Corporate Account Takeover & Information Security Awareness

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, crime ware, most rootkits, and other malicious and unwanted software.

Domestic and International Wire Transfers, Business-to-Business ACH payments, Online Bill Pay, 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 begin monitoring the accounts when victims log onto their Online Banking. Fraudsters collect login credentials and 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 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

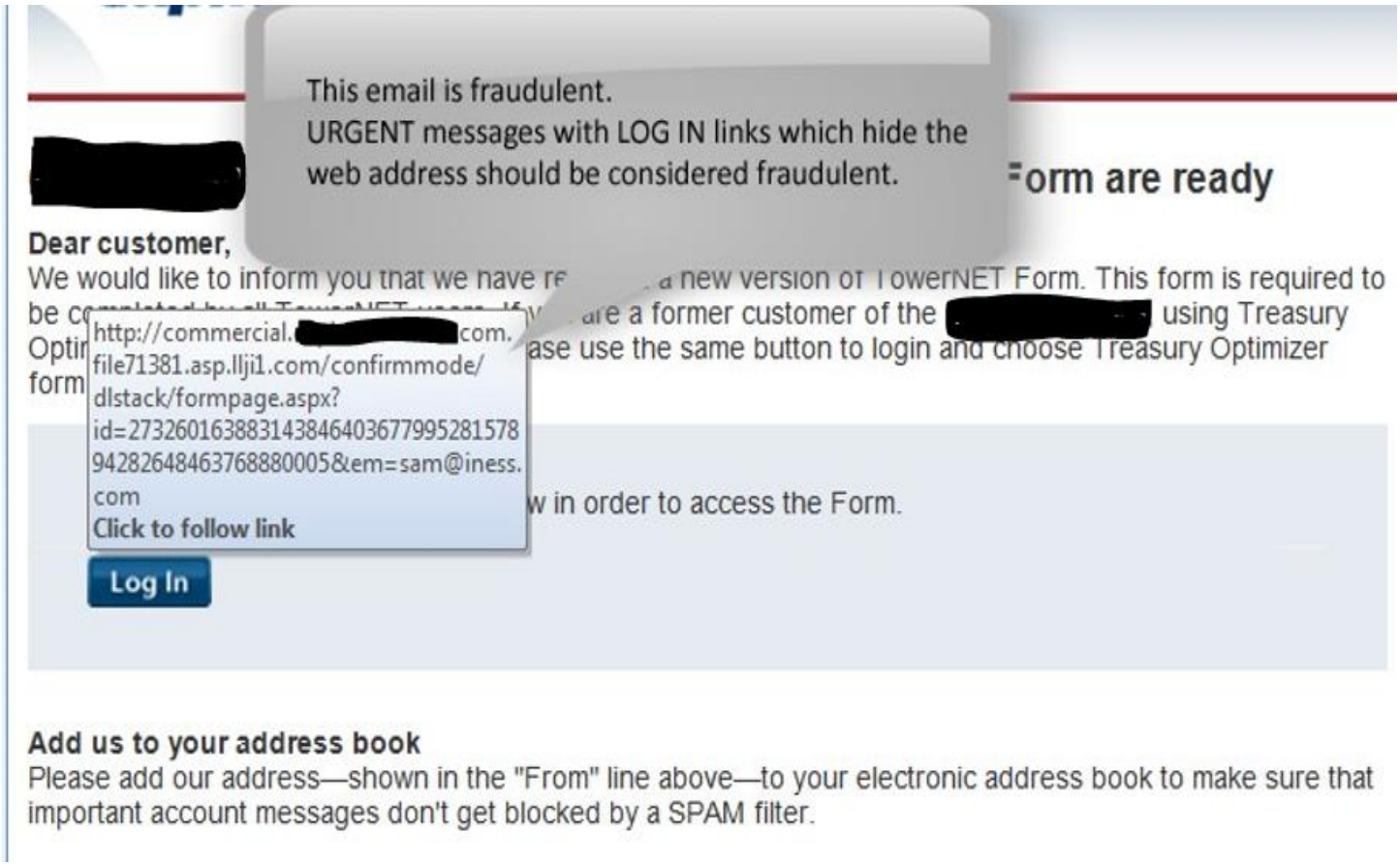
Phishing

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

Examples of Phishing:



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.[redacted]com/srv_8955/customerserv
id=792516599321856258089302763345090421277286337107488264418179782.
2.Follow given instructions.

http://www.[redacted]om.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[redacted], 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 [redacted]

Dear John Doe,

Your credit card ending in 9595 will expire soon. To avoid any disruption to your [redacted] service, please update your credit card expiration date by following these steps:

1. Log in to your [redacted] 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.[redacted]com/us/cgi-bin/
webscr?cmd=_bc-signup
Click to follow link

Or simply get the [redacted] approved almost instantly, and there's no annual fee. Apply today.

Sincerely,
[redacted]

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[redacted]. For
assistance, log in to your [redacted]
page.

To receive email notifications

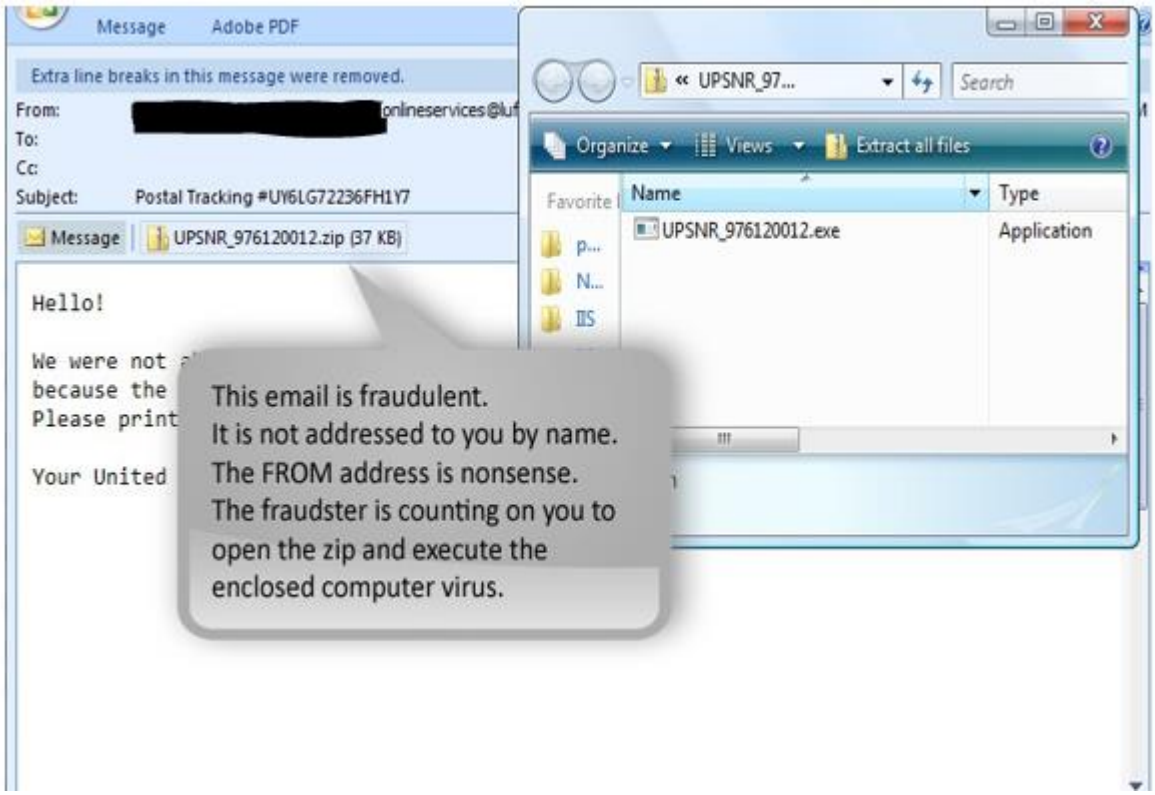
Email Usage

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.

Email 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 can we 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

- Monitoring of IP Addresses
- Use Calendar File – Frequencies, and Limits
- Dual Control Processing of files on separate devices – recommended
- Fax or Out of Band Confirmation

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
- 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.