ACC AMERICA
Association of Corporate Counsel
Southern California Chapter (ACC-SoCal)

STROZ FRIEDBERG
DIGITAL RISK MANAGEMENT & INVESTIGATIONS

# CHECK IN WITHOUT CHECKING IN

**January 25, 2012**
**Anaheim, California**
**Sponsored by Stroz Friedberg**
**Moderator:**
**Kris Ashman**
**Panelists:**
**Jason Smolanoff**
**Camilla Eng**

# E-Discovery

**You are have just received the first set of interrogatories and requests for production in a complex case, and, after speaking with your client, it is apparent that the production will include a large number of e-mails and other electronically stored documents, including the records of certain in-house counsel and others with whom they have communicated regularly.**

# Potential Pitfalls

- With every demand for electronically stored information (ESI) comes an exponentially increasing volume of data to be reviewed for both relevance and privilege.
- With the increasing volume comes an increasing likelihood that privileged information will be inadvertently disclosed to the other side, and that means, in some jurisdictions, the privilege will be waived.

# Inadvertent Waiver

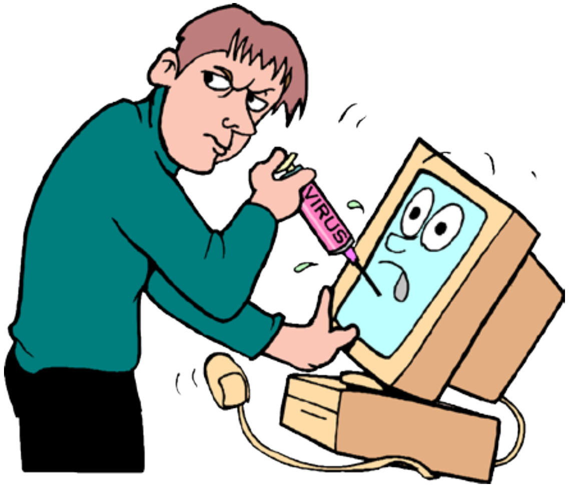
- Even in those jurisdictions that do not follow the strict liability approach to privilege waiver, your actions in managing the production and remedying the error will factor into the court's decision about whether you (or, more accurately, your client) has waived the privilege, and what the scope of that waiver will be.

# Do Hansel and Gretel need an attorney?

## *How your digital breadcrumbs can lead a hacker to you*

# Presentation Overview

- What are digital breadcrumbs?
- Online Reconnaissance Techniques
- Exploitation Methodologies - *Phishing*



# “Digital Breadcrumb” Sources

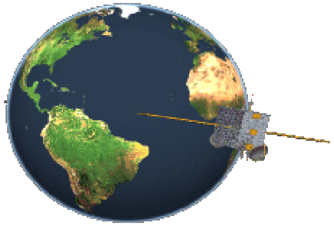
# Overt Indicators

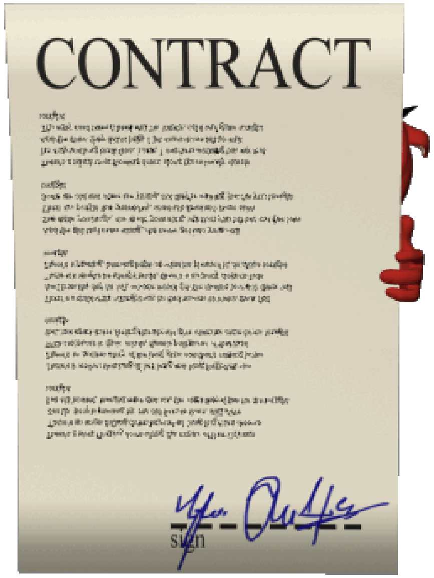
## **Social Engineering**

# Covert Indicators

## METADATA

*"data providing information about one or more aspects of the data"*



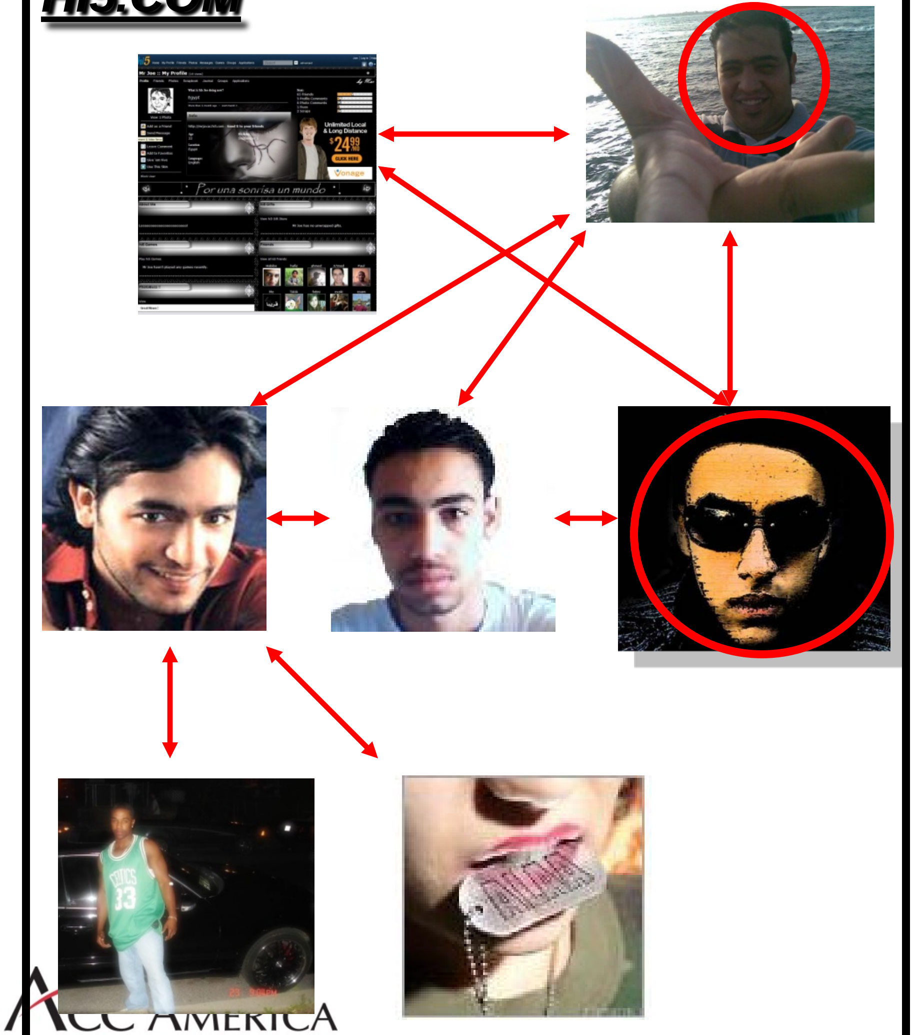


# Online Reconnaissance

- Online Reconnaissance
  - To discover and gather relevant information about a particular person, organization, or online entity
  - Legitimate activity
  - Criminal activity

# Social Networking Data Mining

## HI5.COM



## FACEBOOK

## MYSPACE.COM

d0n

"ReA..L :": GamE Making $$$$"

Male
22 years old

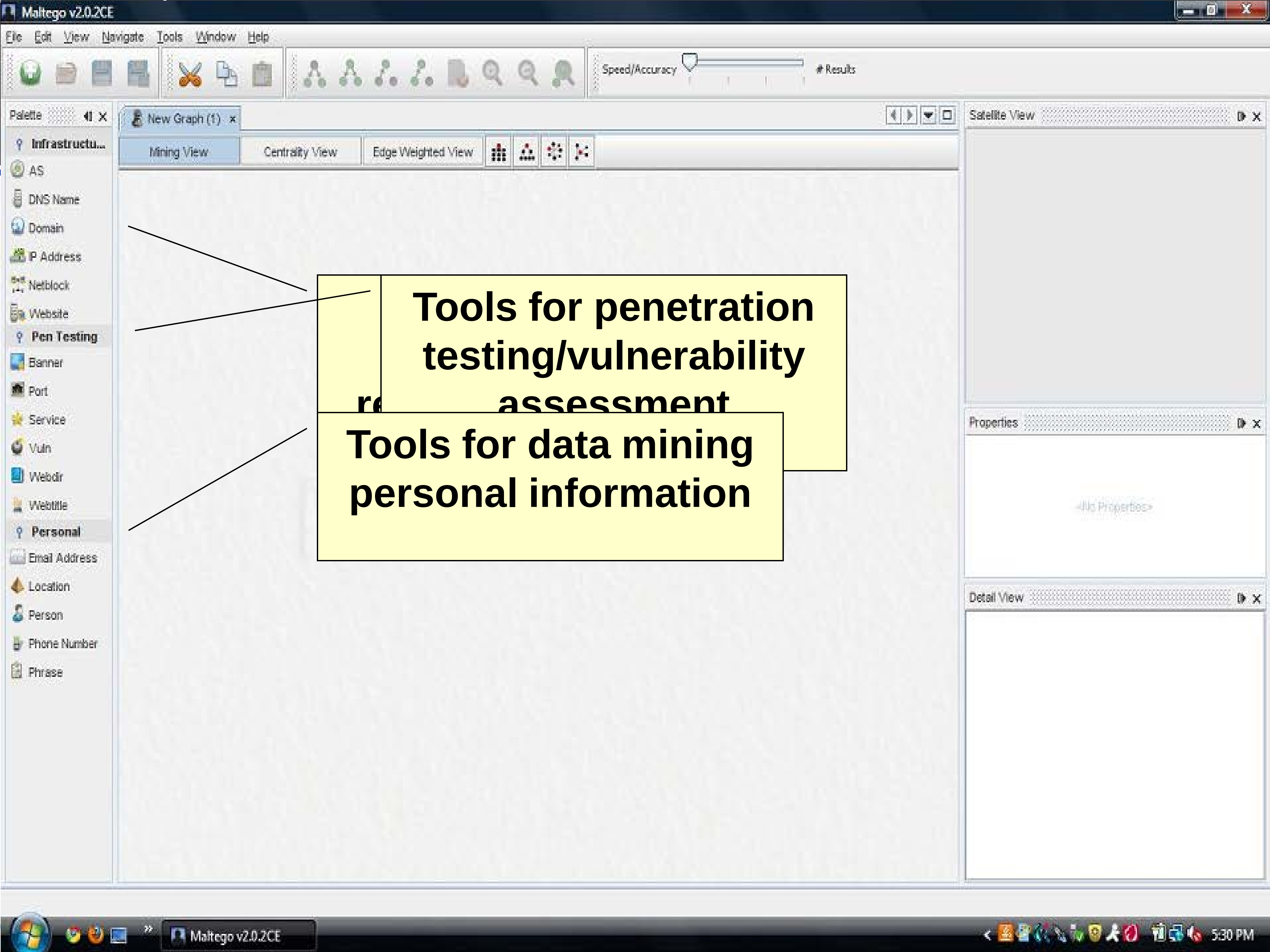
Egypt

Last Login: 9/7/2008

View My: Pics | Videos

# Maltego

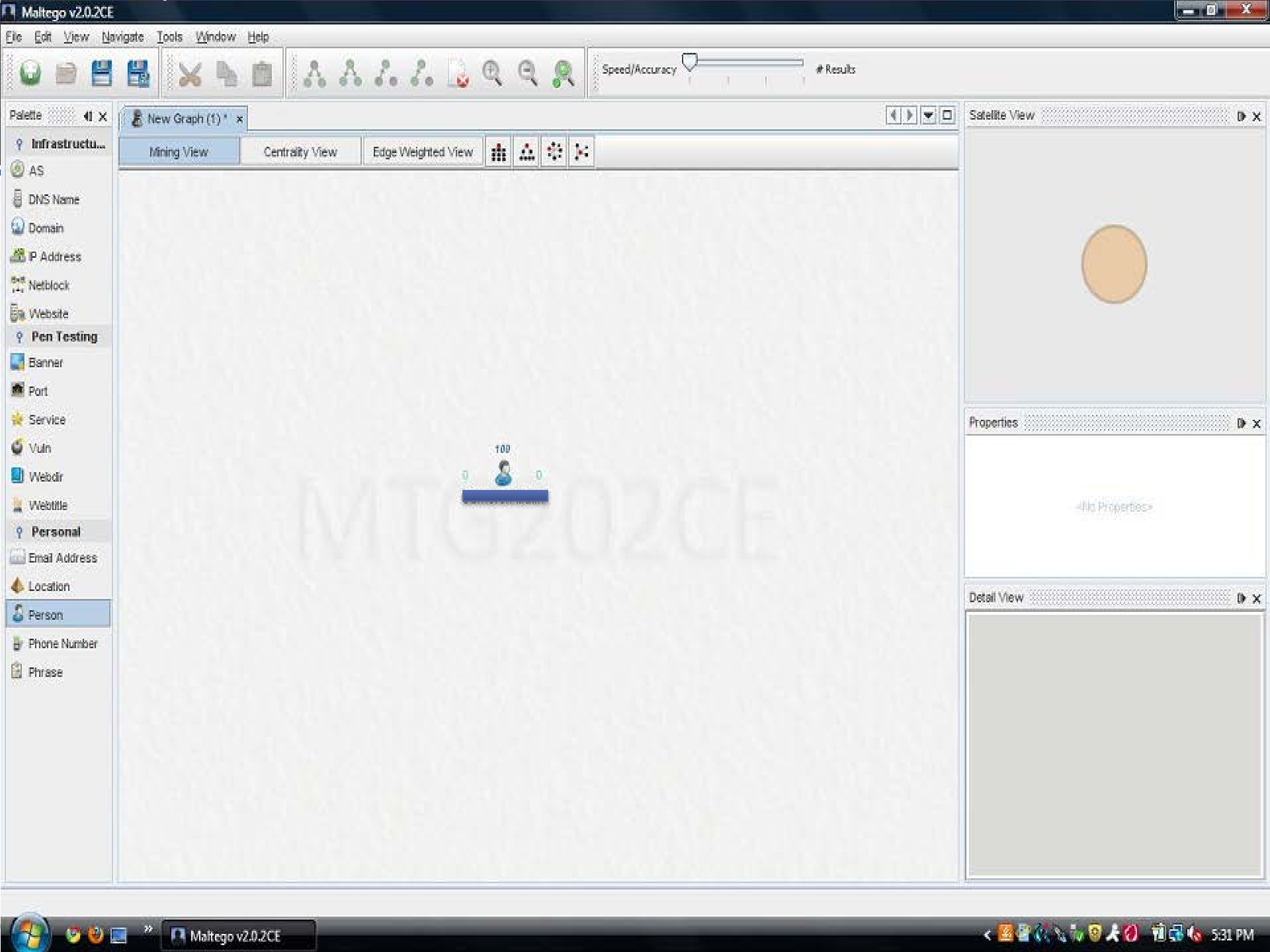
- Mal-what-o?
- Maltego is an open source intelligence and forensics application.
  - It allows for the mining and gathering of information as well as the representation of this information in a meaningful way.
  - Allows you to identify key relationships between information and identify previously unknown relationships between them

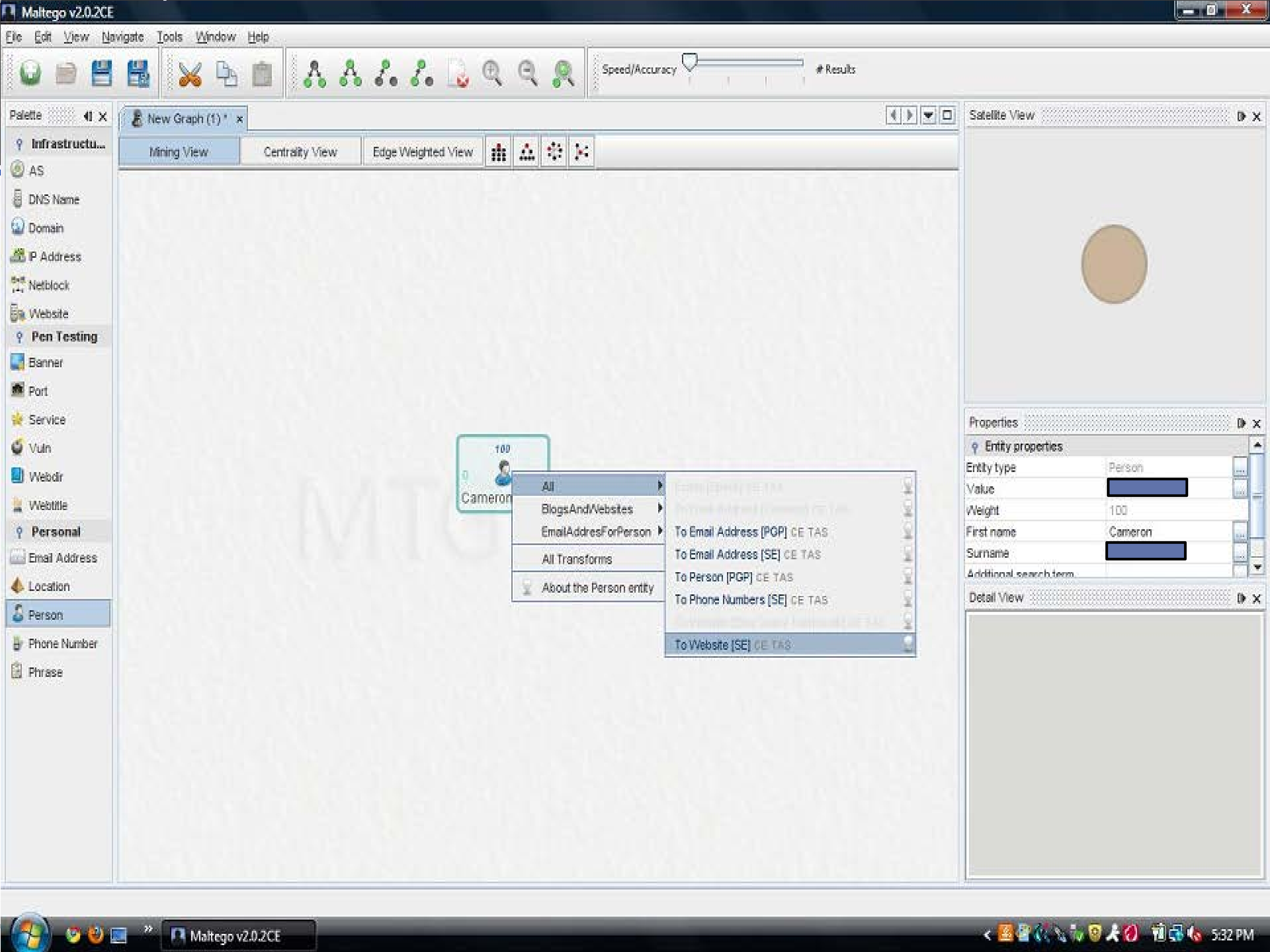


re

Tools for penetration testing/vulnerability assessment

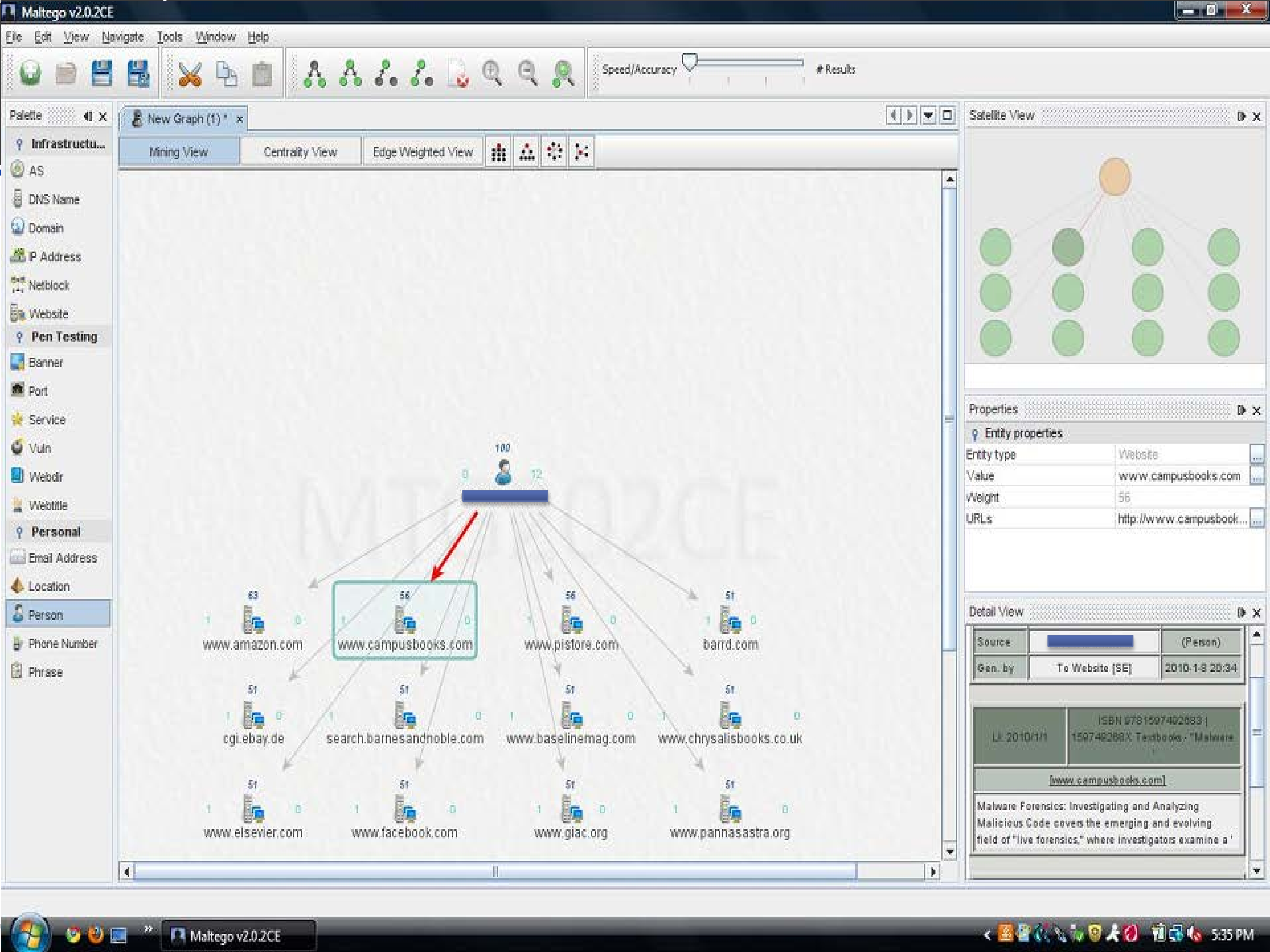
Tools for data mining personal information


Maltego v2.0.2CE
File Edit View Navigate Tools Window Help
Speed/Accuracy
# Results
Palette
Infrastructu...
AS
DNS Name
Domain
IP Address
Netblock
Website
Pen Testing
Banner
Port
Service
Vuln
Webdir
Webtitle
Personal
Email Address
Location
Person
Phone Number
Phrase
New Graph (1) *
Mining View
Centrality View
Edge Weighted View
100
0
0
MTG202CE
Satellite View
Properties
<No Properties>
Detail View
Maltego v2.0.2CE
5:31 PM



Entity properties

| | |
|---|---|
| Entity type | Person |
| Value | [redacted] |
| Weight | 100 |
| First name | Cameron |
| Surname | [redacted] |
| Additional search term | |



[redacted]

Entity properties

| | |
|---|---|
| Entity type | Website |
| Value | www.campusbooks.com |
| Weight | 56 |
| URLs | http://www.campusbook... |

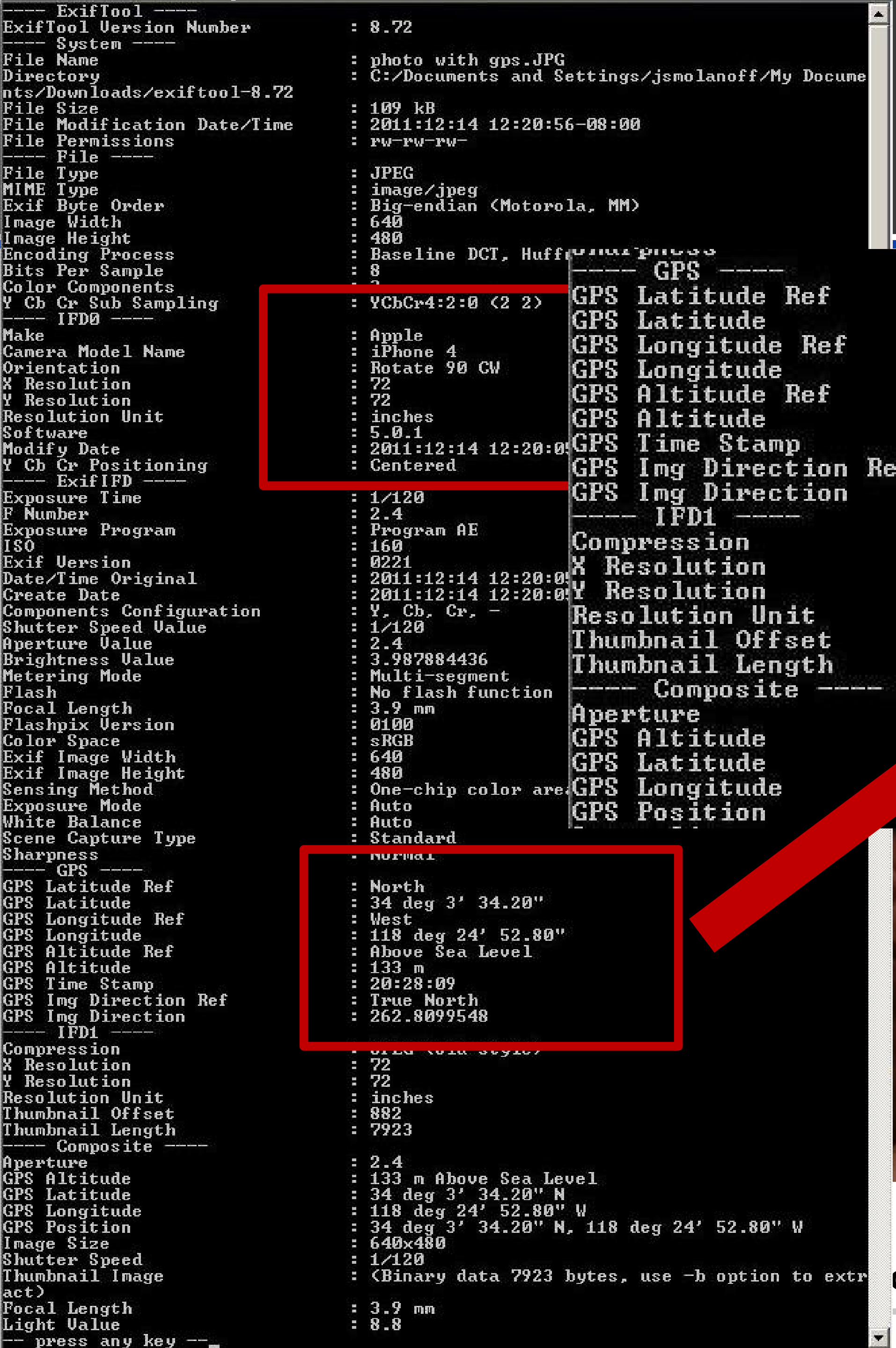
| | | |
|---|---|---|
| Source | [redacted] | (Person) |
| Gen. by | To Website [SE] | 2010-1-8 20:34 |

| | |
|---|---|
| LI: 2010/1/1 | ISBN 9781597492683 \| 159749268X Textbooks - "Malware ' |

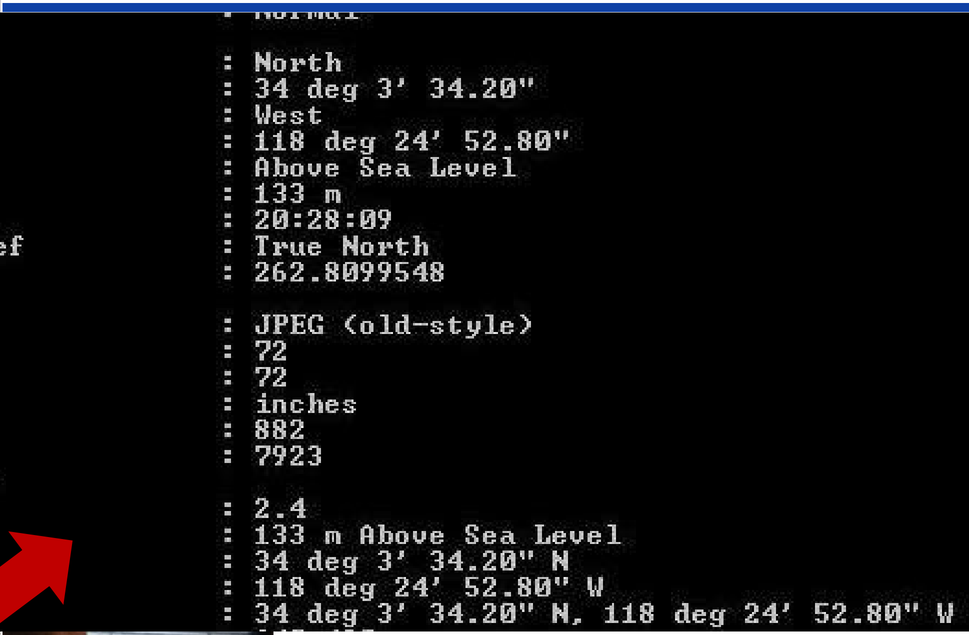
[www.campusbooks.com]

Malware Forensics: Investigating and Analyzing Malicious Code covers the emerging and evolving field of "live forensics," where investigators examine a '

# Metadata Extraction

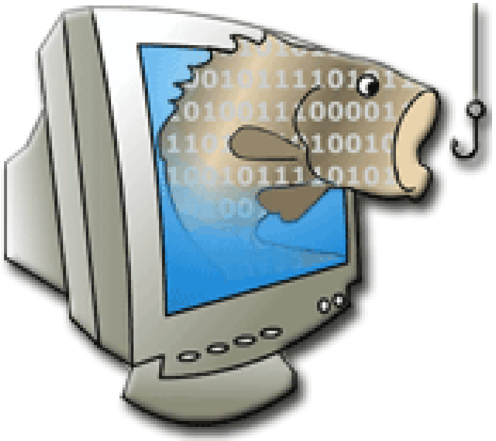


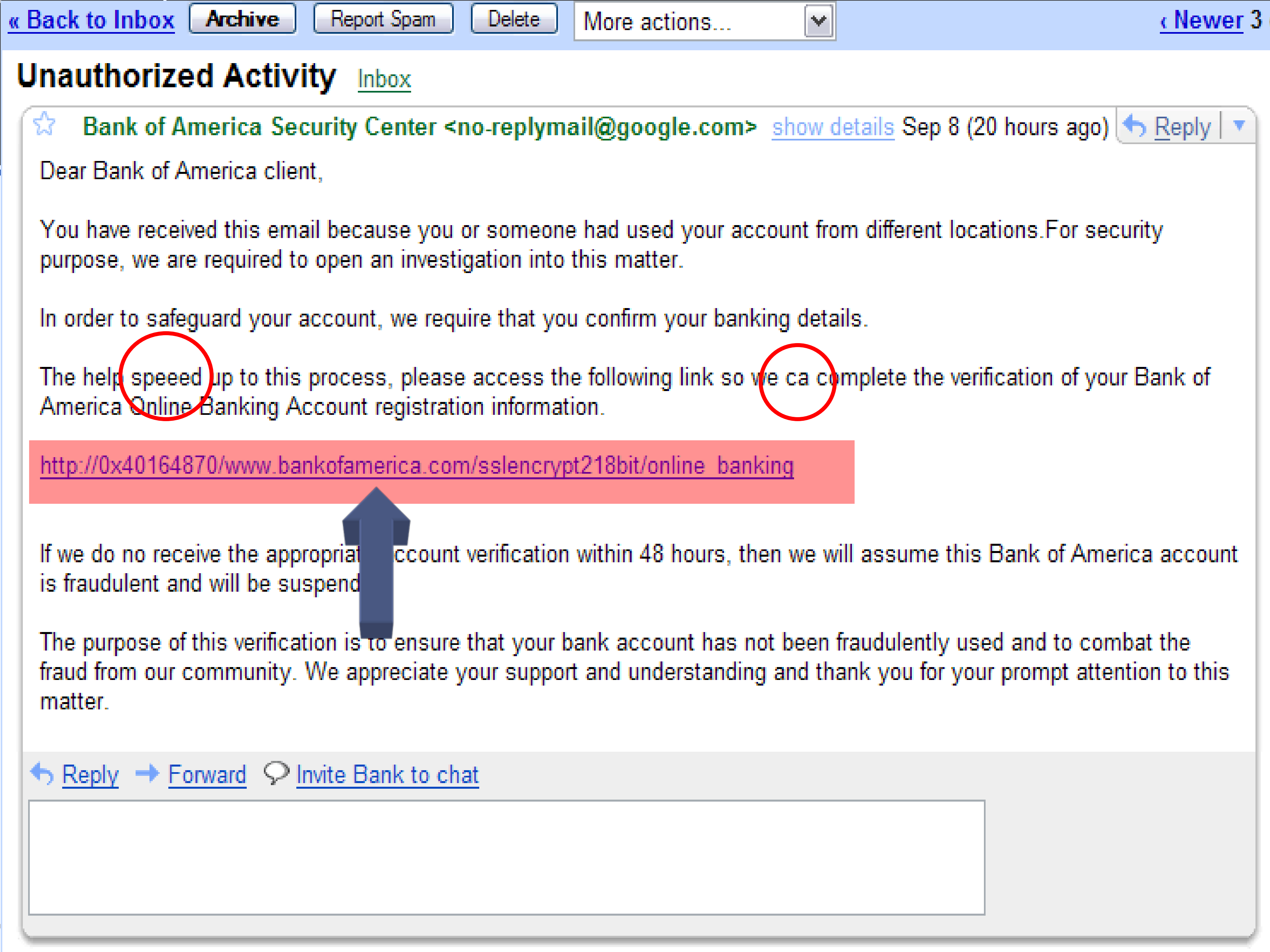
```
---- ExifTool ----
ExifTool Version Number         : 8.72
---- System ----
File Name                       : photo with gps.JPG
Directory                       : C:/Documents and Settings/jsmolanoff/My Docume
nts/Downloads/exiftool-8.72
File Size                       : 109 kB
File Modification Date/Time     : 2011:12:14 12:20:56-08:00
File Permissions                : rw-rw-rw-
---- File ----
File Type                       : JPEG
MIME Type                       : image/jpeg
Exif Byte Order                 : Big-endian (Motorola, MM)
Image Width                     : 640
Image Height                    : 480
Encoding Process                : Baseline DCT, Huff
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
---- IFD0 ----
Make                            : Apple
Camera Model Name               : iPhone 4
Orientation                     : Rotate 90 CW
X Resolution                    : 72
Y Resolution                    : 72
Resolution Unit                 : inches
Software                        : 5.0.1
Modify Date                     : 2011:12:14 12:20:0
Y Cb Cr Positioning             : Centered
---- ExifIFD ----
Exposure Time                   : 1/120
F Number                        : 2.4
Exposure Program                : Program AE
ISO                             : 160
Exif Version                    : 0221
Date/Time Original              : 2011:12:14 12:20:0
Create Date                     : 2011:12:14 12:20:0
Components Configuration        : Y, Cb, Cr, -
Shutter Speed Value             : 1/120
Aperture Value                  : 2.4
Brightness Value                : 3.987884436
Metering Mode                   : Multi-segment
Flash                           : No flash function
Focal Length                    : 3.9 mm
Flashpix Version                : 0100
Color Space                     : sRGB
Exif Image Width                : 640
Exif Image Height               : 480
Sensing Method                  : One-chip color area
Exposure Mode                   : Auto
White Balance                   : Auto
Scene Capture Type              : Standard
Sharpness                       : Normal
---- GPS ----
GPS Latitude Ref                : North
GPS Latitude                    : 34 deg 3' 34.20"
GPS Longitude Ref               : West
GPS Longitude                   : 118 deg 24' 52.80"
GPS Altitude Ref                : Above Sea Level
GPS Altitude                    : 133 m
GPS Time Stamp                  : 20:28:09
GPS Img Direction Ref           : True North
GPS Img Direction               : 262.8099548
---- IFD1 ----
Compression                     : JPEG (old-style)
X Resolution                    : 72
Y Resolution                    : 72
Resolution Unit                 : inches
Thumbnail Offset                : 882
Thumbnail Length                : 7923
---- Composite ----
Aperture                        : 2.4
GPS Altitude                    : 133 m Above Sea Level
GPS Latitude                    : 34 deg 3' 34.20" N
GPS Longitude                   : 118 deg 24' 52.80" W
GPS Position                    : 34 deg 3' 34.20" N, 118 deg 24' 52.80" W
Image Size                      : 640x480
Shutter Speed                   : 1/120
Thumbnail Image                 : (Binary data 7923 bytes, use -b option to extr
act)
Focal Length                    : 3.9 mm
Light Value                     : 8.8
-- press any key --
```



```
Sharpness                       : Normal
---- GPS ----
GPS Latitude Ref                : North
GPS Latitude                    : 34 deg 3' 34.20"
GPS Longitude Ref               : West
GPS Longitude                   : 118 deg 24' 52.80"
GPS Altitude Ref                : Above Sea Level
GPS Altitude                    : 133 m
GPS Time Stamp                  : 20:28:09
GPS Img Direction Ref           : True North
GPS Img Direction               : 262.8099548
---- IFD1 ----
Compression                     : JPEG (old-style)
X Resolution                    : 72
Y Resolution                    : 72
Resolution Unit                 : inches
Thumbnail Offset                : 882
Thumbnail Length                : 7923
---- Composite ----
Aperture                        : 2.4
GPS Altitude                    : 133 m Above Sea Level
GPS Latitude                    : 34 deg 3' 34.20" N
GPS Longitude                   : 118 deg 24' 52.80" W
GPS Position                    : 34 deg 3' 34.20" N, 118 deg 24' 52.80" W
```

# Social Engineering and Phishing Attacks





Unauthorized Activity

Bank of America Security Center <no-replymail@google.com> Sep 8 (20 hours ago)

Dear Bank of America client,

You have received this email because you or someone had used your account from different locations.For security purpose, we are required to open an investigation into this matter.

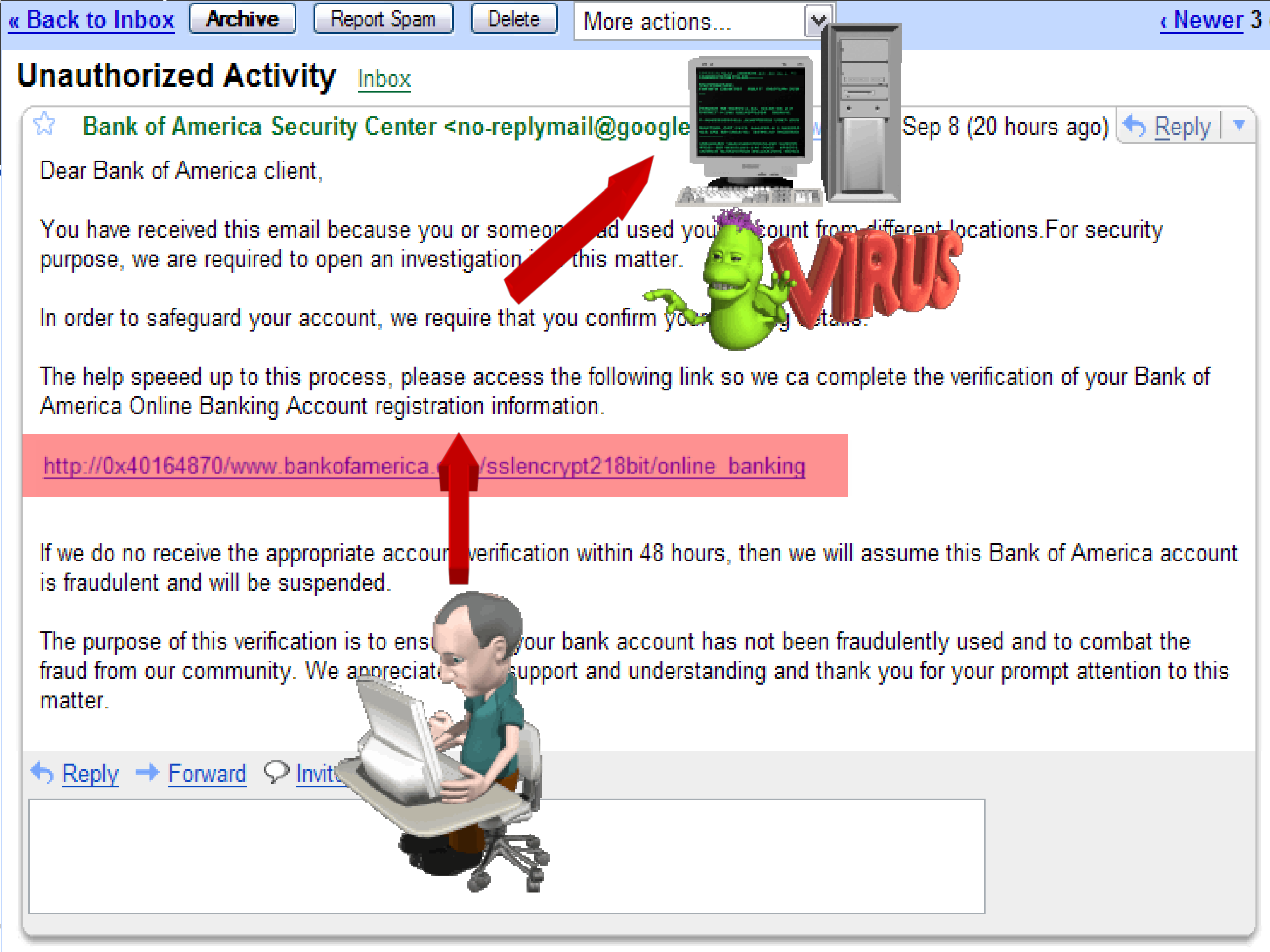
In order to safeguard your account, we require that you confirm your banking details.

The help speeed up to this process, please access the following link so we ca complete the verification of your Bank of America Online Banking Account registration information.

http://0x40164870/www.bankofamerica.com/sslencrypt218bit/online_banking

If we do no receive the appropriat ccount verification within 48 hours, then we will assume this Bank of America account is fraudulent and will be suspend

The purpose of this verification is to ensure that your bank account has not been fraudulently used and to combat the fraud from our community. We appreciate your support and understanding and thank you for your prompt attention to this matter.



## Unauthorized Activity Inbox

Bank of America Security Center <no-replymail@google Sep 8 (20 hours ago)

Dear Bank of America client,

You have received this email because you or someone had used your account from different locations.For security purpose, we are required to open an investigation into this matter.

In order to safeguard your account, we require that you confirm your banking details.

The help speeed up to this process, please access the following link so we ca complete the verification of your Bank of America Online Banking Account registration information.

http://0x40164870/www.bankofamerica.com/sslencrypt218bit/online_banking

If we do no receive the appropriate account verification within 48 hours, then we will assume this Bank of America account is fraudulent and will be suspended.

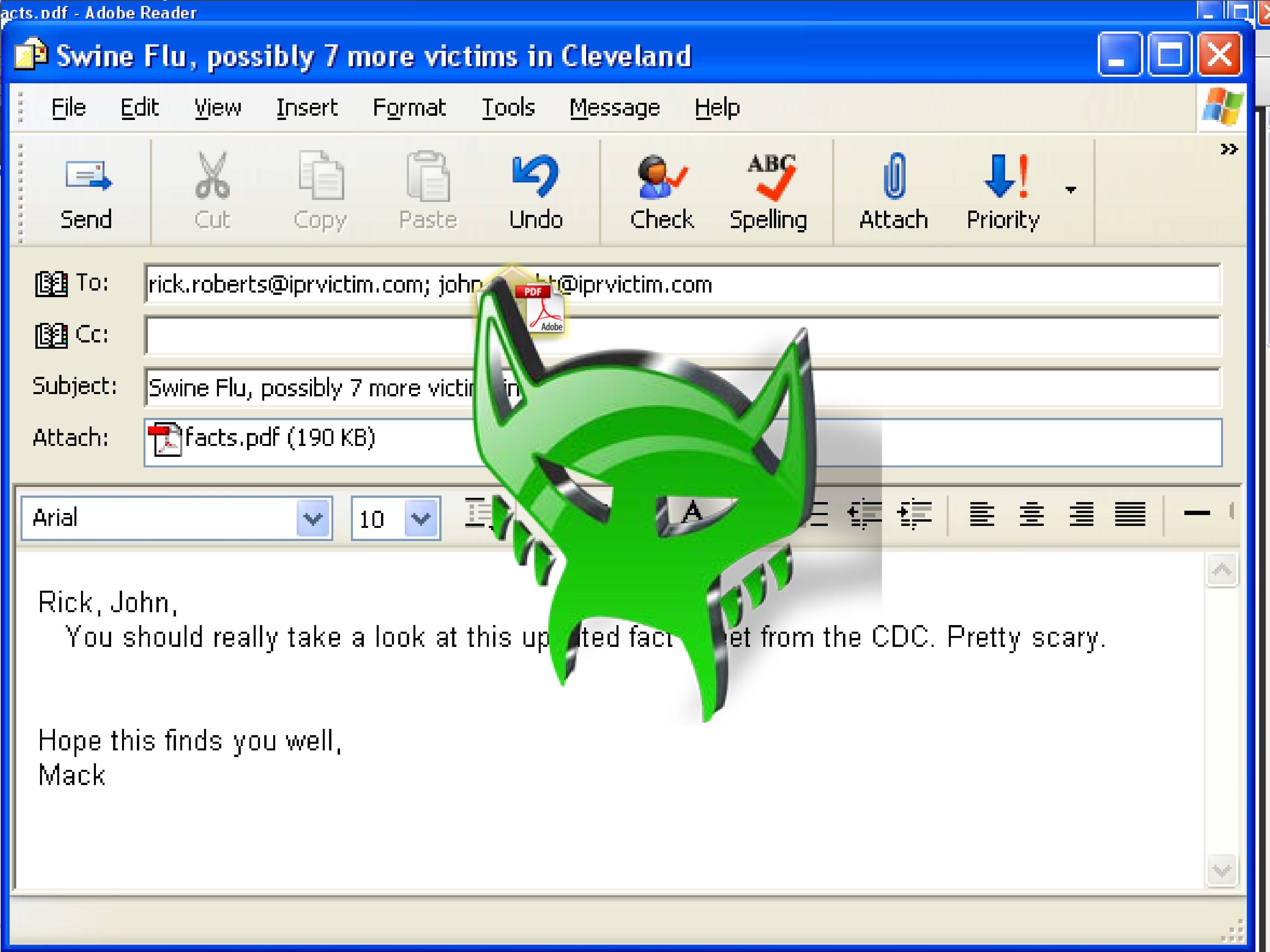
The purpose of this verification is to ensure your bank account has not been fraudulently used and to combat the fraud from our community. We appreciate your support and understanding and thank you for your prompt attention to this matter.

# Targeted Attacks: “Spear Phishing”

Targeted phishing attack

E-mail appears to originate from employer, friend or other *trusted* source

Spear phishing attacks have further evolved, implementing short URL redirection and no file attachments



To: rick.roberts@iprvictim.com; john t@iprvictim.com

Cc:

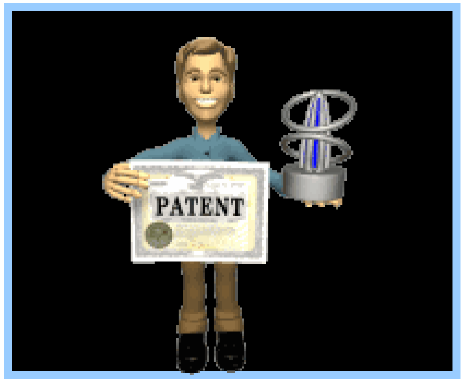
Subject: Swine Flu, possibly 7 more victi in

Attach: facts.pdf (190 KB)

Rick, John,
You should really take a look at this up ted fact et from the CDC. Pretty scary.

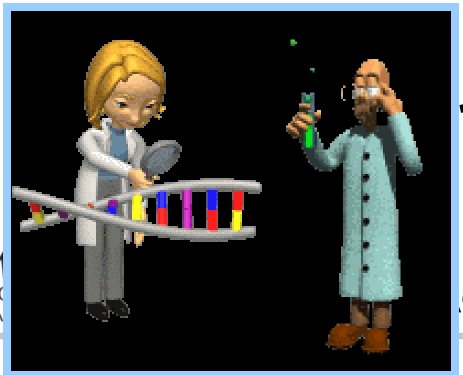
Hope this finds you well,
Mack

# Evolving Victimology



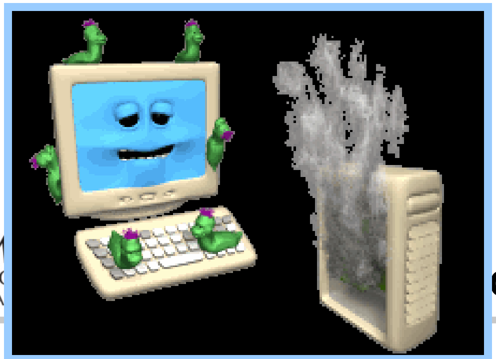
Copyright/Patented Materials

Economic Espionage



Medical/Scientific Research Theft

# Evolving Victimology



Technology/Trade Secrets

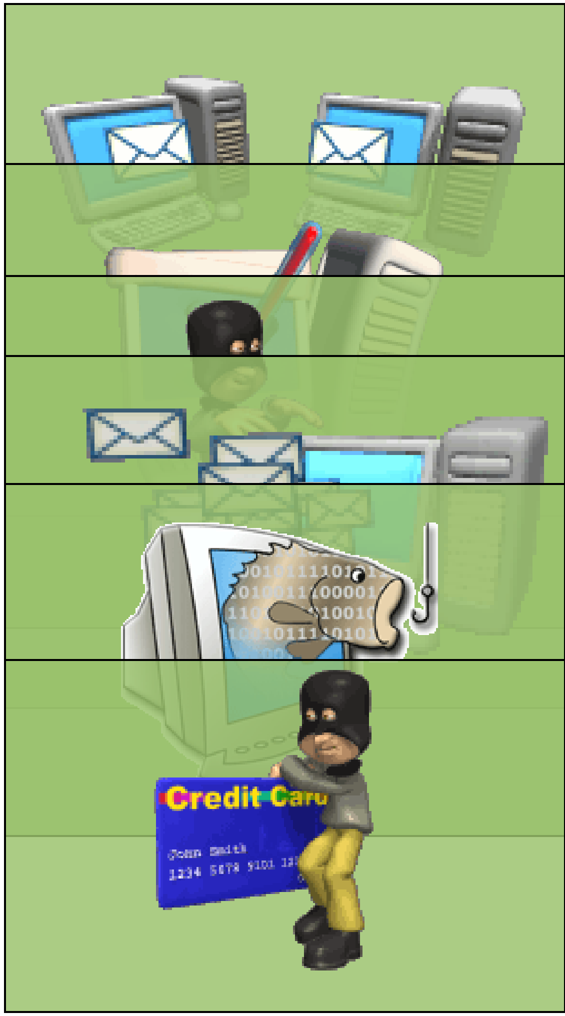
Military Secrets

Attacks Against Infrastructure

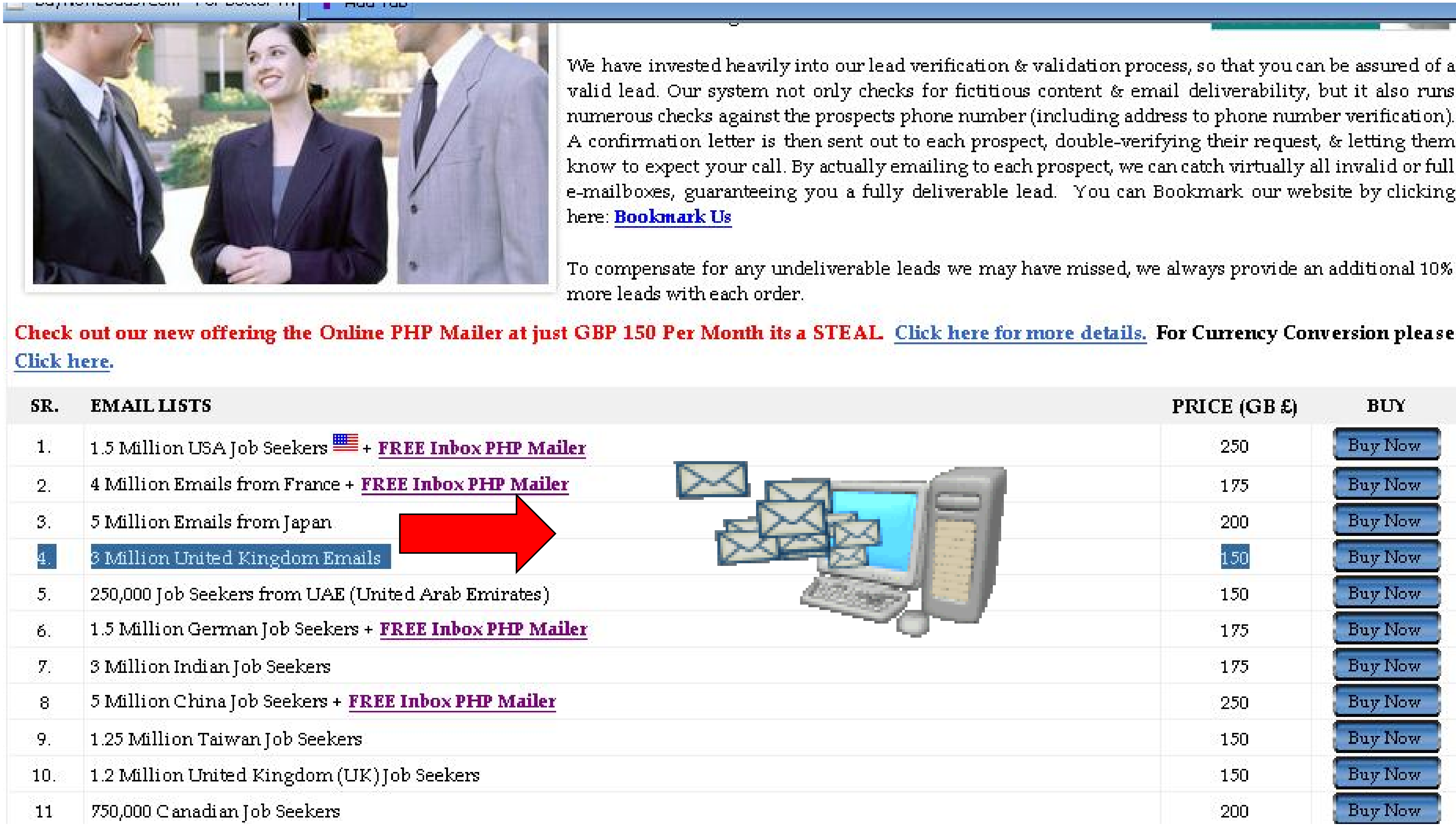
# The Anatomy of a Phishing Scheme: Dissecting the Digital Artifacts

# Evolution of a Phishing Scheme

1. Obtain Victim E-Mail addresses
2. Compromise Victim Server
3. Recruit "Drops"
4. Create Spam E-mail
5. Send Spam Phishing E-mail
6. Collect Victim Information
7. Use Victim Information



# Obtain Victim E-Mail addresses



We have invested heavily into our lead verification & validation process, so that you can be assured of a valid lead. Our system not only checks for fictitious content & email deliverability, but it also runs numerous checks against the prospects phone number (including address to phone number verification). A confirmation letter is then sent out to each prospect, double-verifying their request, & letting them know to expect your call. By actually emailing to each prospect, we can catch virtually all invalid or full e-mailboxes, guaranteeing you a fully deliverable lead. You can Bookmark our website by clicking here: Bookmark Us

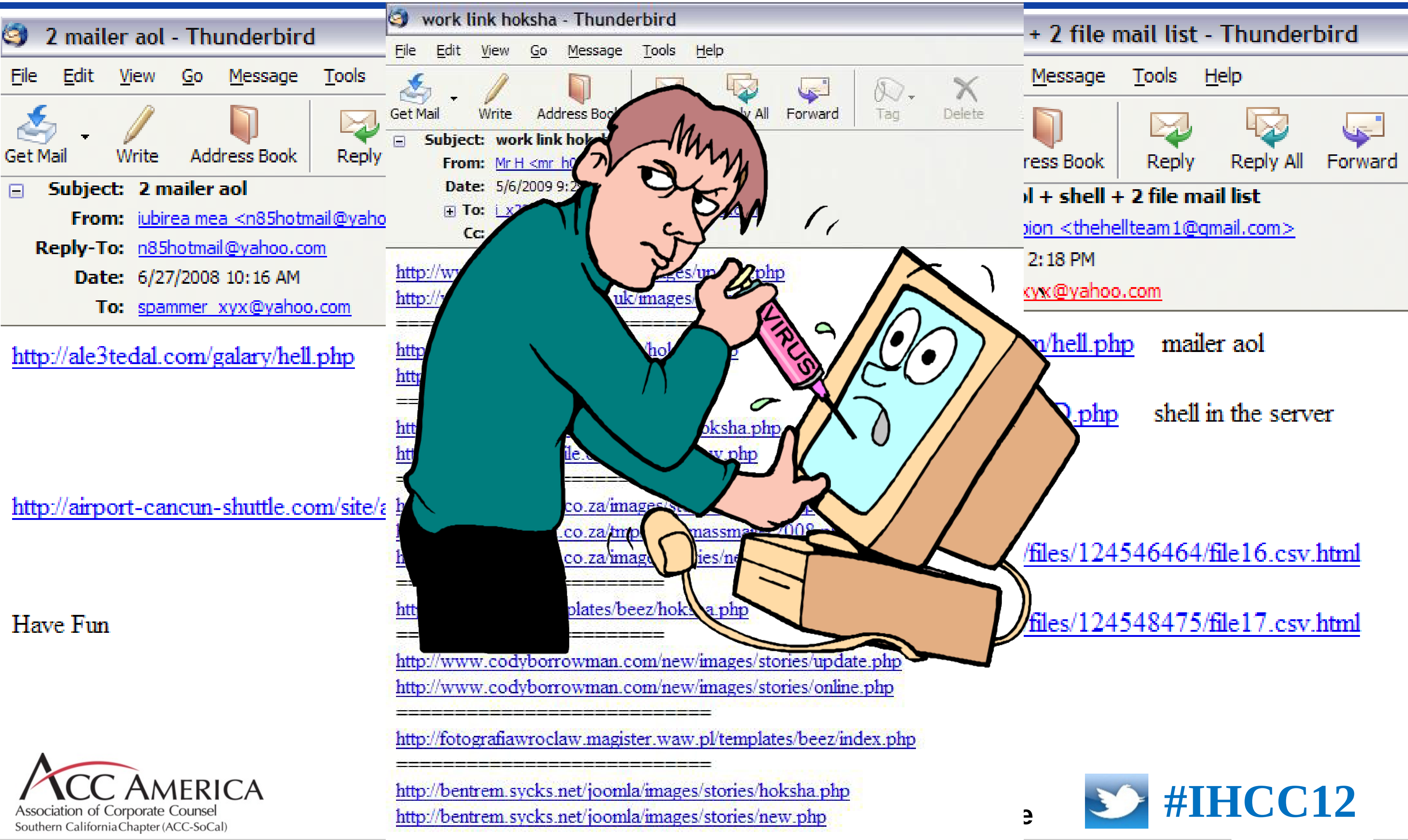
To compensate for any undeliverable leads we may have missed, we always provide an additional 10% more leads with each order.

**Check out our new offering the Online PHP Mailer at just GBP 150 Per Month its a STEAL.** **Click here for more details.** **For Currency Conversion please** **Click here.**

| SR. | EMAIL LISTS | PRICE (GB £) | BUY |
|---|---|---|---|
| 1. | 1.5 Million USA Job Seekers + **FREE Inbox PHP Mailer** | 250 | Buy Now |
| 2. | 4 Million Emails from France + **FREE Inbox PHP Mailer** | 175 | Buy Now |
| 3. | 5 Million Emails from Japan | 200 | Buy Now |
| 4. | 3 Million United Kingdom Emails | 150 | Buy Now |
| 5. | 250,000 Job Seekers from UAE (United Arab Emirates) | 150 | Buy Now |
| 6. | 1.5 Million German Job Seekers + **FREE Inbox PHP Mailer** | 175 | Buy Now |
| 7. | 3 Million Indian Job Seekers | 175 | Buy Now |
| 8 | 5 Million China Job Seekers + **FREE Inbox PHP Mailer** | 250 | Buy Now |
| 9. | 1.25 Million Taiwan Job Seekers | 150 | Buy Now |
| 10. | 1.2 Million United Kingdom (UK) Job Seekers | 150 | Buy Now |
| 11 | 750,000 Canadian Job Seekers | 200 | Buy Now |

STROZ FRIEDBERG
DIGITAL RISK MANAGEMENT & INVESTIGATIONS

# Compromised Computers



2 mailer aol - Thunderbird

Subject: 2 mailer aol
From: iubirea mea <n85hotmail@yaho
Reply-To: n85hotmail@yahoo.com
Date: 6/27/2008 10:16 AM
To: spammer_xyx@yahoo.com

http://ale3tedal.com/galary/hell.php

http://airport-cancun-shuttle.com/site/a

Have Fun

work link hoksha - Thunderbird

Subject: work link hok
From: Mr H <mr_h0
Date: 5/6/2009 9:2
To: i_x
Cc:

http://w ges/up php
http:// uk/images/
===
http /hol
http
==
htt oksha.php
htt ile. w.php
===
h co.za/images/
 co.za/tmp massmail 2008
h co.za/image ies/ne
===
htt plates/beez/hoksha.php
===
http://www.codyborrowman.com/new/images/stories/update.php
http://www.codyborrowman.com/new/images/stories/online.php
============================
http://fotografiawroclaw.magister.waw.pl/templates/beez/index.php
============================
http://bentrem.sycks.net/joomla/images/stories/hoksha.php
http://bentrem.sycks.net/joomla/images/stories/new.php

+ 2 file mail list - Thunderbird

l + shell + 2 file mail list
ion <thehellteam1@gmail.com>
2:18 PM
xyx@yahoo.com

n/hell.php mailer aol

0.php shell in the server

/files/124546464/file16.csv.html

/files/124548475/file17.csv.html

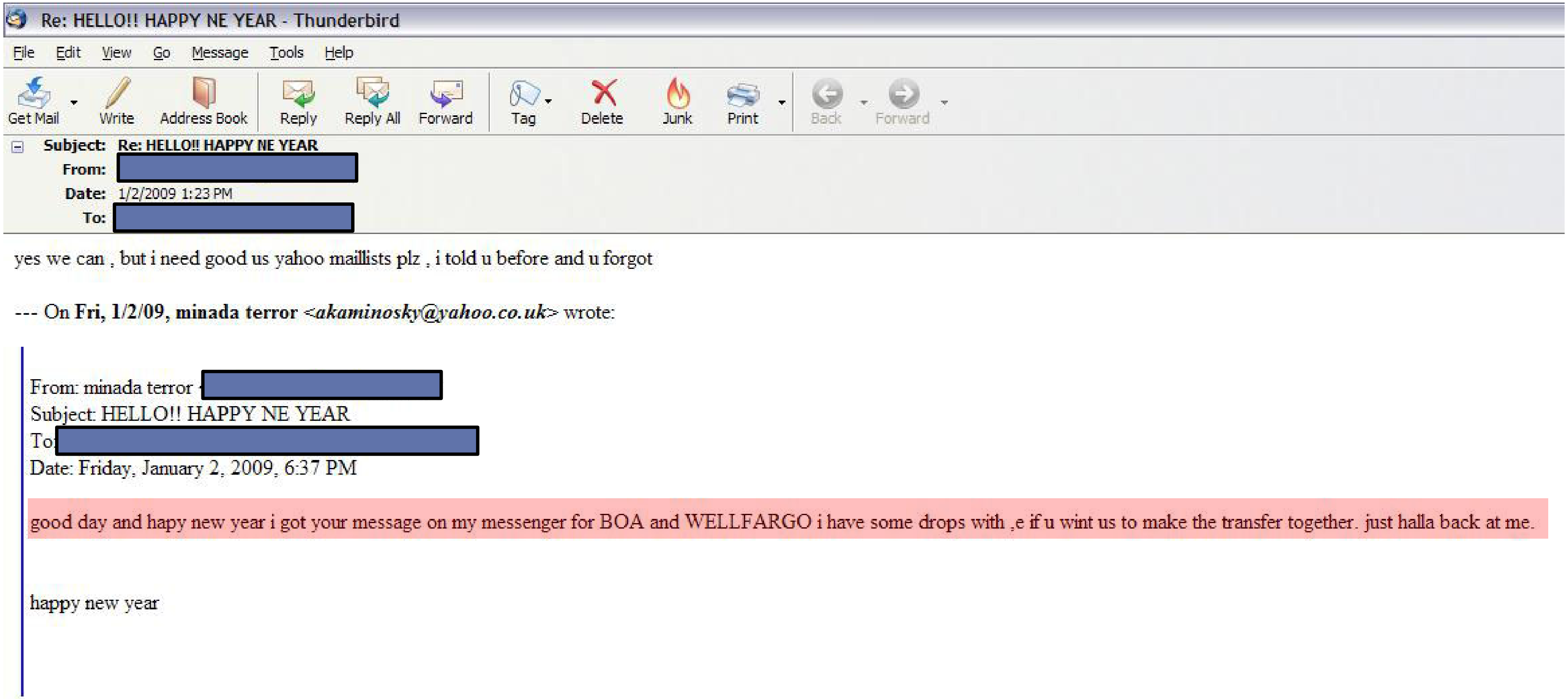
e

ACC AMERICA
Association of Corporate Counsel
Southern California Chapter (ACC-SoCal)

#IHCC12

STROZ FRIEDBERG
DIGITAL RISK MANAGEMENT & INVESTIGATIONS

# Recruit "Drops" (Mules)


Re: HELLO!! HAPPY NE YEAR - Thunderbird
File Edit View Go Message Tools Help
Get Mail
Write
Address Book
Reply
Reply All
Forward
Tag
Delete
Junk
Print
Back
Forward

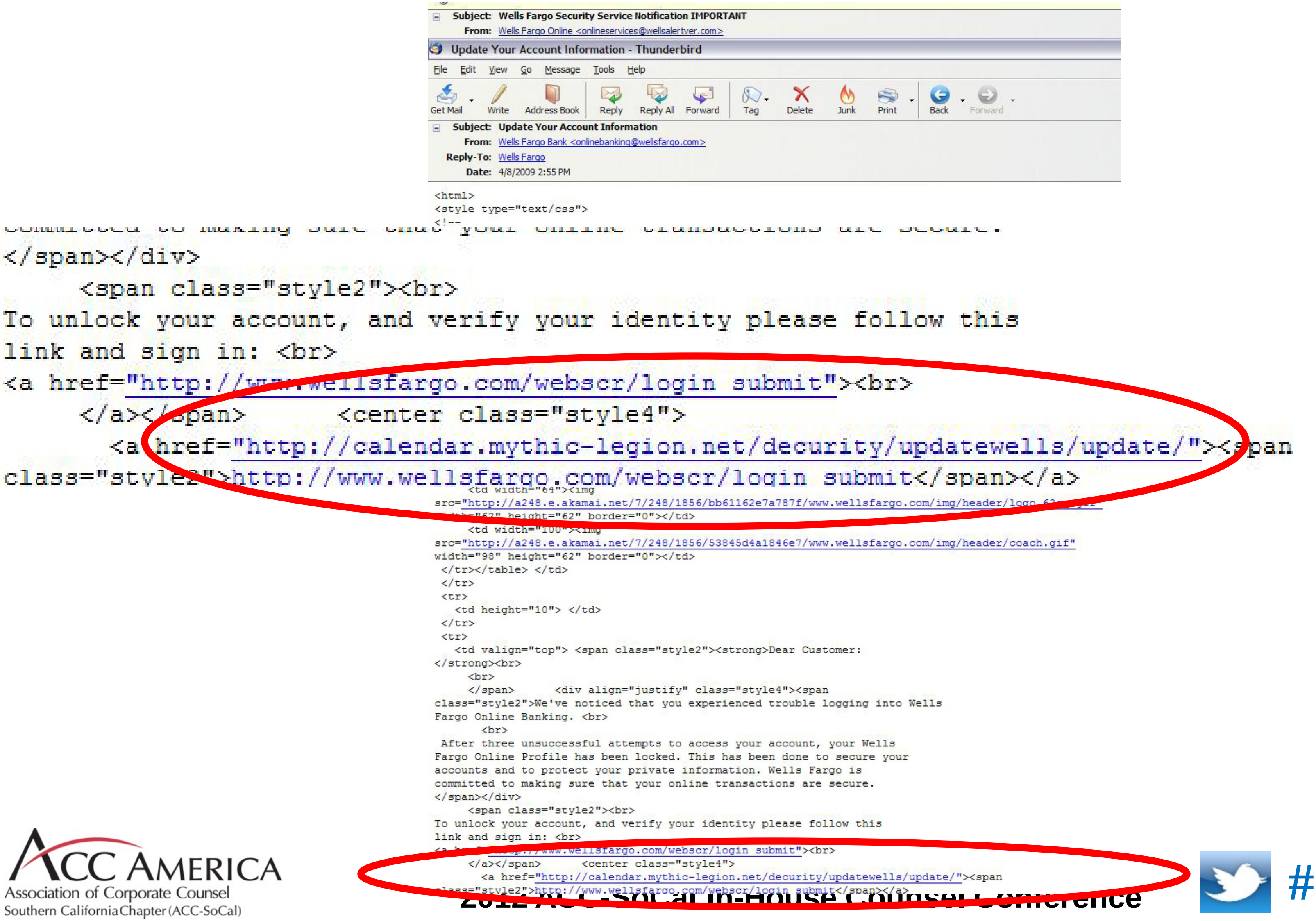
**Subject:** Re: HELLO!! HAPPY NE YEAR
**From:** [redacted]
**Date:** 1/2/2009 1:23 PM
**To:** [redacted]

yes we can , but i need good us yahoo maillists plz , i told u before and u forgot

--- On **Fri, 1/2/09, minada terror** <*akaminosky@yahoo.co.uk*> wrote:

> From: minada terror [redacted]
> Subject: HELLO!! HAPPY NE YEAR
> To: [redacted]
> Date: Friday, January 2, 2009, 6:37 PM
>
> good day and hapy new year i got your message on my messenger for BOA and WELLFARGO i have some drops with ,e if u wint us to make the transfer together. just halla back at me.
>
> happy new year

# Create the phish email-Build in HTML code



Subject: Wells Fargo Security Service Notification IMPORTANT
From: Wells Fargo Online <onlineservices@wellsalertver.com>

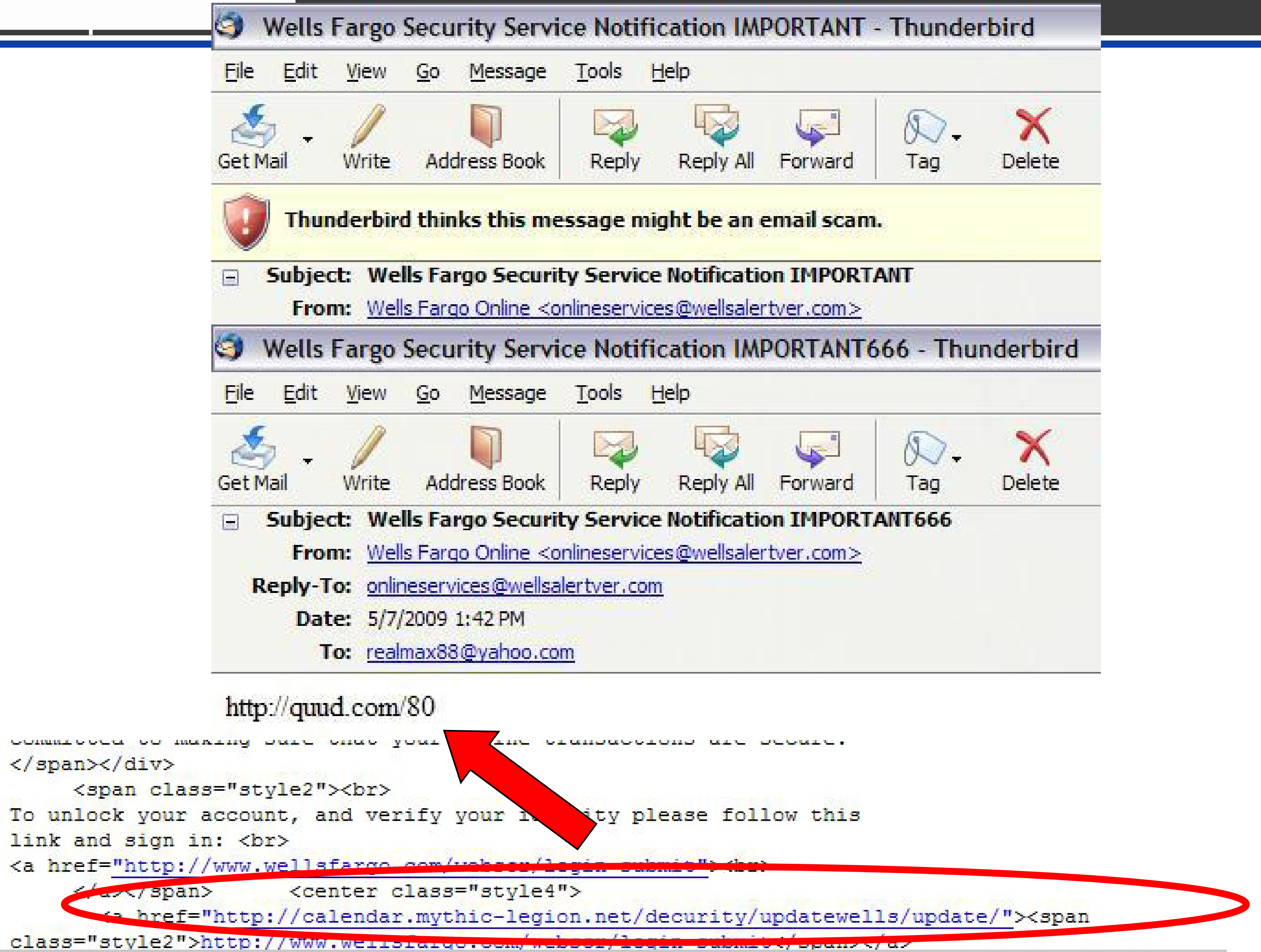
Update Your Account Information - Thunderbird
File Edit View Go Message Tools Help
Get Mail
Write
Address Book
Reply
Reply All
Forward
Tag
Delete
Junk
Print
Back
Forward

Subject: Update Your Account Information
From: Wells Fargo Bank <onlinebanking@wellsfargo.com>
Reply-To: Wells Fargo
Date: 4/8/2009 2:55 PM

```
<html>
<style type="text/css">
<!--
      <td width="64"><img
src="http://a248.e.akamai.net/7/248/1856/bb61162e7a787f/www.wellsfargo.com/img/header/logo_62
width="62" height="62" border="0"></td>
      <td width="100"><img
src="http://a248.e.akamai.net/7/248/1856/53845d4a1846e7/www.wellsfargo.com/img/header/coach.gif"
width="98" height="62" border="0"></td>
 </tr></table> </td>
 </tr>
 <tr>
   <td height="10"> </td>
 </tr>
 <tr>
   <td valign="top"> <span class="style2"><strong>Dear Customer:
</strong><br>
     <br>
     </span>      <div align="justify" class="style4"><span
class="style2">We've noticed that you experienced trouble logging into Wells
Fargo Online Banking. <br>
       <br>
 After three unsuccessful attempts to access your account, your Wells
Fargo Online Profile has been locked. This has been done to secure your
accounts and to protect your private information. Wells Fargo is
committed to making sure that your online transactions are secure.
</span></div>
     <span class="style2"><br>
To unlock your account, and verify your identity please follow this
link and sign in: <br>
<a href="http://www.wellsfargo.com/webscr/login submit"><br>
     </a></span>      <center class="style4">
       <a href="http://calendar.mythic-legion.net/decurity/updatewells/update/"><span
class="style2">http://www.wellsfargo.com/webscr/login submit</span></a>
```

```
committed to making sure that your online transactions are secure.
</span></div>
     <span class="style2"><br>
To unlock your account, and verify your identity please follow this
link and sign in: <br>
<a href="http://www.wellsfargo.com/webscr/login submit"><br>
     </a></span>      <center class="style4">
       <a href="http://calendar.mythic-legion.net/decurity/updatewells/update/"><span
class="style2">http://www.wellsfargo.com/webscr/login submit</span></a>
```

# Short URL Re-direct



Thunderbird thinks this message might be an email scam.

**Subject:** Wells Fargo Security Service Notification IMPORTANT
**From:** Wells Fargo Online <onlineservices@wellsalertver.com>

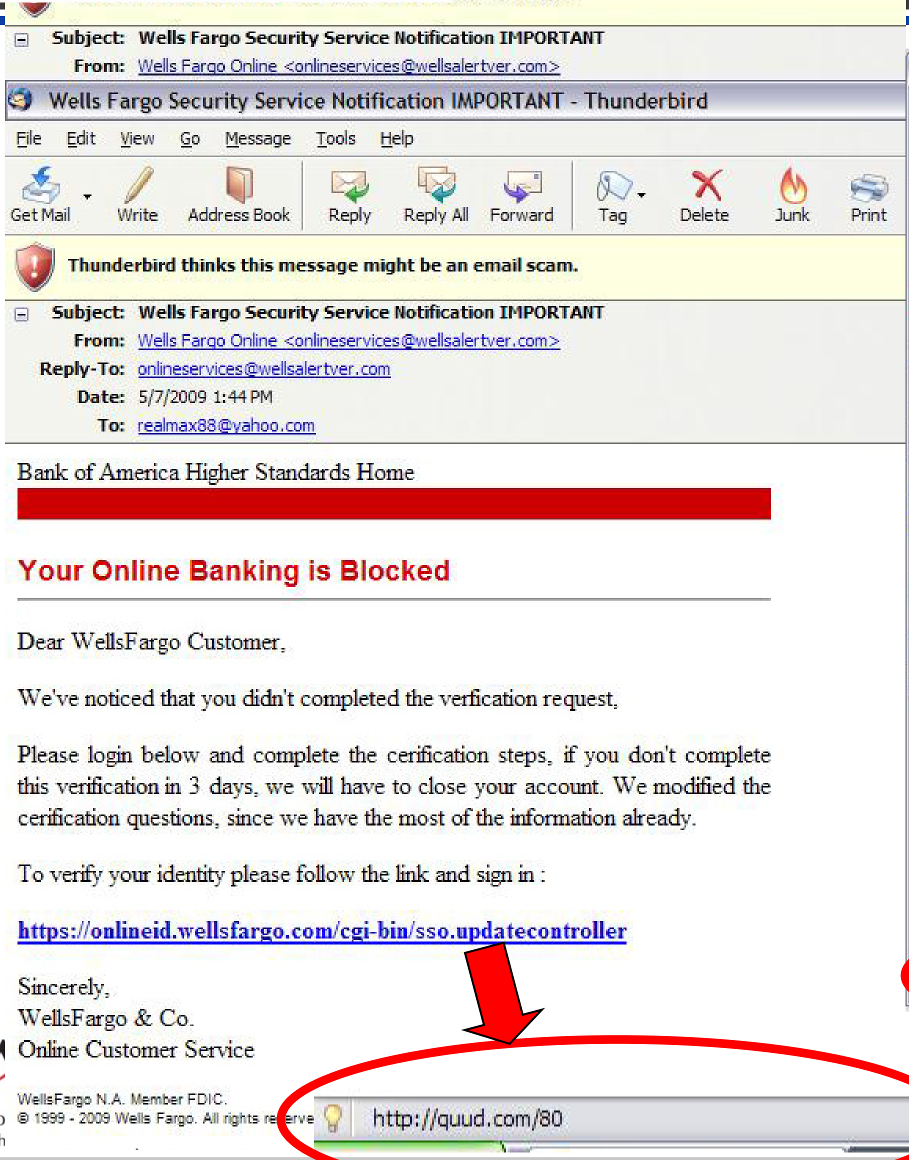
**Subject:** Wells Fargo Security Service Notification IMPORTANT666
**From:** Wells Fargo Online <onlineservices@wellsalertver.com>
**Reply-To:** onlineservices@wellsalertver.com
**Date:** 5/7/2009 1:42 PM
**To:** realmax88@yahoo.com

http://quud.com/80

```
committed to making sure that your online transactions are secure.
</span></div>
    <span class="style2"><br>
To unlock your account, and verify your identity please follow this
link and sign in: <br>
<a href="http://www.wellsfargo.com/webscr/login-submit"> <br>
    </a></span>      <center class="style4">
      <a href="http://calendar.mythic-legion.net/decurity/updatewells/update/"><span
class="style2">http://www.wellsfargo.com/webscr/login-submit</span></a>
```

Association o
Southern Califo

# Activate Hyperlinks



Subject: Wells Fargo Security Service Notification IMPORTANT
From: Wells Fargo Online <onlineservices@wellsalertver.com>

Wells Fargo Security Service Notification IMPORTANT - Thunderbird
File Edit View Go Message Tools Help
Get Mail
Write
Address Book
Reply
Reply All
Forward
Tag
Delete
Junk
Print

Thunderbird thinks this message might be an email scam.

Subject: Wells Fargo Security Service Notification IMPORTANT
From: Wells Fargo Online <onlineservices@wellsalertver.com>
Reply-To: onlineservices@wellsalertver.com
Date: 5/7/2009 1:44 PM
To: realmax88@yahoo.com

Bank of America Higher Standards Home

Your Online Banking is Blocked

Dear WellsFargo Customer,

We've noticed that you didn't completed the verfication request,

Please login below and complete the cerification steps, if you don't complete this verification in 3 days, we will have to close your account. We modified the cerification questions, since we have the most of the information already.

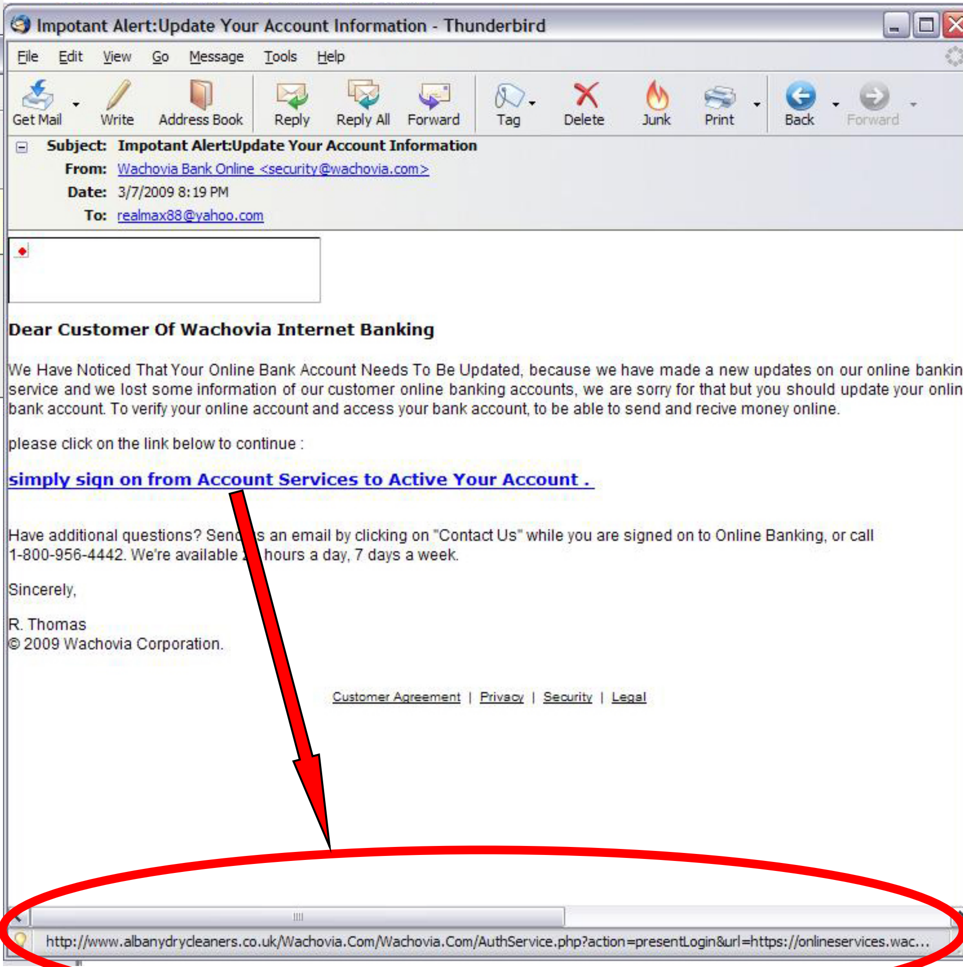
To verify your identity please follow the link and sign in :

https://onlineid.wellsfargo.com/cgi-bin/sso.updatecontroller

Sincerely,
WellsFargo & Co.
Online Customer Service

WellsFargo N.A. Member FDIC.
© 1999 - 2009 Wells Fargo. All rights re erve

http://quud.com/80



Impotant Alert:Update Your Account Information - Thunderbird
File Edit View Go Message Tools Help
Get Mail
Write
Address Book
Reply
Reply All
Forward
Tag
Delete
Junk
Print
Back
Forward

Subject: Impotant Alert:Update Your Account Information
From: Wachovia Bank Online <security@wachovia.com>
Date: 3/7/2009 8:19 PM
To: realmax88@yahoo.com

Dear Customer Of Wachovia Internet Banking

We Have Noticed That Your Online Bank Account Needs To Be Updated, because we have made a new updates on our online bankin service and we lost some information of our customer online banking accounts, we are sorry for that but you should update your onlin bank account. To verify your online account and access your bank account, to be able to send and recive money online.

please click on the link below to continue :

simply sign on from Account Services to Active Your Account .

Have additional questions? Send s an email by clicking on "Contact Us" while you are signed on to Online Banking, or call 1-800-956-4442. We're available hours a day, 7 days a week.

Sincerely,

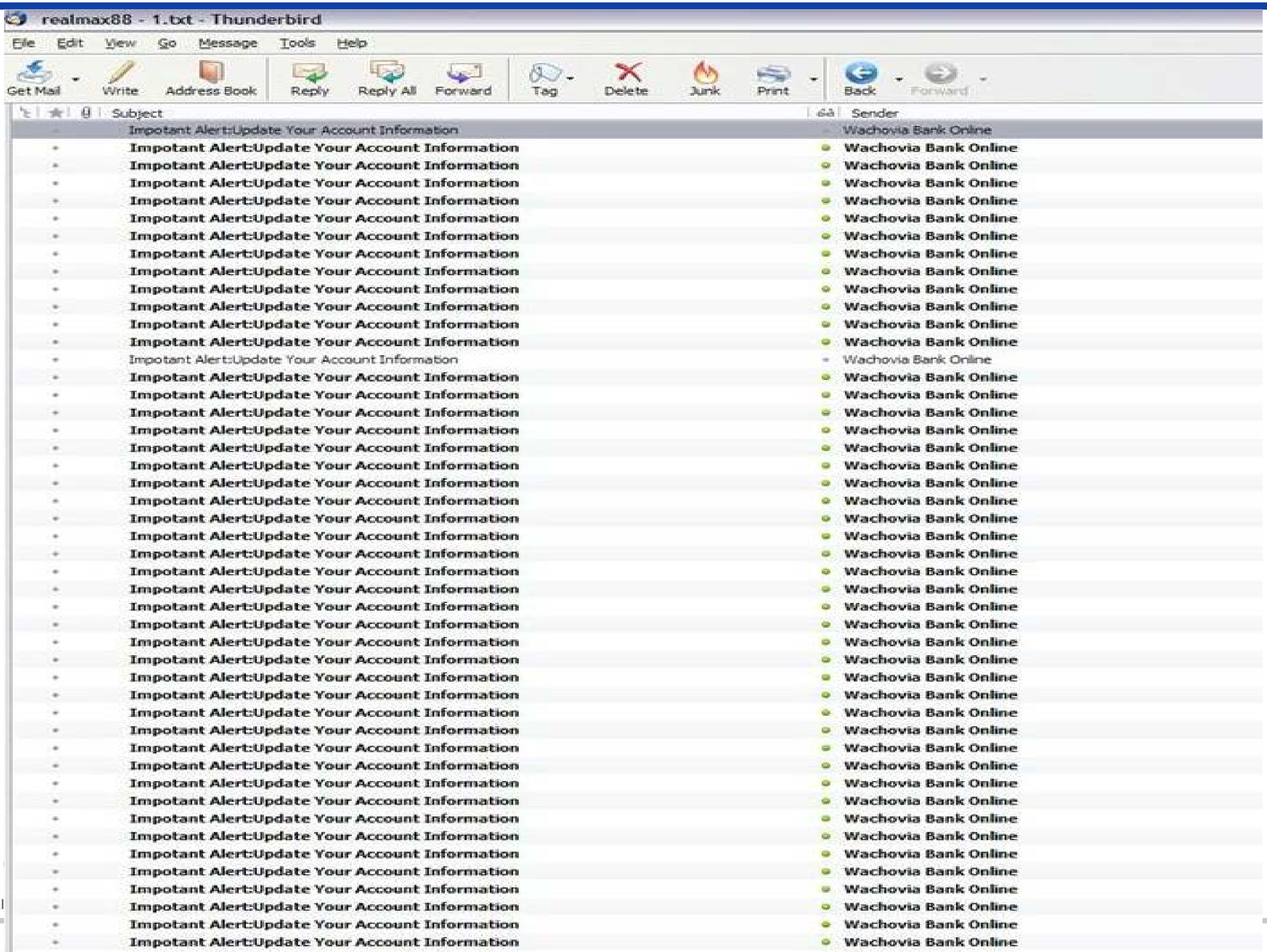
R. Thomas
© 2009 Wachovia Corporation.

Customer Agreement | Privacy | Security | Legal

http://www.albanydrycleaners.co.uk/Wachovia.Com/Wachovia.Com/AuthService.php?action=presentLogin&url=https://onlineservices.wac...

STROZ FRIEDBERG
DIGITAL RISK MANAGEMENT & INVESTIGATIONS

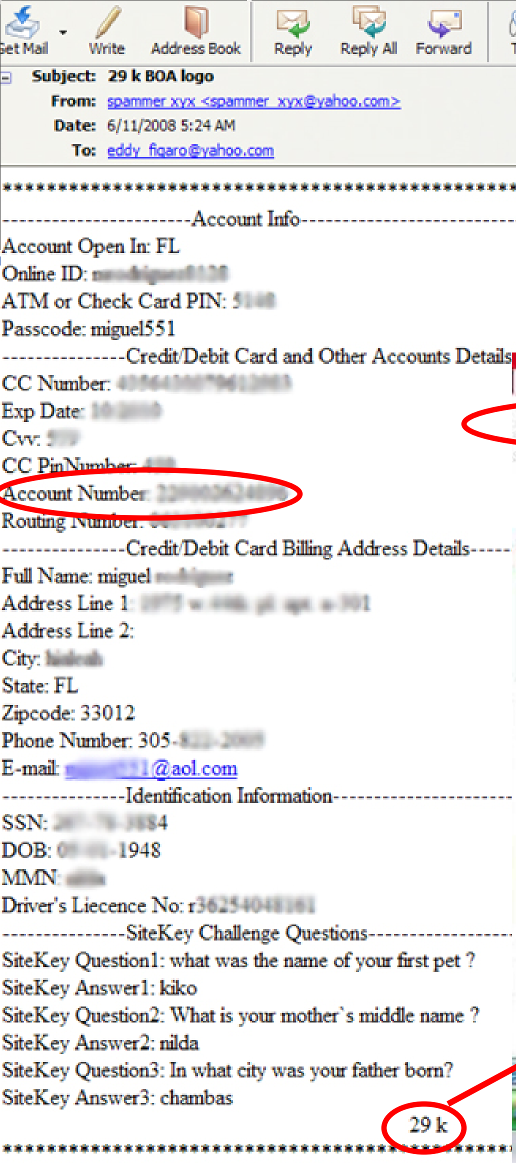
# Create the Phishing e-mail: Testing Phase



| Subject | Sender |
|---|---|
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |
| Impotant Alert:Update Your Account Information | Wachovia Bank Online |

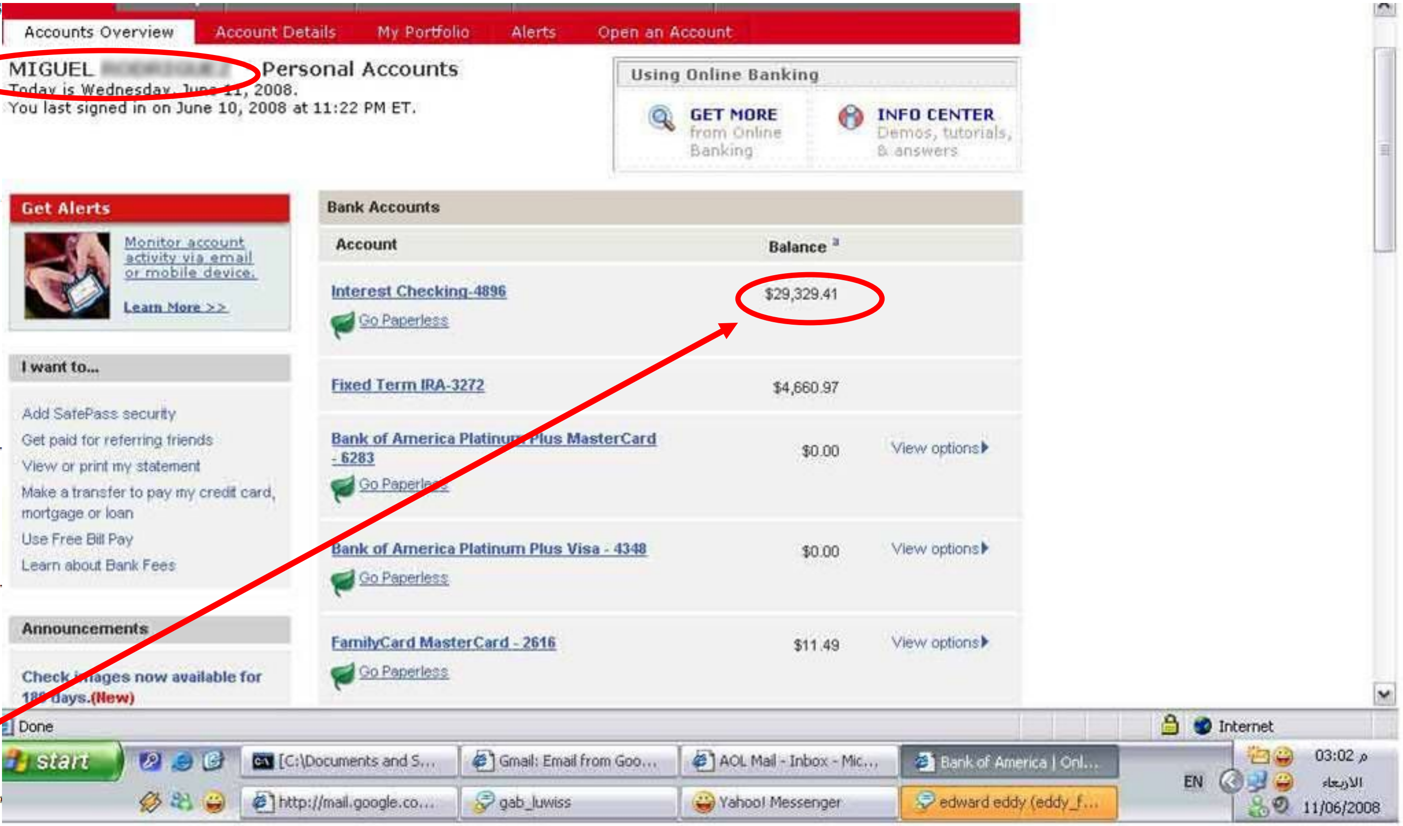
ACC AMERI
Association of Corporate Counsel
Southern California Chapter (ACC-SoCal

# Collect Victim Information



**Subject:** 29 k BOA logo
**From:** spammer xyx <spammer_xyx@yahoo.com>
**Date:** 6/11/2008 5:24 AM
**To:** eddy_figaro@yahoo.com

```
*********************************************************************
--------------------Account Info--------------------------------
Account Open In: FL
Online ID: [redacted]
ATM or Check Card PIN: [redacted]
Passcode: miguel551
--------------Credit/Debit Card and Other Accounts Details
CC Number: [redacted]
Exp Date: [redacted]
Cvv: [redacted]
CC PinNumber: [redacted]
Account Number: [redacted]
Routing Number: [redacted]
--------------Credit/Debit Card Billing Address Details-----
Full Name: miguel [redacted]
Address Line 1: [redacted]
Address Line 2:
City: [redacted]
State: FL
Zipcode: 33012
Phone Number: 305-[redacted]
E-mail: [redacted]@aol.com
--------------Identification Information--------------------
SSN: [redacted]
DOB: [redacted]-1948
MMN: [redacted]
Driver's Liecence No: r[redacted]
--------------SiteKey Challenge Questions----------------
SiteKey Question1: what was the name of your first pet ?
SiteKey Answer1: kiko
SiteKey Question2: What is your mother`s middle name ?
SiteKey Answer2: nilda
SiteKey Question3: In what city was your father born?
SiteKey Answer3: chambas
                                          29 k
*******************************************************
```

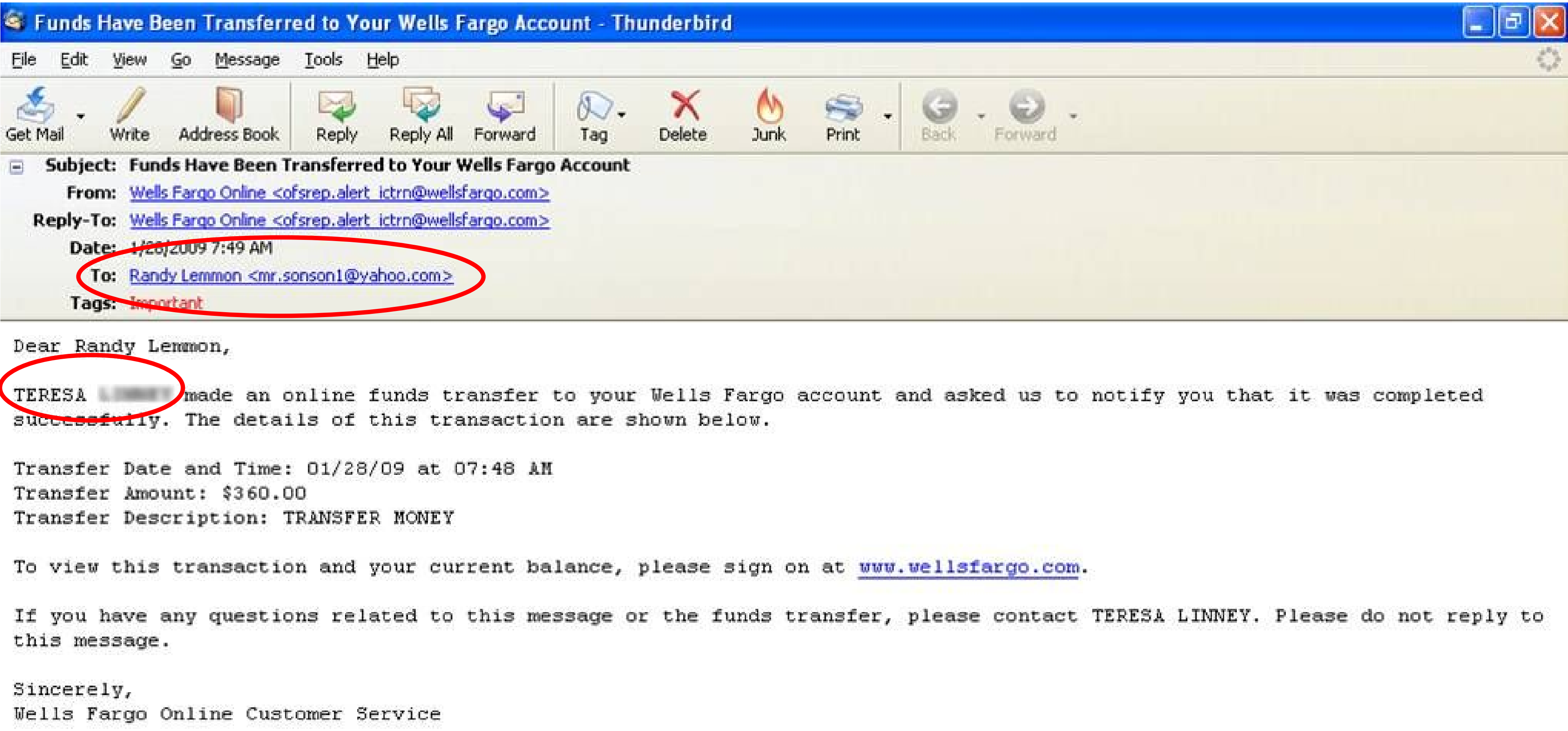


MIGUEL [redacted] Personal Accounts
Today is Wednesday, June 11, 2008.
You last signed in on June 10, 2008 at 11:22 PM ET.

Bank Accounts

| Account | Balance |
|---|---|
| Interest Checking-4896 | $29,329.41 |
| Fixed Term IRA-3272 | $4,660.97 |
| Bank of America Platinum Plus MasterCard - 6283 | $0.00 |
| Bank of America Platinum Plus Visa - 4348 | $0.00 |
| FamilyCard MasterCard - 2616 | $11.49 |

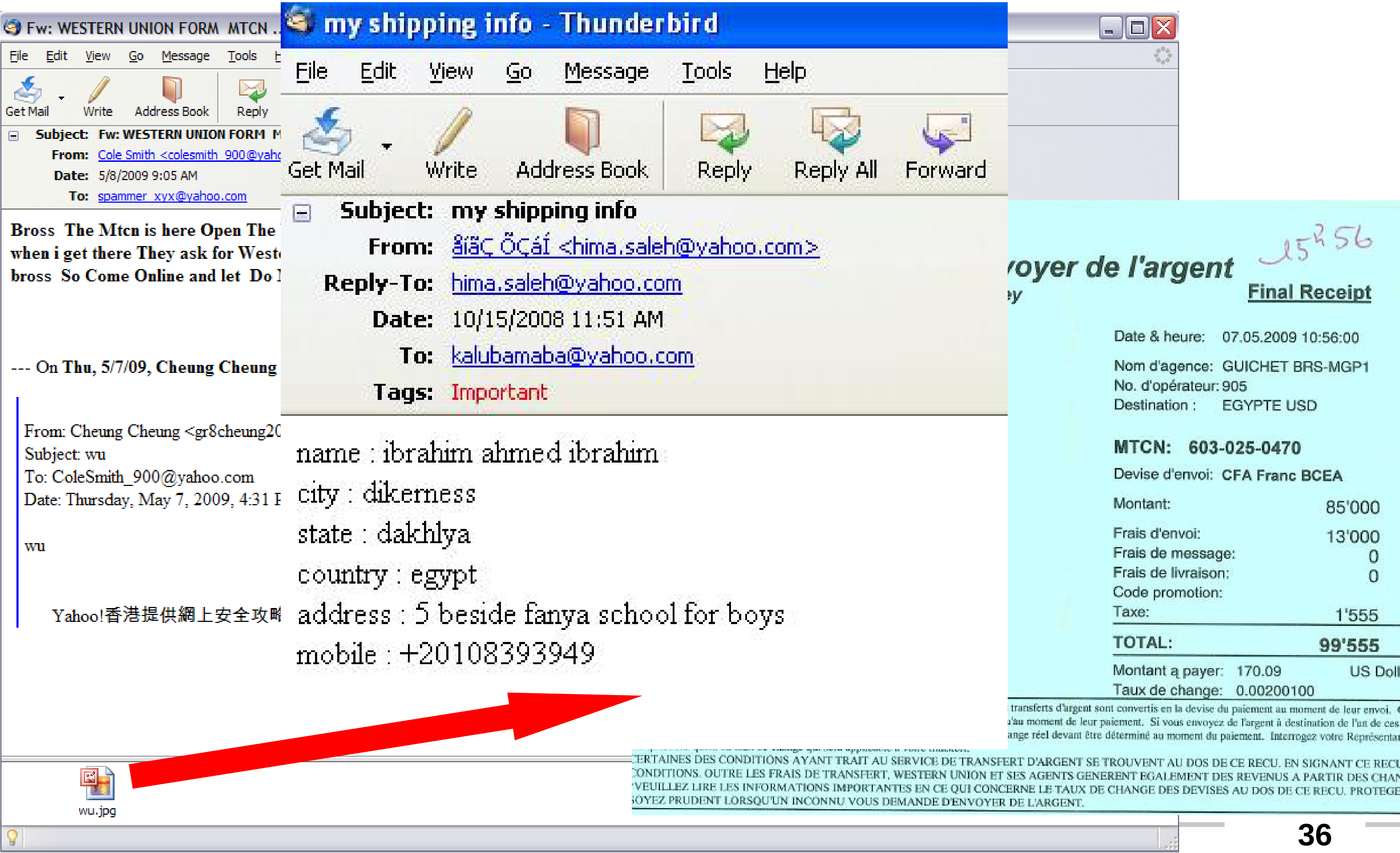
# Wire Transfer $$$ Using Victim Information


Funds Have Been Transferred to Your Wells Fargo Account - Thunderbird
File Edit View Go Message Tools Help
Get Mail
Write
Address Book
Reply
Reply All
Forward
Tag
Delete
Junk
Print
Back
Forward

**Subject:** Funds Have Been Transferred to Your Wells Fargo Account
**From:** Wells Fargo Online <ofsrep.alert_ictrn@wellsfargo.com>
**Reply-To:** Wells Fargo Online <ofsrep.alert_ictrn@wellsfargo.com>
**Date:** 1/28/2009 7:49 AM
**To:** Randy Lemmon <mr.sonson1@yahoo.com>
**Tags:** Important

```
Dear Randy Lemmon,

TERESA [redacted] made an online funds transfer to your Wells Fargo account and asked us to notify you that it was completed
successfully. The details of this transaction are shown below.

Transfer Date and Time: 01/28/09 at 07:48 AM
Transfer Amount: $360.00
Transfer Description: TRANSFER MONEY

To view this transaction and your current balance, please sign on at www.wellsfargo.com.

If you have any questions related to this message or the funds transfer, please contact TERESA LINNEY. Please do not reply to
this message.

Sincerely,
Wells Fargo Online Customer Service
```

# “Drop” (Mule) Payments


Fw: WESTERN UNION FORM MTCN ...
File Edit View Go Message Tools H
Get Mail
Write
Address Book
Reply

Subject: Fw: WESTERN UNION FORM M
From: Cole Smith <colesmith_900@yahc
Date: 5/8/2009 9:05 AM
To: spammer_xyx@yahoo.com

**Bross The Mtcn is here Open The**
**when i get there They ask for West**
**bross So Come Online and let Do I**

--- On **Thu, 5/7/09, Cheung Cheung**

> From: Cheung Cheung <gr8cheung2C
> Subject: wu
> To: ColeSmith_900@yahoo.com
> Date: Thursday, May 7, 2009, 4:31 F
>
> wu
>
> Yahoo!香港提供網上安全攻略

wu.jpg
my shipping info - Thunderbird
File Edit View Go Message Tools Help
Get Mail
Write
Address Book
Reply
Reply All
Forward

Subject: my shipping info
From: ßîãÇ ÕÇáÍ <hima.saleh@yahoo.com>
Reply-To: hima.saleh@yahoo.com
Date: 10/15/2008 11:51 AM
To: kalubamaba@yahoo.com
Tags: Important

name : ibrahim ahmed ibrahim
city : dikerness
state : dakhlya
country : egypt
address : 5 beside fanya school for boys
mobile : +20108393949

voyer de l'argent
ey

15256

**Final Receipt**

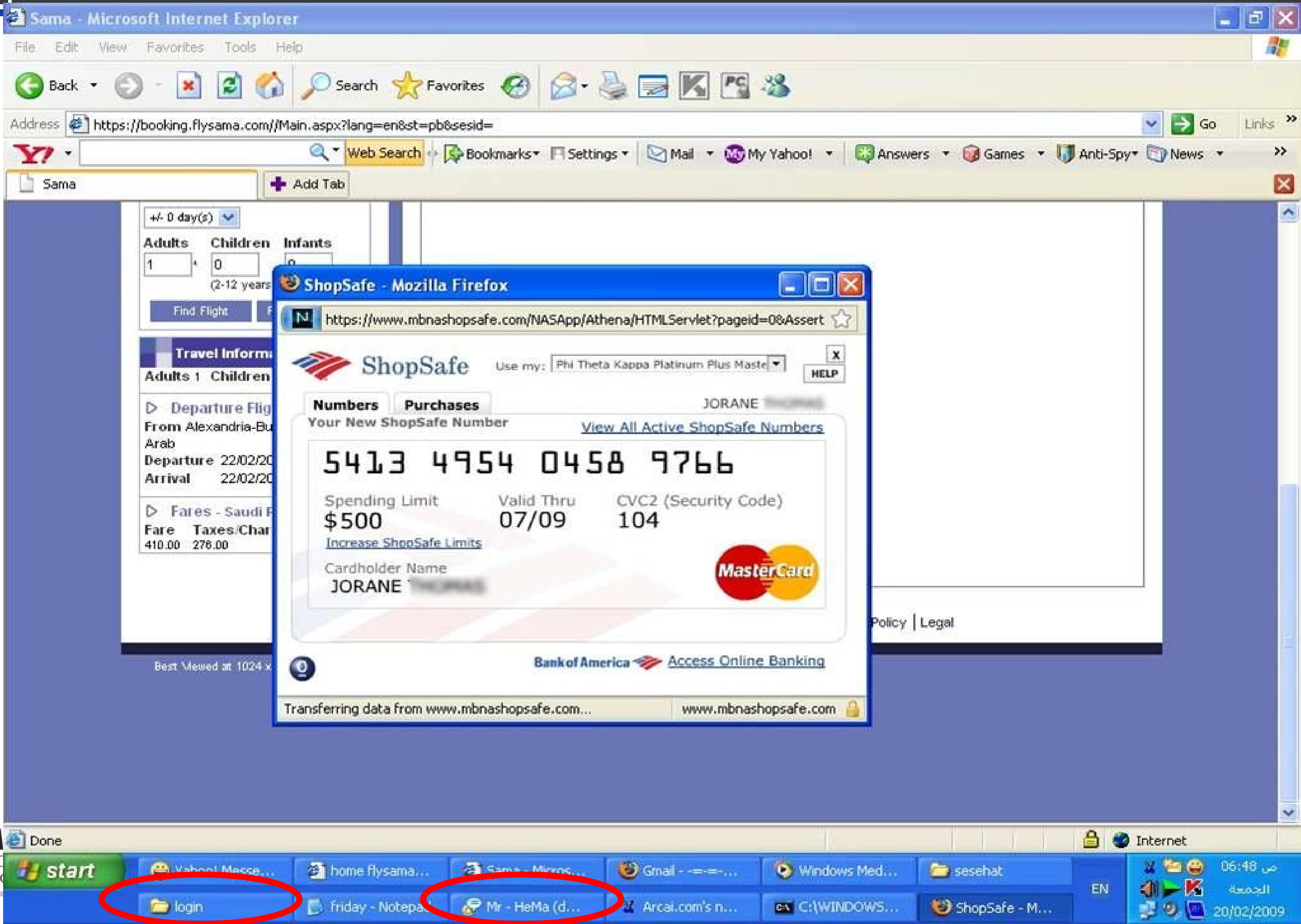
| | |
|---|---|
| Date & heure: | 07.05.2009 10:56:00 |
| Nom d'agence: | GUICHET BRS-MGP1 |
| No. d'opérateur: | 905 |
| Destination : | EGYPTE USD |
| **MTCN:** | **603-025-0470** |
| Devise d'envoi: | **CFA Franc BCEA** |
| Montant: | 85'000 |
| Frais d'envoi: | 13'000 |
| Frais de message: | 0 |
| Frais de livraison: | 0 |
| Code promotion: | |
| Taxe: | 1'555 |
| **TOTAL:** | **99'555** |
| Montant ą payer: | 170.09 US Doll |
| Taux de change: | 0.00200100 |

transferts d'argent sont convertis en la devise du paiement au moment de leur envoi. (
u'au moment de leur paiement. Si vous envoyez de l'argent à destination de l'un de ces
ange réel devant être déterminé au moment du paiement. Interrogez votre Représentan

CERTAINES DES CONDITIONS AYANT TRAIT AU SERVICE DE TRANSFERT D'ARGENT SE TROUVENT AU DOS DE CE RECU. EN SIGNANT CE RECU
CONDITIONS. OUTRE LES FRAIS DE TRANSFERT, WESTERN UNION ET SES AGENTS GENERENT EGALEMENT DES REVENUS A PARTIR DES CHAN
VEUILLEZ LIRE LES INFORMATIONS IMPORTANTES EN CE QUI CONCERNE LE TAUX DE CHANGE DES DEVISES AU DOS DE CE RECU. PROTEGE
SOYEZ PRUDENT LORSQU'UN INCONNU VOUS DEMANDE D'ENVOYER DE L'ARGENT.

STROZ FRIEDBERG
DIGITAL RISK MANAGEMENT & INVESTIGATIONS

# Use Victim Information



Sama - Microsoft Internet Explorer

Address https://booking.flysama.com//Main.aspx?lang=en&st=pb&sesid=

+/- 0 day(s)

Adults 1 Children 0 Infants 0 (2-12 years

Travel Inform

Adults 1 Children

Departure Flig
From Alexandria-Bu
Arab
Departure 22/02/20
Arrival 22/02/20

Fares - Saudi
Fare 410.00 Taxes/Char 276.00

ShopSafe - Mozilla Firefox

https://www.mbnashopsafe.com/NASApp/Athena/HTMLServlet?pageid=0&Assert

ShopSafe Use my: Phi Theta Kappa Platinum Plus Maste

JORANE [redacted]

Your New ShopSafe Number

View All Active ShopSafe Numbers

5413 4954 0458 9766

Spending Limit $500
Valid Thru 07/09
CVC2 (Security Code) 104

Increase ShopSafe Limits

Cardholder Name JORANE [redacted]

Bank of America Access Online Banking

Transferring data from www.mbnashopsafe.com...

www.mbnashopsafe.com

Best Viewed at 1024 x

Policy | Legal

Done

Internet

06:48 ص
الجمعة
20/02/2009

ACC AM
Association of Corporate C
Southern California Chapter (AC

# Significant Take-Away Points

- Normal Internet Activity Leaves a Significant amount of digital breadcrumbs
- This Information is Used for Social Engineering Purposes
- Take Pre-Cautionary Measures to Safeguard your Personal Information
- Check the Links Before Clicking
- Banks NEVER Solicit Account Information via Email

# Panelists

- Kris Ashman, Moderator
  - United States Postal Service, Attorney (Labor & Employment), kristi.j.ashman@usps.gov
- Jason Smolanoff
  - Stroz Friedberg, Vice President
  - jsmolanoff@strozfriedberg.com
- Camilla Eng
  - General Counsel, JM Eagle
  - CamillaEng@JMEagle.com
- Dawn Haghighi
  - Chief Privacy Officer, Princess Cruises