Corporate Account Takeover & Information Security Awareness

Member FDIC

EQUAL HOUSING LENDER

Gulf Coast Bank & Trust Company

Table of Contents

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).
- 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.

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.

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.

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 code required to play a video clip
    - Software shared on peer-to-peer networks
    - A free online malware scanning service

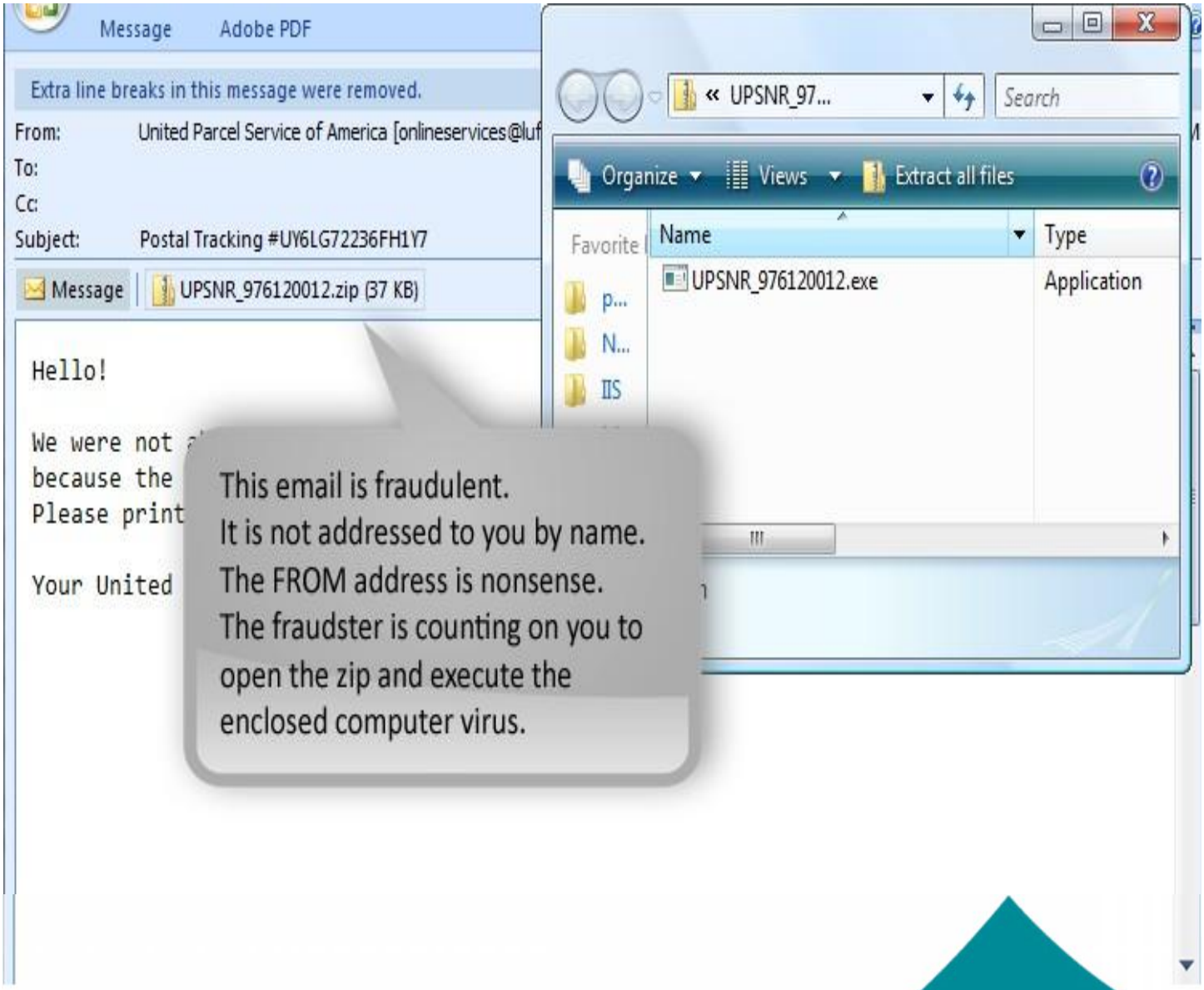
Phishing

- 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

E-Mail Usage

- 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.
- Some experts feel e-mail is the biggest security threat of all.
- It is the fastest, most-effective method of spreading malicious code to the largest number of users.

Example


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.

Personal Best Practices

- **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 and the Bank
- **Contact the Bank** if you:
  - Suspect a Fraudulent Transaction
  - If you are trying to process an Online Wire or ACH Batch and you receive a maintenance page.
  - If you receive an email claiming to be from the Bank and it is requesting personal/company information.

Business Best Practices

- Download and install the Secure Browser required by us to perform your Cash Management transactions.
- Request an IP address restriction on your account so that only the computer(s) you authorize can perform transactions on your account.
- Enable email alerts to advise you on events such as ACH batches initiated, ACH batches processed and Wires transmitted.
- Perform transactions on a dedicated computer that is not used for email or Internet surfing.
- Follow recommendations from your network administrator and/or IT consultant.

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 & all applications as they become available.
- Block Pop-Ups

Other Resources

- www.csbs.org/ec/cato
- http://www.staysafeonline.org/stay-safe-online/
- http://www.microsoft.com/security/default.aspx