Corporate Account Takeover & Information Security Awareness

The information contained in this session may contain privileged and confidential information. This presentation is for information purposes only. Before acting on any ideas presented in this session; security, legal, technical, and reputational risks should be independently evaluated considering the unique factual circumstances surrounding each institution. No computer system can provide absolute security under all conditions. Any views or opinions presented do not necessarily state or reflect those of "Mifflinburg Bank & Trust" or any other entity.

What Will Be Covered?

- What is corporate account takeover?
- How does it work?
- Statistics
- Current trend examples
- What can we do to protect?
- What can businesses do to protect?

What Is Corporate Account Takeover?

A fast growing electronic crime where thieves typically use some form of malware to obtain login credentials to corporate online banking accounts and fraudulently transfer funds from the account(s).

Malware

•Short for *malicious software*, is software designed to infiltrate a computer system without the owner's informed consent.

• Malware includes computer viruses, worms, Trojan horses, spyware, dishonest adware, crimeware, most rootkits, and other malicious and unwanted software.

Fact:
Domestic and international wire transfers, business-to-business ACH payments, online bill pay and electronic payroll payments have all been used to commit this crime.

How Does It Work?

- Criminals target victims by scams.
- Victim unknowingly installs software by clicking on a link or visiting an infected internet site.
- Fraudsters begin monitoring the accounts.
- Victim logs in to their online banking.
- Fraudsters collect login credentials.
- Fraudsters wait for the right time, and then - depending on your controls - they log in after hours, or if you are utilizing a token, they wait until you enter your code. Then they hijack the session and send you a message that online banking is temporarily unavailable.

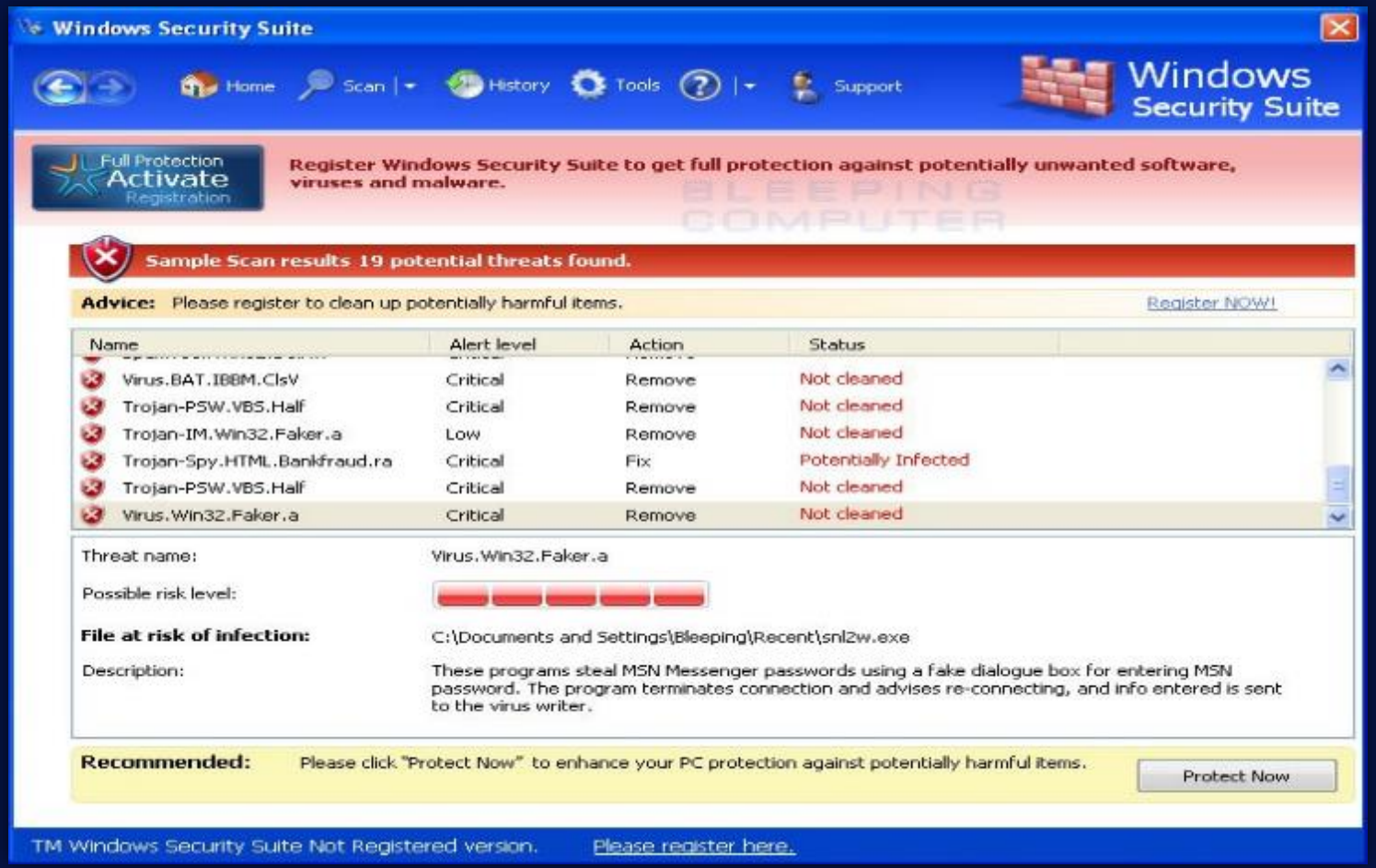
Where Does It Come From?

- Malicious websites (including social networking sites)
- Email
- P2P downloads (e.g. music files, images, PDFs)
- Ads from popular websites
- Web-borne infections:
  - According to researchers, 76% of web resources used to spread malicious programs were found in 5 countries worldwide: United States, Russian Federation, Netherlands, China and Ukraine.

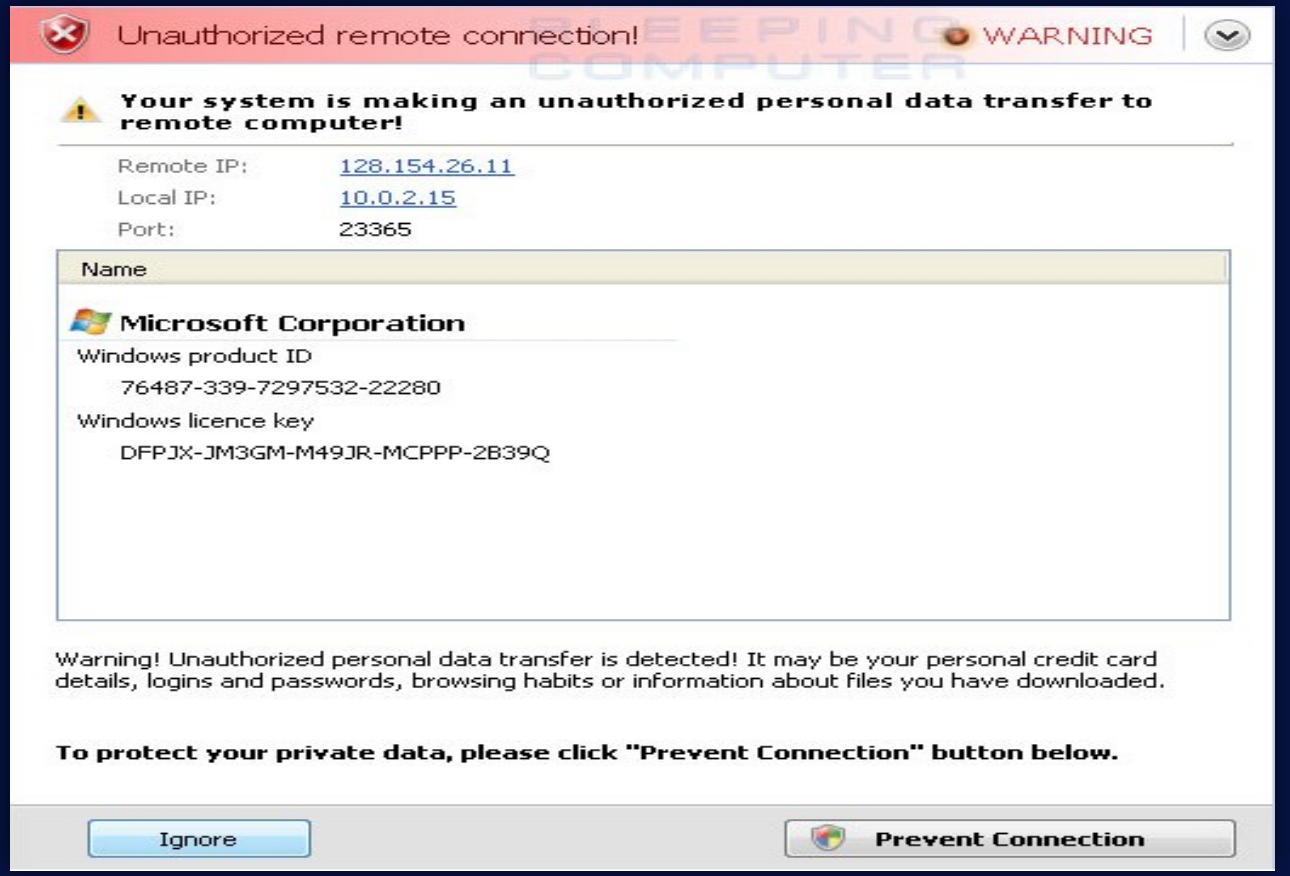
Rogue Software/Scareware

- Form of malware that deceives or misleads users into paying for the fake or simulated removal of malware
- Has become a growing and serious security threat in desktop computing
- Mainly relies on social engineering in order to defeat the security software
- Most have a Trojan horse component, which users are misled into installing
  - Browser plug-in (typically toolbar)
  - Image, screensaver, or ZIP file attached to an email
  - Multimedia codec required to play a video clip
  - Software shared on peer-to-peer networks
  - A free online malware scanning service

Rogue Software/Scareware



Rogue Software/Scareware



Rogue Software/Scareware

Phishing

Criminally fraudulent process of attempting to acquire sensitive information (usernames, passwords, credit card details) by masquerading as a trustworthy entity in an electronic communication

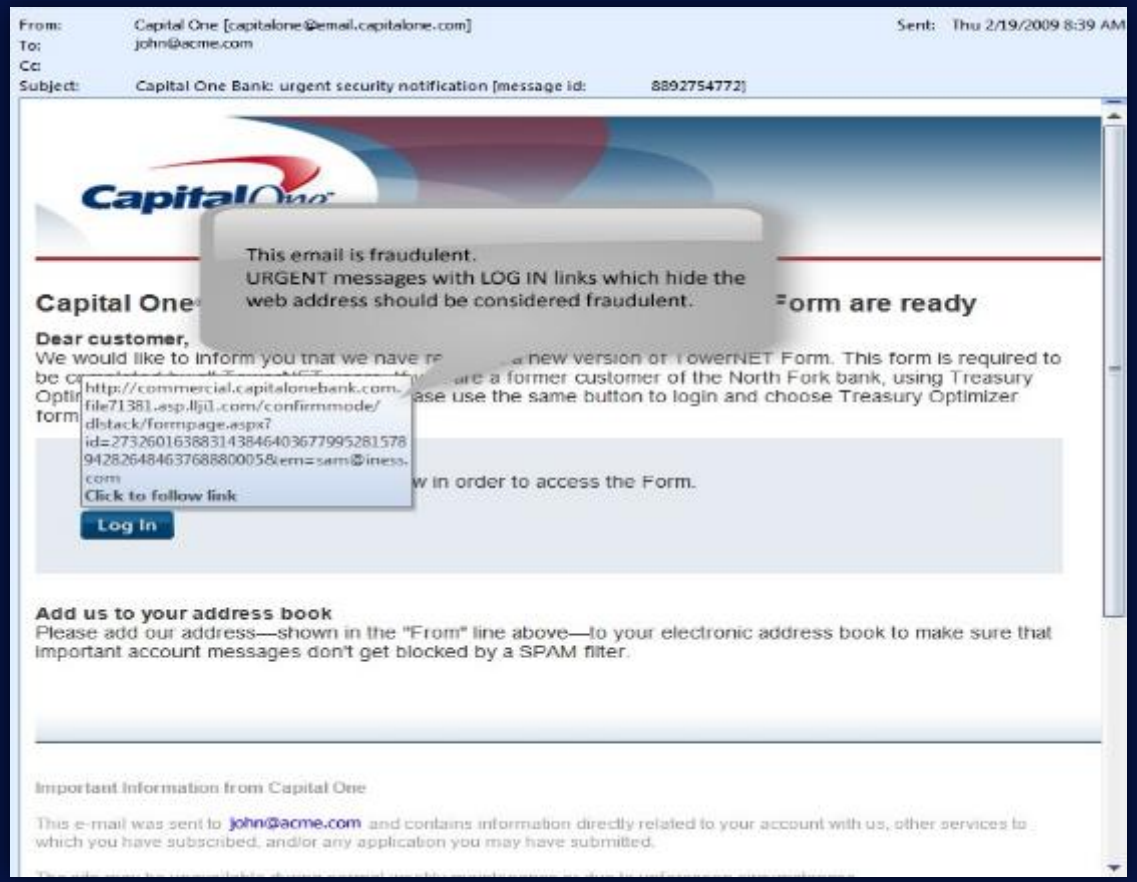
Commonly used means:

- Social networking sites
- Auction sites
- Online payment processors
- IT administrators

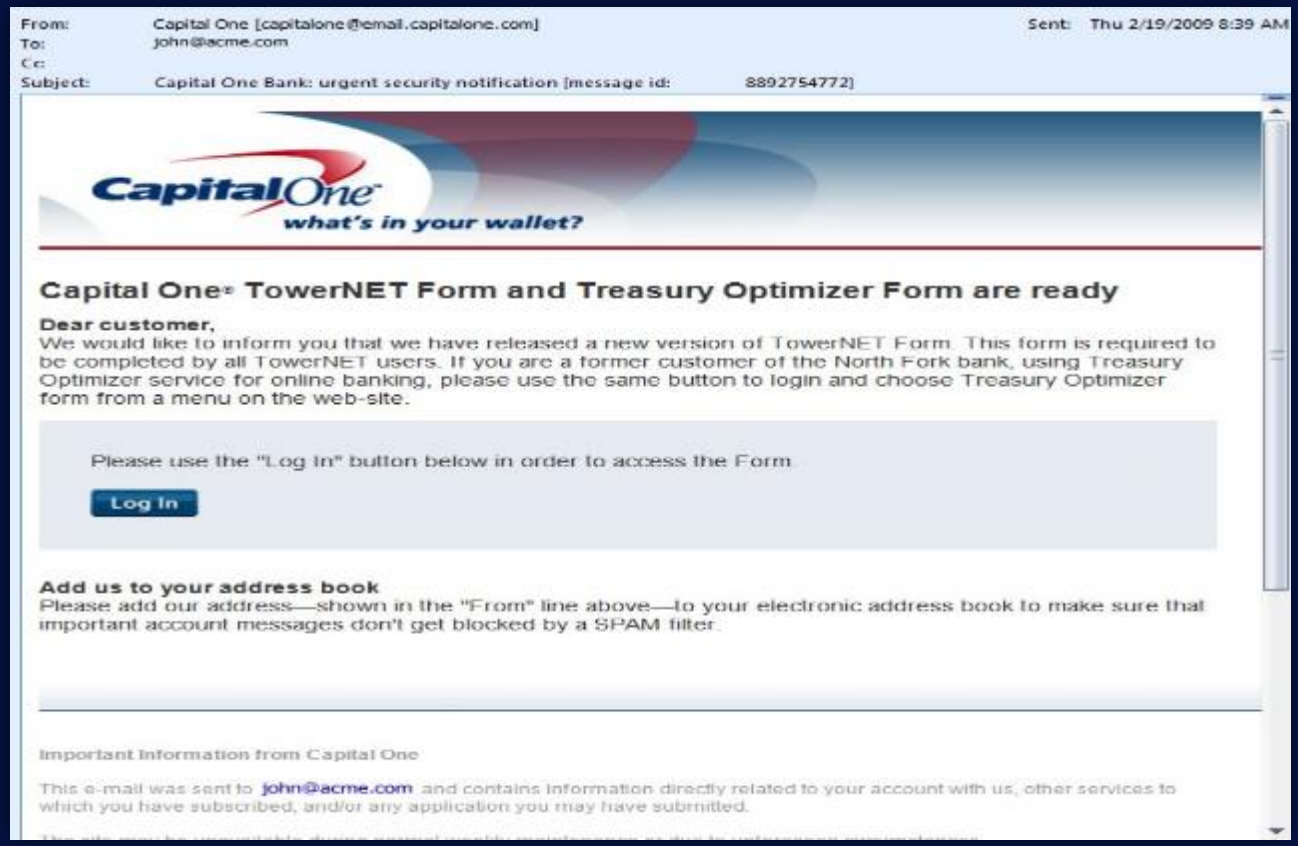
Phishing


Advanced card verification
VISA
Advanced verification.
For security reasons please provide information requested below
Card Type
Debit
Card Number
Expiration Date
/
CVV2
ATM PIN
Process

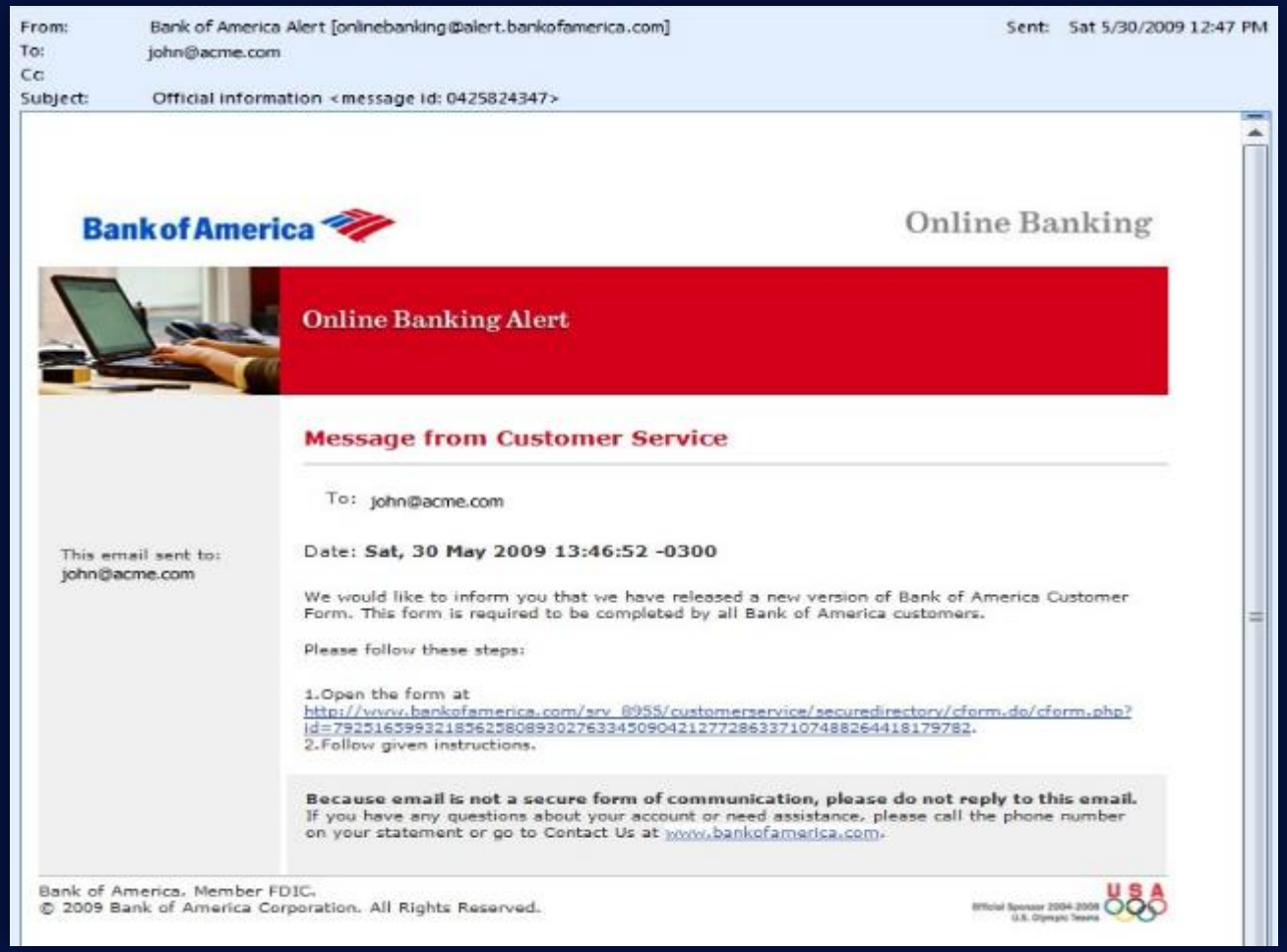
Phishing


From: Capital One [capitalone@email.capitalone.com]
Sent: Thu 2/19/2009 8:39 AM
To: john@acme.com
Cc:
Subject: Capital One Bank: urgent security notification [message id: 8892754772]
This email is fraudulent.
URGENT messages with LOG IN links which hide the web address should be considered fraudulent.
Capital One
Form are ready
Dear customer,
We would like to inform you that we have re
new version of TowerNET Form. This form is required to
be ca
are a former customer of the North Fork bank, using Treasury
Optir
ase use the same button to login and choose Treasury Optimizer
form
http://commercial.capitalonebank.com.
file71381.asp.llpl.com/confirmmode/
dlstack/formpage.aspx?
id=27326016388314384640367799528157894282648463768880005&em=sam@iness.com
Click to follow link
w in order to access the Form.
Log In
Add us to your address book
Please add our address—shown in the "From" line above—to your electronic address book to make sure that important account messages don't get blocked by a SPAM filter.
Important Information from Capital One
This e-mail was sent to john@acme.com and contains information directly related to your account with us, other services to which you have subscribed, and/or any application you may have submitted.

Phishing


From: Capital One [capitalone@email.capitalone.com]
To: john@acme.com
Cc:
Subject: Capital One Bank: urgent security notification [message id: 8892754772]
Sent: Thu 2/19/2009 8:39 AM
Capital One
what's in your wallet?
Capital One® TowerNET Form and Treasury Optimizer Form are ready
Dear customer,
We would like to inform you that we have released a new version of TowerNET Form. This form is required to be completed by all TowerNET users. If you are a former customer of the North Fork bank, using Treasury Optimizer service for online banking, please use the same button to login and choose Treasury Optimizer form from a menu on the web-site.
Please use the "Log In" button below in order to access the Form
Log In
Add us to your address book
Please add our address—shown in the "From" line above—to your electronic address book to make sure that important account messages don't get blocked by a SPAM filter.
Important Information from Capital One
This e-mail was sent to john@acme.com and contains information directly related to your account with us, other services to which you have subscribed, and/or any application you may have submitted.

Phishing



From: Bank of America Alert [onlinebanking@alert.bankofamerica.com] Sent: Sat 5/30/2009 12:47 PM
To: john@acme.com
Cc:
Subject: Official information <message id: 0425824347>

Bank of America

Online Banking

Online Banking Alert

Message from Customer Service

To: john@acme.com

This email sent to:
john@acme.com

Date: **Sat, 30 May 2009 13:46:52 -0300**

We would like to inform you that we have released a new version of Bank of America Customer Form. This form is required to be completed by all Bank of America customers.

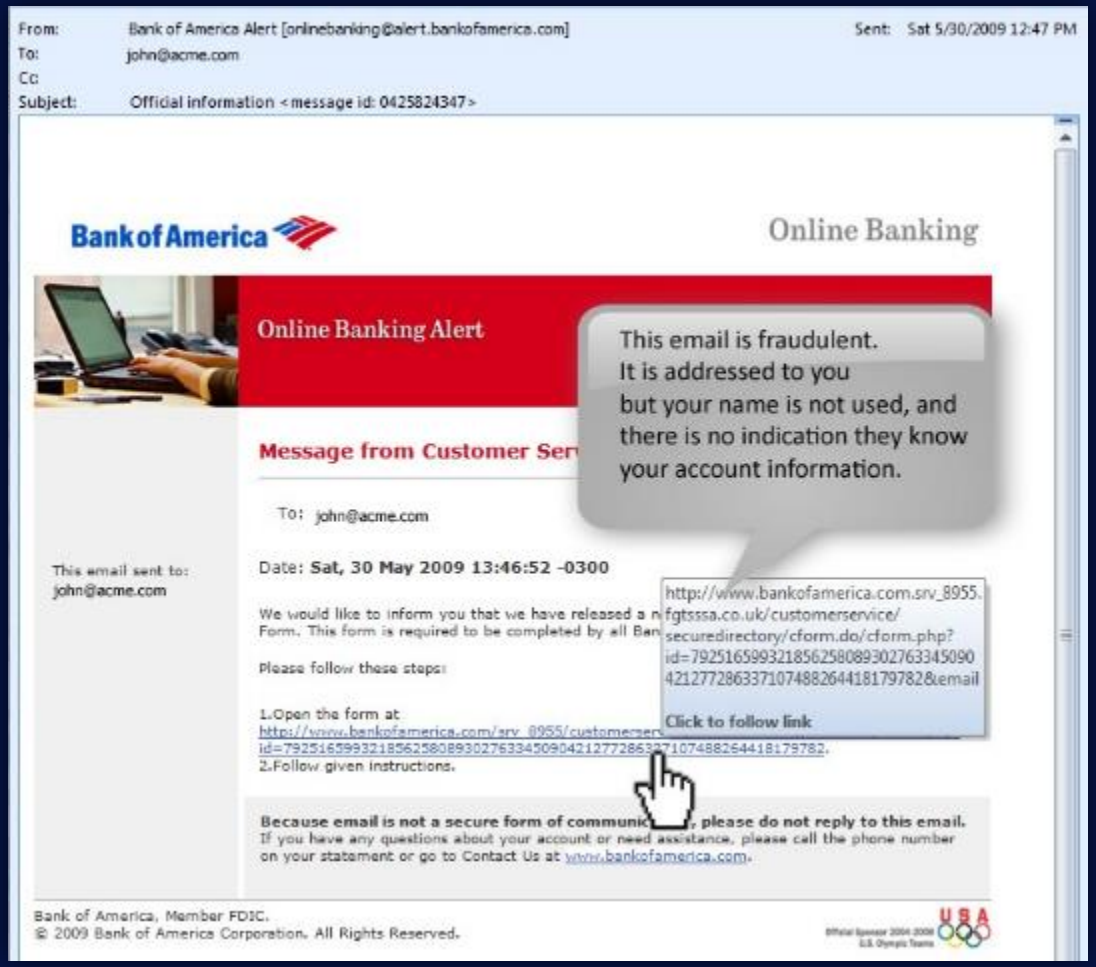
Please follow these steps:

1.Open the form at
http://www.bankofamerica.com/srv_8955/customerservice/securedirectory/cform.do/cform.php?id=792516599321856258089302763345090421277286337107488264418179782.
2.Follow given instructions.

Because email is not a secure form of communication, please do not reply to this email. If you have any questions about your account or need assistance, please call the phone number on your statement or go to Contact Us at www.bankofamerica.com.

Bank of America. Member FDIC.
© 2009 Bank of America Corporation. All Rights Reserved.

Phishing


From: Bank of America Alert [onlinebanking@alert.bankofamerica.com]
Sent: Sat 5/30/2009 12:47 PM
To: john@acme.com
Cc:
Subject: Official information <message id: 0425824347>
Bank of America
Online Banking
Online Banking Alert
This email is fraudulent.
It is addressed to you
but your name is not used, and
there is no indication they know
your account information.
Message from Customer Ser
To: john@acme.com
This email sent to:
john@acme.com
Date: Sat, 30 May 2009 13:46:52 -0300
http://www.bankofamerica.com.srv_8955.
fgtsssa.co.uk/customerservice/
securedirectory/cform.do/cform.php?
id=792516599321856258089302763345090
421277286337107488264418179782&email
Click to follow link
Please follow these steps:
1.Open the form at
2.Follow given instructions.
If you have any questions about your account or need assistance, please call the phone number
on your statement or go to Contact Us at www.bankofamerica.com.
Bank of America, Member FDIC.
© 2009 Bank of America Corporation. All Rights Reserved.

Phishing

From: service@paypal.com
Sent: Wed 8/6/2008 12:22 AM
To: John Doe
Cc:
Subject: Update your credit card information with PayPal

PayPal

Dear John Doe,

Your credit card ending in 9595 will expire soon. To avoid any disruption to your PayPal service, please update your credit card expiration date by following these steps:

1. Log in to your PayPal account.
2. Go to the **Profile** subtab and click **Credit Cards** in the Financial Information column.
3. Choose the credit card that needs updating and click **Edit.**
4. Enter the upda

https://www.paypal.com/us/cgi-bin/webscr?cmd=_bc-signup
Click to follow link

Or simply get the PayP approved almost instantly, and there's no annual fee. Apply today.

Sincerely,
PayPal

Please do not reply to this email. This mailbox is not monitored and you will not receive a response. For assistance, log in to your PayPal account and click the Help link in the top right corner of any PayPal page.

To receive email notifications in plain text instead of HTML, update your preferences.

Phishing


From: service@paypal.com
Sent: Wed 8/6/2008 12:22 AM
To: John Doe
Cc:
Subject: Update your credit card information with PayPal
PayPal
Dear John Doe,
Your credit card ending in 9595 will expire soon. To avoid any disruption to your PayPal service, please update your credit card expiration date by following these steps:
1. Log in to your PayPal account.
2. Go to the Profile subtab and click Credit Cards in the Financial Information column.
3. Choose the credit card that needs updating and click Edit.
4. Enter the upda
https://www.paypal.com/us/cgi-bin/webscr?cmd=_bc-signup
Click to follow link
Or simply get the PayP approved almost instantly, and there's no annual fee. Apply today.
Sincerely,
PayPal
This email is authentic.
It is addressed to you personally.
The sender appears to know the last 4 digits of your account number.
The links are obscured but hovering on the link shows a valid PayPal address.
Please do not reply to this em
assistance, log in to your Pay
page.
To receive email notifications
PayPal Email ID PP031

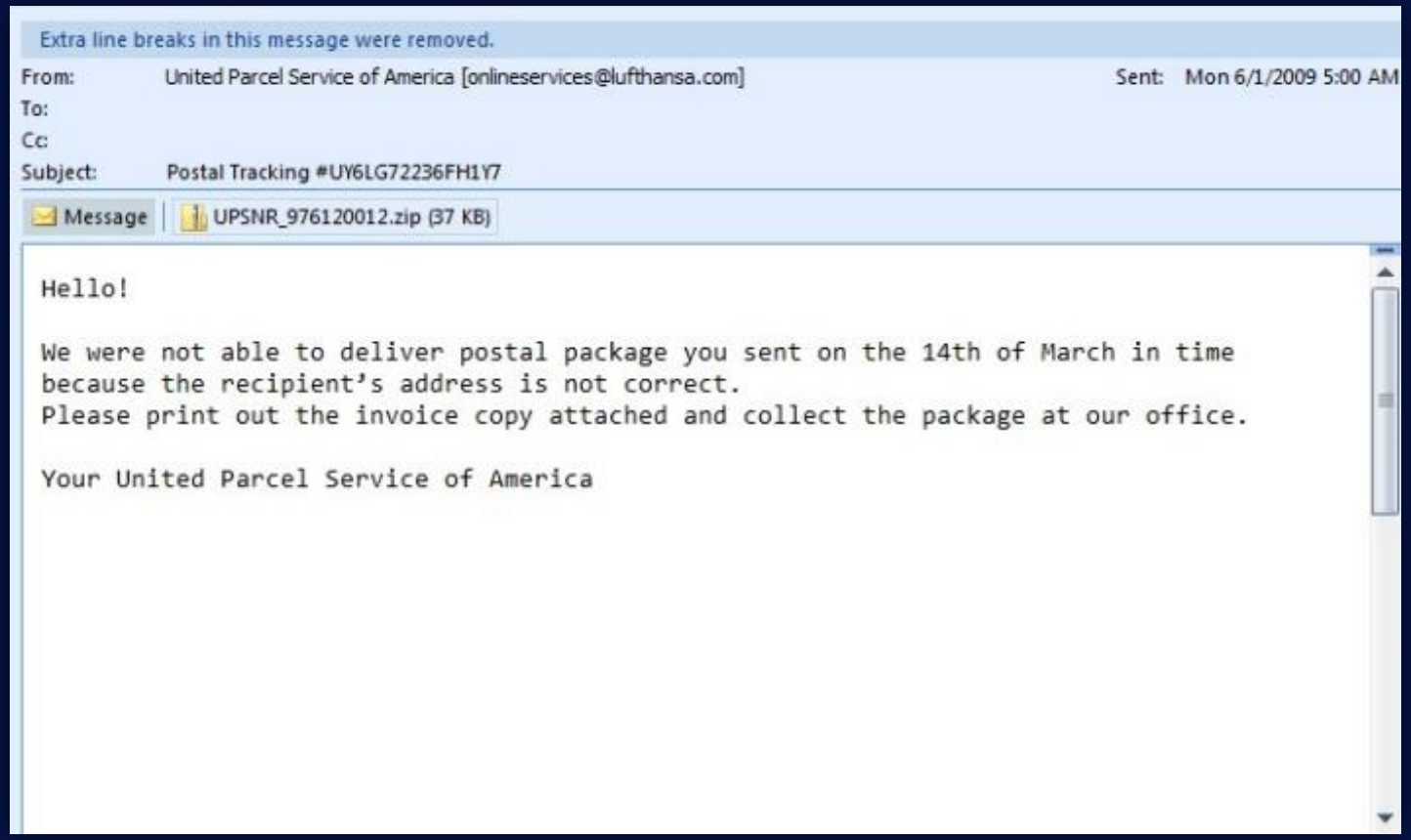
Email Usage

CAUTION!

What may be relied upon today as an indication that an email is authentic may become unreliable as electronic crimes evolve.

This is why it is important to stay abreast of changing security trends.

Email Usage


Extra line breaks in this message were removed.

From: United Parcel Service of America [onlineservices@lufthansa.com] Sent: Mon 6/1/2009 5:00 AM

To:

Cc:

Subject: Postal Tracking #UY6LG72236FH1Y7

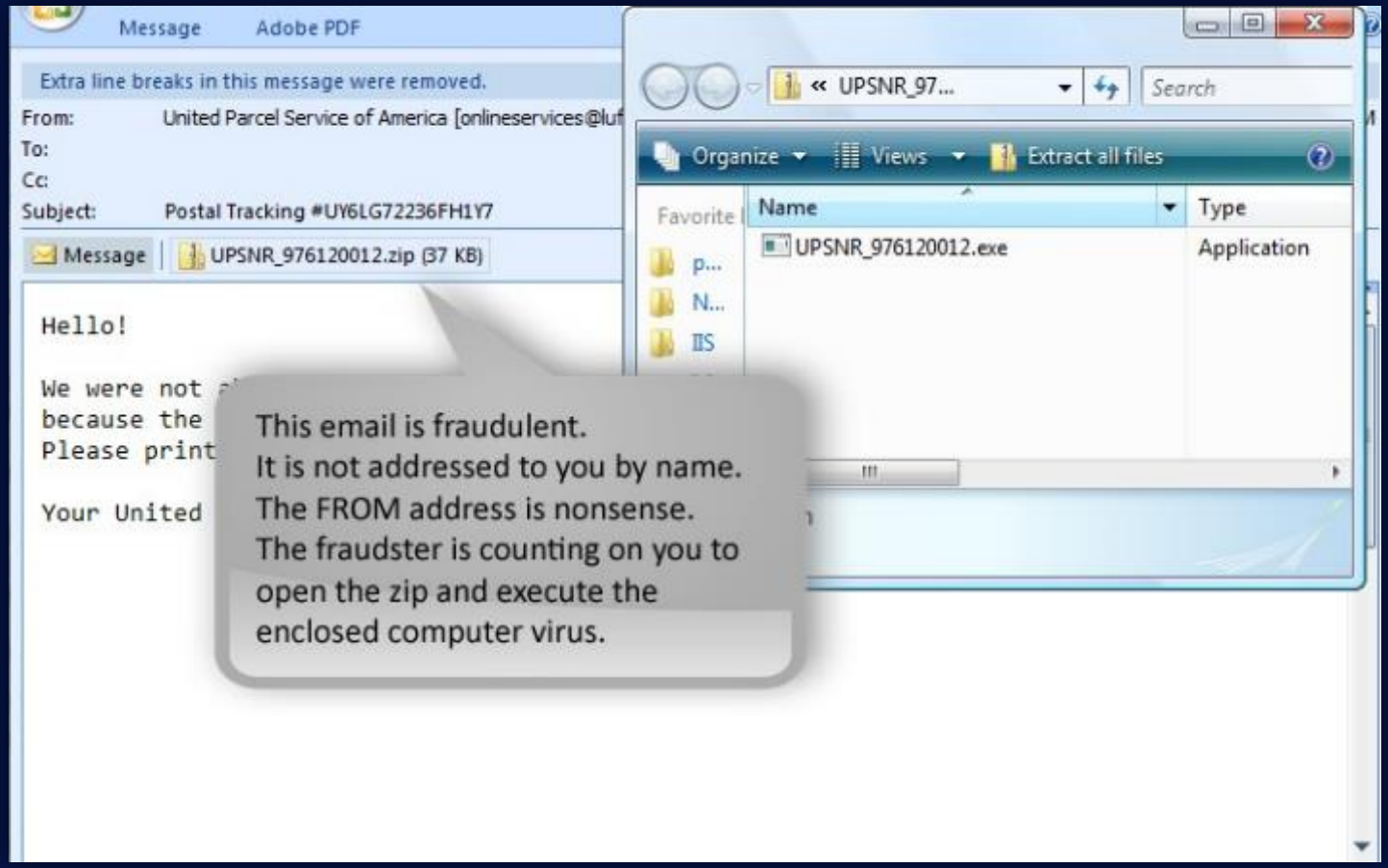
Message | UPSNR_976120012.zip (37 KB)

Hello!

We were not able to deliver postal package you sent on the 14th of March in time because the recipient's address is not correct.
Please print out the invoice copy attached and collect the package at our office.

Your United Parcel Service of America

Email Usage


Message
Adobe PDF
Extra line breaks in this message were removed.
From: United Parcel Service of America [onlineservices@luf
To:
Cc:
Subject: Postal Tracking #UY6LG72236FH1Y7
Message
UPSNR_976120012.zip (37 KB)
Hello!
We were not
because the
Please print
Your United
This email is fraudulent.
It is not addressed to you by name.
The FROM address is nonsense.
The fraudster is counting on you to open the zip and execute the enclosed computer virus.
« UPSNR_97...
Search
Organize
Views
Extract all files
Favorite
Name
Type
UPSNR_976120012.exe
Application

Email Usage

- Some experts feel email is the biggest security threat of all.
- It is the fastest, most effective method of spreading malicious code to the largest number of users.
- It's also a large source of wasted technology resources.

  Examples of corporate email waste:
  - Electronic greeting cards
  - Chain letters
  - Jokes and graphics
  - Spam and junk email

What Can Mifflinburg Bank & Trust Do To PROTECT?

- Provide security awareness training for our employees and customers
- Review our product agreements - make sure that both parties understand their roles and responsibilities
- Make sure our customers are aware of basic online security standards
- Stay informed – attend webinars/seminars and other user group meetings
- Develop a layered security approach

What Can Businesses Do To PROTECT?

- Education is key - train your employees
- Secure your computer and networks
- Limit administrative rights
  - Do not allow employees to install any software without receiving prior approval
- Install and maintain spam filters
- Surf the internet carefully
- Install and maintain real-time anti-virus and anti-spyware desktop firewall and malware detection and removal software
  - Use these tools regularly to scan your computer
  - Allow for automatic updates and scheduled scans

What Can Businesses Do To PROTECT?

- Install routers and firewalls to prevent unauthorized access to your computer or network
  - Change the default passwords on all network devices
- Install security updates to operating systems and all applications as they become available
- Block pop-ups
- Do not open attachments from email
  - Be on the alert for suspicious emails
- Do not use public internet access points
- Reconcile accounts daily

What Can Businesses Do To PROTECT?

- Note any changes in the performance of your computer - dramatic loss of speed, computer locks up, unexpected rebooting, unusual pop-ups, etc.
- Make sure that your employees know how and to whom to report suspicious activity to at your company and the bank
- Contact the bank if you:
  - Suspect a fraudulent transaction
  - Are trying to process an online wire or ACH batch and you receive a maintenance page
  - Receive an email claiming to be from the bank, and it is requesting personal/ company information

Thank you for taking the opportunity to view this information.
We hope that you find it to be useful.

Please contact us if you have any questions or comments.

Mifflinburg Bank & Trust

888-966-6282 | mbtc.com