Corporate Account Takeover

Information Security Awareness
Brought to you by:

Community Credit Union

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 **Community Credit Union** or any other entity.

What will be covered?

1. What is Corporate Account Takeover?
2. How does it work?
3. Statistics
4. Current Trend Examples
5. What can we do to Protect?
6. 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.

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?

1. Criminals target victims by scams
2. Victim unknowingly installs software by clicking on a link or visiting an infected Internet site.
3. Fraudsters began monitoring the accounts
4. Victim logs on to their Online Banking
5. Fraudsters Collect Login Credentials
6. 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.

Statistics

Where does it come from?

Malicious websites (including Social Networking sites)

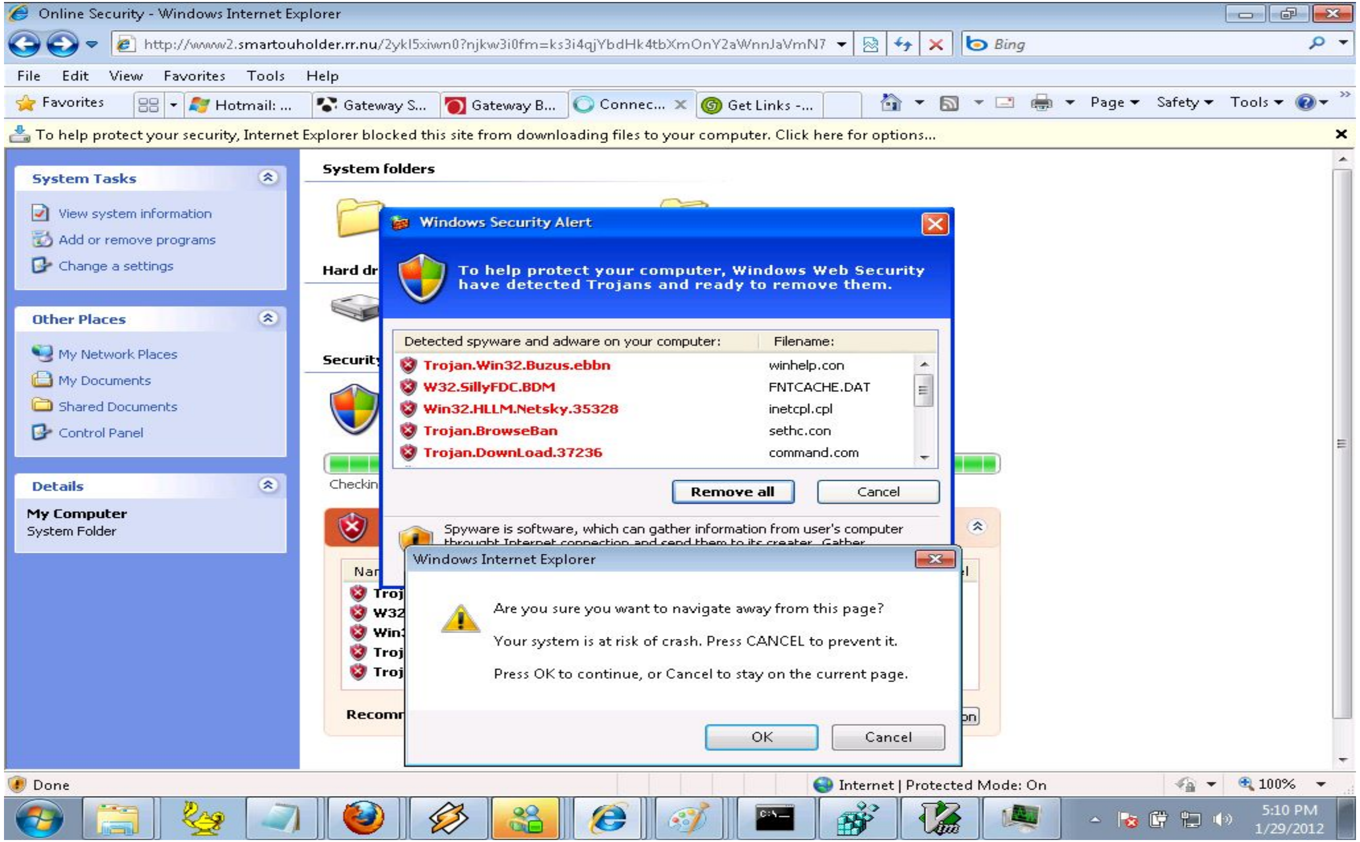
Email

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.

Rogue Software and Scanware



Online Security - Windows Internet Explorer

http://www2.smartouholder.rr.nu/2ykl5xiwn0?njkw3i0fm=ks3i4qjYbdHk4tbXmOnY2aWnnJaVmN7

To help protect your security, Internet Explorer blocked this site from downloading files to your computer. Click here for options...

Windows Security Alert

To help protect your computer, Windows Web Security have detected Trojans and ready to remove them.

Detected spyware and adware on your computer:	Filename:
Trojan.Win32.Buzus.ebbn	winhelp.con
W32.SillyFDC.BDM	FNTCACHE.DAT
Win32.HLLM.Netsky.35328	inetcpl.cpl
Trojan.BrowseBan	sethc.con
Trojan.DownLoad.37236	command.com

Spyware is software, which can gather information from user's computer throught Internet connection and send them to its creater. Gather

Windows Internet Explorer

Are you sure you want to navigate away from this page?

Your system is at risk of crash. Press CANCEL to prevent it.

Press OK to continue, or Cancel to stay on the current page.

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.

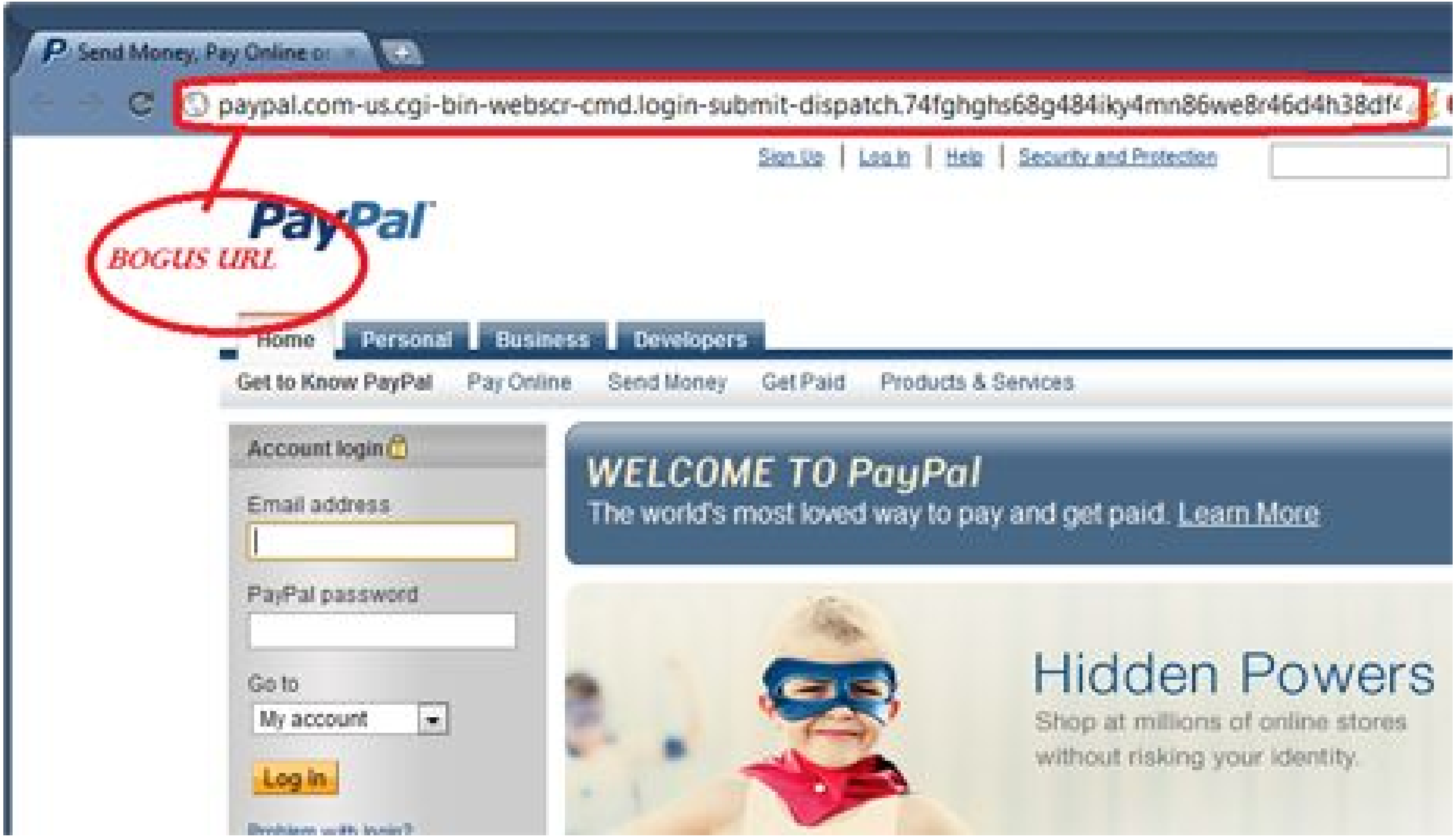
Commonly used means:

Social web sites

Auction sites

Online payment processors

IT administrators



paypal.com-us.cgi-bin-webscr-cmd.login-submit-dispatch.74fghghs68g484iky4mn86we8r46d4h38df4

Account login

Email address

PayPal password

Go to

My account

WELCOME TO PayPal

The world's most loved way to pay and get paid. Learn More

Hidden Powers

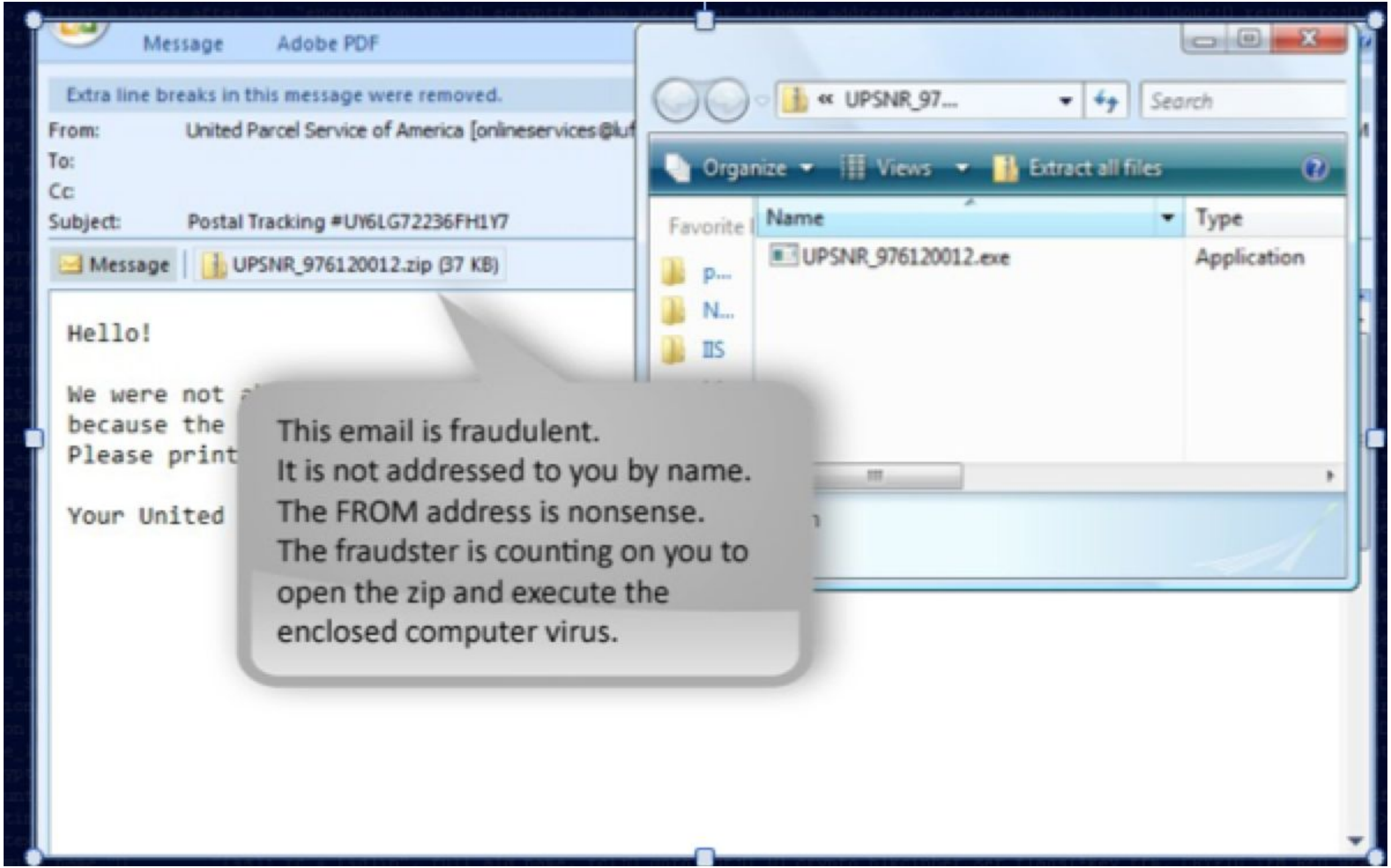
Shop at millions of online stores without risking your identity.

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.



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)

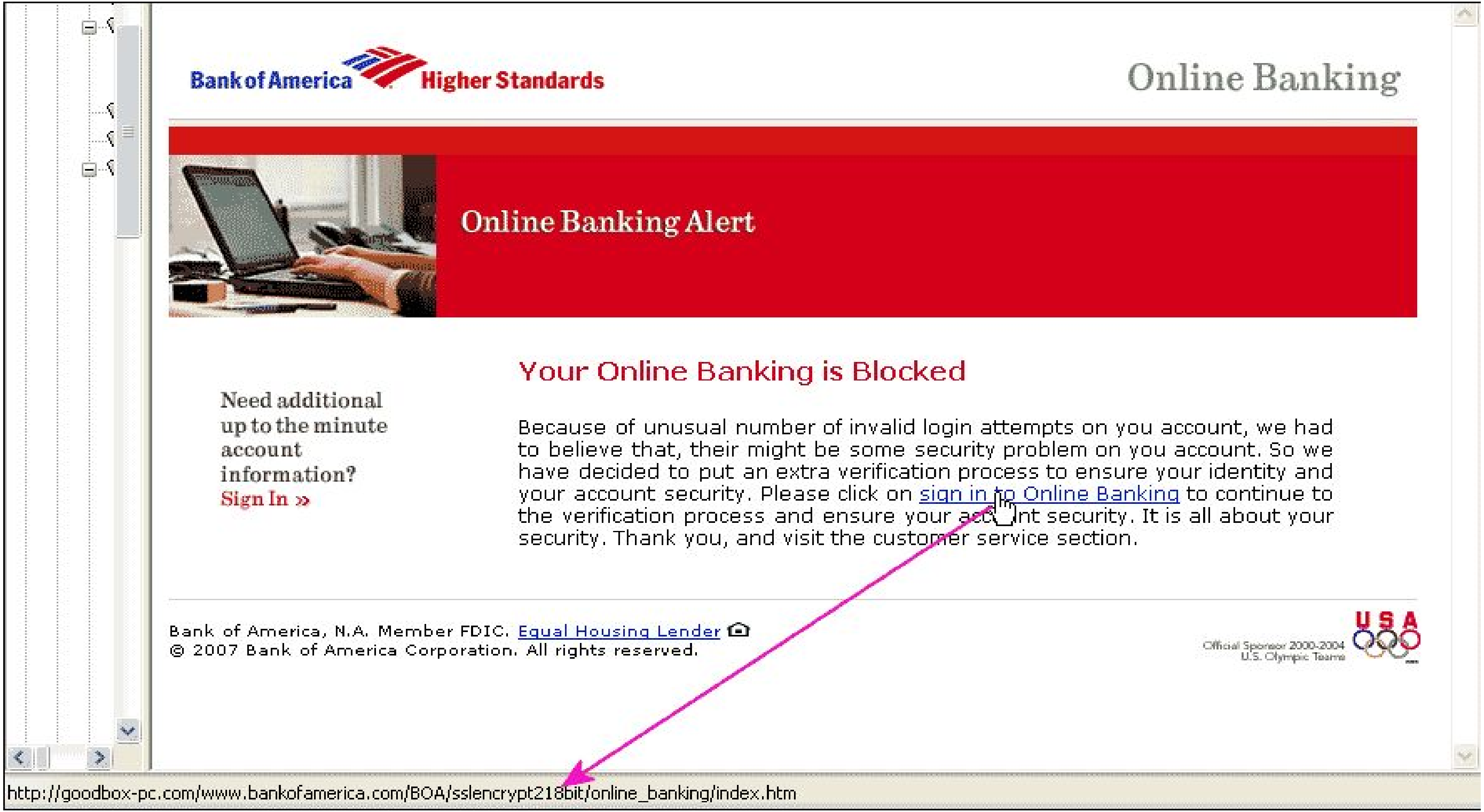
Name	Type
UPSNR_976120012.exe	Application

```
Hello!

We were not a
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.



Bank of America Higher Standards

Online Banking

Online Banking Alert

Your Online Banking is Blocked

Need additional up to the minute account information?
Sign In »

Because of unusual number of invalid login attempts on you account, we had to believe that, their might be some security problem on you account. So we have decided to put an extra verification process to ensure your identity and your account security. Please click on sign in to Online Banking to continue to the verification process and ensure your account security. It is all about your security. Thank you, and visit the customer service section.

Bank of America, N.A. Member FDIC. Equal Housing Lender
© 2007 Bank of America Corporation. All rights reserved.

USA
Official Sponsor 2000-2004
U.S. Olympic Teams

http://goodbox-pc.com/www.bankofamerica.com/BOA/sslencrypt218bit/online_banking/index.htm

Email Usage

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

What can we do to protect?

1. Provide Security Awareness Training for Our Employees & Customers
2. Review our Contracts
3. Make sure that both parties understand their roles & responsibilities
4. Make sure our Customers are Aware of
5. Basic Online Security Standards
6. Stay Informed
7. Attend webinars/seminars & other user group meetings
8. Develop a layered security approach

Layered Security

1. Layered Security approach
2. Monitoring of IP Addresses
3. New User Controls – Administrator can create a new user. Bank must activate user.
4. Calendar File – Frequencies, and Limits
5. Dual Control Processing of files on separate devices – recommended
6. Fax or Out of Band Confirmation
7. Secure Browser Key
8. Pattern Recognition Software

What can businesses do to protect?

1. Education is Key – Train your employees
2. Secure your computer and networks
3. Limit Administrative Rights -Do not allow employees to install any software without receiving prior approval.
4. Install and Maintain Spam Filters
5. Surf the Internet carefully
6. Install & maintain real-time anti-virus & anti-spyware desktop firewall & malware detection & removal software. Use these tools regularly to scan your computer. Allow for automatic updates and scheduled scans.
7. Install routers and firewalls to prevent unauthorized access to your computer or network. Change the default passwords on all network devices.
8. Install security updates to operating systems and all applications as they become available.
9. Block Pop-Ups

What can businesses do to protect?

1. Do not open attachments from e-mail -Be on the alert for suspicious emails
2. Do not use public Internet access points
3. Reconcile Accounts Daily
4. Note any changes in the performance of your computer
5. Dramatic loss of speed, computer locks up, unexpected rebooting, unusual popups, etc.
6. Make sure that your employees know how and to whom to report suspicious activity to at your Company & the Bank
7. Contact the Bank if you:
8. Suspect a Fraudulent Transaction
9. If you are trying to process an Online Wire or ACH Batch & you receive a maintenance page.
10. If you receive an email claiming to be from the Bank and it is requesting personal/company information.

Thank you!