Enterprise Fraud Operations

October - 2017

Ohio Association of Public Treasurers

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.)

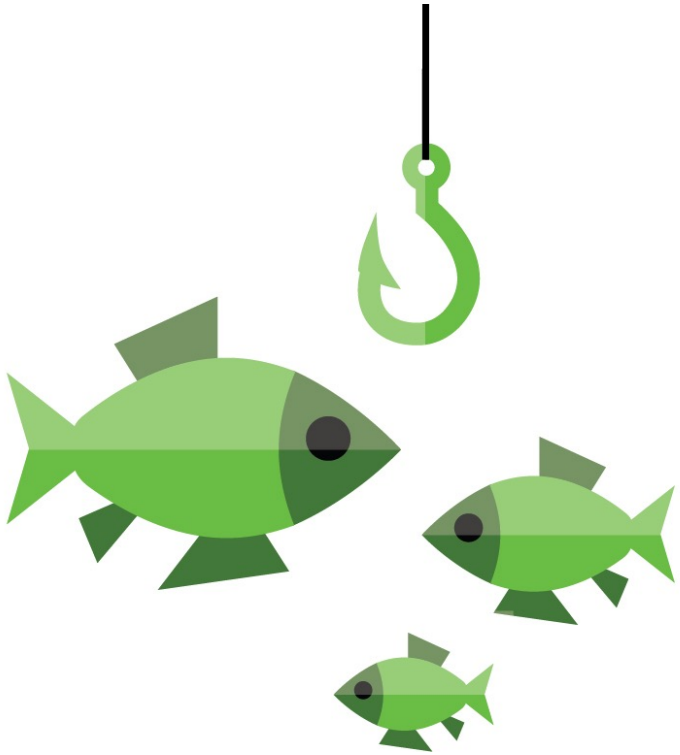
Fraud **tactics are becoming more sophisticated** every day

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

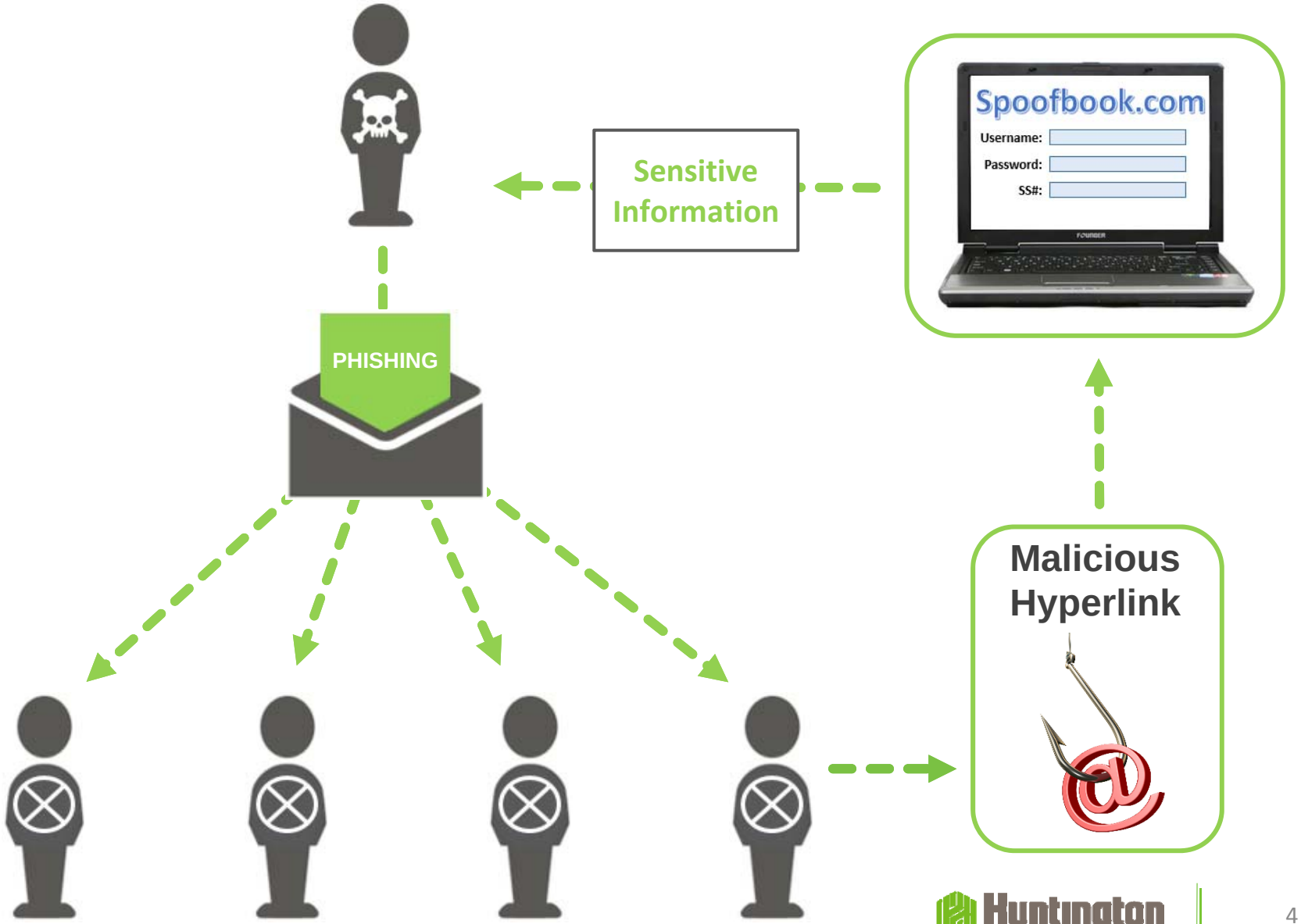
Fraud is ubiquitous in today's business environment and **the threat continues to grow**

What is Phishing?

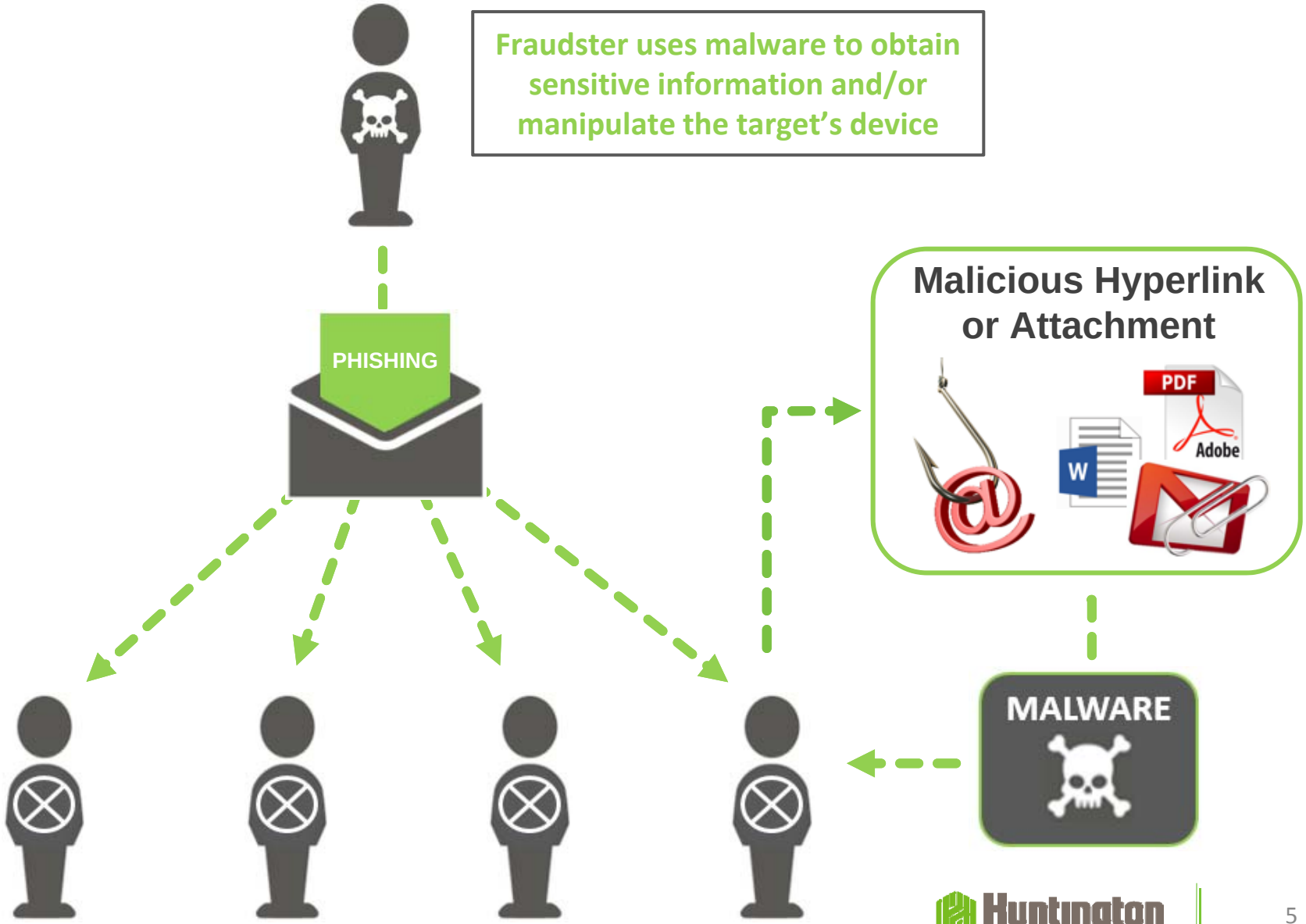
Phishing attacks are typically perpetrated through the use of emails that appear to be sent from a legitimate source. Through deception, recipients of these emails are directed to click on links that send them to websites designed to obtain sensitive information or install malicious software onto their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



Phishing – Using Spoof Websites



Phishing – Installing Malware



SMISHING & VISHING

What is SMISHING? This tactic involves the perpetrator sending an SMS (text) message to the target's smartphone containing a hyperlink that either installs malicious software onto their device or sends them to a website designed to obtain confidential information. In some instances, a phone number will be provided for the target to call, at which point they will be prompted to divulge sensitive information by an individual or an automated system.

- Messages appear to be from a valid source, often posing to be from a bank notifying the target that their account has been blocked – target directed to follow the bad link to unsuspend
- Mobile malware can harvest the data from your cell phone and transmit it back to the fraudster - including contacts (phone & email) and bank information
- Forward suspect text messages to 7726 (SPAM) to have the number blocked by your carrier

What is VISHING? This tactic is the telephone equivalent of phishing and uses phone calls to scam the victim into surrendering sensitive information. The fraudster will leave a voicemail in some instances, citing the urgency of a prompt response.

- These calls are designed to generate fear and evoke an immediate response (i.e. your card account will be closed immediately if you do not call back)
- When connected to an individual, they are often aggressive and will push for information without providing any themselves
- When in doubt, call the entity in question directly at a verified or publicly published phone number

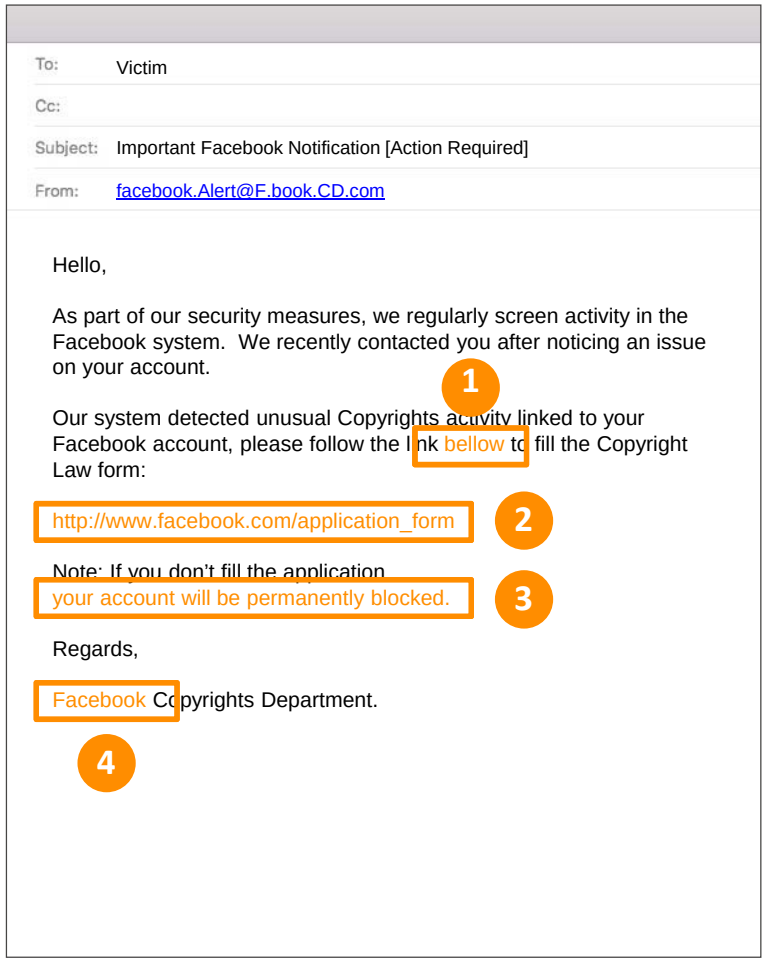
Phishing Email Traits

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

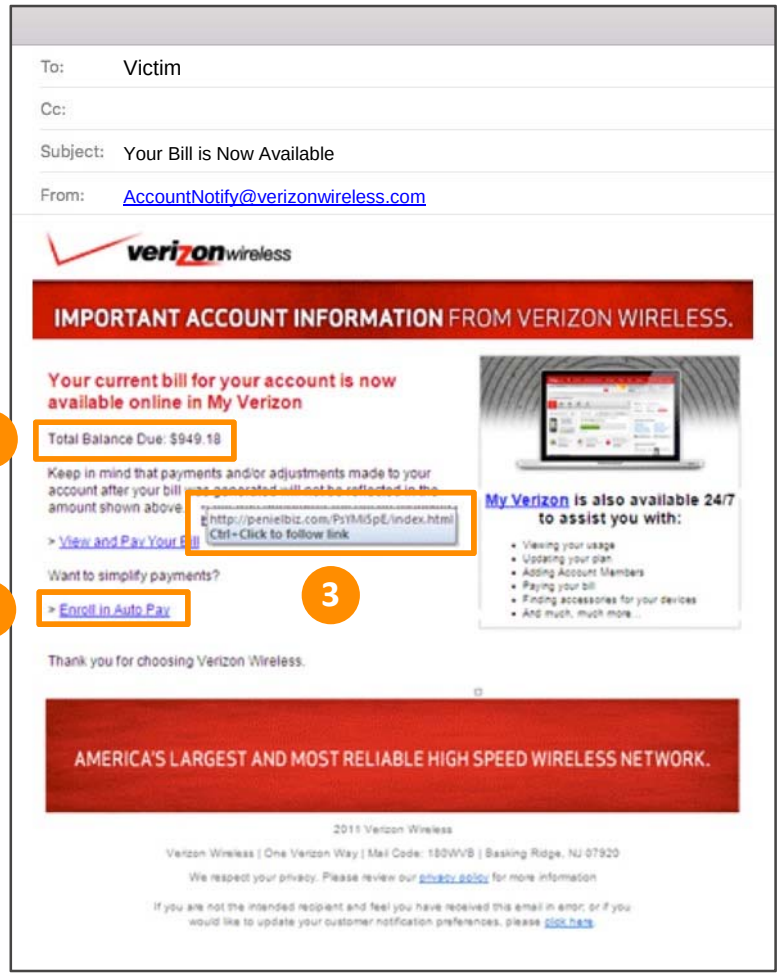
BEWARE OF FAKE LINKS

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)


Anthem
BlueCross BlueShield

Cyber Attack Against Anthem

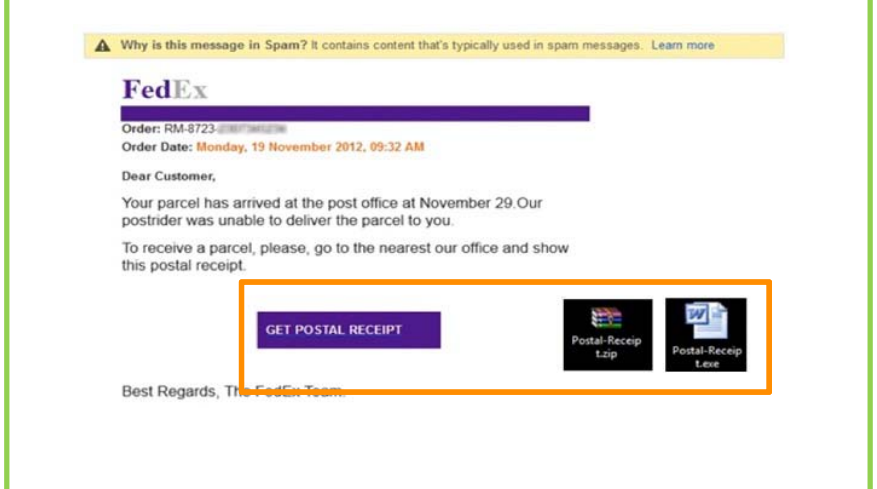
Dear Anthem Client,

We wanted to make you aware of a data breach that may have affected your personal health information and credit card data. The data which was accessed may impact clients who made credit or debit card payments for healthcare or who got treatment during the year 2014.

Your trust is a top priority for Anthem, and we deeply regret the inconvenience this may cause. The privacy and protection of our client's health care information is a matter we take very seriously and we are working diligently to resolve the incident.

To subscribe to a free year of credit card account protection please click on the link below and follow the instructions that will be required:

Click Here To Get Your Free Year Of Credit Card Protection


Why is this message in Spam? It contains content that's typically used in spam messages. Learn more

FedEx

Order: RM-8723-

Order Date: Monday, 19 November 2012, 09:32 AM

Dear Customer,

Your parcel has arrived at the post office at November 29.Our postrider was unable to deliver the parcel to you.

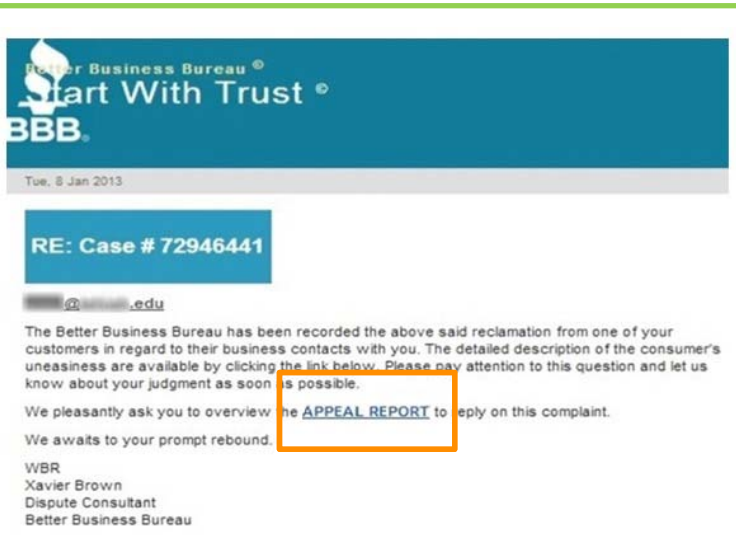
To receive a parcel, please, go to the nearest our office and show this postal receipt.

GET POSTAL RECEIPT

Postal-Receipt.zip

Postal-Receipt.exe

Best Regards, The FedEx Team.


Better Business Bureau ®

Start With Trust ®

BBB

Tue, 8 Jan 2013

RE: Case # 72946441

[redacted]@[redacted].edu

The Better Business Bureau has been recorded the above said reclamation from one of your customers in regard to their business contacts with you. The detailed description of the consumer's uneasiness are available by clicking the link below. Please pay attention to this question and let us know about your judgment as soon as possible.

We pleasantly ask you to overview the APPEAL REPORT to reply on this complaint.

We awaits to your prompt rebound.

WBR
Xavier Brown
Dispute Consultant
Better Business Bureau


LinkedIn

Anandita Chatterji wants to connect with you on LinkedIn.

Anandita Chatterji
Analyst at CGI View Profile

Accept

You are receiving Invitation emails. Unsubscribe

This email was intended for Lindsey [redacted]. Learn why we included this.

LinkedIn Corporation, 2029 Stierlin Ct. Mountain View, CA 94043, USA

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

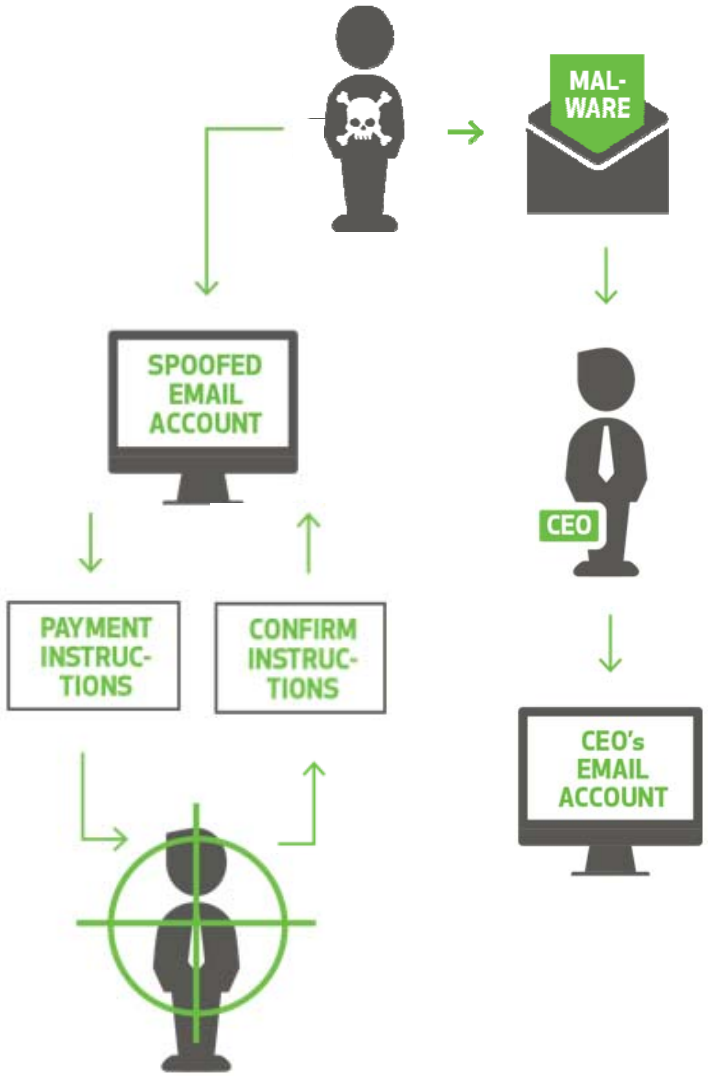
Fraudster uses spear phishing tactics to **compromise the email of a company's CEO**

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@parrington.com	Added extra “r”
pjsmith@lumberinc.com	pjsmith@LumberInc.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

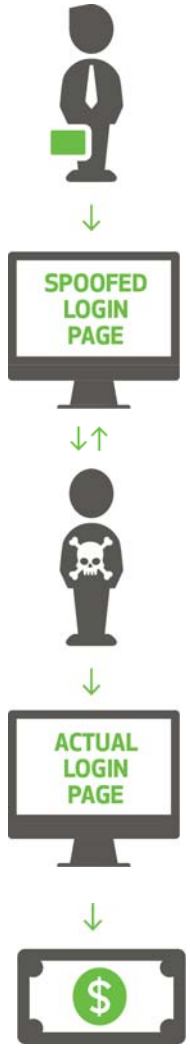
Ransomware

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

Ensure **contact information** is correct

Keep your **login credentials** private/secure

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 of outbound payments

Educate employees about common fraud schemes (PhishMe)

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

Creating a Strong Password

Avoid names, dates, and common phrases

Avoid complete words

There are free password generators available that can assist in creating strong passwords

A strong password contains the following:

- 8 or more characters
- Uppercase & lowercase letters
- Numbers
- Special characters

Keeping Your Credentials Safe

- Avoid writing down login credentials and never leave them out
- Avoid keeping passwords stored in Word documents or spreadsheets (even if they are password protected)
- Avoid using the same password across multiple services
- Consider utilizing a password management application to store and protect your online passwords

Q&A