Fraud Mitigation Strategies for Business

September 2016

Recognizing & Protecting Against Cyber Fraud

Dan Hyland, CFE
VP, Enterprise Fraud Operations

Why is it Important to Remain Vigilant?

Fraud does not discriminate – it occurs everywhere, and no organization is immune

The changing business environment: **with greater convenience and increased payment channels comes greater risk** (mobile banking, remote deposit capture, etc.)

Fraud **tactics are becoming more sophisticated** every day

Fraudsters are **reliant on the actions of their targets**

Fraud is ubiquitous in today's business environment and **the threat continues to grow**

What is Phishing?

Phishing attacks are typically perpetrated through the use of emails that appear to be sent from a legitimate source. Through deception, recipients of these emails are directed to click on links that send them to websites designed to obtain sensitive information or install malicious software onto their device.

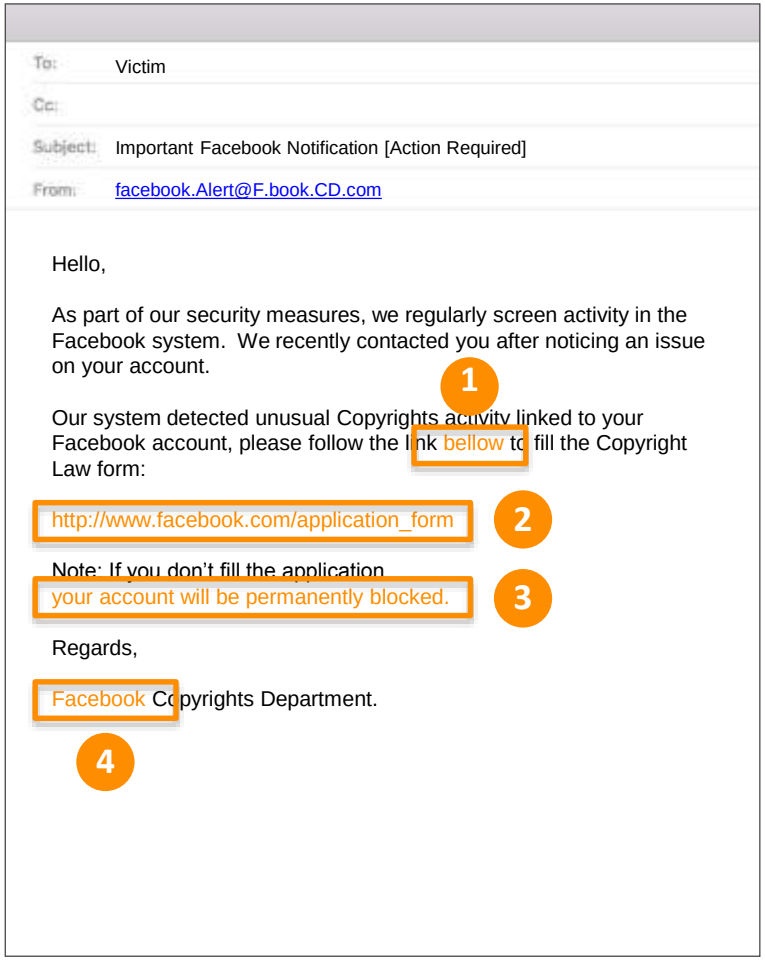
Phishing Email Traits

1. **SPELLING AND BAD GRAMMAR**
   Cybercriminals are not known for their grammar or spelling. If you notice mistakes in an email, it may be malicious.

2. **MALICIOUS LINK**
   Phishing emails will almost always contain a bad link that will either install malware or take you to a malicious website.

3. **CALL-TO-ACTION**
   Many phishing campaigns will use pressure tactics to push victims into clicking on malicious links and/or giving up sensitive information.

4. **POSING AS A RECOGNIZABLE ORGANIZATION**
   Posing as large, easily recognizable companies allow cybercriminals to net a wider population of victims.



Phishing Examples

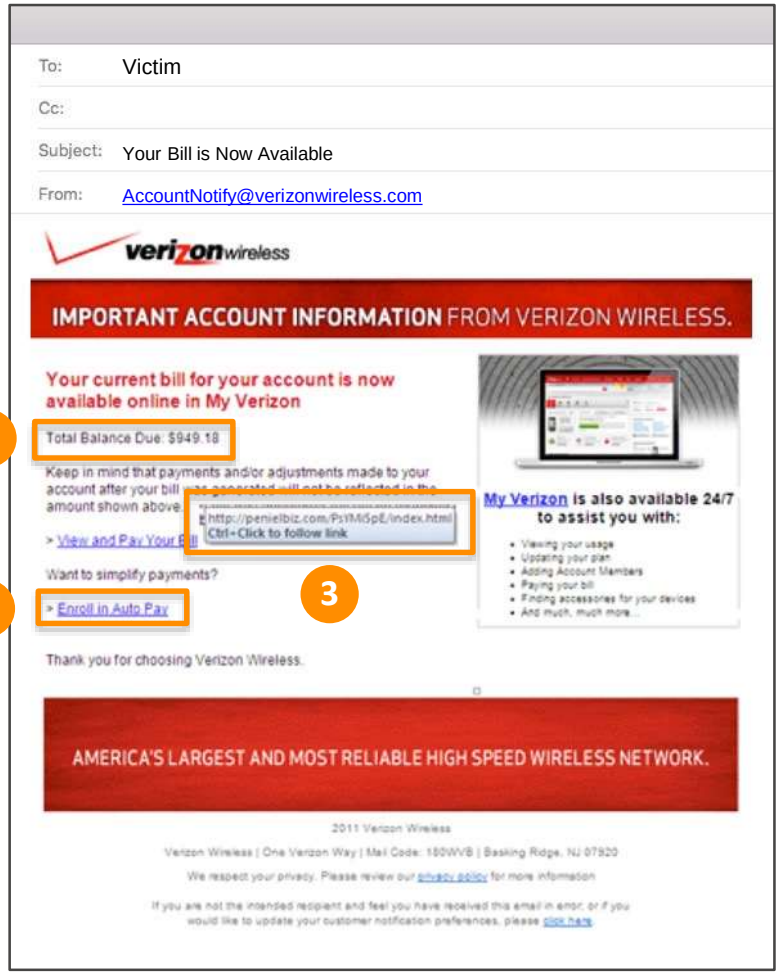
BEWARE OF FAKE LINKS

Always think twice before clicking on a link found in an email.

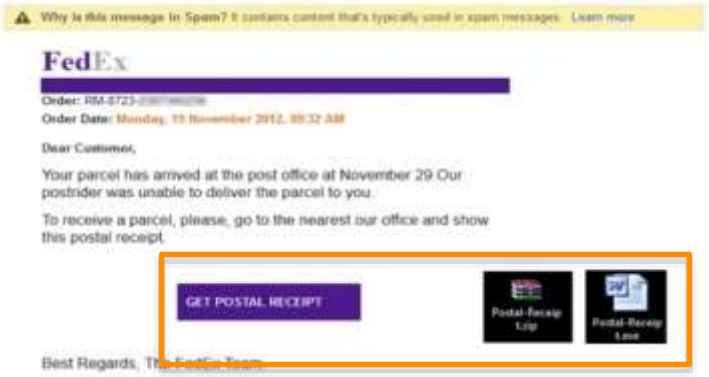
1. **THE HOOK**
   Total Balance Due: $949.18

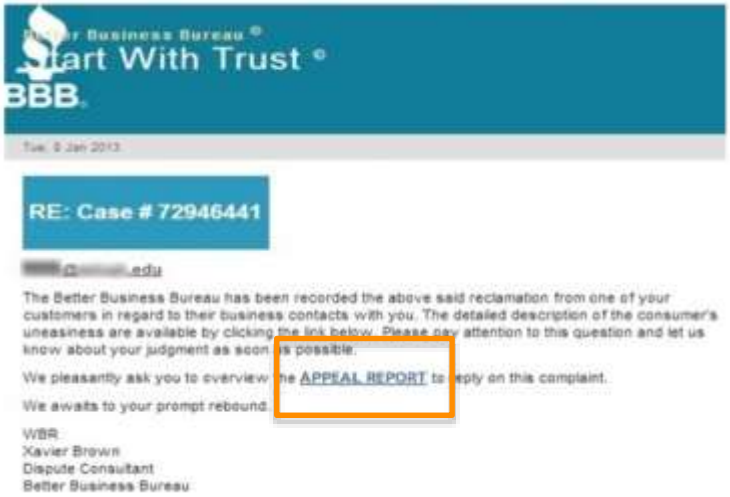
2. **APPROACH LINKS WITH CAUTION**
   All links in this phishing email will deliver malware or send user to a fraudulent site when clicked.

3. **CHECK LINK ACCURACY**
   To confirm where the link is taking you, hover your mouse over (but do not click on) the link to see if the address that appears matches your intended destination.



Phishing Examples (CONTINUED)





Spear Phishing

Unlike standard phishing attempts that are typically sent at random to a wide audience, **spear phishing is a more focused attack directed at a specific individual or organization.** The perpetrator will send an email from what appears to be a trusted source (friend, colleague, vendor, etc.) requesting that the recipient click on a bad link, initiate a monetary payment, or divulge sensitive information.

In a spear phishing attack, the perpetrator leverages information they have obtained on the target to make the correspondence appear more legitimate. **This is often the first step in a masquerading scheme.**

Masquerading Scheme

In a masquerading scheme (also referred to as BEC – Business Email Compromise) a fraudster **poses as a firm's CEO/executive or business partner using a compromised email account, or an email account that appears to be near identical, to facilitate financial crimes.**

"Masquerading" as the legitimate party, the fraudster will send an email to an employee of the target company requesting that a transaction (typically a wire transfer) be executed to a fraudulent beneficiary.

Masquerading - Example Scenario

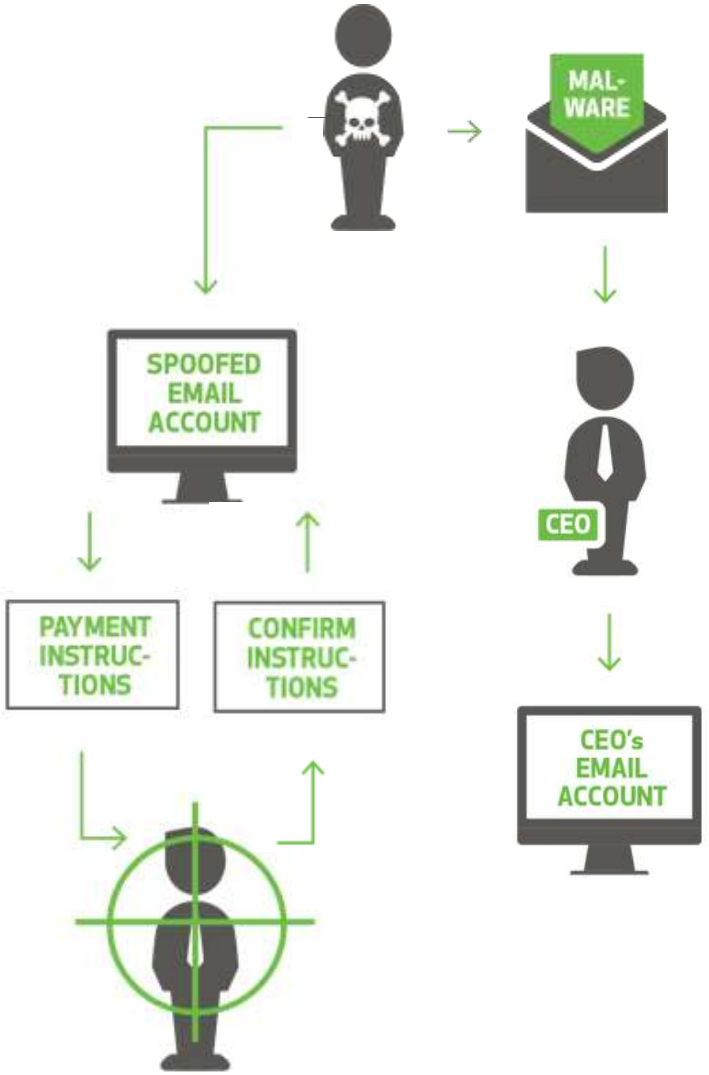
Fraudster uses spear phishing tactics to **compromise the email of a company's CEO**

Access to the CEO's email is acquired, and **the fraudster reviews all available info** (calendar, email history, language/signature/templates used, who executes monetary transactions, etc.)

A payment request is sent to an employee at the target company from an email account created by the fraudster that mirrors or closely resembles the CEO's email account

The **employee confirms the request via email** with the fraudster, who they believe to be the CEO

The employee, believing the request to be legitimate, **initiates the fraudulent payment**



Masquerading - Red Flags

Email contains several **spelling and grammatical errors and/or language not typically used** by the alleged sender.

Includes a **reason that the sender cannot be reached directly** (i.e. “in an important meeting for remainder of day”). Many times, fraudsters will review the calendar of the individual they are posing as and time their attacks during scheduled vacation, all-day meetings, etc.

Includes **a set of circumstances that necessitate expedient action in sending funds.** Failure to execute the requested transaction in a timely fashion will often result in multiple follow-up emails.

Masquerading - Red Flags (CONTINUED)

Can be exceptionally sophisticated in terms of **leveraging information to appear legitimate,** but will always request the use of new or modified payment instructions. The payments are often directed to be charged to a vague cost center (i.e. “admin expenses”).

The **email account used will often be one character off** from the legitimate email being mimicked.

GOOD EMAIL	BAD EMAIL	ALTERATION
john.doe@parington.com	john.doe@par**r**ington.com	Added extra “r”
pjsmith@lumberinc.com	pjsmith@Lumber**I**nc.com	Replaced uppercase “i” with lowercase “l”
s.t.jones@dr-trading.com	s.t.jones@dr**_**trading.com	Replaced hypen with underscore
ellen_hall@abcworks.org	ellen_hall@abcworks**.com**	Replaced .org with .com

What Does a Hacker Want with Your PC?

WEB SERVER
- Phishing Site
- Malware Download Site
- Warez/Piracy Server
- Child Pornography Server
- Spam Site

EMAIL ATTACKS
- Webmail Spam
- Stranded Abroad Scams
- Havesting Email Contacts
- Harvesting Associated Accounts
- Access to Corporate Email

VIRTUAL GOODS
- Online Gaming Characters
- Online Gaming Goods/Currency
- PC Game License Keys
- Operating System License Key

REPUTATION HIJACKING
- Facebook
- Twitter
- LinkedIn
- Google+
- Client-Side Encryption Services

BOT ACTIVITY
- Spam Zombie
- DDoS Extortion Zombie
- Click Fraud Zombie
- Anonymous Proxy
- CAPTCHA Solving Zombie

ACCOUNT CREDENTIALS
- eBay/PayPal Fake Auctions
- Online Gaming Credentials
- Web Site FTP Credentials
- Skype/VoIP Credentials
- Client-Side Encryption Certs

FINANCIAL CREDENTIALS
- Bank Account Data
- Credit Card Data
- Stock Trading Account
- Mutual Fund/401K Account

HOSTAGE ATTACKS
- Fake Antivirus
- Ransomware
- Email Account Ransom
- Webcam Image Extortion

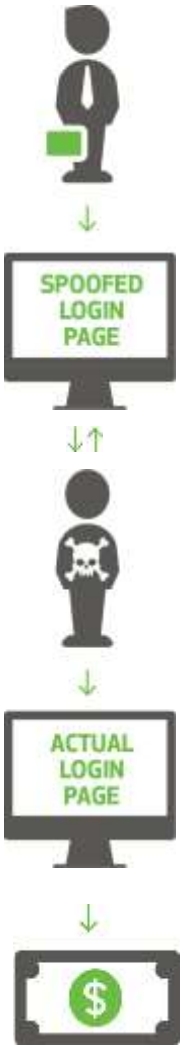
Ransomware

Ransomware is a form of malware that **restricts the target from using their device or retrieving their files until a ransom is paid.** Normal functionality will not be restored by the perpetrator unless an untraceable fee is paid (instructions provided) within a designated period of time. In many cases, ransomware encrypts any files it can access, and the fraudster is the only one with the primary key that can successfully decrypt them. If the payment is made in the allotted period of time, the fraudster claims that they will decrypt the effected files. **Some ransomware demands can be appear to come from legitimate entities (i.e. FBI).**

Man-in-the-Middle Attack

At the highest level, a man-in-the-middle attack is a scenario where a fraudster covertly intercepts and relays messages between two parties who believe that they are communicating directly with each other. This tactic can be used to redirect targets to spoofed login pages and steal their login credentials or other sensitive information.

- Target (whose device has previously been infected with malware) attempts to access online banking website, but is **redirected to cosmetically identical website** controlled by the fraudster
- **Target enters login credentials, which are intercepted by the fraudster** and used to log into the legitimate online banking website
- If the fraudster requires any further credentials they can be obtained through deceiving the target into enter them into the spoofed login page
- Once access is successfully gained, the fraudster initiates unauthorized transactions



Tips to Defend Against Fraud

Update your Operating Systems, browser and software patches to ensure you're running the most up to date technology

Establish **a secure firewall** and install/maintain **antivirus solutions**

Require **dual approval** on monetary transactions, as well as administrative changes

Consider using a **dedicated PC for online banking** or separate PC's for the initiator and approver

Set up **strong passwords** and **avoid password repetition** across multiple sites/applications

Be cautious when using public wifi and consider utilizing a VPN (virtual private network) to protect your network traffic

Tips to Defend Against Fraud (CONTINUED)

Be aware of and **utilize your bank's security measure – Huntington's Business Security Suite**

- ACH Positive Pay
- Check Block
- Check Positive Pay
- Reverse Positive Pay

Review online users and their profiles periodically

Verify routing and account numbers over the phone for any new or modified payment instructions

Educate employees about common fraud schemes (PhishMe)

Take a **measured approach to personal information** shared online

Cyber Liability

Will Carlin
VP, Product Specialist
Ashley Bauer
VP, Marketing Manager

Cyber Risk Activities

Credit Card Processing

Storage of Sensitive Data

Lost or Stolen Devices

Improper disposal of information

Improper Access of information

Employee Actions (malicious or accidental)

Virus transmission

Phishing Attacks

Business Email Compromise

Vendor Activities

Ransomware

First Party Coverage Options

Typical Coverage Components will cover costs the insured incurs for:

Breach Response/Crisis Management

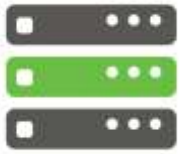
Coverage responds to a network or privacy breach. Coverage includes: breach notification, public relations, forensic consultants, and credit monitoring costs

Cyber Extortion or Loss

Coverage responds to a threat by third party to commit a network security or privacy breach

Business Interruption Extra Expense Loss

Coverage responds to loss of income resulting from a network security breach or a network attack and extra expenses incurred to restore network to original condition



Data Restoration Coverage

Coverage responds to cost to restore data destroyed or altered as a result of a network security breach

Third Party Liability Coverage Options

Components will cover claim expenses and damages the insured is legally obligated to pay as a result of the following:

Network Security Liability

Provides coverage for actions that the Insured is legally liable for claims made against the Insured for a Network Security Breach or Failure

Privacy Liability

Provides coverage for actions that the Insured is legally liable for claims made against the Insured for a Privacy Breach of PII, PHI or Corporate Confidential Information

Regulatory Coverage

Provides coverage for actions or proceedings and fines/penalties against the Insured by a regulatory agency resulting from a violation of a Privacy Law

Website Media / Multimedia

Provides coverage for actions that the Insured is legally liable for claims made against the Insured for a Media Peril of content on the Insured's Internet Site or may cover general Media Perils

Professional Liability

Provides coverage for acts, errors or omissions in the rendering or failure to render professional services to a client of the Insured

Fraud Insurance Tools

Below highlighted are insurance tools to assist in fraud

Insurance Product	Product Description
Cyber Liability *Typically a separate policy*	Coverage for damages when private, personal and financial information is compromised due to a data breach or network intrusion. While not all cyber policies are the same, typical coverage includes incident management, regulatory defense, business interruption and extra expense, network extortion, digital assets, privacy liability, network security liability, and internet media liability.
Computer Fraud *Part of a Crime Policy*	Coverage for the theft of money, securities, or property by using a computer to transfer covered property from the insured's premises or bank to another person or place.
Funds Transfer Fraud *Part of a Crime Policy*	Coverage for the erroneous transferring of funds to or from a financial account of the insured based upon instructions fraudulently transmitted by a non-employee.
Business Email Compromise/Masquerading *Added by Endorsement to either Cyber or Crime*	Coverage for criminals deceptively gaining the confidence of an employee to induce him or her to voluntarily part with money or securities.

Average Cost of Cyber Claim Services*

	2013	2014	2015
Average cost of crisis services	$365,000	$366,484	$499,710
Average cost of defense	$258,000	$698,797	$434,354
Average cost of settlement	$88,000	$558,520	$880,839

*2014 and 2015 NetDiligence Cyber Claims Study

Takeaways

Cyber is an Operational Risk for **every business**

Regulatory **environment will continue to evolve**

Each cyber insurance policy is different, check exclusions

Developing Coverages

Capacity is available

Losses will push **pricing pressure** upward

Q&A