SAMPLE PRESENTATION FOR INSTITUTION EMPLOYEES

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 **“Your Institution Name”** or any other entity.

What will be covered?

- What is Corporate Account Takeover?
- How does it work?
- Types of Security Threats and Countermeasures
- Current Trends
- How to Protect?
- How to Detect?
- What to do when Fraud happens to me??

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).

Cyber threats to financial institutions and other national critical infrastructure is real and growing at an alarming rate.

Estimated 40,000 Chinese hacking groups

Average age ~ 2X years

Income: $2-3 Million per year

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 on to their Online Banking
- Fraudsters Collect Login Credentials
- Fraudsters wait for the right time and then depending on your controls – they login after hours or if you are utilizing a token they wait until you enter your code and then they hijack the session and send you a message that Online Banking is temporarily unavailable.

Types of Security Threats & Countermeasures

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.

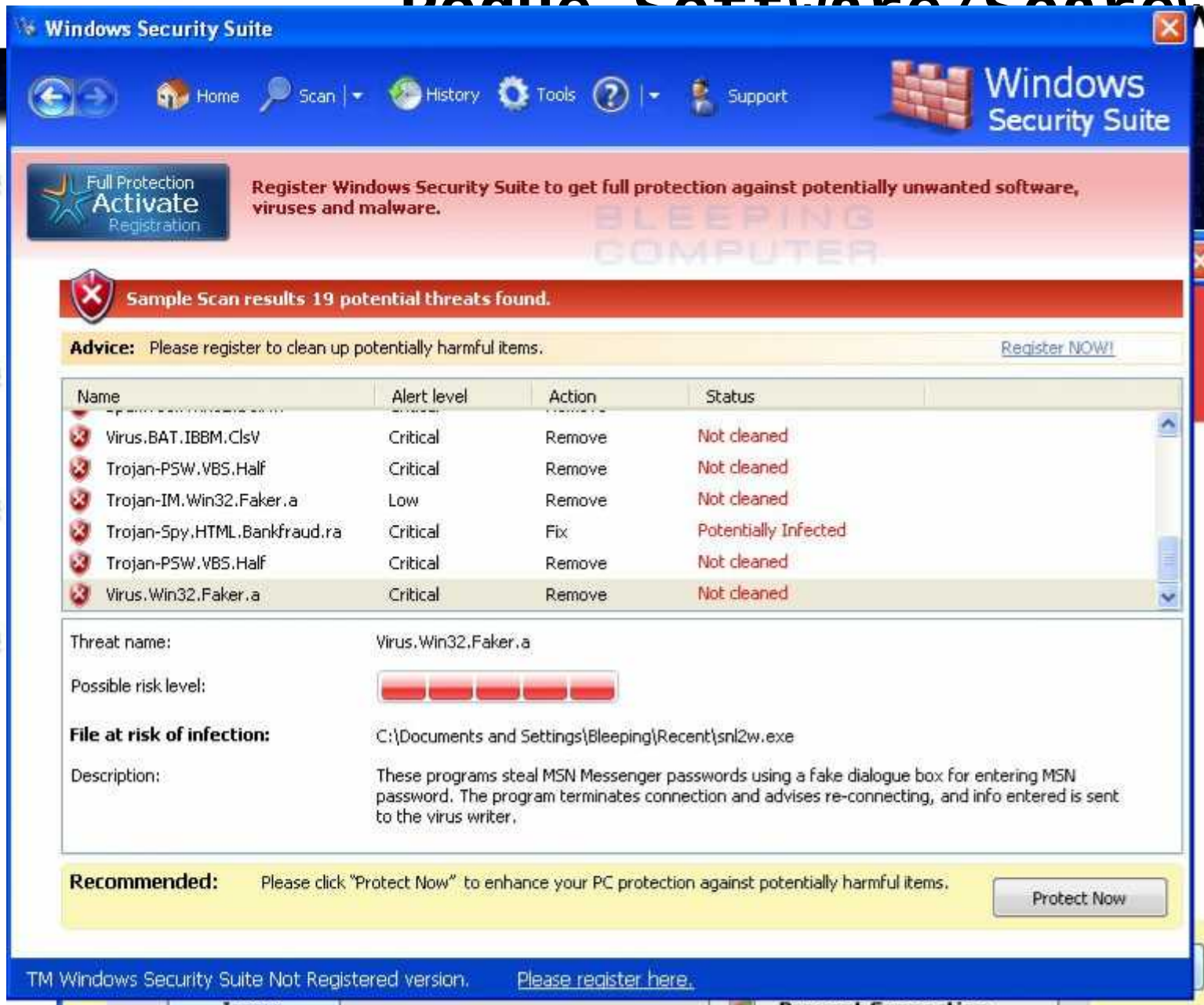
Viruses

- A computer program that can copy itself and infect a computer.
- The term "virus" is also commonly, but incorrectly used to refer to other types of malware, adware, and spyware programs that do not have the reproductive ability.
- Some viruses try to avoid detection by killing the tasks associated with antivirus software before it can detect them.

Spyware

- Type of malware that is installed on computers and collects little bits of information at a time about users without their knowledge.
- The presence of spyware is typically hidden from the user, and can be difficult to detect.
- It can install additional software, redirecting Web browser, change computer settings, different home pages, and/or loss of Internet.

Rogue Software/Scareware



Phishing

- Criminally fraudulent process of attempting to acquire sensitive information (usernames, passwords, credit card details) by masquerading as a trustwor
commun
- Commor
  - Social
  - Auctio
  - Online
  - IT adm

From: Capital One [capitalone@email.capitalone.com]
To: john@acme.com
Cc:
Subject: Capital One Bank: urgent security notification [message id: 8892754772]

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.

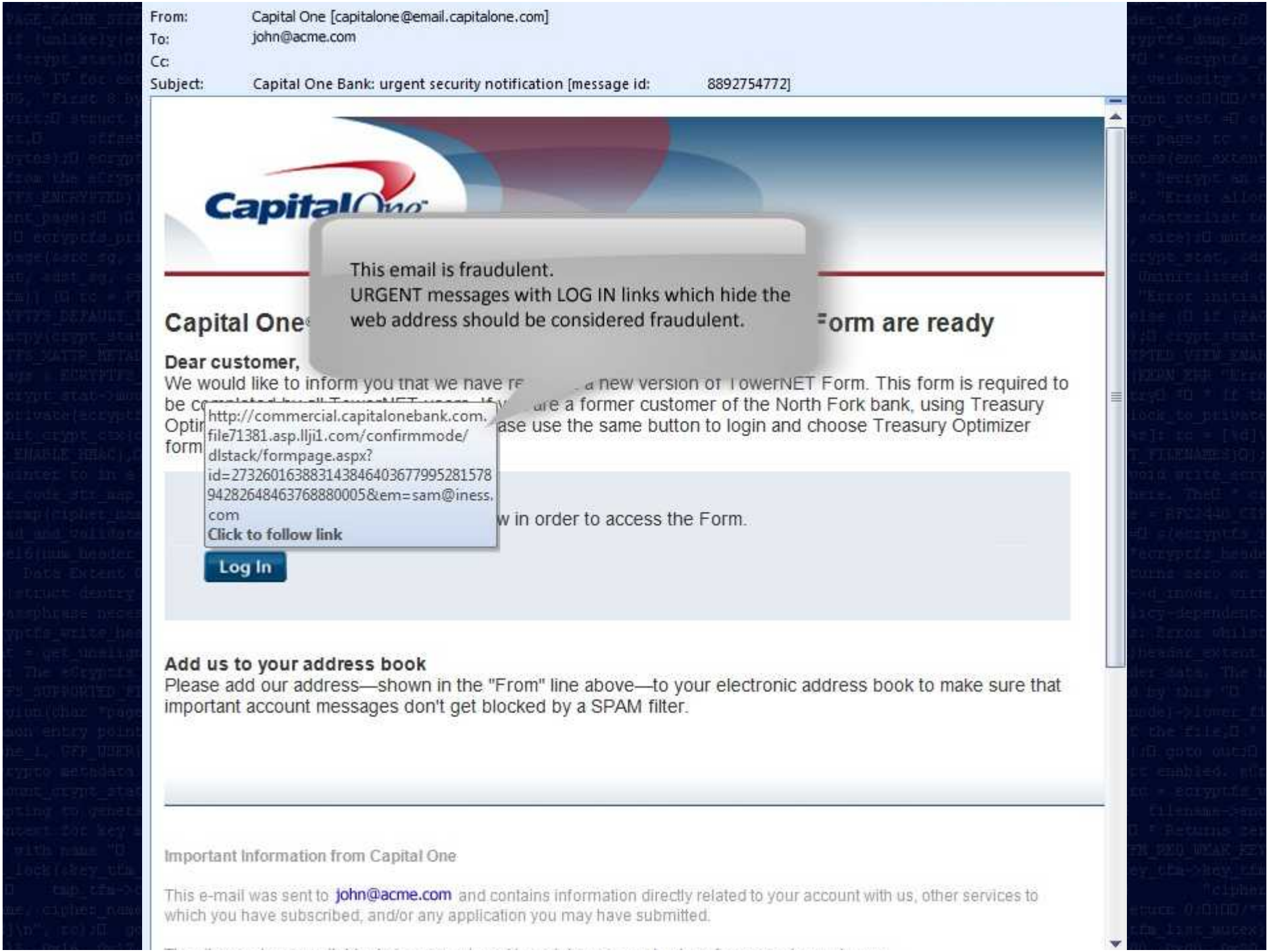
Please use the "Log In" button below in order to access the Form.

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.


From: Capital One [capitalone@email.capitalone.com]
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
orm are ready
Dear customer,
We would like to inform you that we have re a new version of TowerNET Form. This form is required to be co
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.llji1.com/confirmmode/dlstack/formpage.aspx?id=2732601638831438464036779952815789428264846376888000 5&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.

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.

Official Sponsor 2004-2008 U.S. Olympic Teams USA

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**

We would like to inform you that we have released a n
Form. This form is required to be completed by all Ban

Please follow these steps:

1.Open the form at
http://www.bankofamerica.com/srv_8955/customerser
id=792516599321856258089302763345090421277286337107488264418179782.
2.Follow given instructions.

http://www.bankofamerica.com.srv_8955.
fgtsssa.co.uk/customerservice/
securedirectory/cform.do/cform.php?
id=792516599321856258089302763345090
421277286337107488264418179782&email

Click to follow link

Because email is not a secure form of communic , 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.

USA
Official Sponsor 2004-2008 U.S. Olympic Teams

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

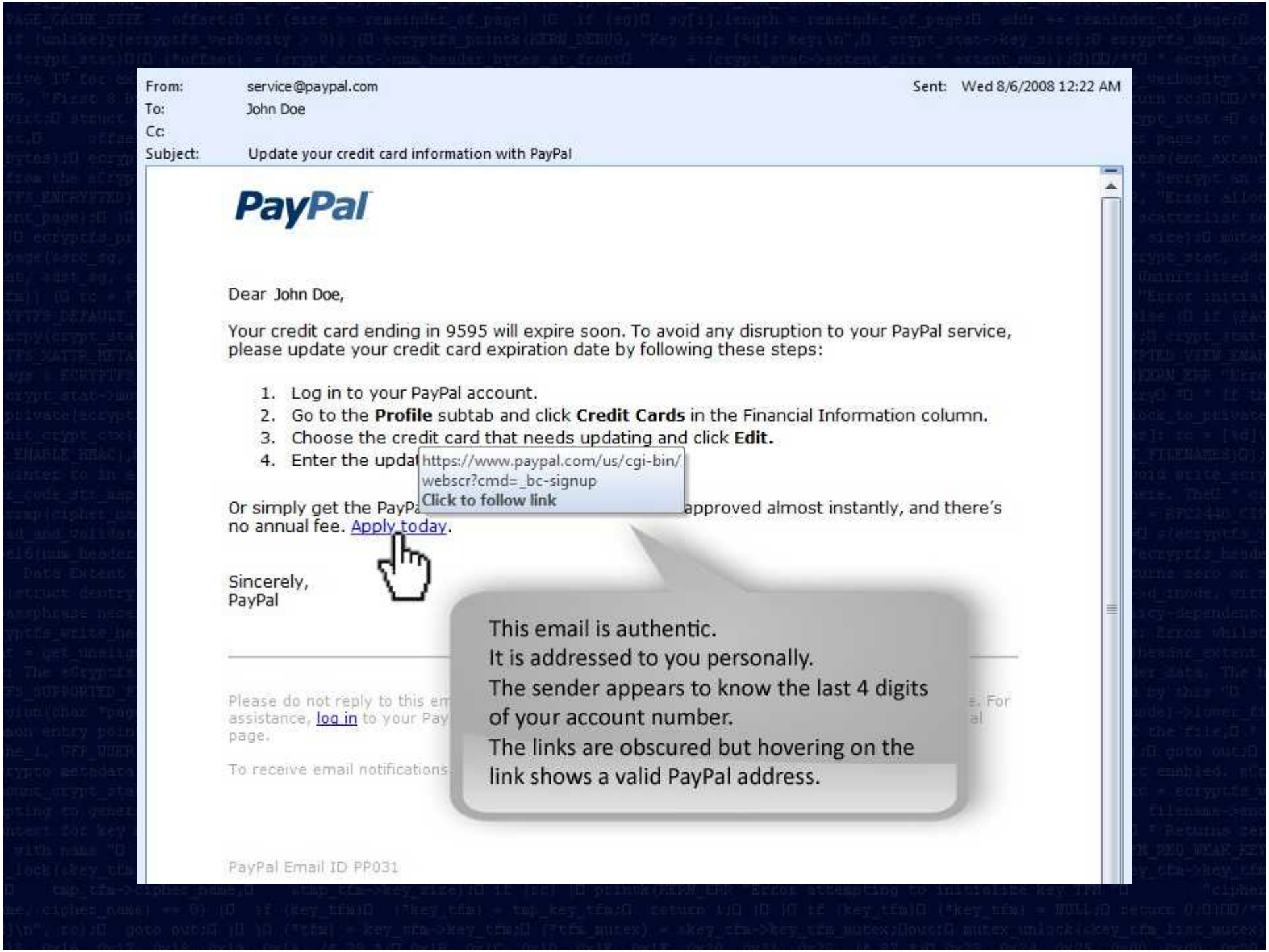
https://www.paypal.com/us/cgi-bin/webscr?cmd=_bc-signup
Click to follow link

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.


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
approved almost instantly, and there's no annual fee. Apply today.
Sincerely,
PayPal
Please do not reply to this em
assistance, log in to your Pay
page.
To receive email notifications
PayPal Email ID PP031
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.

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:

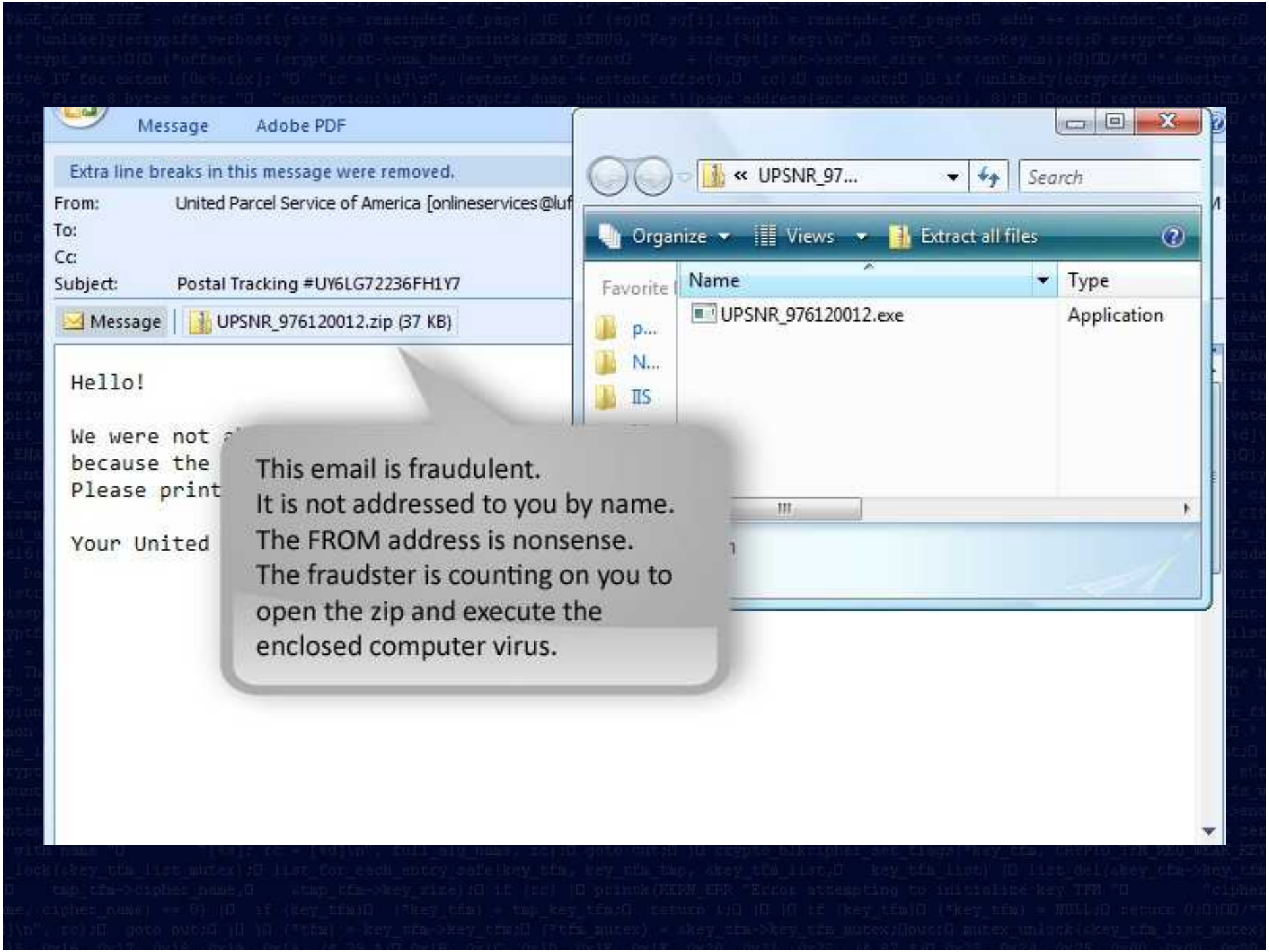
Subject: Postal Tracking #UY6LG72236FH1Y7

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


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
« UPSNR_97...
Search
Organize
Views
Extract all files
Favorite
Name
Type
UPSNR_976120012.exe
Application
p...
N...
IIS
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.

E-mail Usage

- Some experts feel e-mail is the biggest security threat of all.
- The fastest, most-effective method of spreading malicious code to the largest number of users.
- Also a large source of wasted technology resources.
- Examples of corporate e-mail waste:
  - Electronic Greeting Cards
  - Chain Letters
  - Jokes and graphics
  - Spam and junk e-mail

Hoaxes

- Hoaxes attempt to trick or defraud users.
- A hoax could be malicious, instructing users to delete a file necessary to the operating system by claiming it is a virus.
- It could also be a scam that convinces users to send money or personal information.
- Phishing attacks fall into this category.

Statistics

- **Where does it come from?**
  - **Malicious websites (including Social Networking sites)**
  - **Email**
  - **P2P Downloads (e.g. LimeWire)**
  - **Ads from popular web sites**
- **Web-borne infections:**

According to researchers in the first quarter of 2011, 76% of web resources used to spread malicious programs were found in 5 countries worldwide ~ United States, Russian Federation, Netherlands, China, & Ukraine.

What your institution can do!

PROTECT

- **Know your Customers - Develop a Risk Assessment:**
  - **Determine which customers are high-risk**
  - **Types of transactions – wires, institution to institution, SEC Code, daily files, high limits/frequencies, financial stability**
- **Provide Ongoing Security Awareness Training for BOTH Employees & Corporate Customers**
  - **TRAIN! TRAIN! TRAIN!**
- **Make sure that your Customers are Aware of Basic Online Security Practices**
- **Review your Contracts**

  Make sure that you clearly state roles & responsibilities of both parties and dispute resolution processes
- **Stay Informed**

  Attend webinars/seminars & other user group meetings
- **Develop a layered security approach**
- **Perform a Due Diligence review of any third-party service providers for Online Banking Services**

What your institution can do!

DETECT

Detection is closely associated with protection because some measures that protect also help identify fraud.

- **Layered Security**

It has already been proven that a single layer is easy for hackers to get through. If one layer develops a security weakness then hopefully the other layers will provide sufficient protection.

Monitoring of IP Addresses

New User Controls

Calendar File – Frequencies and Limits

Dual Control

Fax or Out of Band Confirmation

Secure Brower or Secure Browser Key

Pattern Recognition Software

- **Train institution employees on Fraud warning signs**

What your institution can do!

RESPOND

- **Make sure your Incident Response Plan(IRP) includes procedures for a Corporate Account Takeover (Make sure that your IRP includes after-hours contact information for Corporate Customers)**
- **Make sure that "all" employees are trained, with specialized training for employees that process Wires or ACH Transactions.**
- **Update IRP to include the directory for FED ACH routing number contact information http://www.fededirectory.frb.org/search_ACH.cfm**
- **Make sure you have a Notice of Fraudulent Activity in your IRP**
- **Procedures for processing a Fraudulent ACH file alert**
- **Establish procedures for customer relations and documentation of recovery efforts**
- **Develop a contingency plan to recover or suspend any systems suspected of being compromised**
- **Make sure your IRP has procedures and contact information for the US Secret Service as well as other law enforcement and regulatory agencies**

What your institution can do!

RESPOND (Cont.)

- Contact customer to verify fraudulent transactions
- Reverse all suspected fraudulent transactions
- Send a “fraudulent ACH file or wire alert” through FedLine
- Distribute list of transactions to a group of employees with calling assignments and instructions to call on the largest items first
- Ask the institutions to place a hold on the funds - send Notice of Fraudulent Activity letter

What your institution can do!

SAMPLE

Forwarded by /MPLS/FRS

From: John Doe/MPLS/FRS
To: MPLS/FRS@FRS
Date: 11/26/2010 05:35 PM
Subject: Fw: Templates

A FRAUDULENT file was processed for (Bank Name & ABA) in error on (mm/dd/yy). The original file was processed on _____ (mm/dd/yy) with settlement of _____ (mm/dd/yy). The FRAUDULENT file was processed on (mm/dd/yy) and will settle on (mm/dd/yy). A reversal file was processed on (mm/dd/yy) and will settle on _____ (mm/dd/yy). For additional information, contact _____ (Bank Name) at (Bank's phone number).

_____ *(Bank Name & ABA)* hereby assumes all responsibility and liability for any processing errors, losses, damages and liability in any way arising out of the transmission of the broadcast message. _____ *(Bank Name and ABA)* also agrees to indemnify and hold harmless the Federal Reserve Bank, its agents and employees, from and against all claims, damages, lawsuits, and expenses, including reasonable attorneys' fees, in any way arising out of the transmission of the broadcast message.

What your Customers can do!

PROTECT

- Education is Key – Train employees
- Install and Maintain Real Time Anti-virus/Anti-spyware/ Firewall software and keep it up to date
- 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 security updates to operating systems and all applications as they become available
- Block Pop-Ups
- Do not open attachments from e-mail
- Do not use public Internet access points
- Recommend dual control from separate devices

What your Customers can do!

DETECT

- Education is Key – Train their employees
- Reconcile Accounts Daily
- Be on the alert for suspicious emails
- Anti-virus/Anti-spyware/Firewall software and keep it up to date

  Perform a full scan at least once a month
- Note any changes in the performance of your computer

  Dramatic loss of speed, computer locks up, unexpected rebooting, unusual popups, etc.

What your Customers can do!

RESPOND

- **Education is Key – Train their employees**

  Make sure that their employees know how and to whom to report suspicious activity to at the Company & the Institution

  Contact the institution:

  >If they Suspect a Fraudulent Transaction

  >If they are trying to process an Online Wire or ACH Batch & receive a maintenance page.

  >If they receive an email claiming to be from the institution and it is requesting personal/company information.

Questions or Comments