

Program eTwinning



E - safety - bezpieczny Internet



Mariusz Bodeńko
Białystok, 04.12.2013

O mnie...

- ⊕ Obecnie od kilku lat administrator sieci i systemów wykorzystywanych w zakładzie produkcyjnym, odpowiedzialny za ich działanie i rozwój oraz bezpieczeństwo infrastruktury, sieci i systemów.
- ⊕ Absolwent studiów magisterskich o kierunku elektrotechnika i informatyka oraz studiów podyplomowych o kierunku inżynierskie bazy danych i CAD na Politechnice Lubelskiej.

Bezpieczeństwo w sieci

- ⊕ Ochrona danych i prywatności,
- ⊕ Poczucie bezpieczeństwa w działaniach realizowanych w sieci,
- ⊕ Bezpieczeństwo procesów biznesowych,
- ⊕ Bezpieczeństwo systemów komputerowych,
- ⊕ i wiele innych definicji jednak w każdym przypadku jest to fundament poprawnego funkcjonowania świata w dobie Internetu.

Czy to takie istotne...?

- ⊕ Każdego dnia na świecie pojawia się ok. 200 000 próbek szkodliwego oprogramowania (Kaspersky Lab).
- ⊕ 90% respondentów (firm) uważa że zagrożeń jest znacznie mniej, 6% firm szacuje prawidłowo.
- ⊕ 66% uczestników tego samego badania padło co najmniej raz w ciągu ostatnich 12 miesięcy ofiarą ataku z wykorzystaniem złośliwego oprogramowania.
- ⊕ Użytkownicy indywidualni: 8 na 10 zna zagadnienia bezpieczeństwa i 6 na 10 pada ofiarą ataków

Poziom świadomości

- ⊕ 24% poprawnych szacunków - Bliski Wschód
- ⊕ Ameryka Północna i Południowa, Europa Zachodnia, rejon Azji i Pacyfiku: 5 - 7%,
- ⊕ Rosja: 4 %.

Ofiary ataków:

- ⊕ 72 % firm w Ameryce Południowej
- ⊕ 71 % firm w Rosji
- ⊕ 70 % firm w Ameryce Północnej
- ⊕ 68 % Rejon Azji i Pacyfiku
- ⊕ 63 % Europa Zachodnia

Zagrożenia w sieci.

Czy warto o tym mówić?

Wg Raportu Nortona (Symantec):

- ⊕ 556 mln ofiar, z tego w Polsce 7,2 mln - daje do ponad 1,5 mln ofiar dziennie lub 18 na sekundę;
- ⊕ 50% dorosłych internautów, w Polsce to 49% padło ofiarą cyberprzestępczości, otrzymało nagie zdjęcia od obcych, było nękanie lub zastraszane on-line;
- ⊕ 41% dorosłych internautów, w Polsce to 40% padło ofiarą szkodliwego oprogramowania, wirusów, hakerów, włamań i kradzieży.

Ryzykowne zachowania w portalach społecznościowych

- ⊕ 12% użytkowników przyznaje się że ktoś włamał się na ich konta lub podszywał się pod nich;
- ⊕ 39% (w Polsce 36%) użytkowników nie wylogowuje się po każdej sesji;
- ⊕ 1/4 (w Polsce 3/10) użytkowników przekazuje swoje hasła innym;
- ⊕ 31% (w Polsce 36%) użytkowników nawiązuje znajomości z nieznanymi osobami.

Zanik granic pomiędzy pracą a zabawą

- ⊕ 49% (w Polsce 43%) dorosłych, pracujących użytkowników wykorzystuje swoje prywatne urządzenie do pracy i zabawy;
- ⊕ 36% (w Polsce 45%) twierdzi że ich firmy nie posiadają polityki używania sprzętu służbowego w celach prywatnych;
- ⊕ 30% (w Polsce 21%) rodziców pozwala dzieciom robić zakupy i pobierać pliki na służbowych urządzeniach;
- ⊕ 34% (w Polsce 28%) korzysta z portali społecznościowych za pomocą urządzeń służbowych.

Urządzenia mobilne bez ochrony

- ✦ 48% urządzeń mobilnych pozbawionych jest jakiegokolwiek ochrony (nawet podstawowej!);
- ✦ 2/3 dorosłych łączy się z Internetem przez urządzenia mobilne;
- ✦ Ilość luk w zabezpieczeniach urządzeń mobilnych (zagrożeń) podwoiła się w porównaniu do roku 2010;
- ✦ 31% (w Polsce 34%) użytkowników urządzeń mobilnych otrzymało wiadomość od nieznanej osoby z prośbą o kliknięcie nieznanego łącza lub wybranie nieznanego numeru w celu np. odsłuchania wiadomości.

Stan wiedzy o zabezpieczeniach

- ⊕ 89% użytkowników usuwa podejrzane e-maile od nieznanymi nadawców;
- ⊕ 83% użytkowników ma przynajmniej podstawowy program antywirusowy;
- ⊕ 42% użytkowników nie otwiera załączników lub łączy w niechcianych wiadomościach e-mail lub sms;
- ⊕ 40% dorosłych użytkowników (w Polsce 46%) nie wie jak zmieniły się formy cyberprzestępstw w ostatnich latach, jakie są skutki oddziaływania szkodliwego oprogramowania na komputer oraz że może ono działać w ukryciu aby utrudnić rozpoznanie że komputer został zainfekowany.

Ile kosztuje cyberprzestępczość?

- ⊕ Globalne koszty cyberprzestępczości: 110 mld USD z tego 85% to efekty oszustw, kradzieży, wyłudzeń, oraz niezbędnych napraw;
- ⊕ 197 USD w przeliczeniu na jedną ofiarę;
- ⊕ W Polsce koszty cyberprzestępczości to: 4,8 mld PLN;
- ⊕ 672 PLN w przeliczeniu na jedną ofiarę.

Pułapki...

Poszukujemy współpracowników, którzy gotowi są podjąć się dodatkowej pracy.
Praca zajmie 1-2 godziny w tygodniu i nie wymaga żadnego wkładu pieniężnego.
Istotą pracy jest przetwarzanie napływających z Twojego miasta zamówień.

Jest to prosta praca, której można nauczyć się w ciągu 10 minut i będzie można regularnie wykonywać ją dla naszej firmy.

Za każde przetworzone zamówienie otrzymasz od 200 do 500 EUR

Opiata - natychmiastowa!

Jeśli tylko zechcesz - będziesz mógł stale zwiększać ilość przetwarzanych zamówień.
Niestety my nie możemy zagwarantować zatrudnienia dla wszystkich chętnych,
dlatego proponujemy od razu wysłać nam swoje zgłoszenie.

Zwiększy to Twoją szansę, aby zostać członkiem naszego zespołu.

Co należy podać w zgłoszeniu:

Imię i nazwisko:

Adres e-mail:

Miasto, w którym mieszkasz:

Wniosek należy wysłać na nasz adres e-mail: xxx@xxx.com

Odpowiedź otrzymasz w ciągu dwóch dni roboczych.

Pułapki...



Trzy gimnazjalistki w ciąży po zabawie w słoneczko - nagranie wyciekło do internetu [FILM]



Piotr [redacted] komentował(a) Onet News:
05409



**ZABAWA W SŁONECZKO ZAKOŃCZONA
CIAŻA, FILM WYCIĘKL DO SIĘCI**

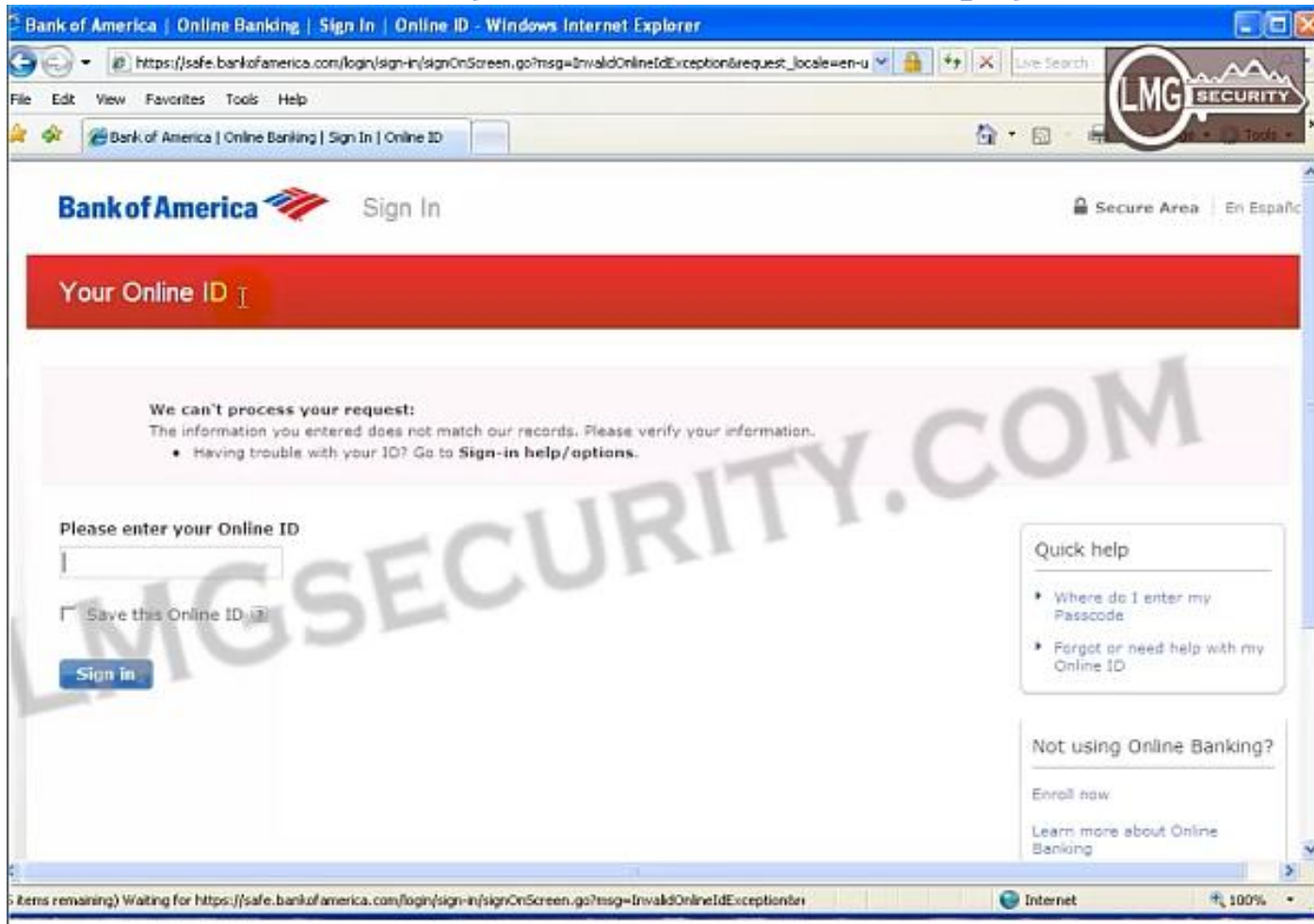
Trzy gimnazjalistki w ciąży po zabawie w słoneczko - nagranie wyciekło do Internetu [FILM]
twoje-miastofo.pl
310 642 wyświetlenia - zobacz jak się teraz bawi młodzież [BEZ CENZURY]

Lubię to! · Dodaj komentarz · 47 minut(y) temu · 

Ważna aktualizacja systemu - wymagane natychmiastowe działanie



Idziemy na e-zakupy I



Bank of America | Online Banking | Sign In | Online ID - Windows Internet Explorer

https://safe.bankofamerica.com/login/sign-in/signOnScreen.go?msg=InvalidOnlineIdException&request_locale=en-u

File Edit View Favorites Tools Help

Bank of America | Online Banking | Sign In | Online ID

Bank of America Sign In

Secure Area En Español

Your Online ID

We can't process your request:
The information you entered does not match our records. Please verify your information.

- Having trouble with your ID? Go to [Sign-in help/options](#).

Please enter your Online ID

Save this Online ID

Quick help

- Where do I enter my Passcode
- Forgot or need help with my Online ID

Not using Online Banking?

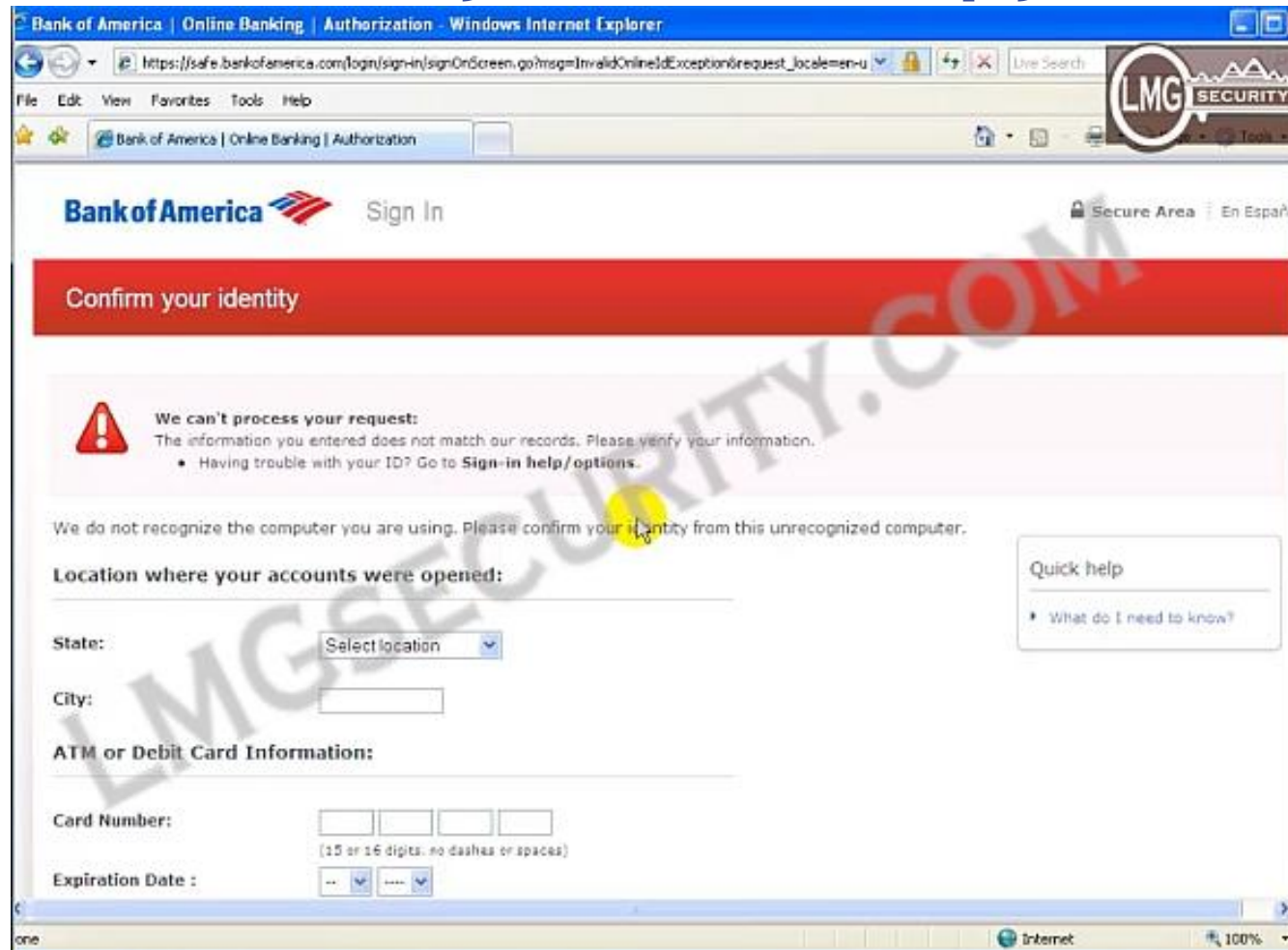
Enroll now

Learn more about Online Banking

Items remaining) Waiting for https://safe.bankofamerica.com/login/sign-in/signOnScreen.go?msg=InvalidOnlineIdException&request_locale=en-u

Internet 100%

Idziemy na e-zakupy II



Bank of America | Online Banking | Authorization - Windows Internet Explorer

https://safe.bankofamerica.com/login/sign-in/signOnScreen.go?msg=InvalidOnlineIdException&request_locale=en-u

File Edit View Favorites Tools Help

Bank of America | Online Banking | Authorization

Bank of America Sign In

Secure Area En Español

Confirm your identity

We can't process your request:
The information you entered does not match our records. Please verify your information.

- Having trouble with your ID? Go to [Sign-in help/options](#).

We do not recognize the computer you are using. Please confirm your identity from this unrecognized computer.

Location where your accounts were opened:

State:

City:

ATM or Debit Card Information:

Card Number:
(15 or 16 digits, no dashes or spaces)

Expiration Date:

Quick help

- [What do I need to know?](#)

Internet 100%

Wirtualny pieniądz. Bitcoin

Komunikat z dnia 18.11.2013r. godz. 17:00

SERWER PLATFORMY BIDEXTREME ZOSTAŁ ZAATAKOWANY PRZEZ HACKERÓW

W wyniku ataku hackerskiego został okradziony portfel BTC i LTC. Fakt ten został zgłoszony organom ścigania.

Zostały skradzione waluty BTC i LTC należące do wszystkich Użytkowników. W przypadku ich odzyskania zostaną one zwrócone Użytkownikom zgodnie ze stanem salda na dzień 17.11.2013r.

Środki pieniężne przechowywane na rachunku bankowym platformy należące do Użytkowników są bezpieczne.

Środki pieniężne będą zwracane Użytkownikom na bieżąco.

W pierwszej kolejności zostaną zwrócone wszystkie wpłaty dokonane w dniach 16.11. – 18.11., zostaną one w dniu dzisiejszym zwrócone na konta ich nadawców.

W dniu dzisiejszym zostanie także zlecona wypłata środków dla Użytkowników, którzy mają zdefiniowane konta bankowe - na kontach Użytkownika.

Pozostałe osoby, które nie posiadają zdefiniowanych kont bankowych zostaną poddane weryfikacji, celem zwrotu środków pieniężnych ich właścicielom.

Osoby poddające się weryfikacji zobowiązane są:

prześłać skan dowodu osobistego lub innego dokumentu ze zdjęciem na adres: weryfikacja.bidextreme@wp.pl, podając w tytule maila swój nick Użytkownika, posługując się przy tym mailem używanym do rejestracji na platformie bidextreme,

- dokonać przelewu identyfikacyjnego w wysokości 1,00 zł
na rachunek 67 1140 1111 0000 4157 9200 1002

z własnego imiennego rachunku bankowego należącego do danego Użytkownika, podając w tytule przelewu swój nick Użytkownika.

Przepraszamy naszych Użytkowników za utrudnienia, niemniej jednak zmuszeni jesteśmy zawiesić działalność platformy bidextreme do czasu wyjaśnienia sprawy.

Zespół Bidextreme

Uściślenie komunikatu z dnia 18.11.2013r. z godz. 17:00

SERWER PLATFORMY BIDEXTREME ZOSTAŁ ZAATAKOWANY PRZEZ HACKERÓW

Szanowni Użytkownicy

Na chwilę obecną będą zwracane tylko środki pieniężne PLN, które na dzień 17.11.2013r. przed atakiem hackerskim były przypisane do kont Użytkowników.

Trwają czynności zmierzające do odzyskania skradzionych walut BTC i LTC, w przypadku ich odzyskania zostaną one niezwłocznie przywrócone do kont Użytkowników.

Zespół Bidextreme

Wirtualny pieniądz. Bitcoin

- ✦ wykradzono portfel online (ten, który znajdował się na serwerze giełdy).
- ✦ włamywacze nie uzyskali dostępu do konta bankowego serwisu, a więc fundusze użytkowników Bidextreme przeznaczone na zakup Bitcoinów lub pochodzące ze sprzedaży w serwisie są bezpieczne i będą zwracane.
- ✦ serwis przełączył się na ...adres e-mail założony na Wirtualnej Polsce, co może wskazywać na to, że nie ufa także swoim serwerom pocztowym.

NSA. Wróg czy przyjaciel?

NSA (Agencja Bezpieczeństwa Krajowego USA) szpieguje za pomocą złośliwego oprogramowania 50 000 sieci komputerowych na świecie (jedna w Polsce)!



Dziękuję za uwagę. Zapraszam na warsztaty.



Mariusz Bodeńko
mbod@o2.pl