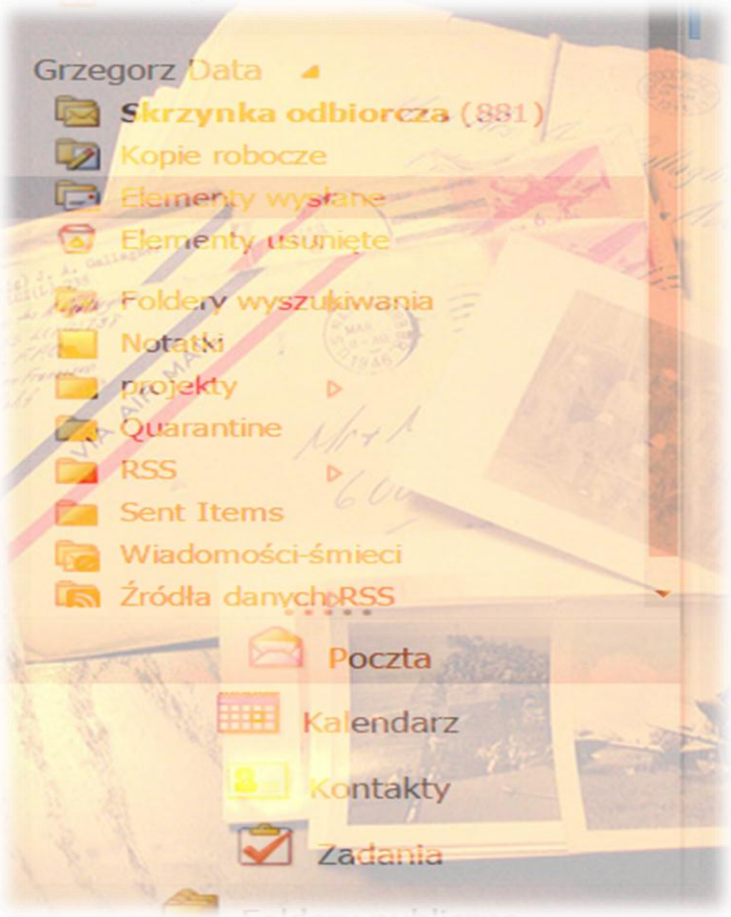
Okręgowy Inspektorat
Służby Więziennej
w Rzeszowie



BEZPIECZNA POCZTA ELEKTRONICZNA

Instrukcja bezpiecznego użytkowania służbowej poczty elektronicznej oraz wykrycia prób ataku socjotechnicznego

STRESZCZENIE

Poczta elektroniczna to podstawowa usługa internetowa, której używa się w Służbie Więziennej, Pełni wiele funkcji. Służy do komunikacji pomiędzy funkcjonariuszami i pracownikami SW oraz instytucjami i firmami zewnętrznymi, jest kanałem zdobywania informacji, E-mail stanowi również podstawową broń w arsenale cyberprzestępców – jest narzędziem do wysyłania spamu, wirusów oraz przeprowadzania ataków phishingowych. Bezpieczne korzystanie z poczty elektronicznej powinno być zatem podstawową umiejętnością każdego internauty. Ważną umiejętnością w dzisiejszych czasach jest również rozpoznanie ataku socjotechnicznego. W powszechnym, błędnym mniemaniu wielu osób przestępcy internetowi używają zaawansowanych narzędzi i technologii, aby włamać się do komputerów, na konta internetowe i urządzenia mobilne. Nic bardziej mylnego!. Cyberprzestępcy nauczyli się, że jednym z najprostszych sposobów, aby wykraść informacje lub włamać się na komputer jest po prostu oszukanie Ciebie.

kpt. Grzegorz Data
OISW w Rzeszowie

Zabezpieczenie komputera

Właściwe korzystanie z poczty elektronicznej wiąże się z umiejętnością zabezpieczenia komputera przed działaniami przestępców oraz eliminacji zagrożeń pochodzących z zewnątrz, do których należą:

- spam, czyli niezamawiane wiadomości zawierające m.in. reklamy różnych usług i produktów,
- złośliwe oprogramowanie, czyli wirusy, trojany, rootkity, scareware, ransomware przesyłane w postaci załączników do e-maili lub pobierane po kliknięciu na odnośnik zawarty w wiadomości pochodzącej od przestępcy,
- phishing, czyli atak, którego celem jest wyłudzenie poufnych danych użytkownika poczty e-mail.

ADWARE - DARMOWE PROGRAMY UŻYTKOWE, ZAWIERAJĄCE FUNKCJĘ WYŚWIETLANIA REKLAM
BACKDOOR - PRZEJMUJE KONTROLĘ NAD ZAINFEKOWANYM KOMPUTEREM UMOŻLIWIAJĄC WYKONANIE NA NIM CZYNNOŚCI ADMINISTRACYJNYCH ŁĄCZNIE Z USUWANIEM I ZAPISEM DANYCH
KEYLOGGER - WYSTĘPUJE W DWÓCH POSTACIACH: PROGRAMOWEJ I SPRZĘTOWEJ. ODCZYTUJE I ZAPISUJE WSZYSTKIE NACIŚNIĘCIA KLAWISZY UŻYTKOWNIKA. DZIĘKI TEMU ADRESY, KODY, CENNE INFORMACJE MOGĄ DOSTAĆ SIĘ W NIEPOWOŁANE RĘCE
RANSOMWARE (ANG. RANSOM – OKUP) –POLEGA NA WNIKNIĘCIU DO WNĘTRZA ATAKOWANEGO KOMPUTERA I PRÓBIE WYŁUDZENIA OKUPU I NP. ZASZYFROWANIU DANYCH NALEŻĄCYCH DO UŻYTKOWNIKA. ODSZYFROWANIE DANYCH MOŻLIWE JEST PO ZAPŁACENIU OKUPU
SPYWARE - OPROGRAMOWANIE ZBIERAJĄCE INFORMACJE O OSOBIE FIZYCZNEJ LUB PRAWNEJ BEZ JEJ ZGODY.
ROOTKIT - JEDNO Z NAJNIEBEZPIECZNIEJSZYCH NARZĘDZI HAKERSKICH. W NAJNOWSZYCH WERSJACH POTRAFI ZAGNIEŹDZIĆ FLASH BIOS-U PŁYTY GŁÓWNEJ. W TAKIM WYPADKU NIE USUNIE GO Z KOMPUTERA NAWET CAŁKOWITE FORMATOWANIE DYSKU TWARDEGO.
STEALWARE/PARASITEWARE - PROGRAMY „ZŁODZIEJSKIE" DO OKRADANIA PŁACĄCYCH ZA POŚREDNICTWEM INTERNETUPODMIENIAJĄCE STRONĘ BANKU ALBO ZMIENIAJĄCE NUMER KONTA BANKOWEGO
WIRUS - PROGRAM LUB FRAGMENT WROGIEGO WYKONALNEGO KODU, KTÓRY DOŁĄCZA SIĘ, NADPISUJE LUB ZAMIENIA INNY PROGRAM W CELU REPRODUKCJI SAMEGO SIEBIE BEZ ZGODY UŻYTKOWNIKA

Przede wszystkim upewnij się, że Twój system operacyjny jest zabezpieczony programem antywirusowym. Pracujący służbowy program antywirusowy McAfee sygnalizowany jest ikonką w prawym dolnym rogu 

Umiejętność samodzielnego rozpoznawania zagrożeń

Bezpieczne korzystanie z poczty e-mail to również umiejętność rozpoznawania zagrożeń, które nie zostały wychwycone przez filtr antyspamowy lub program antywirusowy. Nie zdarza się to często, ale pamiętaj, że przestępcy zawsze są o jeden krok do przodu przed twórcami zabezpieczeń.
Przeglądając wiadomości w skrzynce e-mail, wyrób w sobie nawyk odpowiadania na kilka prostych pytań opracowanych przez ekspertów ds. bezpieczeństwa z organizacji CERT. Celem tych pytań jest pomoc w identyfikacji niebezpiecznych e-maili.

1. **Czy znasz nadawcę wiadomości?**
2. **Czy otrzymywałeś już inne wiadomości od tego nadawcy?**
3. **Czy spodziewałeś się otrzymać tę wiadomość?**
4. **Czy tytuł wiadomości i nazwa załącznika mają sens?**
5. **Czy wiadomość nie zawiera złośliwego oprogramowania – jaki jest wynik skanowania antywirusowego?**

Pozytywne odpowiedzi na powyższe pytania zwiększą prawdopodobieństwo, że dana wiadomość nie będzie stanowiła zagrożenia dla Twojego systemu.

Negatywna odpowiedź na przynajmniej jedno z pytań powinna wzbudzić Twoją czujność i zachęcić do podjęcia działań, które zabezpieczą Cię przed atakiem, takich jak rezygnacja z odpowiedzi na wiadomość, nieklikanie w odnośniki umieszczone w e-mailu lub skasowanie wiadomości bez jej otwierania.

Wiedza i zdrowy rozsądek

Samo oprogramowanie i znajomość zasad bezpiecznego korzystania z poczty e-mail nie gwarantują jednak pełnego bezpieczeństwa. Konieczne jest także kierowanie się zdrowym rozsądkiem oraz - w zależności od rozwoju sytuacji - podejmowanie odpowiednich działań przez użytkownika poczty elektronicznej.

UŻYJ ZDROWEGO ROZSĄDKU. JEŚLI TREŚĆ WIADOMOŚCI E-MAIL JEST PODEJRZANA LUB ZBYT OBIECUJĄCA, NAJPRAWDOPODOBNIEJ JEST TO ATAK.

Phishing

Phishing to jeden z najpopularniejszych ataków opartych o wiadomości e-mail, ale także coraz częściej o wiadomości na portalach społecznościowych. Przestępcy internetowi próbują Cię oszukać i spowodować, abyś podjął działanie zgodnie z ich zamierzeniami. Atakujący bardzo skrupulatnie przygotowują treść takich wiadomości. Mogą udać, że mail pochodzi od kogoś kogo znasz, jak na przykład od kolegi lub firmy, której ufasz. Potrafią nawet podrobić logo banku lub wysłać wiadomość z podobnego adresu. Cyberprzestępcy wysyłają takie wiadomości do tysięcy, a nawet milionów odbiorców na całym świecie. Doskonale wiedzą, że im więcej takich wiadomości roześlą, tym więcej osób będą mogli oszukać. Ten sposób jest podobny do sposobu znanego z łowienia ryb: im większą masz sieć, tym więcej złowisz ryb. Ataki typu phishing mają najczęściej następujące cele:

PRZYKŁADY OSTATNICH MAILI

- FAKTURA ORANGE: DO SKRZYNEK TRAFIA WIADOMOŚĆ UDAJĄCA FAKTURĘ OD FIRMY ORANGE
- POTWIERDZENIE ODBIORU PACZKI INPOST - PRZESTĘPCY ROZSYŁAJĄ WIADOMOŚCI UDAJĄCE POWIADOMIENIA OD PACZKOMATÓW. WIADOMOŚĆ ZAWIERA ZŁOŚLIWY ZAŁĄCZNIK, INSTALUJĄCY NA KOMPUTERZE OFIARY KONIA TROJAŃSKIEGO. WIADOMOŚC WYGLĄDA JAK POWIADOMIENIE Z INPOSTU.
- BIOMIR ŚRODKI CZYSTOŚCI, FAKTURA ZA LISTOPAD
- PRÓBA DORĘCZENIA PRZESYŁKI DHL „KURIER W MOMENCIE DOSTARCZENIA ZAMÓWIENIA PRÓBOWAŁ ZADZWONIĆ POD NUMER TELEFONU PODANY W FAKTURZE, ALE NUMER NIE ODPOWIADAŁ…"
- PAŃSKIEJ FIRMIE PRYZNANY AUDYT – MAIL Z BŁĘDAMI STYLISTYCZNYMI ZAWIERAJĄCY INFORMACJĘ O AUDYCIE, KTÓRY MA SIĘ ODBYĆ W FIRMIE
- INFORMACJA O ZAMIARZE WSZCZĘCIA KONTROLI

Wyłudzanie informacji

Celem atakującego jest zmanipulowanie Cię tak, abyś kliknął na link, który zabierze Cię na stronę pytającą o login i hasło, Twój ulubiony kolor czy nazwisko panieńskie matki. Takie strony bliźniaczo przypominają na przykład znane strony banku, jednak są zaprojektowane tylko po to, żeby wykraść dane potrzebne do uzyskania dostępu do Twojego konta bankowego czy numer karty kredytowej.

Przejęcie kontroli nad komputerem poprzez złośliwy link

Tym razem celem atakującego jest zainfekowanie Twojego komputera. Aby to osiągnąć wysyłają do Ciebie wiadomość z linkiem. Po kliknięciu na taki link zostajesz przekierowany na stronę, która w tle przeprowadza atak na Twoją przeglądarkę internetową i kiedy atak ten się powiedzie, przestępca uzyskuje kontrolę na Twoim komputerem.

Przejęcie kontroli nad komputerem poprzez złośliwe załączniki

Złośliwe wiadomości mogą zawierać zainfekowane załączniki, takie jak pliki PDF , dokumenty Microsoft Office a ostatnio spakowane programem RAR lub ZIP rzekome faktury zabezpieczone hasłem (oprogramowanie antywirusowe nie może sprawdzić zaszyfrowanych załączników). Jeśli otworzysz taki załącznik, atakuje on Twój komputer i jeśli atak się powiedzie, przestępca uzyskuje nad nim kontrolę.

Scam

Niektóre maile to po prostu próby oszustwa, zastraszenia i kradzieży. Klasycznym przykładem są wiadomości informujące o wygranej w loterii, albo że jakaś ważna osobistość potrzebuje przelać miliony dolarów do Twojego kraju i chciałaby Ci zapłacić za pomoc w tym transferze. Następnie zostajesz poinformowany, że musisz zapłacić opłatę manipulacyjną zanim otrzymasz pieniądze. Kiedy zapłacisz, już nikt się nie odzywa i kontakt się urywa..

WIRUSY VBKLIP, BANATRIX. ZŁOŚLIWE OPROGRAMOWANIE PODMIENIA SKOPIOWANY PRZEZ UŻYTKOWNIKA NUMER KONTA BANKOWEGO I WKLEJA DO FORMULARZA NUMER KONTA ZŁODZIEJA. OFIARĄ WIRUSA PADŁO JUŻ 3000 UŻYTKOWNIKÓW. ZWYKLE ZAMIAST WPISYWAĆ CYFRA PO CYFRZE NUMER KONTA, NA JAKIE CHCEMY WYSŁAĆ PIENIĄDZE, KOPIUJEMY CAŁY CIĄG LICZB I WKLEJAMY GO DO ODPOWIEDNIEGO POLA W FORMULARZU. JEŻELI NASZ KOMPUTER JEST ZAINFEKOWANY WIRUSEM, SKOPIOWANY NUMER KONTA ZOSTANIE ZMIENIONY, A DO FORMULARZA WKLEI SIĘ NUMER KONTA BANKOWEGO ZŁODZIEJA. WYSTARCZY JUŻ TYLKO POTWIERDZIĆ TRANSAKCJĘ, ŻEBY PIENIĄDZE TRAFIŁY DO KOGOŚ INNEGO. PAMIĘTAJMY O TYM, ŻEBY NA SAMYM KOŃCU WERYFIKOWAĆ DANE PRZELEWU NA MONITORZE I POTWIERDZENIU OPERACJI NP. SMS'EM. WYSTARCZY SPRAWDZIĆ CZTERY OSTATNIE CYFRY. JEŚLI TAM SIĘ COŚ ZMIENIŁO, TO CAŁY NUMER RACHUNKU TEŻ JEST JUŻ INNY.

Jak się chronić

Zazwyczaj otwieranie wiadomości e-mail jest bezpieczne. W większości przypadków, aby atak się powiódł, to Ty musisz zrobić coś po przeczytaniu takiego e-maila. Poniżej znajduje się kilka wskazówek, jak rozpoznać, że otrzymana wiadomość to atak.

Bądź podejrzliwy jeśli jakikolwiek e-mail wymaga natychmiastowego działania lub powoduje wrażenie pilności. To znany trik, aby zmusić ludzi do szybkiego działania.

- Zachowaj ostrożność jeśli wiadomość zawiera załącznik, szczególnie jeśli nie spodziewałeś się takiej wiadomości. Przykładami są: lista płac, nieplanowane zwolnienia albo mail od urzędu skarbowego.
- Bądź podejrzliwy w stosunku do e-maili adresowanych podobnie jak „Dear Customer" / "Drogi Kliencie" lub w inny, bardzo ogólny sposób.
- E-mail wymaga podania szczególnie ważnych informacji jak numeru karty kredytowej czy haseł.
- Nadawca twierdzi, że jest z dużej organizacji, ale mail zawiera dużo błędów i jest wysłany z adresu @gmail.com, @yahoo.com, lub @hotmail.com, @wp.pl, @interia.pl.
- Jeśli link wydaje Ci się podejrzany, najedź na niego myszką (nie klikając). Wówczas ukaże się prawdziwy adres, pod który zaprowadziłby Cię ten odnośnik

jeśli byś na niego kliknął. Link, który widzisz w wiadomości może być zupełnie inny niż miejsce, do którego rzeczywiście prowadzi.

Dostajesz wiadomość od znajomego, ale jej ton lub zastosowane zwroty po prostu nie pasują do tej osoby. Jeśli masz podejrzenia, spytaj nadawcy czy się z Tobą kontaktował. Cyberprzestępcy mogą bardzo łatwo podrobić e-mail od znajomego bądź kolegi z pracy. Aby bezpiecznie korzystać z poczty elektronicznej, należy po prostu użyć zdrowego rozsądku. Jeśli coś wydaje się podejrzane lub zbyt obiecujące, to zapewne jest to atak. Dla zachowania bezpieczeństwa zgłoś otrzymanie takiej wiadomości bezpośredniemu przełożonemu lub służbie informatycznej.

Spear fishing

Chociaż zwykły phishing jest wciąż skuteczny, pojawił się nowy rodzaj ataku o nazwie spear phishing. Koncepcja jest taka sama: przestępcy wysyłają e-maile do swojej ofiary, udając znaną jej organizację lub zaufaną osobę. Jednak w przeciwieństwie do tradycyjnego phishingu, treść tych wiadomości jest wyraźnie ukierunkowana. Zamiast wysyłać e-maile do milionów potencjalnych ofiar, cyberprzestępcy wysyłają wiadomości spear phishingowe (czyli ukierunkowane od ang. sprear – włócznia, spearfishing łowienie kuszą) do nielicznych, wybranych osób. W przeciwieństwie do zwykłego phishingu, stosując phishing ukierunkowany atakujący przeprowadza wywiad środowiskowy potencjalnych ofiar. Zapoznaje się z treścią profilu na Facebooku lub wiadomościami jakie zostały zamieszczone na stronie służbowej czy w zamówieniach publicznych. Na podstawie takiego rozpoznania, przestępcy tworzą spersonalizowaną wiadomość e-mail, której treść wydaje się być zupełnie sensowna dla potencjalnego celu ataku. Takie działanie sprawia, że odbiorcy wiadomości łatwiej stają się ofiarami ataku.

Skuteczność spear phishingu

Spear phishing jest wykorzystywany kiedy cyberprzestępca chce przeprowadzić atak konkretnie na Ciebie lub na Służbę Więzienną . Inaczej niż w przypadku zwykłych przestępców chcących ukraść pieniądze, osoba wykorzystująca spear phishing ma bardzo konkretne cele. Zazwyczaj jest to uzyskanie dostępu do poufnych informacji służbowych. Może się też zdarzyć tak, że próby włamania do Twojej organizacji są jednym z etapów uzyskania dostępu do innej organizacji. Przestępcy stosujący takie techniki grają o dużą stawkę i są w stanie poświęcić czas i energię aby przeprowadzić wyczerpujące śledztwo przed atakiem. Sprawdzają dokładnie stronę internetową Służby Więziennej i wybierają sobie trzy kluczowe osoby. Następnie wnikliwe badają strony tych osób na, Twitterze i Facebooku aby stworzyć jak najobszerniejszy zbiór informacji o nich. Po przeanalizowaniu wszystkich zebranych informacji o tych wybranych osobach, atakujący przygotowują wiadomość e-mail podając się za dostawcę, z którym organizacja rzeczywiście współpracuje. E-mail zawiera załącznik udający fakturę, pismo służbowe lub opinię prawną które w rzeczywistości są zainfekowanym plikiem. Dwie z trzech osób, na które był ukierunkowany atak, dają się oszukać przez spear phishingowy e-mail i otwierają zainfekowany załącznik, dając tym samym przestępcom całkowity dostęp do swoich komputerów, a ostatecznie do wszystkich wiadomości.

SPEAR PHISHING SĄ ZNACZNIE BARDZIEJ NIEBEZPIECZNYM ZAGROŻENIEM PONIEWAŻ ATAKUJĄCY PRZEPROWADZAJĄ ATAK UKIERUNKOWANY KONKRETNIE NA CIEBIE I SŁUŻBĘ WIĘZIENNĄ

Ataki typu spear phishing są znacznie bardziej niebezpiecznym zagrożeniem niż proste ataki typu phishing, ponieważ atakujący przeprowadzają atak ukierunkowany konkretnie na Ciebie i Służbę. To znacznie zwiększa szanse na sukces atakujących. Te ataki są także o wiele trudniejsze do wykrycia

Jak się chronić

Pierwszym krokiem do ochrony siebie przed atakami ukierunkowanymi jest zrozumienie, że Ty też możesz stać się jego celem. Prawdopodobnie zarówno Ty, jak i Służba jesteście w posiadaniu poufnych informacji, na których mogłoby komuś zależeć albo takich, które mogłyby być wykorzystane do dostępu do innej organizacji, która mogłaby być ostatecznym celem ataku. Kiedy zdasz sobie sprawę, że Ty sam też możesz być celem, podejmij następujące środki ostrożności w celu ochrony siebie i swojej organizacji:

- Ogranicz informacje jakie o sobie umieszczasz w takich miejscach jak fora, Facebook czy LinkedIn. Im większą ilością danych się dzielisz, tym łatwiej atakującemu przygotować spear phishingowy e-mail, który będzie wydawał się sensowny i prawdziwy
- Jeśli otrzymasz podejrzaną wiadomość e-mail, w której ktoś prosi aby otworzyć załącznik, kliknąć w link albo żąda podania poufnych informacji, dobrze sprawdź wiadomość zanim wykonasz te czynności.
- Jeśli e-mail wydaje się pochodzić od firmy lub osoby którą znasz, skorzystaj ze swojej własnej książki adresowej, aby skontaktować się z nadawcą i sprawdzić czy to na pewno on wysłał tę wiadomość.
- Stosuj się do obowiązującej polityki bezpieczeństwa i korzystaj z dostępnych narzędzi zabezpieczających, takich jak programy antywirusowe, szyfrowanie i aktualizacje.
- Pamiętaj, że technologia nie jest w stanie wyłapać i zapobiec wszystkim atakom wykorzystującym e-mail, a zwłaszcza ukierunkowanym wiadomościom spear phishingowym. Jeśli na pierwszy rzut oka e-mail wydaje Ci się nieco dziwny, przeczytaj go bardzo uważnie. Jeśli masz najmniejszą obawę, że otrzymałeś właśnie e-mail z phishingiem lub jeśli padłeś ofiarą phishingu ukierunkowanego, natychmiast skontaktuj ze służbą informatyczną.

Socjotechnika

Socjotechnika (inaczej inżynieria społeczna) jest rodzajem ataku psychologicznego polegającym na tym, że atakujący nakłania swoją ofiarę do wykonania jakiejś czynności. Socjotechnika istnieje od tysięcy lat - oszustwa i naciągacze to przecież nic nowego. Jednak oszuści komputerowi doskonale wiedzą, że użycie tych technik w Internecie jest wyjątkowo skuteczne i może być stosowane na milionach osób. Najprostszym sposobem, aby zrozumieć, jak działa inżynieria społeczna, jest przyjrzenie się przykładom z życia.
Odbierasz telefon od kogoś podającego się za pracownika serwisu komputerowego, informatyka z innej jednostki albo wsparcie techniczne firmy, której oprogramowania używasz na służbowym komputerze. Rozmówca wyjaśnia, że zauważył, że Twój komputer zachowuje się dziwnie, np. skanuje Internet lub wysyła spam, i są przekonani, że jest on zainfekowany. Chce pomóc Ci przez zbadanie problemu i zabezpieczenie komputera. Następnie używając niezrozumiałych dla przeciętnego użytkownika terminów technicznych prowadzi Cię przez wiele skomplikowanych kroków, próbując stwierdzić, że Twój komputer jest zainfekowany. Przykładowo, może poprosić o sprawdzenie, czy masz pewne pliki na komputerze i pokaże Ci krok po kroku jak je znaleźć. Po zlokalizowaniu plików rozmówca będzie zapewniał, że pliki te są oznaką zainfekowania komputera, gdy w rzeczywistości są to popularne pliki systemowe znajdujące się na każdym komputerze.

Kiedy już wmówi Ci, że twój komputer jest zainfekowany, będzie Cię skłaniać do odwiedzenia danej strony lub poprosi o przyznanie zdalnego dostępu do komputera, aby mógł go naprawić. Należy pamiętać, że podobne ataki socjotechniczne nie ograniczają się do rozmów telefonicznych. Mogą zdarzyć się przy użyciu niemal każdej technologii, w tym ataków phishingowych poprzez e-mail, SMS, wiadomość na portalach społecznościowych jak Facebook czy Twitter lub czatach internetowych. Najważniejsze jest, aby wiedzieć, na co zwracać uwagę.

Wykrywanie / Powstrzymanie ataku socjotechnicznego

Najprostszym sposobem obrony przed atakami inżynierii społecznej jest zachowanie zdrowego rozsądku. Jeśli coś wydaje się podejrzane lub niewłaściwe, może to być atak socjotechniczny. Oto powszechne symptomy wskazujące na atak socjotechniczny:

- Ktoś tworzy wrażenie potrzeby podjęcia bardzo szybko decyzji. Jeśli czujesz się pod presją by szybko podjąć decyzję, bądź podejrzliwy
- Ktoś prosi o informacje, do których nie powinien mieć dostępu ani nie powinien ich znać.
- Coś zbyt piękne, aby mogło być prawdziwe. Typowym przykładem jest przekazanie informacji o wygranej na loterii, pomimo że nigdy nie brało się w niej udziału.
- Podrzucenie w okolicach wejścia do jednostki lub pendrive'a lub płyty CD-ROM, które zawierają program trojański, lub inne złośliwe oprogramowanie. Znalazca z reguły będzie chciał sprawdzić zawartość znalezionego nośnika (na komputerze służbowym) a zwłaszcza jeśli na pendrivie znajdzie się dokument o nazwie np. dodatki_służbowe.doc.
- Prośba skierowana do funkcjonariusza lub pracownika o podanie ważnych informacji, lub przekazanie ich dalej na odpowiedni numer, który jest sfałszowany.

Jeśli podejrzewasz, że ktoś próbuje zrobić z Ciebie ofiarę ataku socjotechnicznego, nie komunikuj się więcej z tą osobą, należy natychmiast zgłosić ten fakt do służby informatyki.

Zapobieganie atakom socjotechnicznym w przyszłości

Na szczęście istnieją środki ostrożności, które można podjąć, aby nie narażać się na przyszłe ataki socjotechniczne.

Nigdy nie dziel się swoim hasłem

Żadna szanująca się organizacja nigdy nie skontaktuje się z prośbą o podanie hasła. Jeśli ktoś prosi o podanie hasła, to jest próba ataku socjotechnicznego.

CYBERPRZESTĘPCY ZNAJDUJĄ CO CHWILĘ NOWE SPOSOBY DZIAŁAŃ SOCJOTECHNICZNYCH, PO TO BY WEJŚĆ W POSIADANIE CENNYCH DLA ICH INFORMACJI. DLATEGO MUSIMY BYĆ CZUJNI NA KAŻDYM KROKU, BY SAMEMU NIE OFIAROWAĆ CYBERPRZESTĘPCY TYCH DANYCH, KTÓRE SĄ CHRONIONE PRZEZ NASZE SYSTEMY INFORMATYCZNE.

Nie udostępniaj zbyt wiele

Im więcej atakujący wiedzą o tobie, tym łatwiej jest wprowadzić Cię w błąd i nakłonić do robienia tego, czego chcą. Nawet udostępnianie z pozoru nieznaczących szczegółów,

które z czasem połączone w całość, może stworzyć kompletny obraz Ciebie. Im mniej udostępniasz publicznie na portalach społecznościowych, w recenzjach produktów lub na publicznych forach i listach mailingowych, tym mniej prawdopodobne, że zostaniesz zaatakowany.

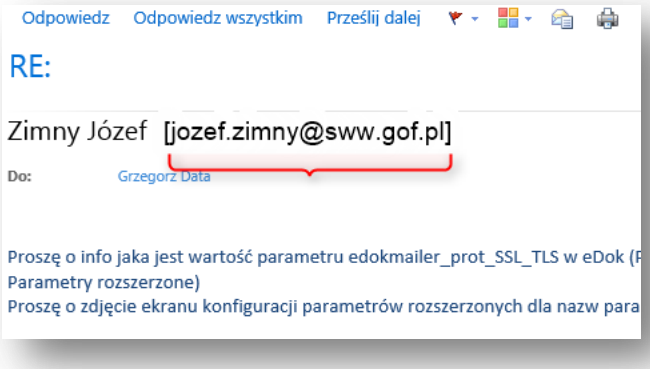
Sprawdź kontakt

Czasami, z uzasadnionych powodów, może zadzwonić do Ciebie ktoś z banku, wydawca karty kredytowej, dostawca usług telefonii komórkowej lub innych organizacji. Jeśli masz jakiekolwiek wątpliwości co do tego, czy pytanie o udzielenie informacji jest uzasadnione, poproś osobę, która dzwoni o jej imię i nazwisko i numer telefonu. Następnie weź numer telefonu tej firmy z zaufanego źródła, takiego jak numer na odwrocie karty kredytowej, numer z wyciągu bankowego, albo numer na stronie internetowej firmy (wpisz sam adres URL w przeglądarce). Tym sposobem, kiedy sam wykonujesz telefon, wiesz, że naprawdę z rozmawiasz z tym za kogo się podają. Choć może wydawać się, że te czynności mogą być kłopotliwe, warto jest je wykonać dla ochrony tożsamości i swoich danych osobowych.

Rzeczpospolita w roku 2011 opisała przypadek 25-letniego Pawła Mitera, który zespoofował adres e-mail należący do pracownika Kanelarii Prezydenta RP i napisał do TVP list proszący o czas antenowy dla nowego programu o polityce oraz zatrudnienie wskazanej przez siebie osoby jako prowadzącego. Oczywiście wskazaną osobą był Paweł. Przekręt nawet się udał, Paweł, nazywany przez pracowników TVP "człowiekiem z Kancelarii Prezydenta" podpisał kontrakt na 39 tys. złotych, VIP-owską przepustkę i — jak twierdzi — szereg innych benefitów, w tym samochód z kierowcą.
za: http://www.rp.pl/artykul/624250-Praca-w-TVP-po-falszywym-e-mailu-z-Kancelarii-Prezydenta.html

Próba rozpoznania fałszywego maila

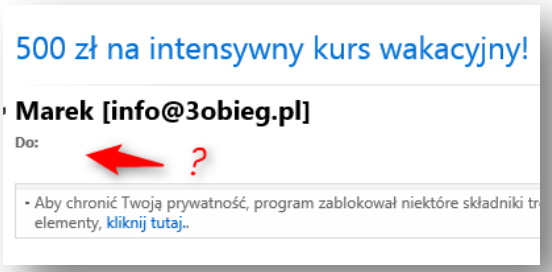
Nieprawidłowa nazwa w adresie mailowym nadawcy



Zagrożeniem może być e-mail, który zawiera błędnie zapisaną nazwę nadawcy, np. dyrektor@sw.gow.pl lub w ogóle nie zawiera nazwy firmy/instytucji. Najprawdopodobniej oznacza to, że pochodzi od nierozpoznanej domeny i jest wynikiem oszustwa., z której spodziewamy się go otrzymać.

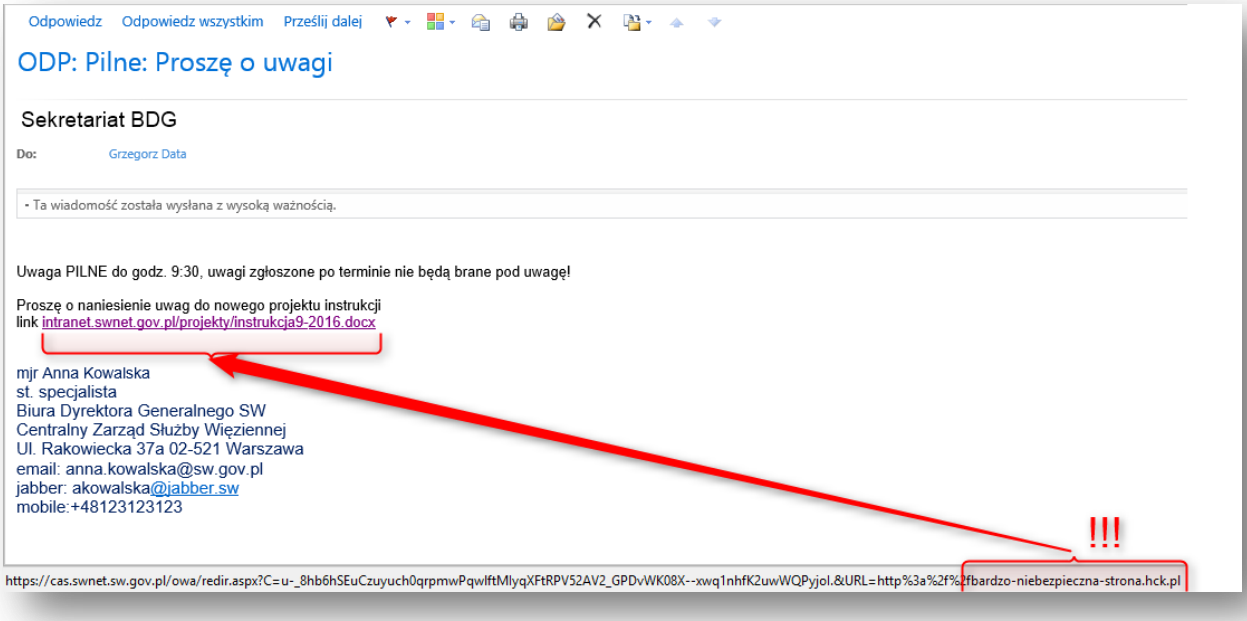
Brak Twojego adresu w polu DO: (lub TO:)

Twoje podejrzenia może wzbudzić zarówno brak Twojego adresu mailowego, jak i komunikat „undisclosed recipients" w polu OD: (TO:) – fałszywe maile wysyłane są do setek potencjalnych ofiar jednocześnie. Maile od zaufanych nadawców skierowane są tylko i wyłącznie do Ciebie.



Nieprawidłowy adres URL

W treści fałszywego e-maila znajdziesz link do strony, przez którą np. masz dokonać aktualizacji swoich danych. Nigdy nie korzystaj z linków, podawanych w e-mailach, a jeśli chcesz sprawdzić URL, wklej adres do nowego okna przeglądarki i zobacz, czy zawiera poprawną nazwę firmy/instytucji (może różnić się jedną literą od oryginalnej, jak np. http://sw.gow.pl) oraz czy jej adres wymusza szyfrowaną komunikację z serwerem (https://).



Błędy w temacie i treści wiadomości

Popularną techniką stosowaną przez cyberoszustów jest używanie w tytułach e-maili słów z błędami ortograficznymi i gramatycznymi, a także cyframi zamiast liter i wielkimi literami w środku wyrazów. Ma to na celu ominięcie filtrów antyspamowych. Celowe jest także zamieszczanie błędów w treści maila. Internetowi przestępcy stosują tę taktykę, aby trafić do mniej doświadczonych użytkowników. Wiedzą, że jeśli otrzymają odpowiedź na takiego maila, włożą mniej wysiłku w pozyskanie od niego osobistych informacji.

Brak logo instytucji i zdjęć w treści maila

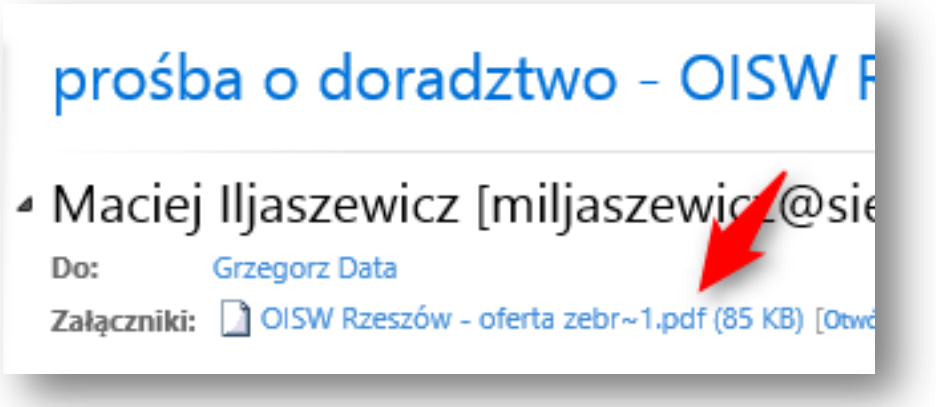
Na dobrze skonstruowaną wiadomość mailową składają się teksty i obrazy. W sfałszowanym mailu brak jest grafiki i logo firmy/instytucji, pod którą podszywa się nadawca. Zazwyczaj znajduje się w niej sam tekst. Wiadomość też znacznie różni się od tych przesyłanych do tej pory przez zaufanego nadawcę

Żądanie podania osobistych informacji

Maile od fałszywych nadawców nawołują do natychmiastowego wykonania jakiejś czynności, np. „musisz kliknąć w swoje konto teraz". Zawierają też ostrzeżenie o podaniu i/lub aktualizacji informacji osobistych dotyczących Twojego konta bankowego/profilu w serwisie (numeru PESEL lub konta czy haseł dostępu). Pamiętaj, że żadne zaufane instytucje nie będą żądać podania osobistych informacji przez e-mail.

Podejrzane załączniki

Jeśli po raz pierwszy otrzymałeś wraz z mailem od swojego banku załącznik, to prawdopodobnie ktoś chce Cię oszukać. Większość instytucji i sprzedawców nie wysyła załączników w e-mailach. Wiadomości, które mogą być naprawdę groźne, zawierają załączniki w formatach: .exe, .scr, .zip, .com, .bat .rar, Jeśli otrzymasz taki załącznik – nie otwieraj go. Największą czujność zachowaj gdy rozpakowanie załącznika wymaga wpisania hasła znajdującego się w mailu

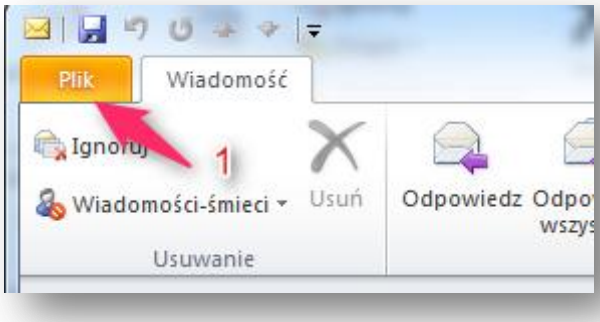


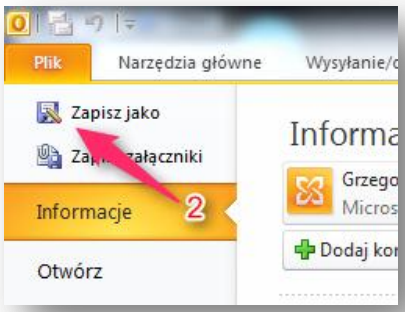
QUIZ

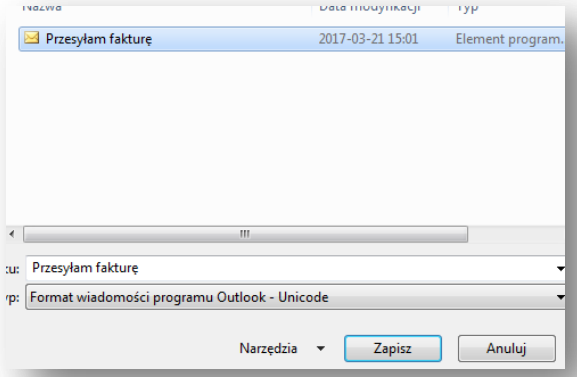
Wejdź na stronę https://quiz.securityinside.pl/quiz/start tam przygotowano quiz, w którym sprawdzisz czy potrafisz odróżnić e-mail nadesłany przez uczciwego nadawcę od spreparowanej przez oszustów wiadomości.

Postępowanie z podejrzanym mailem

Po otrzymaniu podejrzanej korespondencji należy zapisać wiadomość z menu (Plik/Zapisz jako/Zapisz)

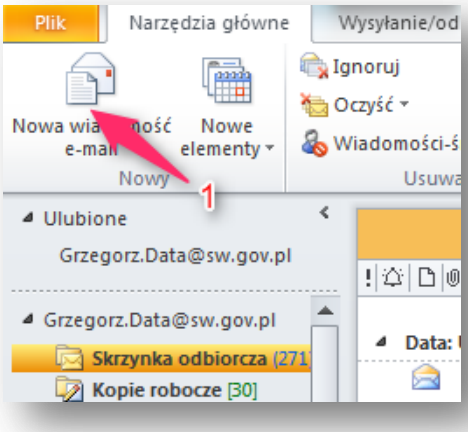


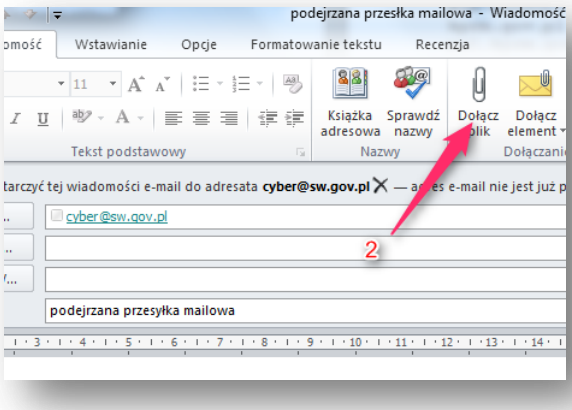


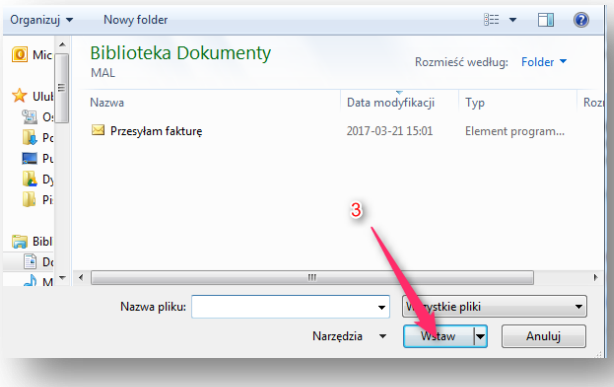


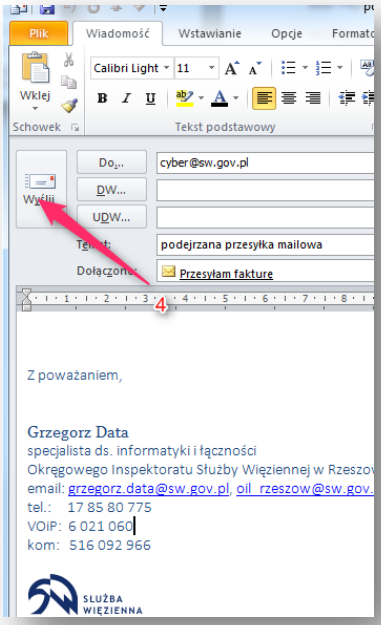
i przesłać jako załącznik na adres:

cyber@sw.gov.pl









Analiza nagłówka maila

(raczej dla zaawansowanych**)**

Rozpoznać fałszywego maila można analizując jego nagłówki i zapoznać się z nagłówkami Received (są dopisywane do e-maila w kolejności od dołu do góry). Prawdziwe e-maile w nagłówkach **Received** posiadają adresy serwerów pocztowych obsługujących pocztę dla danej domeny. (z reguły smtp.instytucja.pl, mx.instytucja.pl, poczta.instytucja.pl albo HT2.swnet.sw.gov.pl , w wypadku Służby Więziennej). Fałszywe emaile, w nagłówkach **Received** będą miały nazwy innych, niezwiązanych ze spoofowaną domeną, serwerów pocztowych. Skąd wiadomo jaki serwer odpowiada za wysyłkę poczty z danej domeny? Tego nie da się ustalić, serwer poczty przychodzącej ma nazwę zazwyczaj zbliżoną do serwera poczty wychodzącej (ale nie musi). Pewną wskazówką, co do tego które serwery obsługują pocztę dla danej domeny może być wynik polecenia:

```
root@ubuntu:~# host -t MX sw.gov.pl
sw.gov.pl mail is handled by 5 edge2dmz.swnet.sw.gov.pl.
sw.gov.pl mail is handled by 0 edge1dmz.swnet.sw.gov.pl.
root@ubuntu:~# host -t MX ms.gov.pl
ms.gov.pl mail is handled by 10 poczta.ms.gov.pl.
ms.gov.pl mail is handled by 10 poczta1.ms.gov.pl.
ms.gov.pl mail is handled by 10 poczta2.ms.gov.pl.
root@ubuntu:~# host -t MX kprm.gov.pl
kprm.gov.pl mail is handled by 3 mx1.kprm.gov.pl.
```

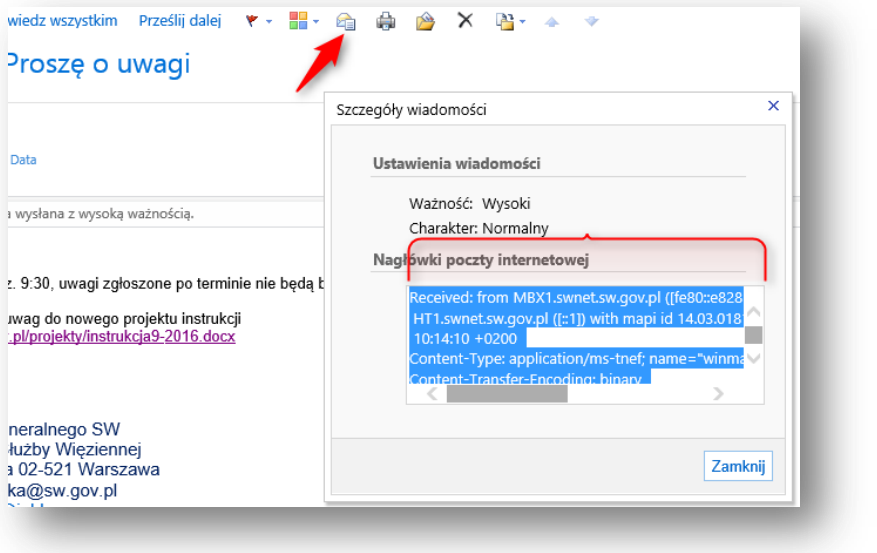
lub na komputerach z systemem Windows :

```
C:\Users\021036gdat>nslookup
Default Server: UnKnown
Address: 172.27.3.36
> set q=mx
> sw.gov.pl
```

```
Server: UnKnown
Address: 172.27.3.36
Non-authoritative answer:
sw.gov.pl    MX preference = 5, mail exchanger = edge2dmz.swnet.sw.gov.pl
sw.gov.pl    MX preference = 0, mail exchanger = edge1dmz.swnet.sw.gov.pl
edge2dmz.swnet.sw.gov.pl    internet address = 10.1.1.33
edge1dmz.swnet.sw.gov.pl    internet address = 10.1.1.31

> ms.gov.pl
Server: UnKnown
Address: 172.27.3.36
Non-authoritative answer:
ms.gov.pl    MX preference = 10, mail exchanger = poczta.ms.gov.pl
ms.gov.pl    MX preference = 10, mail exchanger = poczta2.ms.gov.pl
ms.gov.pl    MX preference = 10, mail exchanger = poczta1.ms.gov.pl
poczta.ms.gov.pl    internet address = 91.224.144.4
poczta2.ms.gov.pl    internet address = 91.224.144.8
poczta1.ms.gov.pl    internet address = 91.224.144.7

> kprm.gov.pl
Server: UnKnown
Address: 172.27.3.36
Non-authoritative answer:
kprm.gov.pl    MX preference = 3, mail exchanger = mx1.kprm.gov.pl
mx1.kprm.gov.pl internet address = 91.198.194.18
```



Porównanie maila wysłanego z naszej domeny sw.gov.pl i maila fałszywego

Received: from WSUS (172.31.33.12) by HT2.swnet.sw.gov.pl (192.168.0.204) with Microsoft SMTP Server id 14.3.181.6; Mon, 9 May 2016 00:11:30 +0200 MIME-Version: 1.0 From: <grzegorz.data@sw.gov.pl> Date: Mon, 9 May 2016 00:11:30 +0200 Subject: =?utf-8?B?V1NVUzogUG9kc3Vtb3dhbmlIIHN0YW51IGFrdHVhbGl6YWNqaSB6IHNlcndlcmEgV1NVUw==?= Content-Type: text/html; charset="utf-8" Content-Transfer-Encoding: base64 Message-ID: <4083bd6f-cd47-4ded-b232-f34b4881547a@HT2.swnet.sw.gov.pl> To: Undisclosed recipients:; **Return-Path: grzegorz.data@sw.gov.pl** X-MS-Exchange-Organization-AuthSource: HT2.swnet.sw.gov.pl X-MS-Exchange-Organization-AuthAs: Anonymous X-NAI-Spam-Rules: 2 Rules triggered MID_NUM_LC_DASH=0.2, RV5666=0 X-NAI-Spam-Version: 2.2.0.9309 : core <5666> : inlines <4775> : streams <1632204> : uri <2205904>	Received: from BDG (134.24.55.254) by HT2.swnet.sw.gov.pl (192.168.0.204) with Microsoft SMTP Server id 14.3.181.6; Mon, 9 May 2016 00:11:30 +0200 MIME-Version: 1.0 From: <bdg@sw.gov.pl> Date: Mon, 9 May 2016 00:11:30 +0200 Subject: =?utf-8?B?V1NVUzogUG9kc3Vtb3dhbmlIIHN0YW51IGFrdHVhbGl6YWNqaSB6IHNlcndlcmEgV1NVUw==?= Content-Type: text/html; charset="utf-8" Content-Transfer-Encoding: base64 Message-ID: <4083bd6f-cd47-4ded-b232-f34b4881547a@HT2.swnet.sw.gov.pl> To: Undisclosed recipients:; **Return-Path: bdg@sw.gov.pl** Received: from **helium.brandedinternet.net** (122.137.business-**adsl.cybersmart.co.za**. [196.41.122.137]) by HT2.swnet.sw.gov.pl with ESMTPS id x6si1538164wiw.36.2012.06.06.03.56.00 (version=TLSv1/SSLv3 cipher=OTHER); Wed, 06 Jun 2012 03:56:01 -0700 (PDT) Received-SPF: neutral (HT2.swnet.sw.gov.pl : 196.41.122.137 is neither permitted nor denied by best guess record for domain of no-reply@ sw.gov.pl client-ip=196.41.122.137; Authentication-Results: HT2.swnet.sw.gov.pl ; spf=neutral (HT2.swnet.sw.gov.pl : 196.41.122.137 is neither permitted nor denied by best guess record for domain of no-reply@ sw.gov.pl) smtp.mail=no-reply@ sw.gov.pl. Date: Wed, 06 Jun 2012 03:56:01 -0700 (PDT) Message-Id: <4fcf3741.064eb40a.2e05.7be6SMTPIN_ADDED@HT2.swnet.sw.gov.pl> Received: from [77.120.120.131] (helo=**s2.zavtra.com.ua**) by **helium.brandedinternet.net** with esmtpa (Exim 4.69) (envelope-from <no-reply@ sw.gov.pl >) id 1ScD8R-0002Ku-4e for grzegorz.data@sw.gov.pl; Wed, 06 Jun 2012 12:06:39 +0200X-MS-Exchange-Organization-AuthSource: HT2.swnet.sw.gov.pl X-MS-Exchange-Organization-AuthAs: Anonymous X-NAI-Spam-Rules: 2 Rules triggered MID_NUM_LC_DASH=0.2, RV5666=0 X-NAI-Spam-Version: 2.2.0.9309 : core <5666> : inlines <4775> : streams <1632204> : uri <2205904>

Źródła:
Dr Lance Hayden jest Phishing i oszustwa w e-mailach
Biuletyn bezpieczeństwa internetowego OUCH
Alissa Torres Socjotechnika
Krzysztof Gontarek Bezpieczne korzystanie z poczty elektronicznej
Lenny Zeltser Spearfishing
www.niebezpiecznik.pl
www.zaufanatrzeciastrona.pl
www.cert.pl
www.cert.gov.pl