The First State Bank, Louise Texas – Member FDIC

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 **The First State Bank, Louise** 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.

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 began 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.

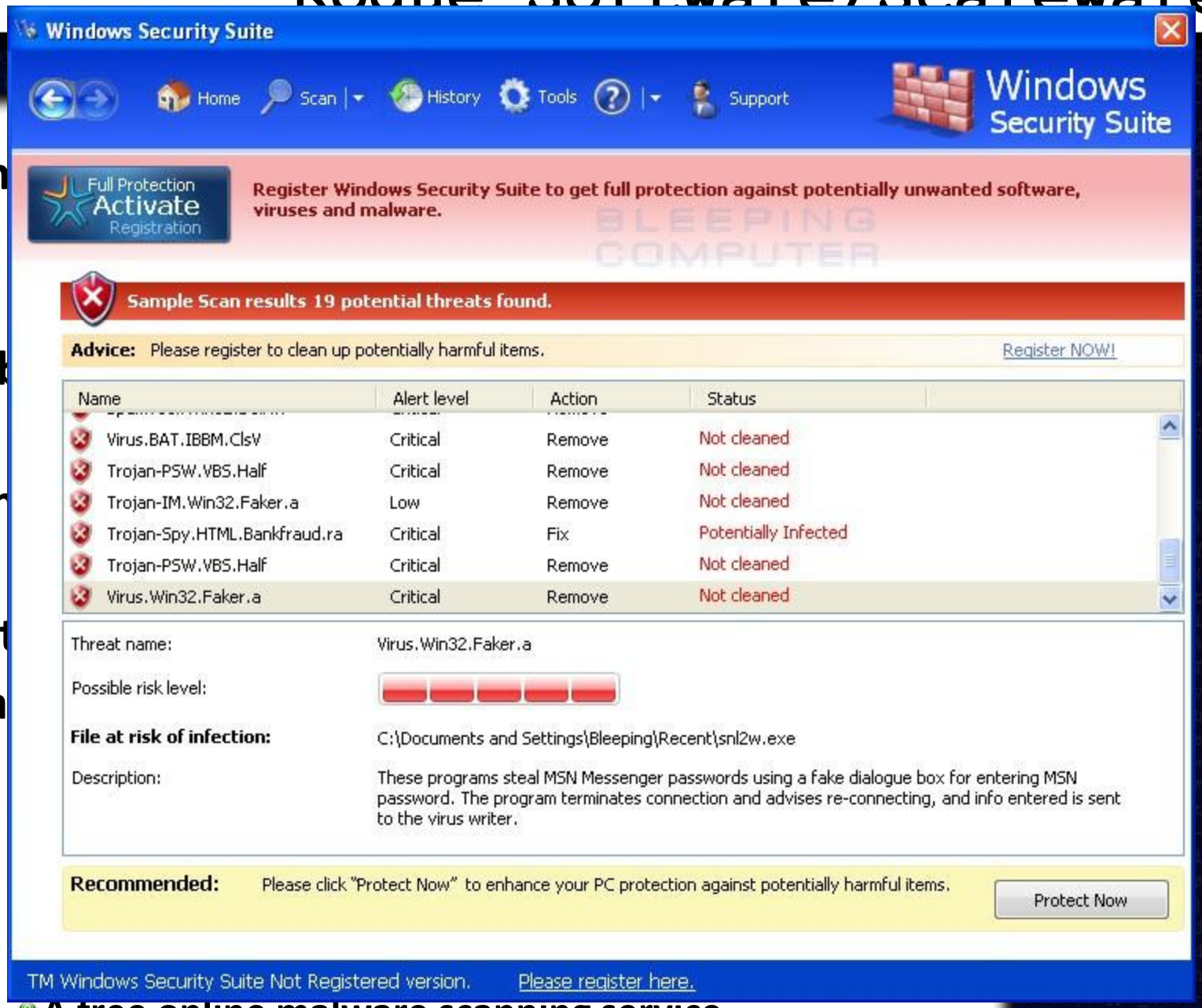
Statistics

- **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/Scareware

- Form
- Has
- Mair
- Most users a



- A free online malware scanning service

Phishing

- Criminally fraudulent process of attempting to acquire sensitive information (u… card de… tr… onic co…
- Comm…
  - Soci…
  - Auc…
  - Online payment processors
  - IT administrators



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 Optim... 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=2732601638831438464036779952815789428264846376888005&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]
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

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.

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

From: Bank of America Alert [onlinebanking@alert.bankofamerica.com]
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

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
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 updat

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

Or simply get the PayPa 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

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 updat

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

Or simply get the PayPa 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 . For assistance, log in to your Pay al page.

To receive email notifications

PayPal Email ID PP031

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.

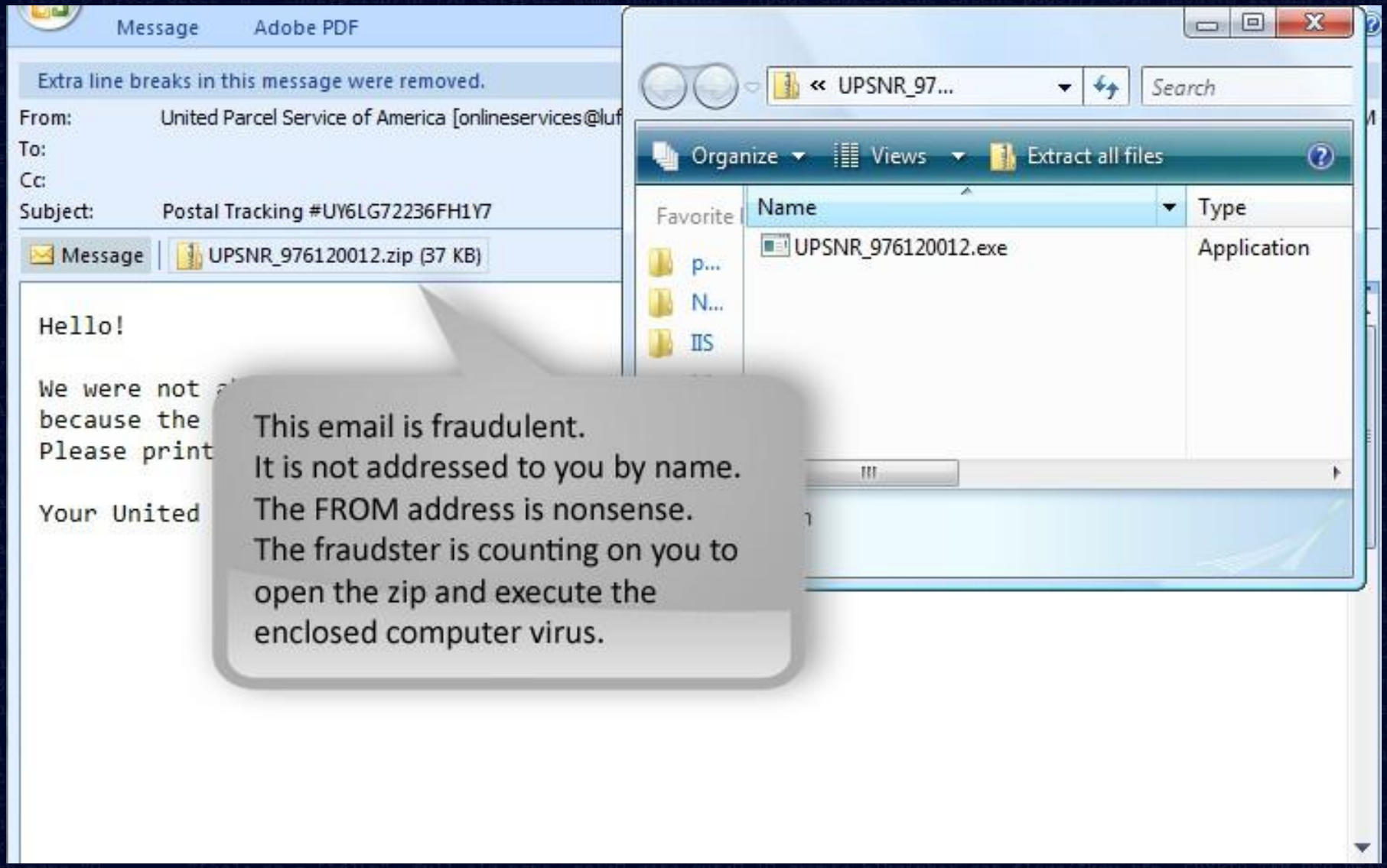
From: United Parcel Service of America [onlineservices@lufthansa.com]
To:
Cc:
Subject: Postal Tracking #UY6LG72236FH1Y7

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
p...
N...
IIS
Name
Type
UPSNR_976120012.exe
Application
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

What we can do to PROTECT?

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

Layered Security

Layered Security approach

- **Monitoring of IP Addresses**
- **New User Controls – Administrator can create a new user. Bank must activate user.**
- **Calendar File – Frequencies, and Limits**
- **Dual Control Processing of files on separate devices – recommended**
- **Fax or Out of Band Confirmation**
- **Secure Browser Key**
- **Pattern Recognition Software**

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 & 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.**
- **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**

What can Businesses do to Protect?

- **Do not open attachments from e-mail -Be on the alert for suspicious emails**
- **Do not use public Internet access points**
- **Reconcile Accounts Daily**
- **Note any changes in the performance of your computer**

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

- **Make sure that your employees know how and to whom to report suspicious activity to at your Company & the Bank**

Contact the Bank if you:

>Suspect a Fraudulent Transaction

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

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

If you have questions
or comments please contact
your local banking center,
or email us via
www.fsblouise.com