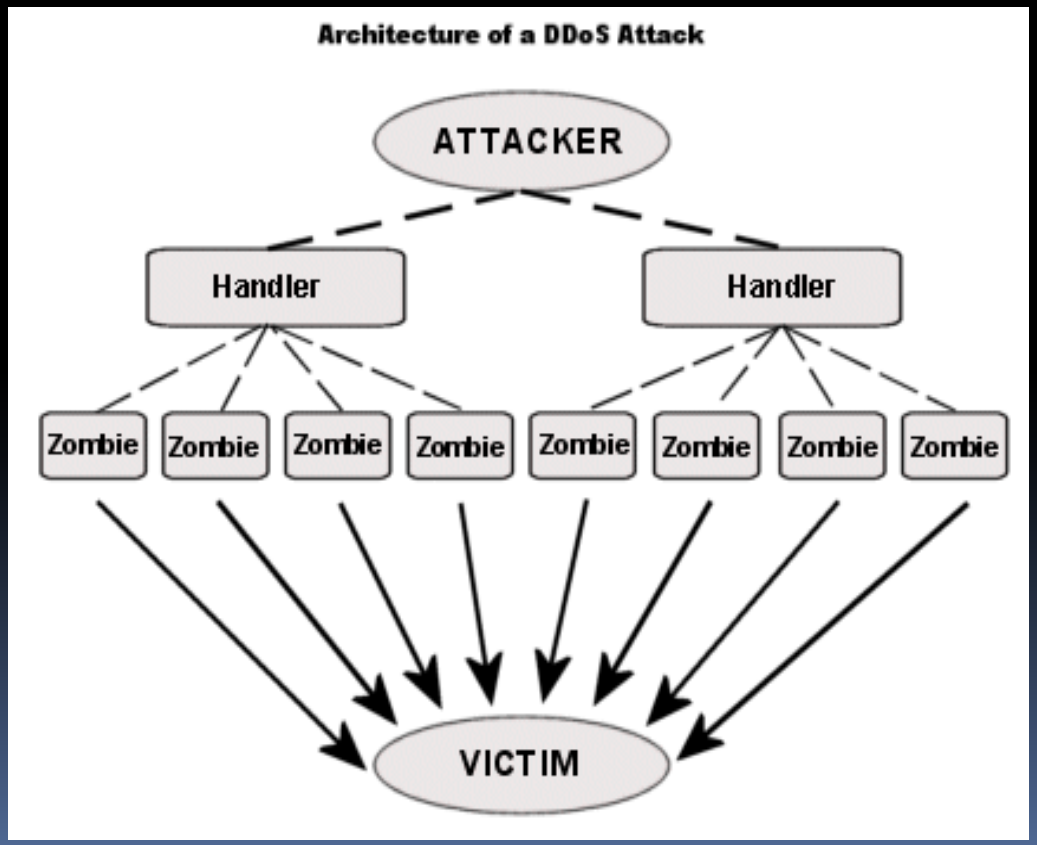
Jeśli dla potwierdzenia transakcji w sklepie musisz wprowadzić PIN, zrób to tak, by nikt, łącznie z Tobą, nie widział wpisywanego kodu.

Zwracaj uwagę na to, co sprzedawca robi z Twoja kartą. Powinien przejechać jej paskiem magnetycznym przez czytnik w terminalu POS. Później nie powinien już wprowadzać ani zbliżać karty do innych urządzeń.

Kontroluj na bieżąco stan swojego konta, jeśli zauważysz transakcje, których nie dokonałeś, natychmiast informuj o tym bank i zastrzeż swoją kartę.

Ataki techniczne

DoS (Denial of Service) to typ ataku sieciowego, który polega na wysłaniu do zaatakowanego systemu (komputera) tak dużej ilości danych, że zaatakowany komputer nie jest w stanie nadążyć z ich obsługą. W wyniku ataku komputer może znacznie spowolnić swoje działanie, lub zawiesić się. Celem ataku może być również całe łącze zaatakowanego użytkownika, które może ulec przepełnieniu pakietami - śmieciami. Najczęściej ataki tego typu powstają na skutek manipulacji protokołami sieciowymi, które umożliwiają zalew (ang. floods) pakietami zaatakowanego komputera. Przykłady tego typu ataków to m. in. ICMP flooding, SYN flooding. Atak DoS, w którym bierze udział duża liczba komputerów (atakujących), nad którymi wcześniej przejęto kontrolę, nazywany jest rozproszonym atakiem **DDoS** (Distributed Denial of Service).



Ataki techniczne

Spoofing (ang. spoof – naciąganie, szachrajstwo) – technika ataków internetowych opierająca się na umieszczaniu w sieci preparowanych, modyfikowanych lub uszkodzonych pakietów danych.
Najpopularniejsze techniki oparte na spoofingu to:

- IP spoofing,
- ARP Spoofing,
- E-mail spoofing.

Ataki techniczne

IP Spoofing - termin określający fałszowanie źródłowego adresu IP w wysyłanym przez komputer pakiecie sieciowym. Takie działanie może służyć ukryciu tożsamości atakującego (np. w przypadku ataków DoS), podszyciu się pod innego użytkownika sieci i ingerowanie w jego aktywność sieciową lub wykorzystaniu uprawnień posiadanych przez inny adres (atak wykorzystany przez Kevina Mitnicka w celu dostania się do komputera Tsutomu Shimomury).

Ataki techniczne

ARP spoofing to atak sieciowy w sieci Ethernet pozwalający atakującemu przechwytywać dane przesyłane w obrębie segmentu sieci lokalnej. Przeprowadzony tą metodą atak polega na rozsyłaniu w sieci LAN odpowiednio spreparowanych pakietów ARP zawierających fałszywe adresy MAC. W efekcie pakiety danych wysyłane przez inne komputery w sieci zamiast do adresata trafiają do osoby atakującej pozwalając jej na podsłuchiwanie komunikacji.

Ataki techniczne

E-mail spoofing to fałszerstwo nagłówka e-mail w taki sposób, że wiadomość wydaje się pochodzić od innego nadawcy niż w rzeczywistości.

Ataki techniczne

Atak na serwer poczty — to kolejny rodzaj hakerskiej działalności. Jego konsekwencją jest utrata kontroli nad przepływającą korespondencją (e-maile kierowane do konkretnej osoby mogą zostać odczytane i dostać się w posiadanie niepowołanych osób, możliwe jest także fałszowanie korespondencji i wprowadzenie w firmiedezorganizacji pracy). Ulubionymi przez hakerów sposobami atakowania są *ataki na* serwer główny, które prowadzą do utraty kontroli nad całą siecią, wiążą się z utratą wszystkich danych, z zakłóceniami pracy dowolnych usług sieciowych w całej firmie. Po przejęciu kontroli nad głównym serwerem możliwe jest przechwytywanie danych wędrujących wewnątrz sieci, a co za tym idzie — poznanie struktury wewnętrznejfirmy. Możliwe jest fałszowanie danych przesyłanych siecią, blokowanie wiadomości przesyłanych między szefem a współpracownikami.

Ataki techniczne

Hijacking — to metoda polegająca na przechwytywaniu transmisji odbywającej się między dwoma systemami. Dzięki niej możliwe jest przechwycenie dostępu do szczególnie chronionych programów. Ze względu na wysoki stopień skomplikowania jest specjalnością elity hakerskiej.

Ataki techniczne

Aktywne rozsynchronizowanie — jest to atak polegający na aktywnym rozsynchronizowaniu. Polega na tym, że haker wymusza siłą lub podstępem rozsynchronizowanie dwóch końców połączenia TCP, w efekcie czego komputery nie mogą wymieniać danych. Następnie, używając trzeciego komputera głównego (przyłączonego do fizycznego łącza przesyłającego pakiety TCP), włamywacz przechwytuje rzeczywiste pakiety i tworzy ich zamienniki, akceptowane przez oba połączone ze sobą komputery. Pakiety wygenerowane przez trzeci komputer zastępują pakiety oryginalne, które byłyby wymienione przez połączone systemy.

Ataki techniczne

Przechwycenie sesji — to rodzaj ataku, który prawdopodobnie jest największym zagrożeniem dla serwerów przyłączonych do Internetu. Czasem bywa on nazywany „aktywnym węszeniem" (w odróżnieniu od omawianego wcześniej „węszenia biernego"). Chociaż sposób ten przypomina nieco podsyłanie numerów sekwencji TCP, jest groźniejszy, gdyż w tym wypadku haker zamiast odszyfrowywać adresy IP, uzyskuje dostęp do sieci i wymusza akceptację swojego adresu IP jako adresu sieciowego. Idea polega na tym, że włamywacz przejmuje kontrolę nad komputerem łączącym go z siecią, a następnie odłącza ten komputer i „oszukuje" serwer, podając się za legalnego użytkownika. Przechwytywanie w protokole TCP stanowi większe niebezpieczeństwo niż podszywanie się pod IP, ponieważ po udanym przechwyceniu haker ma na ogół dużo większy dostęp do systemu.

Ataki techniczne

Sniffing (podsłuchiwanie pakietów) — jest to metoda zdobywania systemu polegająca na przechowywaniu przesyłanych przez sieć niezaszyfrowanych informacji. Można w ten sposób zdobyć hasło użytkownika i uzyskać dostęp do danego konta.

Złośliwe oprogramowanie

Wirus komputerowy to złośliwy program (zazwyczaj niewielki, często fragment kodu) ukryty wewnątrz innego programu czy pliku (jako jego nosiciela), którego zadaniem jest powielanie się (rozprzestrzenianie) w jak największej ilości kopii.

Powielanie następuje w momencie uruchamiania zainfekowanego programu czy pliku, bez wiedzy i zgody użytkownika.

Programy tego typu na ogół posiadają również funkcje destrukcyjne oraz innego typu złośliwe zaplanowane funkcje (np. uprzykrzające, czy nawet uniemożliwiające użytkownikowi korzystanie z komputera).

Złośliwe oprogramowanie

Rodzaje wirusów i sposoby ich rozpowszechniania się

Istnieje bardzo wiele różnych rodzajów wirusów oraz sposobów ich działania i rozpowszechniania się. Chociażby w zależności od sposobu rozprzestrzeniania się i infekcji czy w zależności od skutków jakie wywołują, czyli te groźniejsze i mniej niebezpieczne.

Złośliwe programy często mają postać mieszaną, czyli łączą w sobie kilka różnych funkcji (tzw. hybrydowe), np. mogą rozpowszechniać się jak robak i zawierać funkcje trojana oraz infekować na różne sposoby.

Złośliwe oprogramowanie

Rodzaje wirusów i sposoby ich rozpowszechniania się

Należy tu przede wszystkim pamiętać, że mówiąc o wirusach mamy na myśli również wiele innych rodzajów złośliwego oprogramowania poza klasycznym wirusem, takie jak:robaki, konie trojańskie i inne, które powszechnie nazywane są wirusami.

Wirus w tradycyjnym rozumieniu rozprzestrzenia się za pomocą nosiciela jakim jest inny program czy plik, natomiast w przypadku robaków odbywa się to w sposób zautomatyzowany z wykorzystaniem własnych mechanizmów rozprzestrzeniania się.

Złośliwe oprogramowanie

Rodzaje wirusów i sposoby ich rozpowszechniania się

Zwykle rozprzestrzenianie się następuje poprzez sieć z wykorzystaniem poczty elektronicznej i słabości (luk) systemów.

Obecnie poza pocztą elektroniczną najczęstszą drogą rozprzestrzeniania się wirusów i innych złośliwych programów są strony internetowe.

Złośliwe oprogramowanie

W jaki sposób może zostać zainfekowany komputer wirusem?
Komputer może zostać zainfekowany złośliwym programem przede wszystkim poprzez:

- **bezpośrednie (ręczne) uruchomienie zainfekowanego programu lub pliku** w momencie, gdy m. in.:

  klikasz na podejrzany link, który prowadzi do zainfekowanego programu i w ten sposób uruchamiasz go (np. na stronie internetowej, w otrzymanej wiadomości e-mail, czy otrzymany poprzez komunikator internetowy) czy klikasz na **podejrzany komunikat** (np. pojawiający się podczas przeglądania stron internetowych)

Złośliwe oprogramowanie

W jaki sposób może zostać zainfekowany komputer wirusem?

otwierasz zainfekowany plik, zwłaszcza nieznanego pochodzenia (np. ściągnięty poprzez sieć wymiany plików peer-to-peer) lub **załącznik** (np. otrzymany pocztą elektroniczną, w szczególności, gdy jest nieznanego źródła), czy nawet otwierasz **podejrzaną stronę internetową** (poprzez luki w systemie lub oprogramowaniu, np. przeglądarce internetowej). W przypadku stron internetowych największe ryzyko zainstalowania złośliwego oprogramowania jest, gdy odwiedzasz serwisy, które np. rozpowszechniają nielegalne oprogramowanie, czy treści erotyczne. Ale niestety może zdarzyć się, że strona poważnej firmy jest podatna na atak, co może skutkować przejęcie jej przez przestępców i zmodyfikowanie w ten sposób (w jej kodzie osadzono niebezpieczne komponenty), aby infekowały komputery odwiedzających je internautów złośliwym kodem

Złośliwe oprogramowanie

W jaki sposób może zostać zainfekowany komputer wirusem?

uruchamiasz zainfekowany program, zwłaszcza niewiadomego pochodzenia, np. ściągnięty bezpośrednio z internetu na komputer czy nawet skopiowany na płytę CD, czy inny nośnik danych

Wiadomości nakłaniające do otwarcia zainfekowanego pliku czy kliknięcia na odnośnik prowadzący do zainfekowanego kodu mogą być również pod pozorem zainstalowania najnowszych aktualizacji oprogramowania czy zapoznania się z nowymi zagrożeniami, np. o nowym groźnym wirusie (są to tzw. fałszywe ostrzeżenia).

- **automatyczne wykorzystanie słabości systemowych** (luk) przez złośliwy program, np. w przypadku rozprzestrzeniania się robaków internetowych

Złośliwe oprogramowanie

Skutki zainfekowania komputera wirusem, czyli niebezpieczeństwo z nimi związane

Wirusy i inne złośliwe programy to jedne z najbardziej groźnych i najpowszechniejszych zagrożeń internetowych. Skutki działań wirusa mogą być różne, zależne przede wszystkim od jego typu i przeznaczenia. Zainfekowanie komputera wirusem czy innym złośliwym programem może powodować m. in.:

Złośliwe oprogramowanie

Skutki zainfekowania komputera wirusem, czyli niebezpieczeństwo z nimi związane

- **wyświetlanie rożnych złośliwych napisów czy komunikatów na ekranie**
- **uszkadzanie bądź kasowanie danych**
- **spowalnianie pracy komputera czy obciążanie sieci** (w tym łącza internetowego)
- **utrudnianie lub uniemożliwianie pracy na komputerze** (np. nie możesz uruchomić niektórych programów)
- **blokowanie urządzeń** (np. klawiatury)**, unieruchamianie komputera czy nawet fizyczne uszkodzenie komputera** (np. poprzez ciągłe włączanie i wyłączanie jakiegoś urządzenia)

Złośliwe oprogramowanie

Skutki zainfekowania komputera wirusem, czyli niebezpieczeństwo z nimi związane

Ponadto, skutkiem zainfekowania komputera wirusem czy innym złośliwym programem może być umożliwienie przejęcia nad nim kontroli (włamanie) osobie nieupoważnionej i wykorzystanie go do nieuprawnionych działań (np. hostowania podrobionej strony tzw. phishingu, rozsyłania spamu), kradzież poufnych informacji (np. hasła, nr kart płatniczych, dane osobowe) itp.

Złośliwe oprogramowanie

Robak komputerowy (internetowy) swoim działaniem przypomina wirusa komputerowego, jednakże do powielania się wykorzystuje on przede wszystkim sieć. Do zainfekowania kolejnych komputerów robaki wykorzystują bądź znane błędy (luki) w oprogramowaniu systemu lub aplikacji, bądź nieostrożność czy niewiedzę samych użytkowników. Robak po zarażeniu danego komputera usiłuje wysłać swoją kopię w e-mailu z zainfekowanym załącznikiem lub próbuje połączyć się bezpośrednio z innymi komputerami. Dodatkową cechą robaka może być zawarty w nim mechanizm konia trojańskiego lub inne cechy utrudniające użytkownikowi korzystanie z komputera. Obecnie granica pomiędzy wirusami i robakami komputerowymi zaciera się i bardzo często nie można danego programu sklasyfikować jednoznacznie.

Złośliwe oprogramowanie

Programy szpiegujące (określane często jako **spyware**, ale też jako programy wywiadowcze czy inwigilacyjne) to programy, których zadaniem jest, jak sama nazwa wskazuje, szpiegowaniei działań użytkownika komputera, na którym zostały zainstalowane. Szkodliwe i niechciane programy tego typu, bez zgody i wiedzy użytkownika zbierają informacje o nim i jego aktywności podczas pracy z komputerem i przekazują je swoim autorom lub innej nieuprawnionej osobie. Do zbieranych informacji należeć mogą m. in. adresy stron internetowych odwiedzanych przez użytkownika, adresy e-mail, dane o komputerze, hasła, numery kart kredytowych, dane osobowe.

Złośliwe oprogramowanie

Na podstawie zbieranych danych (lub aby zebrać dane), programy tego typu czasami mogą wyświetlać reklamy (patrz: adware) czy powodować inne zaplanowane szkodliwe funkcje (np. zmiana konfiguracji przeglądarki, aby wymuszać przeglądanie określonych witryn). Terminem spyware zazwyczaj określane są również inne niechciane programy, które realizują podobne funkcje, czyli monitorowania działań użytkownika na komputerze (bez jego wiedzy i zgody) i/lub inne funkcje powiązane z tymi działaniami. Do takich programów należą m. in. adware, trojany, keyloggery, monitory systemu. Tego typu oprogramowanie zaliczane jest do tzw. oprogramowania przestępczego (crimeware), czyli takiego, które jest używane z zamiarem popełnienia przestępstwa w sieci (np. kradzież tożsamości).

Złośliwe oprogramowanie

Koń trojański (trojan) jest to program, który umożliwia zdalne przejęcie pełnej kontroli nad danym komputerem. Instalacja może nastąpić bez wiedzy użytkownika poprzez wykorzystanie luk w bezpieczeństwie systemu lub przy użyciu metod socjotechnicznych (np. poprzez uruchomienie niewinnie wyglądającego programu przez niczego niepodejrzewającego użytkownika). Koń trojański może być "zaszyty" w dowolnych aplikacjach pochodzących z niezaufanych stron internetowych, wygaszaczach ekranu, czy nawet specjalnie spreparowanych plikach (.jpg).

Złośliwe oprogramowanie

Koń trojański po zainstalowaniu na zaatakowanym komputerze oczekuje na instrukcje od intruza. Konie trojańskie mogą być wyposażone w wiele różnych funkcji. Oprócz możliwości zdalnego wykonywania komend, można podsłuchiwać komunikację ofiary z innymi komputerami, przechwytywać hasła użytkownika, przejąć sterowanie urządzeniami komputera (klawiatura, mysz, CD-ROM, monitor). Programy takie umożliwiają również rozsyłanie spamu.

Złośliwe oprogramowanie

Adware (określane często jako programy reklamowe) to program, którego funkcją jest wyświetlanie reklam, zwykle w postaci banerów reklamowych czy wyskakujących okienek. Niestety, programy tego typu często instalowane są na komputerze bez zgody i wiedzy jego użytkownika, często są również łączone z innymi złośliwymi i niechcianymi programami, np. programami szpiegującymi (w tym przypadku, zwykle tego typu program zbiera informacje o użytkowniku komputera, na którym jest zainstalowany i na tej podstawie wyświetla mu reklamy).

Złośliwe oprogramowanie

Dialer to program komputerowy, który umożliwia łączenie się z internetem za pomocą modemu telefonicznego (połączenie dial-up), dlatego zwany jest również programem dostępowym. Program tego typu zazwyczaj realizuje połączenie do płatnych zasobów internetowych. Najczęściej jednak dialery utożsamia się ze złośliwymi programami, które bez wiedzy i zgody użytkownika instalują się na komputerze i realizują połączenie z krajowym lub zagranicznym numerem dostępowym o podwyższonej płatności.

Złośliwe oprogramowanie

W jaki sposób może zostać zainstalowany w Twoim komputerze niechciany dialer?

Niechciane dialery mogą zostać zainstalowane na naszym komputerze najczęściej gdy odwiedzasz strony internetowe o tematyce erotycznej, z nielegalnym oprogramowaniem, zazwyczaj poprzez wprowadzenie w błąd przez twórcę danego oprogramowania. Często trafiamy na odnośniki prowadzące do plików (.exe) o mylącej nazwie, np. pod pozorem ściągnięcia porcji zdjęć czy filmów, czy poprzez aktywne elementy strony internetowej (np. skrypty Active X) akceptując bez większego zastanowienia różne okienka (nawet przyciskając przycisk "nie" czy zamykając okienko), instalując w ten sposób złośliwy program.

Złośliwe oprogramowanie

Skutki działania niechcianych dialerów

Obecność niechcianego dialera na Twoim komputerze może powodować m. in.:

- otrzymanie rachunku telefonicznego opiewającego na bardzo wysoką kwotę
- brak dostępu do innych stron internetowych niż ta, na którą zaprogramowany jest dialer
- ustawienie strony startowej na zaprogramowaną w dialerze, nawet pomimo dokonania zmiany w ustawieniach przeglądarki
- pojawienie się nieznanej dotąd ikonki dialera, w prawym dolnym rogu ekranu (zasobnik systemowy)
- otwieranie dużych ilości tzw. pop up'ów (samoczynnie wyskakujących okienek), najczęściej z treściami dla dorosłych
- ustawienie połączenia domyślnego z numerem o podwyższonej płatności (np. 0700…)
- brak dostępu do zasobów sieci przy próbie połączenia za pomocą innego numeru dostępowego niż zaprogramowany przez dialer

Złośliwe oprogramowanie

Rootkit to program zmieniający działanie systemu operacyjnego poprzez m. in. ukrywanie procesów, plików czy połączeń sieciowych, które umożliwiają utrzymanie kontroli nad systemem. Rootkit infekuje jądro i usuwa ukrywane programy z listy procesów i plików zwracanych do programów. Zazwyczaj rootkity ukrywają inne złośliwe programy, takie jak trojany, spyware czy tylne furtki przed narzędziami zabezpieczającymi system. Rootkit może się dostać do komputera podobnie jak inne złośliwe programy (np. wraz trojanem).

Złośliwe oprogramowanie

Rootkity same w sobie nie stanowią zagrożenia, ale jednocześnie są to jedne z najgroźniejszych narzędzi hakierskich, bo służą do ukrywania w systemie plików, programów, procesów oraz samych siebie (mogą wykonywać różne niepożądane czynności, np. ukrywać złośliwą działalność trojanów) i w związku z tym bardzo trudno usunąć ich z zainfekowanego systemu.

Złośliwe oprogramowanie

Exploit to program, skrypt lub część kodu umożliwiająca zdalne (poprzez sieć) przejęcie kontroli na systemem (komputerem), wykorzystując dziury (luki) w programach i systemach operacyjnych. Exploity wykorzystują różne techniki ataku i luki. Jedną z najczęstszych technik ataku wykorzystywaną przez exploity jest przepełnienie bufora (ang. buffer overflow). Szczególnie groźne są exploity zero-day. Tak mówimy o atakach, które następują natychmiast po ogłoszeniu informacji o podatności na atak danego systemu (dla których producent nie przygotował jeszcze łaty).

Złośliwe oprogramowanie

Backdoor to (tylne drzwi, tylna furtka, tylne wejście) - luka w zabezpieczeniach systemu komputerowego utworzona umyślnie w celu późniejszego wykorzystania (zazwyczaj poprzez umieszczenie złośliwego programu). Backdoor jest zazwyczaj pozostawiany w systemie przez intruza, który włamał się poprzez inną lukę w oprogramowaniu. Może być umyślnie utworzony przez twórcę danego programu, czy poprzez uruchomienie trojana przez użytkownika. Wykryć i usunąć backdoor'a można w wielu przypadkach (zazwyczaj tych bardziej znanych) programem antywirusowym

Złośliwe oprogramowanie

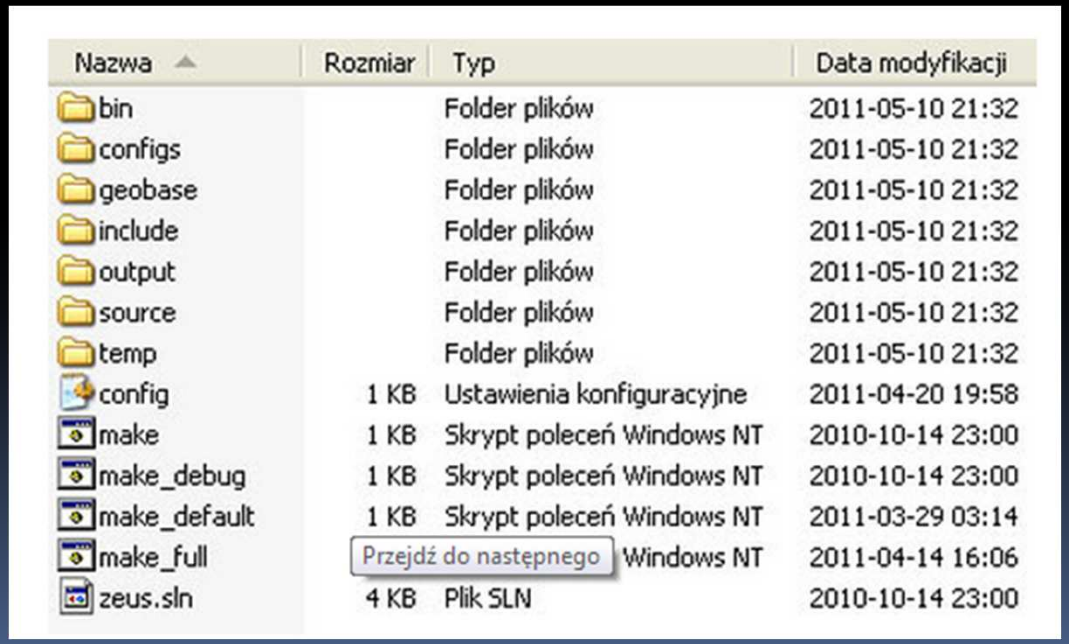
Złośliwe oprogramowanie (ang. malicious software - malware) to również narzędzia spamerskie i wszelkiego rodzaju inne narzędzia hakerskie, które służą do działań szkodliwych, przestępczych i zazwyczaj przydatnych w przynoszeniu korzyści finansowych osobom niepowołanym (czyli zazwyczaj napisane w celu osiągnięcia przez jego twórcę wymiernych korzyści finansowych). Oprogramowanie używane z zamiarem popełnienia przestępstwa w sieci (np kradzież tożsamości) nazywane jest często jako oprogramowanie przestępcze (tzw. crimeware).

8 najbardziej spektakularnych ataków hakerskich

Ten incydent pokazuje, że ofiarą ataku elektronicznego może paść nawet całe państwo. Stuxnet to wirus, który zakłóca pracę komputerów przemysłowych. Rząd Iranu oficjalnie przyznał, że atak na sieć teleinformatyczną kraju opóźnił między innymi uruchomienie elektrowni atomowej oraz że zainfekowanych zostało prawie 60 procent komputerów w kraju.
Po przeanalizowaniu kodu Stuxnetu podejrzenie o jego stworzenie padło na Jednostkę 8200, czyli wywiad elektroniczny izraelskiej armii (wroga Iranu).

8 najbardziej spektakularnych ataków hakerskich

Według raportu FBI w okresie od marca 2010 do kwietnia 2011 roku z amerykańskich banków i firm ukradziono ponad 20 milionów dolarów (z czego odzyskano 9). Do kradzieży były wykorzystywane między innymi robaki ZeuS i SpyBot. Wszystkie pieniądze trafiały na konta firm zarejestrowanych w jednej z chińskich prowincji. Po przelaniu pieniędzy szkodniki kasowały twarde dyski zainfekowanych komputerów. Kod źródłowy Zeusa od niedawna może ściągnąć każdy.



8 najbardziej spektakularnych ataków hakerskich

W odwecie za pozwanie hakera Geohota, który złamał zabezpieczenia konsoli PlayStation 3, z serwerów Sony wyciekły dane ponad 100 milionów użytkowników, nawet kilka milionów numerów kart kredytowych oraz plany sieci korporacyjnej. Sieć PlayStation Network (PSN) nie działała przez ponad miesiąc.

8 najbardziej spektakularnych ataków hakerskich

Niemieckiemu operatorowi telekomunikacyjnemu Deutsche Telekom ukradziono bazę zawierającą nazwiska, adresy, e-maile i numery telefonów klientów należącej do koncernu sieci T-Mobile. Firma przyznała się dopiero dwa lata później.

8 najbardziej spektakularnych ataków hakerskich

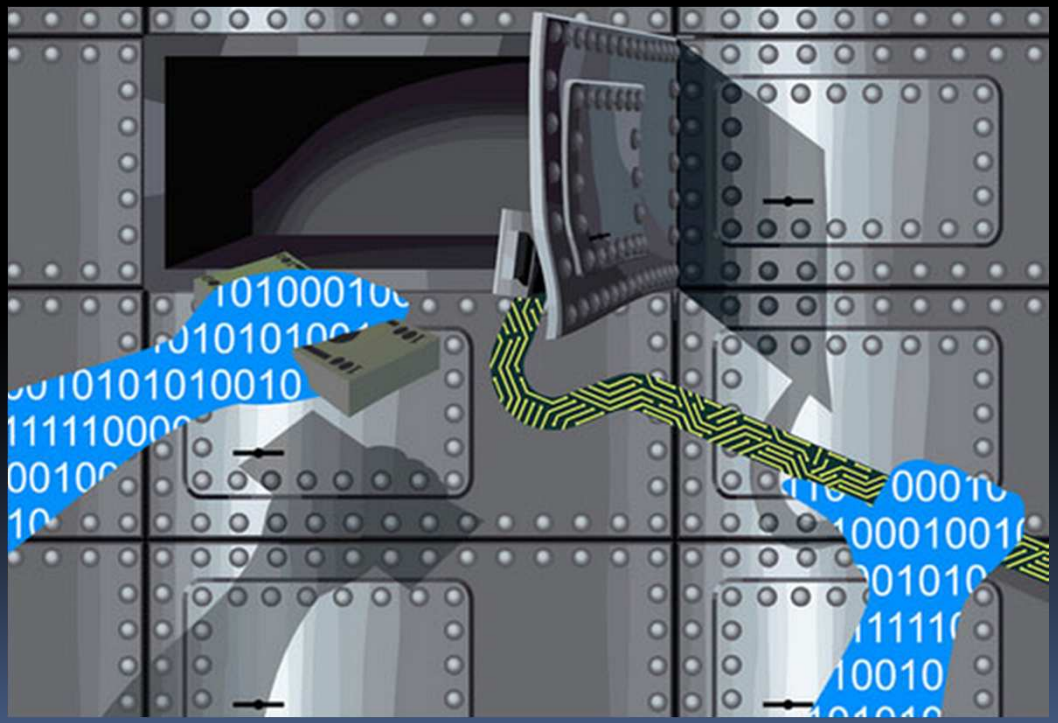
Strach pomyśleć, jakie skutki dla światowej gospodarki spowodowałoby sparaliżowanie systemu informatycznego Międzynarodowego Funduszu Walutowego (IMF). Na razie, "na szczęście", cyberprzestępcom udało się wykraść tylko e-maile i niezidentyfikowane dokumenty. Mówi się, że za atakiem może stać rząd jednego z "wrogich" krajów.

8 najbardziej spektakularnych ataków hakerskich

Demaskatorski portal Wikileaks po potężnym ataku DDoS znika z sieci tuż przed planowanym ujawnieniem depeszy wysyłanych przez ambasadorów USA. W odwecie za utrudnianie finansowania serwisu organizacja Anonimowi atakuje strony amerykańskich instytucji finansowych (PayPal, MasterCard, Visa, Bank of America).

8 najbardziej spektakularnych ataków hakerskich

O tym, jak cenne dla przestępców są nasze dane, świadczy atak na firmę Epsilon, która zajmuje się dostarczaniem marketingowych baz danych takim gigantom, jak Citibank, Visa czy Disney. Z serwerów Epsilona wyciekło "tylko" dwa procent bazy, co w wypadku tej firmy daje i tak gigantyczny wynik.



8 najbardziej spektakularnych ataków hakerskich

Grupa hakerów pod nazwą LulzSec zaatakowała kilkanaście serwisów. Włamano się między innymi na serwery amerykańskiego senatu i wywiadu CIA oraz zablokowano telefony w centrali FBI.

Zagrożenia związane z siecią bezprzewodową (WiFi)

Niebezpieczeństwo włamania, podsłuchu czy wykradnięcia danych wzrasta w przypadku sieci bezprzewodowej, gdyż medium transmisyjnym są fale radiowe (powietrze). Nieograniczony dostęp do medium transmisyjnego ma wpływ na poziom bezpieczeństwa zarówno infrastruktury sieciowej narażonej na nieautoryzowane wykorzystanie, jak i przesyłanych danych ulegających naruszeniu czy utracie. Tak więc, ataki na sieć bezprzewodową zazwyczaj mają dwa cele.

Zagrożenia związane z siecią bezprzewodową (WiFi)

Po pierwsze atakujący szuka określonych danych lub chce wyrządzić szkodę (np. poprzez zainstalowanie wirusa), w drugim przypadku napastnikowi może chodzić o znalezienie niezabezpieczonej sieci WiFi z dostępem do internetu, aby wykorzystać ten dostęp na własne potrzeby. Poszukiwanie otwartych (niezabezpieczonych) bezprzewodowych sieci nazywane jest jako **wardriving**, a osoba, która to robi **wardriver**.

Zagrożenia związane z siecią bezprzewodową (WiFi)

Zagrożeniem przy korzystaniu z sieci WiFi może być również dodatkowy punkt dostępowy (tzw. Rouge Access Point, czyli stacja bazowa pod przykrywką) podstawiony przez włamywacza. Atakujący podszywając się pod punkt dostępowy może gromadzić wszelkie przekazywane dane. Umieszczanie w sieci dodatkowego urządzenia np. jako punkt dostępowy czy pomiędzy punktem dostępowym a klientem i przechwytywanie całego ruchu nazywane jest jako atak typu **man in the middle** a narzędzia do podsłuchiwania jako tzw. **sniffery**.

Zagrożenia związane z siecią bezprzewodową (WiFi)

Możliwość łatwego dostępu do zasobów sieci bezprzewodowej, która nie jest należycie zabezpieczona może prowadzić w dalszej konsekwencji do utraty osobistych danych, poprzez straty finansowe, aż po odpowiedzialność karną.