BPM

How to Avoid Becoming the Next Phish Victim

David Trepp, M.S./Partner

Housekeeping

- Questions and Comments
  - Please have your microphone muted when you are not speaking to the group
  - Feel free to unmute and speak up, or chat message, when you have a question

- CPE Credit Rules
  - You will need to listen for & write down **3 code words** throughout the class in order to receive CPE credits for the one hour of training; the code words will be in **bold, underlined, in red font**
  - At about five minutes before the end of the class, you will receive a survey from Survey Monkey
  - You will need to type in each of the code words and submit the survey in order to receive CPE
  - The expectation is that you complete the survey as soon as you receive it. We will only leave the survey open until half an hour after the class ends, and CPE will not be granted after this time

BPM Fast Facts

BPM at a Glance

40+ Partners

500+ Employees

Founded **1986**

Services

Advisory
Audit
Corporate Tax
Employee Benefit Plan Audits
High Net Worth
International Tax
IT Assurance
Risk Assurance
SEC Compliance

Industry Knowledge

Consumer Business

Financial Services

Life Science

Nonprofit

Private Client Services

Real Estate

Technology

Locations

San Francisco
Menlo Park
Walnut Creek
San Jose
Santa Rosa
St. Helena
Cayman Islands
Bengaluru
Eugene
Orange County
Stockton
Seattle
Fairfield

One of the 50 largest public accounting and advisory firms in the country.

David Trepp
Partner, IT Assurance

- US Army Veteran
- M.S. Chemistry
- Serial Tech Entrepreneur
- Professional Interests
  - Securing Authentication
  - Securing Interconnected Systems
- Personal Interests
  - Rock Climbing
  - Bicycle Touring
  - Information Science
    - Thermodynamics

Information Security Perspective

- BPM Infosec assessment team personnel ***are not*** experts at planning, building, or managing information security (Infosec) controls

- BPM Infosec assessment team personnel ***are*** experts at defeating information security controls and providing Infosec controls assurance

- This introductory presentation will provide a hacker's perspective on phishing attacks

Contents

- Why Social Engineering Attacks?
- Common Phish Attack Techniques
- How to Avoid Becoming the Next Phish Victim

Questions/comments are encouraged

Why Social Engineering Attacks?

Common Attack Vectors

- Human

- Physical

- Technical

Alone *and* Combined

What is Social Engineering?

"The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes."

-quizlet.com

Infosec Concepts: Risk Assessment

Risk: A *measure* of the extent to which a person or organization is threatened by a potential circumstance or event (threat); a function of impact and likelihood

Risk = Likelihood * Impact

What is the likelihood of a threat agent exploiting a threat?

- High Likelihood: Facing the Internet, Technically easy to defeat
- Low Likelihood: Hidden within network, Technically challenging

What is the impact of a successful exploit?

- Low Impact: Inconvenience
- High Impact: Disruption of service, Disclosure of sensitive information, and/ or fraudulent transaction

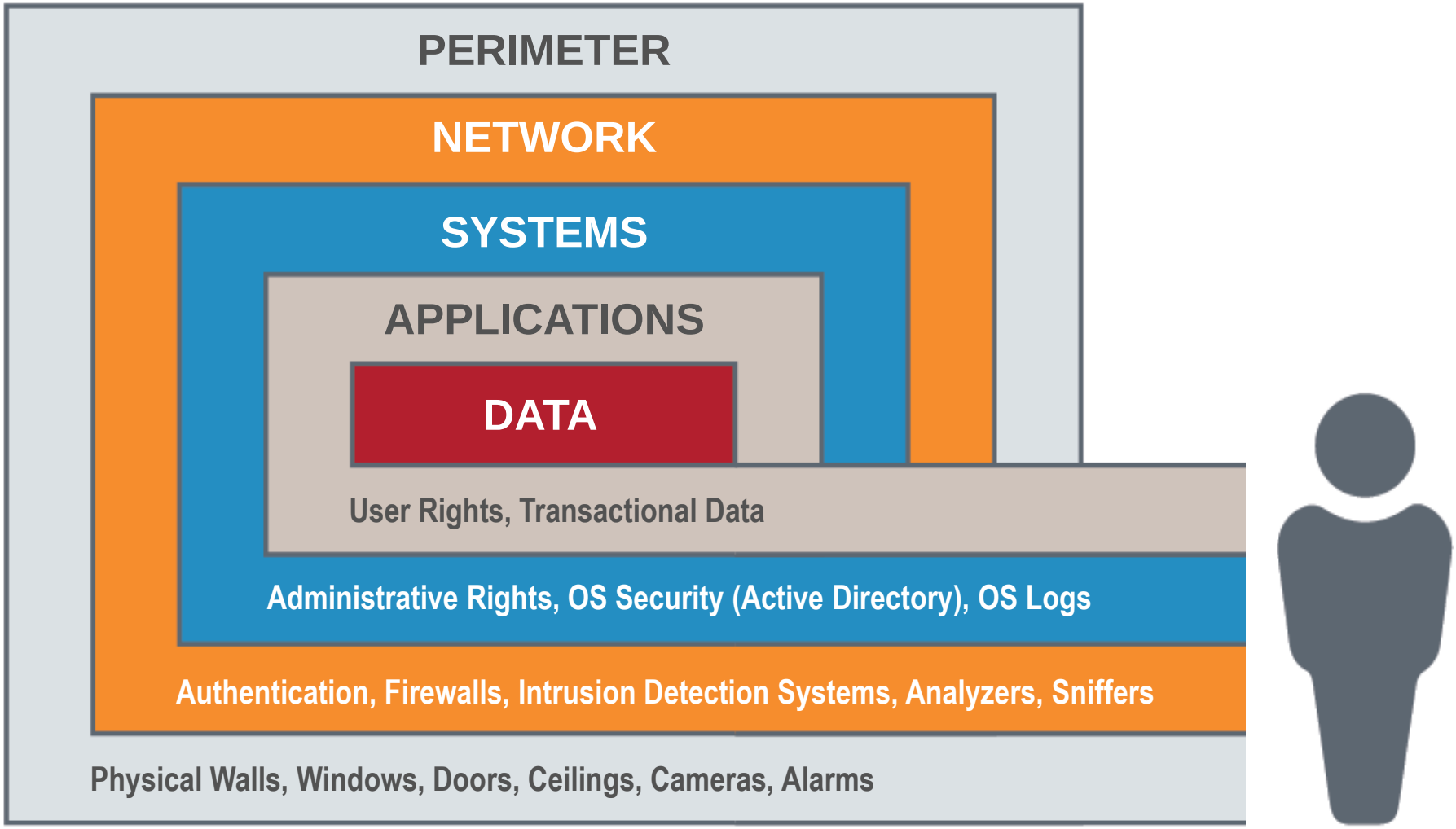
See NIST Special Publication 800-30, Guide for Conducting Risk Assessments

Why Is Social Engineering So Likely To Succeed?

- Civilization couldn't exist without an innate "assumption of **truth**"
- Application software often gets patches and updates; Human software is still in Version 1.0
- Human cognitive abilities generally decline when faced with unusual circumstances
- Statistics suggest the average employee fails four social engineering attacks before becoming inoculated

Source:
Saturday Morning Breakfast Cereal
www.smbc-comics.com

Why Is Social Engineering So High Impact?



Social Engineering Quotes

"*Amateurs hack systems, professionals hack people*."

--Bruce Schneier – Cryptography Bigshot

"*Companies spend millions of dollars on firewalls and secure access devices, and it's money wasted because none of these measures address the weakest link in the information security chain: the people who use, administrate and operate computer systems.*"

--Kevin Mitnick – Infamous Social Engineer

Common Types of Phishing

- **Phishing**: Typical email-based social engineering attack
  - Usually casts a wide net, *e.g.* ransomware campaigns
- **Spear Phishing**: Customized phish, targeting specific individuals or groups
  - Timely topic
  - Portray insider knowledge
  - Often uses spoofed (faked) sender address
- **Whaling**: Targets Executives
- **Vishing**: Via phone
- **Smishing**: Via SMS or Text
- **Search Engine Phishing/Domain Squatting**: Spoofed web pages

Historical note: The “ph” in phishing gives a nod to first generation hackers, originally referred to as phone phreaks

Phishing Leads to Breaches*

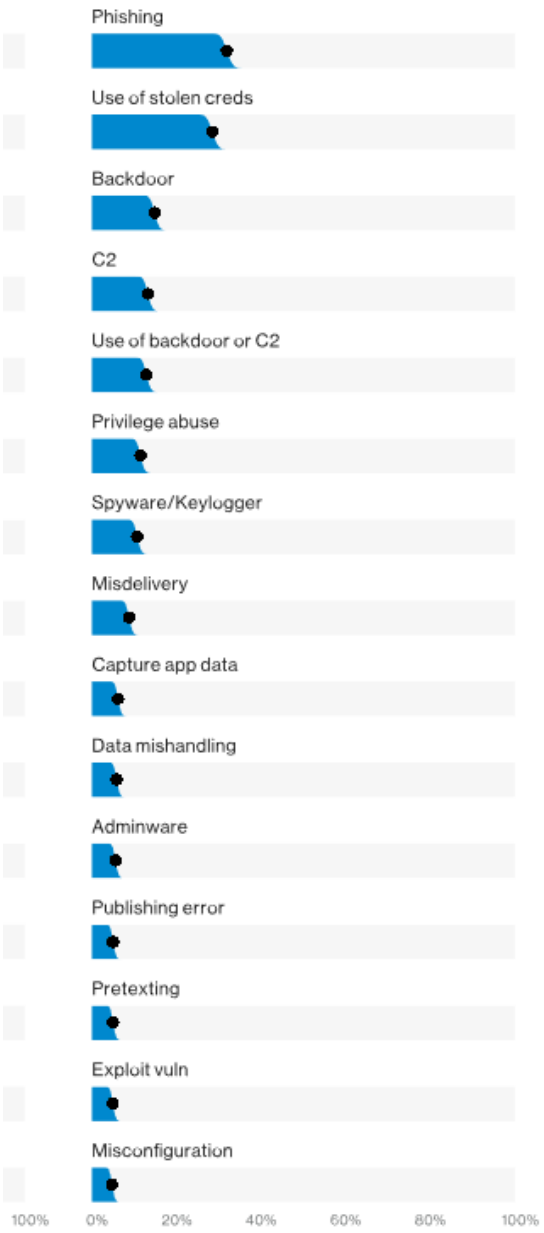


Figure 12. Top threat action varieties in breaches (n=1,774)

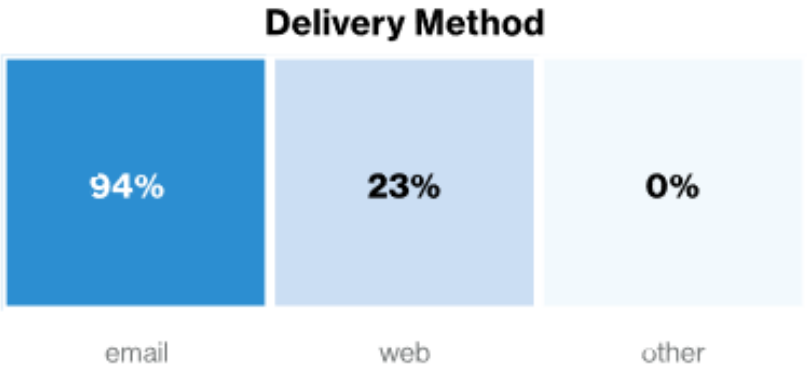


Figure 19. Malware types and delivery methods

* 2019 Verizon Data Breach Investigations Report

Impact of a Successful Phish

- Bitcoin mining
- Ransomware extortion
- VPN (remote) access
- Webmail access
- Compromise of affected system
- Compromise of all connected systems

Common Phish Attack Techniques

Information Gathering for Spearphising

Google Searches

Social Networking Websites

Badge images

Digital Foot-Printing

Organization's Website

Calls to Reception

Vendor Press Releases

Tech Support Forums

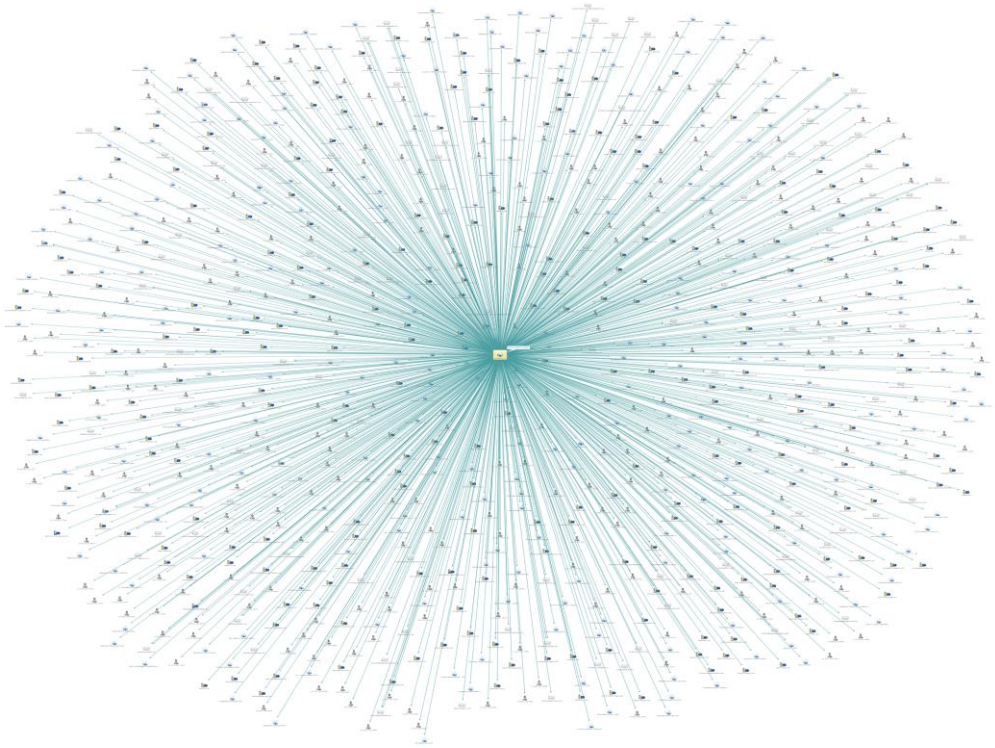
Newsletters & Annual Reports

After Hours Reception & Dial-By-Name Voicemail Systems

Business & DNS Registration Records

Business Networking Sites:

- LinkedIn
- Jigsaw
- Zoominfo



A Few Common Spearphish Scripts

- Security Patch
- Employee Wellness Program
- Employee Survey
- Fundraising Effort
- New System/Software
- Billing/Payables/ACH Action
- RFP/Business Opportunity
- Job Applicant
- Contest **Winner**
- Angry Customer
- Friendly Bank

General Phish Example: Craigslist Reference

you have received a voice message on_craigslist

Neal Evans <neal1032@gmx.com>

Sent: Sat 12/1/2018 3:04 PM

To: recruiting@infoatrisk.com

Hi,

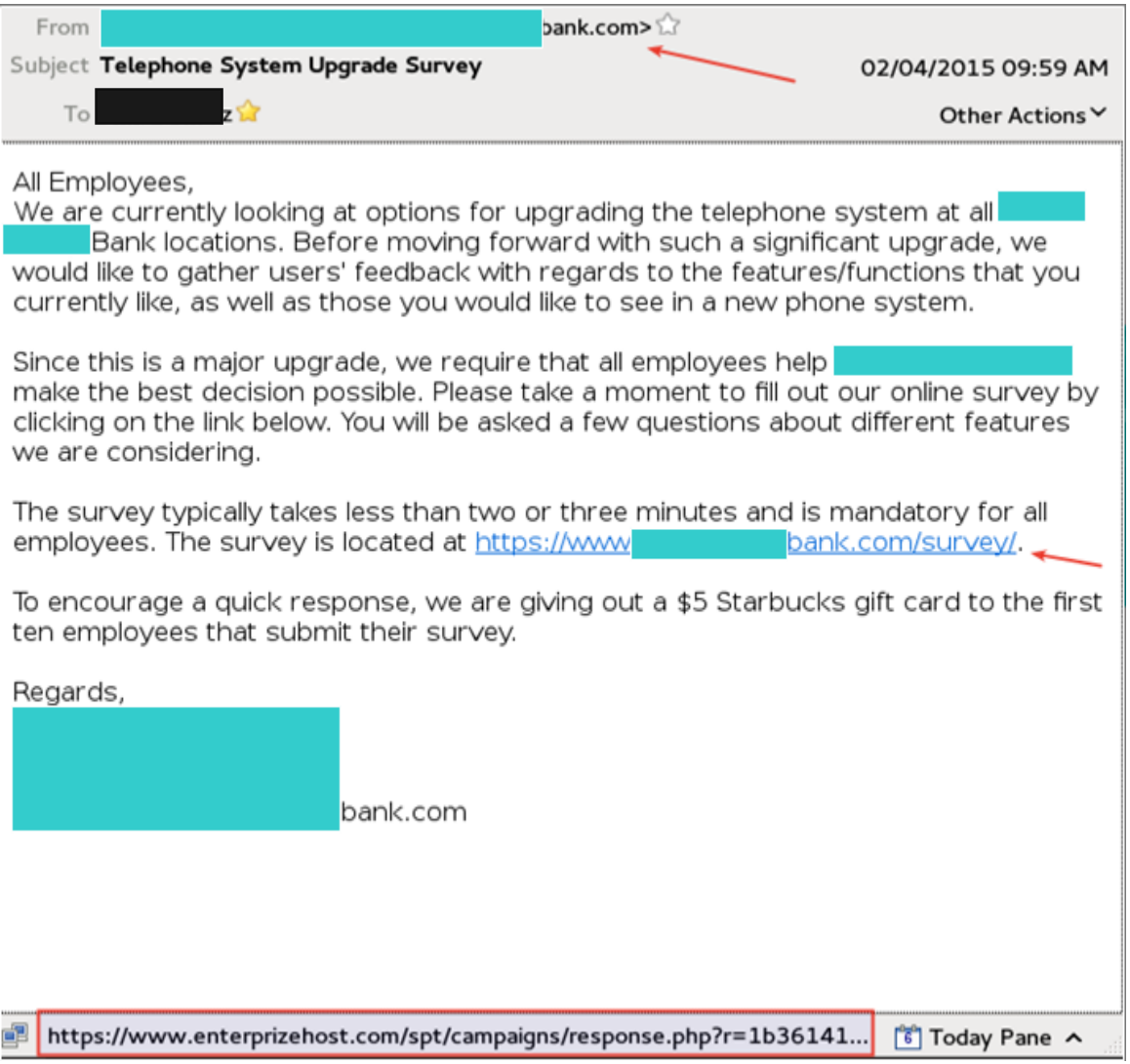
if your property is still for sale on_craigslist

click here to see my offers **My offers**

Thank you

to stop receiving emails: click here

Hallmarks of a Sophisticated Spearphish



- Sender name is *spoofed* to appear to have been sent by a co-worker
- Subject matter is topical
- Appears to contain a valid URL

(but note the lower dialog box showing the actual URL)

- Demands an activity that seems harmless
- Tempts the user with a promised gift card reward

Spearphish Example: Impersonating CEO

From: James Wallace <christiffany1999@gmail.com>
Sent: Thursday, July 4, 2019 9:33 AM
To: [redacted]@bpmcpa.com>
Subject: REQUEST

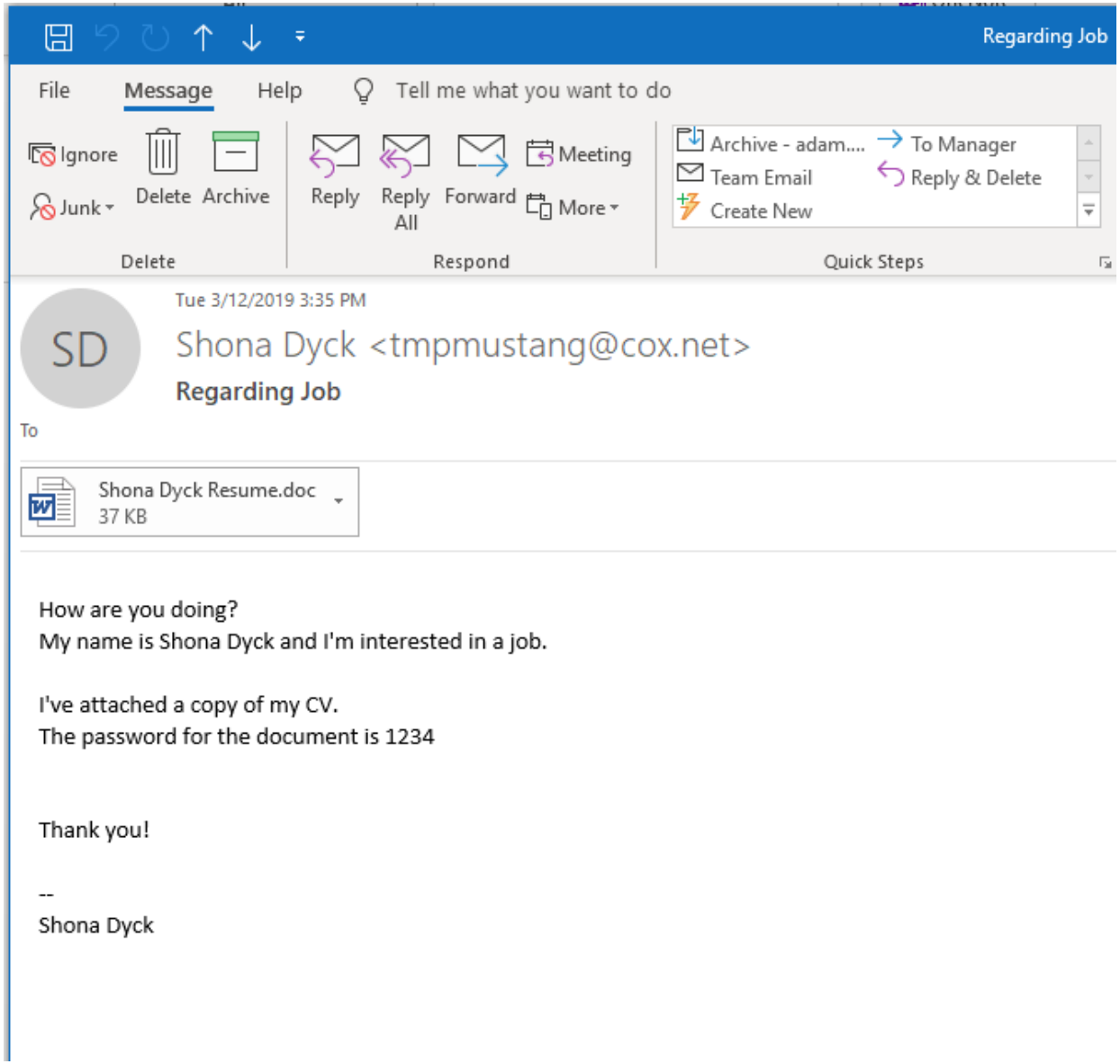
Have you got a minute? I need you to complete a task.

I am very busy can't talk right now. So just reply me back as soon as you can.

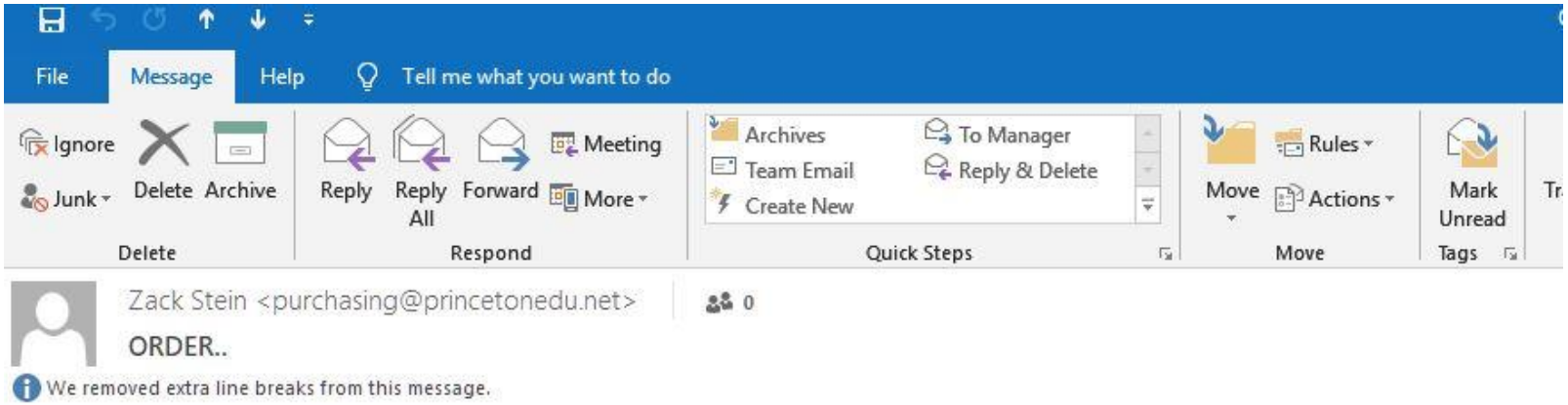
--

Sent From 4G Wireless Phone

Spearphish Example: Targeting HR



Spearphish Example: Targeting Tech Firms



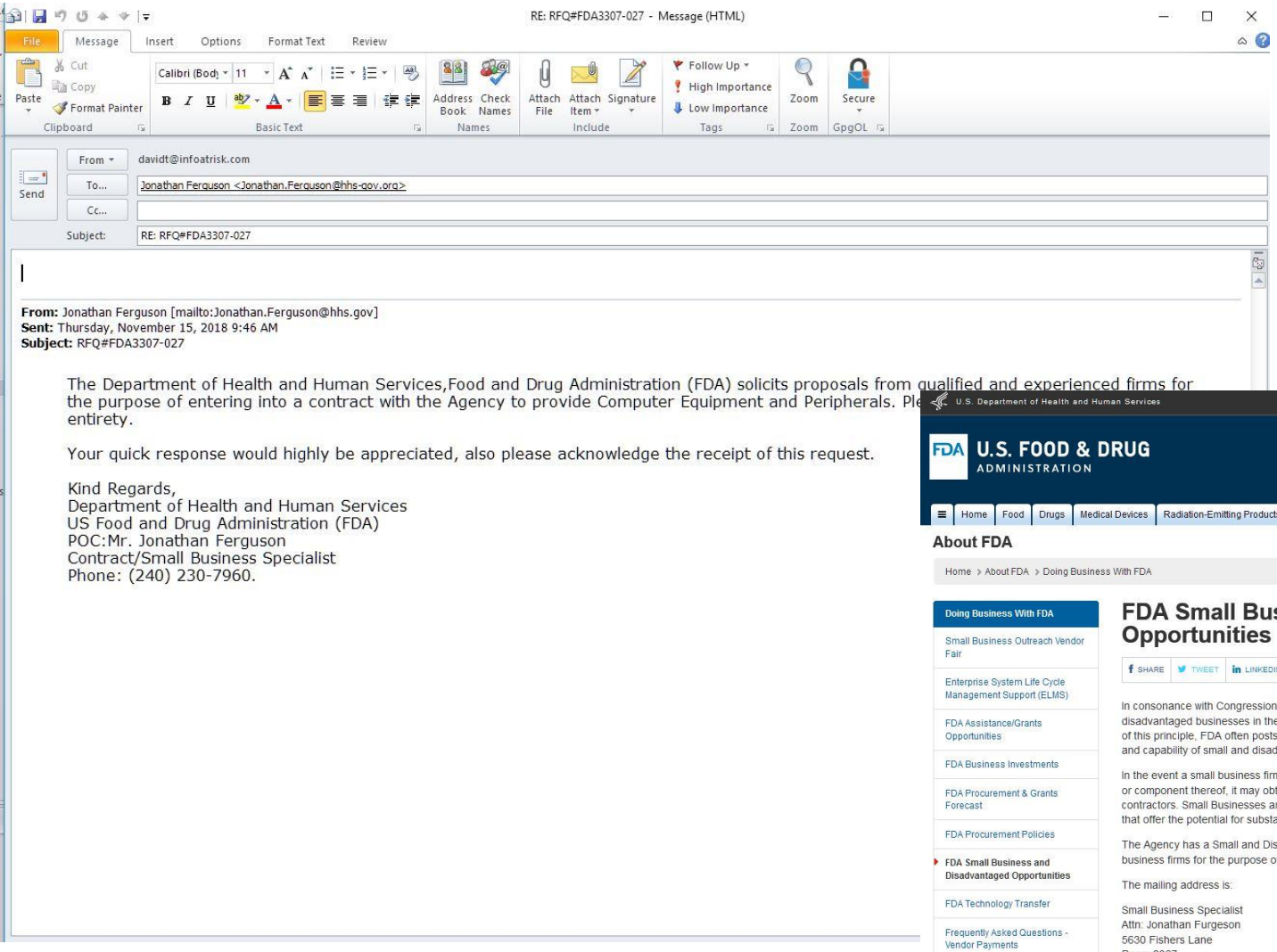
Dear sales,
Good morning from Princeton university can you please assist us with quote for below items

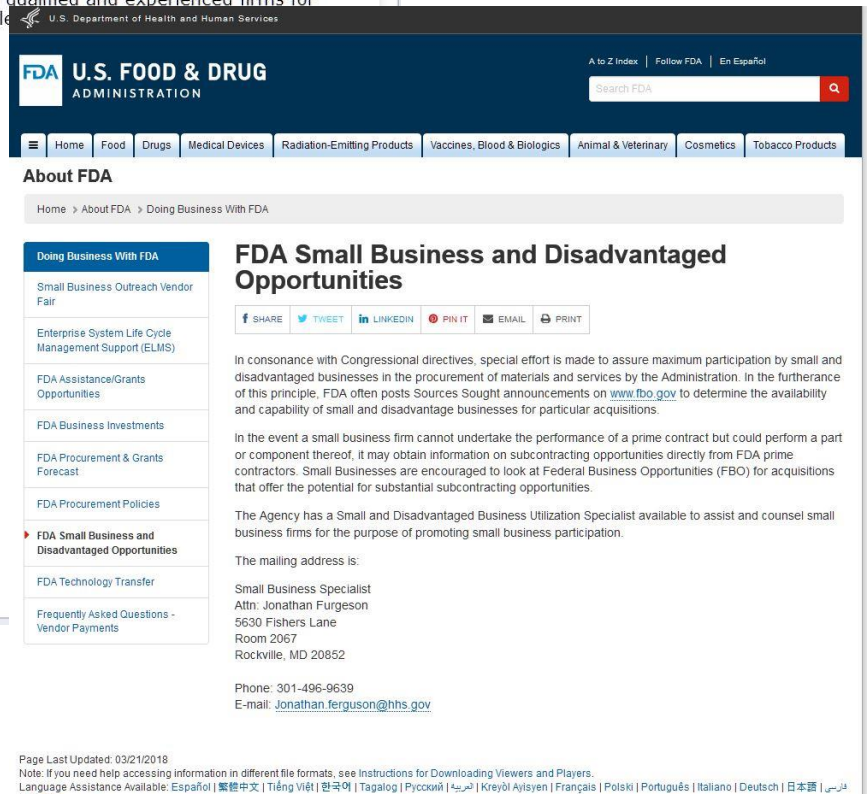
1. Fluke 754 Documenting Process Calibrator 2. STDR1000100 Seagate backup plus slim 1TB 3. HP CE341A: HP 651A Cyan Original

Payment terms: Net10 Days

Zack Stein
Title: Senior Buyer
Princeton University
Office of Finance & Treasury
701 Carnegie Center
Princeton, NJ 08540

Example: Targeting Tech Firms (Legit Official)





Spearphish Example: Targeting CPA Firms

Reply Reply All Forward

Thu 7/4/2019 11:07 AM

Nathan Wright <nathan@concretethewrightway.com>

Tax 2018: Personal Tax for Nathan

To

TaxPre Docs.pdf
40 KB

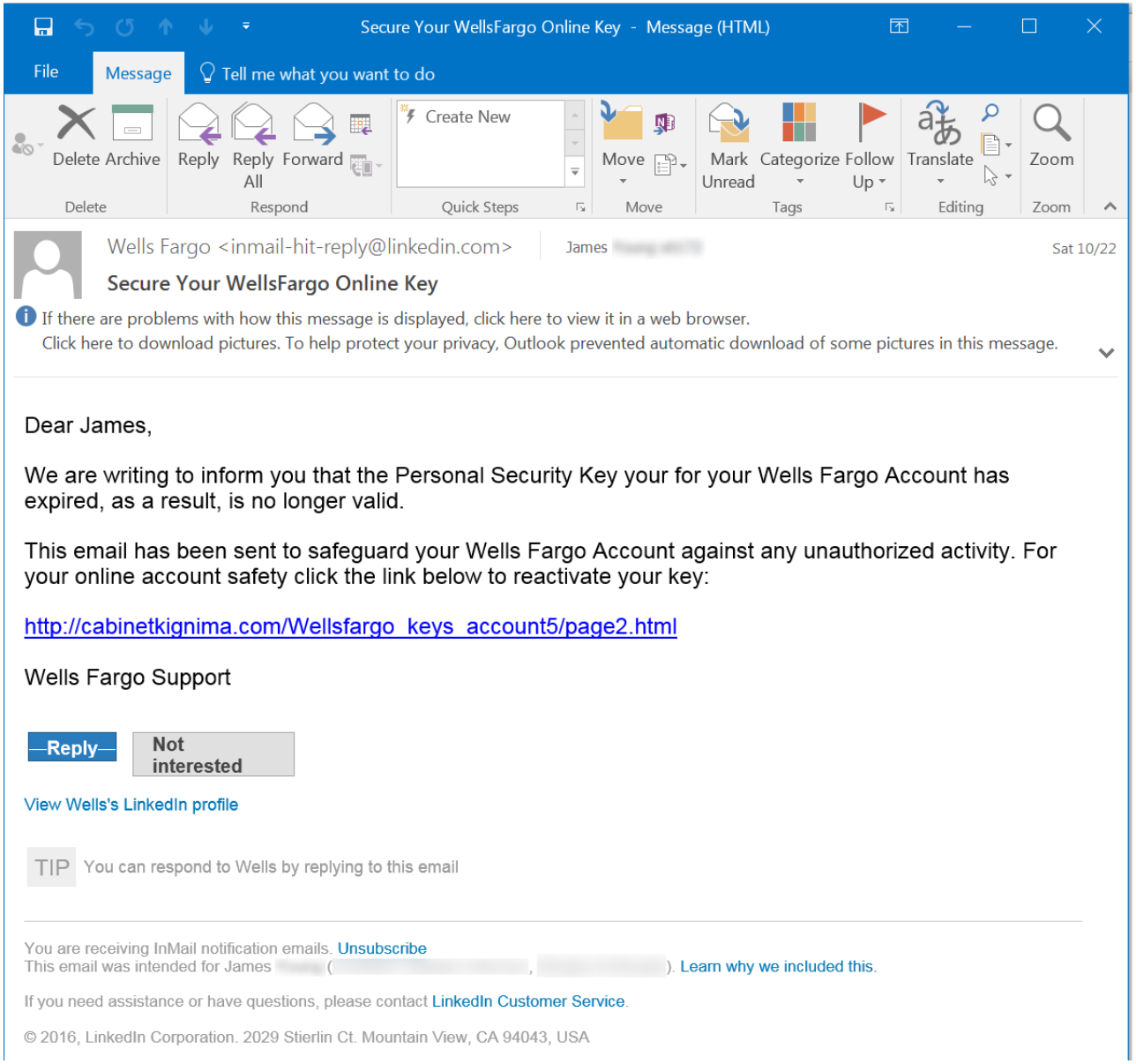
Hi

Attached are my Tax documents. Please prepare a Draft and let me know to contact.

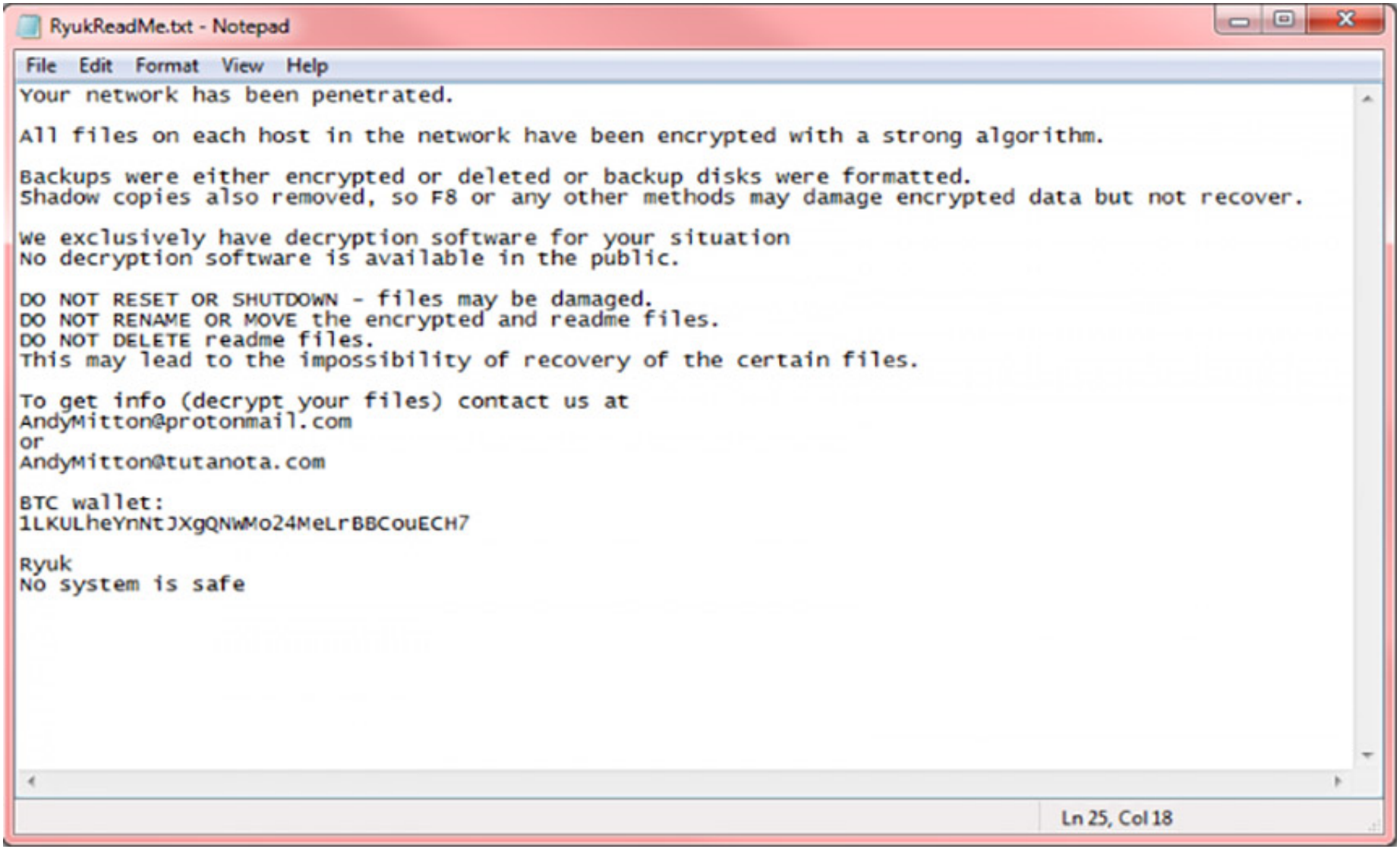
Sincerely.

Nathan Wright
President
203-303-7198
Construction & Maintenance Service Company

Spearphish Example: Friendly Bank



Typical Ransomware Message



Common Vishing (Voice Phishing) Scripts

Tried & True

- Impersonating Microsoft tech support
- Impersonating IRS, Law Enforcement, Social Security Administration, etc.

Latest & Greatest: Customers

- Impersonating bank fraud officer
  - *"Your account at ABC Bank is showing potentially fraudulent activity…"*
- Impersonating company rep, with spoofed callerID
  - *"Your (credit card, debit card, etc.) at Acme Company has been compromised…"*
- Impersonating complaints department, with spoofed callerID
  - *"I'm from the customer service department at Acme Company, and I'm calling about your recent Yelp review*

Latest & Greatest: Employees

- All Employees
  - Internal or third-party vendor tech support
- Human Resources
  - Submitting a "resume" with embedded malware
- Customer Service and/or Help Desk
  - Complaint
  - Emergency
- Accounting
  - Change of vendor payables address
  - Urgent payment/expense
    - AI aided C-Level voice "deep-fakes"

Vishing On The Rise

THE WALL STREET JOURNAL.

U.S. Edition ▾ | September 6, 2019 | Print Edition | Video

Home World U.S. Politics Economy Business Tech Markets Opinion Life & Arts Real Estate WSJ. Magazine

PRO CYBER NEWS

Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case

Scams using artificial intelligence are a new challenge for companies

By Catherine Stupp

Updated Aug. 30, 2019 12:52 pm ET

BBC Sign in | News | Sport | Reel | Worklife | Travel | Future

NEWS

Home | Video | World | US & Canada | UK | Business | Tech | Science | Stories

England | Local News | Regions | Sheffield & South Yorkshire

Phone bank scam: Ex-police officer tricked out of £15,000

8 October 2019 Share

CRIME

Deputies: Don't wire money to scammers who claim they've kidnapped your daughter

The Placer County Sheriff's Office is warning about phone calls where the perpetrator tells the victim they've kidnapped their daughter.

Author: Allison Sylte

Published: 3:03 PM PDT October 11, 2019

Updated: 3:03 PM PDT October 11, 2019

Digital Assistant and Chat Vishing/Smishing

WhatsApp vulnerability exploited through malicious GIFs to hijack chat sessions

Personal files and messages are at risk in unpatched builds of the app.

By Charlie Osborne for Zero Day | October 3, 2019 -- 10:45 GMT (03:45 PDT) | Topic: Security

Using a steganographic attack (malware embedded in an image/video), chat sessions, files and messages are disclosed

Researchers expose how Amazon Echo and Google Home can steal passwords

Security researchers unveil a new vulnerability in smart home speakers.

Asivechowdhury/Wikimedia (CC-BY-SA)

Mikael Thalen— 2019-10-22 02:47 pm

After hackers have commandeered the device, the user hears:

"Your device needs to be updated, please confirm your password for the update"

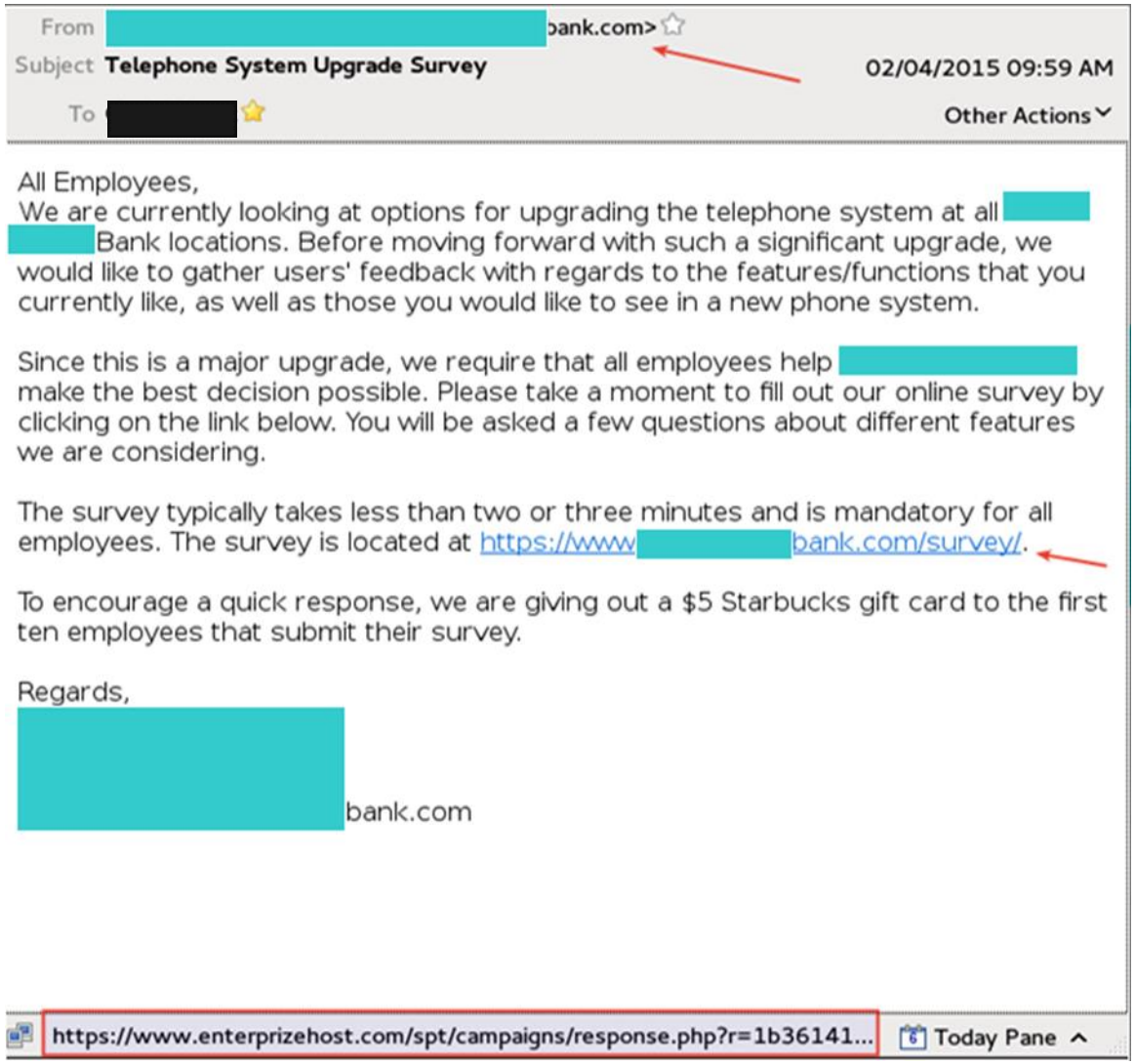
How to Avoid Becoming the Next Phish Victim

General Social Engineering Warning Signs

- Requests anything out-of-the-ordinary
  - Offer to help with problem you didn't know you had
  - Offer that sounds too good to be true
- Name-drops, claims of authority, or urgency
  - Cavalier attitude
- Compliments, flatters, or flirts
- Promises reward or threats for non-compliance
- Refuses or gets uncomfortable when asked to provide supporting information

Everyone is the Security Officer

Identifying Phish Emails



Hit “Reply” and check if the recipient’s name is the same as the (alleged) sender’s name

If the topic is unusual, beware

If it offers something for nothing, or otherwise sounds too good to be true…it probably is

If it asks you to provide anything, think twice before complying (especially credentials)

Hover over Links/URLs to ensure they’re going to where they are purported to leaded

Check signature blocks for consistency

Beware of attachments!

Business Email System Controls

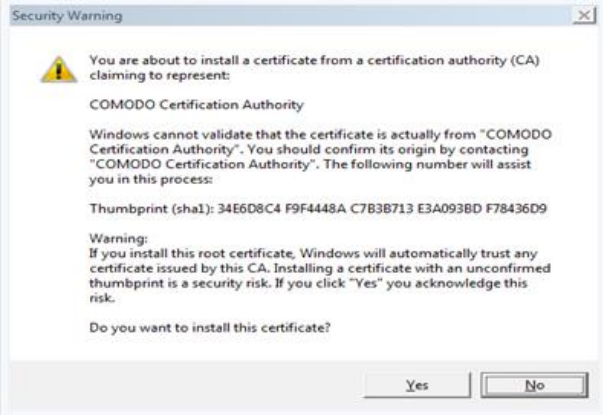
- Prohibit email address enumeration
- Prohibit email address spoofing
- Prohibit malicious attachments
  - See tools like Mimecast or Barracuda
  - Disable macros in Word and Excel
- Prohibit malicious links
  - See tools like Mimecast or Barracuda
  - Disable scripting for browsers

Safe Computing with Email

- If you must use email for sensitive data, use encryption tools
  - PGP
  - Zixmail
- For personal email, consider encrypted email apps
  - Hushmail
  - Protonmail
- Sanitize the contents of your inbox, sent, trash, etc.
- Use multi-factor authentication (MFA) for webmail access
- Password protect attachments
  - Deliver the password via a separate communications medium
- Better yet, don’t use email for sensitive information
  - Consider a secure document exchange service (with MFA)
    - Dropbox
    - Box

Vishing & Smishing Defenses

- Keep your phone, and message apps, patched/updated
- Disable scripting on smartphone browsers
  - Be suspicious of all pop ups and dialog boxes
  - Consider a popup blocker
- Don’t trust callerID
  - Hang up and call back at a known good number
  - You can’t even trust voice recognition



A common online banking attack toolkit asks the user to install a malicious root certificate

CPE Credit Rules

- You will be receiving an email from Joel Segovia shortly.

  Hit "reply" to make sure it's from him before proceeding to survey monkey

- This email contains a link to the Survey Monkey survey.

- Please fill it out with all of your code words in the order they were given.

- Remember, the expectation is that you complete it right away, as the survey will close half-an-hour after the end of today's class. No CPE will be granted after this time.

A recording of this presentation will be sent to all attendees

Conclusion

Social engineering is effective because of humans' "assumption of truth"

Social engineering is impactful because humans have privileges to access sensitive systems & data

Phishing is the most common, and successful, social engineering attack vector

- Impacts include bitcoin mining, ransomware, or worse

Identifying phish attacks requires constant vigilance

Thank You

Questions or Comments?