Huntington

Fraud Mitigation and Cyber Strategies for Public Entities

April 2019

1

Recognizing & Protecting Against Fraud

2

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**

3

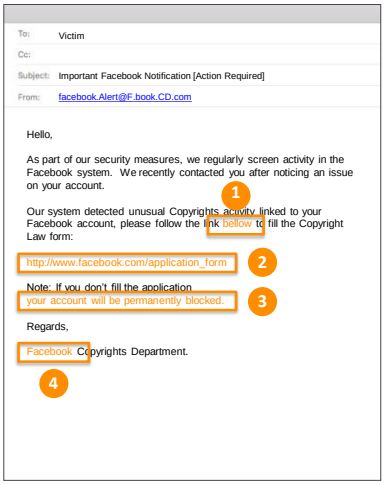
What is Phishing?

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.

4

Phishing Email Traits

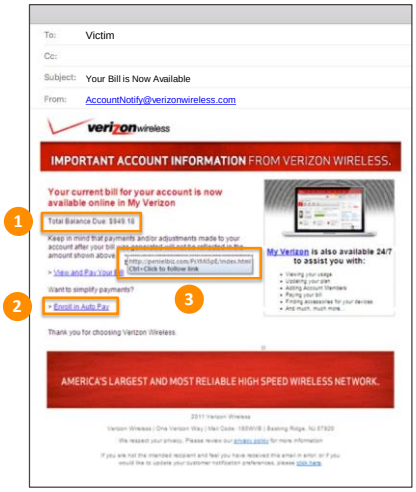
1. **SPELLING AND BAD GRAMMAR**
   Cybercriminals are not known for their grammar or spelling. If you notice mistakes in an email, it may be malicious.
2. **MALICIOUS LINK**
   Phishing emails will almost always contain a bad link that will either install malware or take you to a malicious website.
3. **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.



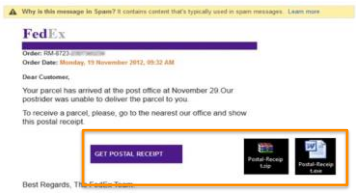
Phishing Examples

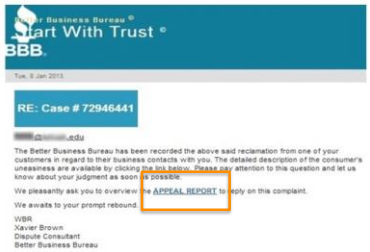
BEWARE OF FAKE LINKS
Always think twice before clicking on a link found in an email.

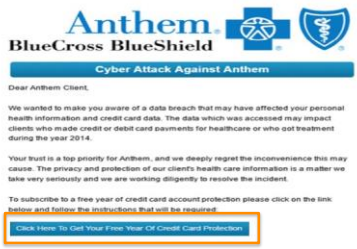
1. **THE HOOK**
   Total Balance Due: $949.18
2. **APPROACH LINKS WITH CAUTION**
   All links in this phishing email will deliver malware or send user to a fraudulent site when clicked.
3. **CHECK LINK ACCURACY**
   To confirm where the link is taking you, hover your mouse over (but do not click on) the link to see if the address that appears matches your intended destination.



Phishing Examples (CONTINUED)







7

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.**

8

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.

Huntington | 9

9

Masquerading - Example Scenario

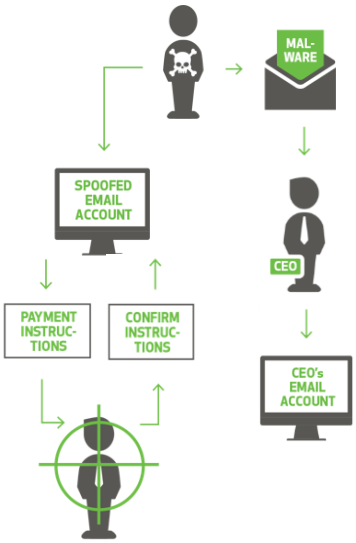
Fraudster uses spear phishing tactics to **compromise the email of a company's CEO**

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**



Huntington | 10

10

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.

11

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

12

Check Fraud Types

Altered checks primarily refers to a method to **modify handwriting and information on the check** such as the **payee or amount**. When an attempt to **erase information** from the entire check is made, it is called **check washing**.

Forgery can often occur when an **employee of a business issues a check without proper authorization**. Fraudsters will also **steal a check, endorse it and present for payment** or cash at the financial institution while using fake personal identification.

Counterfeiting can either mean wholly **fabricating a check using readily available desktop publishing equipment** consisting of a personal computer, scanner, sophisticated software and high-grade laser printer or simply duplicating a check with advanced color photocopiers.

13

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

14

Ransomware

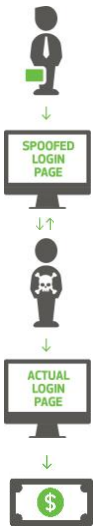
Ransomware is a form of malware that **restricts the target from using their device or retrieving their files until a ransom is paid.** Normal functionality will not be restored by the perpetrator unless an untraceable fee is paid (instructions provided) within a designated period of time. In many cases, 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).**

15

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



16

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

Huntington | 17

17

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
  - Teller Positive Pay
  - Payee 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)

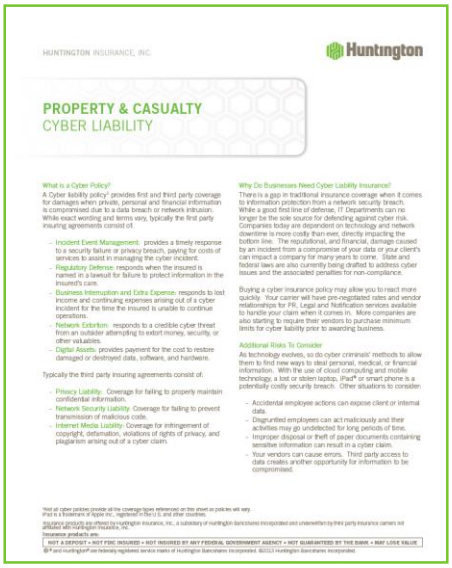
Take a **measured approach to personal information** shared online

Keep **check stock in a secure / locked** location

Huntington | 18

18

Cyber Insurance



HUNTINGTON INSURANCE, INC.

Huntington

PROPERTY & CASUALTY
CYBER LIABILITY

What is a Cyber Policy?

A Cyber liability policy* provides first and third party coverage for damages when private, personal and financial information is compromised due to a data breach or network intrusion. While exact wording and terms vary, typically the first party insuring agreements consist of:

- Incident Event Management: provides a timely response to a security failure or privacy breach, paying for costs of services to assist in managing the cyber incident.
- Regulatory Defense: responds when the insured is named in a lawsuit for failure to protect information in the insured's care.
- Business Interruption and Extra Expense: responds to lost income and continuing expenses arising out of a cyber incident for the time the insured is unable to continue operations.
- Network Extortion: responds to a credible cyber threat from an outsider attempting to extort money, security, or other valuables.
- Digital Assets: provides payment for the cost to restore damaged or destroyed data, software, and hardware.

Typically the third party insuring agreements consist of:

- Privacy Liability: Coverage for failing to properly maintain confidential information.
- Network Security Liability: Coverage for failing to prevent transmission of malicious code.
- Internet Media Liability: Coverage for infringement of copyright, defamation, violations of rights of privacy, and plagiarism arising out of a cyber claim.

Why Do Businesses Need Cyber Liability Insurance?

There is a gap in traditional insurance coverage when it comes to information protection from a network security breach. While a good first line of defense, IT Departments can no longer be the sole source for defending against cyber risk. Companies today are dependent on technology and network downtime is more costly than ever, directly impacting the bottom line. The reputational, and financial, damage caused by an incident from a compromise of your data or your client's can impact a company for many years to come. State and federal laws are also currently being drafted to address cyber issues and the associated penalties for non-compliance.

Buying a cyber insurance policy may allow you to react more quickly. Your carrier will have pre-negotiated rates and vendor relationships for PR, Legal and Notification services available to handle your claim when it comes in. More companies are also starting to require their vendors to purchase minimum limits for cyber liability prior to awarding business.

Additional Risks To Consider

As technology evolves, so do cyber criminals' methods to allow them to find new ways to steal personal, medical, or financial information. With the use of cloud computing and mobile technology, a lost or stolen laptop, iPad® or smart phone is a potentially costly security breach. Other situations to consider:

- Accidental employee actions can expose client or internal data.
- Disgruntled employees can act maliciously and their activities may go undetected for long periods of time.
- Improper disposal or theft of paper documents containing sensitive information can result in a cyber claim.
- Your vendors can cause errors. Third party access to data creates another opportunity for information to be compromised.

*Not all cyber policies provide all the coverage types referenced on this sheet as policies will vary.
iPad is a trademark of Apple Inc., registered in the U.S. and other countries.

Insurance products are:
NOT A DEPOSIT • NOT FDIC INSURED • NOT INSURED BY ANY FEDERAL GOVERNMENT AGENCY • NOT GUARANTEED BY THE BANK • MAY LOSE VALUE

With the continuous threat and advancement of fraud schemes, companies should evaluate options which will minimize their exposure and enhance peace-of-mind

- Cyber liability provides first and third party coverage for damages when private, personal and financial information is compromised due to a data breach or network intrusion
- Contact your Huntington Insurance partner for additional information

Q&A

21