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 Union Community Bank 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 prevent CATO?
- What can Businesses do to prevent CATO?
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).
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.
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.
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 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 e-mail.
Multimedia codec required to play a video clip.
Software shared on peer-to-peer networks
A free online malware scanning service
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
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 applications you may have submitted.

The site may be unavailable during normal weekly maintenance or due to unforeseen circumstances.
This email is fraudulent.

URGENT messages with LOG IN links which hide the web address should be considered fraudulent.

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 Optimize, please use the same button to login and choose Treasury Optimizer form.


Click to follow link

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.

The site may be unavailable during normal weekly maintenance or due to unforeseen circumstances.
Message from Customer Service

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:

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.
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.
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 updated card number at https://www.paypal.com/us/cgi-bin/webscr?cmd=_bc-signup

Or simply get the PayPal card that is 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.
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 updated information or simply get the PayPal Card 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.
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.
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
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.
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 Can Businesses Do To Prevent CATO

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 Prevent CATO

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