"Don't Be Phooled!": What You Need to Know about Phishing

Session 51, February 12, 2019

Lee Kim, JD, CISSP, CIPP/US, FHIMSS

Director of Privacy and Security, HIMSS

Conflict of Interest

Lee Kim, JD, CISSP, CIPP/US, FHIMSS

Has no real or apparent conflicts of interest to report.

Agenda

- Introduction
  - Phishing and Phishers
  - Phishing by Design
- Phishing examples (actual samples—redacted)
- Psychology of Phishing
  - Attacker Perspective
  - Victim Perspective
- Anatomy of a Phishing Attack
- New phishing techniques
- Mitigating Phishing
- Security awareness tips

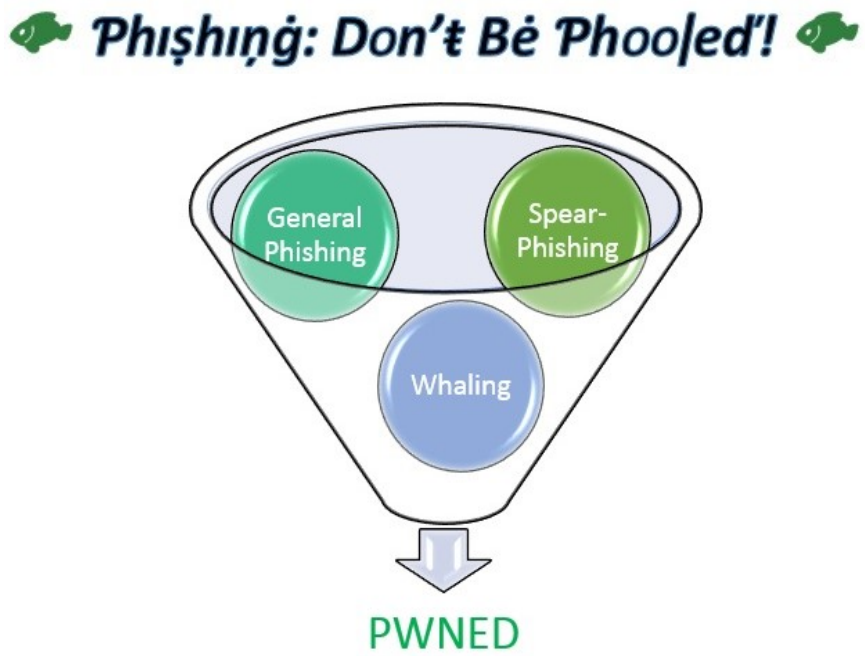
Learning Objectives

- Explain the psychology of phishing attacks from the attackers' and victims' perspectives
- Illustrate the anatomy of a phishing attack from the attacker's perspective, including the tools and tactics that are used
- Discuss new phishing attacks and how spear-phishing has evolved with artificial intelligence and good old fashioned reconnaissance
- Recognize advanced targeted phishing attacks such as spear-phishing
- Discuss mitigation techniques to mitigate the phishing threat

Why Should We Care?

- Phishing e-mails are the most typical initial point of compromise for significant security incidents at healthcare organizations.
- Online scam artists responsible for phishing & spear-phishing are the #1 identified threat actor for significant security incidents.
- 58 percent of healthcare organizations conduct phishing tests, but the remaining 42 percent either do not test or do not know.
  - A large portion of the organizations that do not test are non-acute care organizations.
- The phishing click rate is 10 percent or less for healthcare organizations.
- Phishing is a significant problem for healthcare organizations and others.
- In essence, phishing exploits the human and is an effective attack vector.

Introduction: US DHS AEP paper



01011001 01001111 01010101 00100000 01001000 01000001
01010110 01000101 00100000 01000010 01000101 01000101
01001110 00100000 01010000 01010111 01001110 01000101
01000100 00100001

Introduction: US DHS AEP paper

- Links to 2018 US Department of Homeland Security Analytic Exchange Program paper and tip sheet:
  - https://www.dhs.gov/sites/default/files/publications/2018_AEP_Vulnerabilities_of_Healthcare_IT_Systems.pdf
  - https://www.himss.org/library/phishing-dont-be-phooled
- Authored by the Vulnerabilities of Healthcare Information Technology Systems Team (AEP team)
- Unclassified paper and tip sheet with no caveats (may be freely shared)
- Product of a public-private partnership

Phishing and Phishers

- Findings from the 2018 HIMSS Cybersecurity Survey:
  - Most recent significant security incidents by online scam artists conducting phishing & spear-phishing attacks
  - Initial point of compromise is most often a phishing email
- Phishing is not just a healthcare problem, it's a societal problem
  - Top threat for all sectors (academia, government, industry) and individuals
- Everyone has heard of phishing, but phishers are still successful at getting in with about an average 10% click rate in healthcare.
  - Why?
    - Poor detection rate (human + tech)
    - Hard to detect: 'Phooled'! [The letters "p", "o", "l", and "d" are not standard characters.] (homoglyph attacks)
    - Trickery and deceit

Phishing by Design

- General Phishing
  - May not target specific individuals (untargeted)
  - May originate from a well-known company, agency, university, or individual
  - Very prevalent
  - Poor grammar, spelling, and “too good to be true” claims
  - Often elicits sensitive information or may contain a malicious link or attachment
  - Often large volume; attackers cast a wide net
    - Unfortunately, some recipients may take the bait (it’s all in the numbers)

Phishing by Design

- Spear-phishing
  - Cost effective, fast, and inexpensive (and effective!)
    - Thus, we are seeing a greater volume and higher velocity of spear-phishing attempts (and attacks)
  - Intel collection & analysis may be automated with AI
    - Social media
    - Websites
    - Personal and business web pages and social media accounts, message boards, etc.
      - Examples: current and past projects, business associates and vendors, colleagues and friends, etc.
  - But, bad intelligence = bad results (more likely a recipient may detect that it's fake)

Phishing by Design

- Whaling
  - Targets: C-suite executive (CFO, CEO, or other CxO), celebrities, politicians
  - (Note: Some also use the term “whaling” to mean that an attacker is masquerading as a high-powered individual)
  - Examples:
    - Trick or deceive the C-suite executive:
      - Divulge bank account information, employee information, corporate financial information
      - Transfer funds to an account that is controlled by the attacker

Example of General Phishing

Tue 3/7/2017 9:20 AM

USPS <usps@uspsdelivery.com>

SPAM Shipment status change notification for parcel #61621750

To Sheri

Your package could not be delivered by our courrier because no person was present at your address.
Your signature is required to successfully deliver the parcel.

Shipping service: Next Day Air
Box size: Large
Date : Mar 7th 2017

A new delivery can be scheduled, by calling the number on the delivery notice we left at your address. You need to confirm the shipping information, including the address and tracking number, wich can be found on the notice.

An electronic copy of the delivery notice can be viewed online on the USPS website:
https://tools.usps.com/web/pages/view.invoice?
id=61621750&dest=s[redacted]@[redacted]com

The shipment will be cancelled and the package returned to the sender if a new delivery is not scheduled within 24 hours.

Thanks for shipping with USPS

Example of Spear-Phishing

From: Betty W Doyle <
Date: September 11, 2017 at 11:13:06 AM EDT
To:
Subject: 1757064939:90

This email has been automatically generated and sent to you because BBB has got a complaint, claiming that your company is violating the Fair Labor Standards Act.

You can download the text file with the explanation of abuse by following the link https://bit.ly/2jhnSC8

We also request that you send a response within 48 hours to us. This response should contain information about what you plan to do with it.

Important notice:
When replying to us, leave the compliant ID "1757064939:90" unchanged in the subject .

Better Business Bureau
Abuse Department
Betty W Doyle

Examples of Spear-Phishing

accounting@ <
Tue 12/6/2016 7:27 AM

To: Technical Support;

Sure , it's done. Where do i send it?

On Mon, Nov 23, 2016 at 1:19 PM, support@[redacted].com wrote:
Can you print this insurance for me ? my printer isn't working
Health Insurance # 413660

http://baoonhd.vn/api/get.php?id=c3VwcG9ydEBib3N0b25wYWluY2FyZS5jb20N

Examples of Whaling

From: Steve [mailto:
Sent: Thursday, February 1, 2018 1:14 PM
To: Mike
Subject: [No Subject]

Michael,

Are you in the office?

Steve

On February 1, 2018 at 1:15 PM Mike <> wrote:

Yes if you want to call

Michael

Controller

Examples of Whaling

Today

Steven [redacted] | [redacted]@[redacted].com]

Sent: Tuesday, June 09, 2015 1:07 PM

To: Mike [redacted]

Michael,

How soon can you process a domestic wire transfer? I need a transaction taken care of.

Thanks,

Steven [redacted]

Examples of Whaling

Thu 3/16/2017 7:51 AM

Vincent [redacted]

RE: divorce papers

To Mike [redacted]

The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

My name is Vincent and I am a senior partner at LLP.
Your spouse has contracted me to prepare the divorce papers.
Here is the first draft , please contact me as soon as possible:

http://www. [redacted] -law.com/papers/divorce [redacted] doc

Thank you

Senior Partner

Phone: [redacted]
Fax: [redacted]

Psychology of Phishing

- Attacker perspective
  - Exploit the weaknesses in decision making and human behavior of the recipient(s)
  - Characteristics of message:
    - Sense of urgency (e.g., respond now)
    - Persuasive and/or polite statements
    - May prey on recipient's fear(s) (e.g., current events, user account restrictions, job loss, etc.)
    - May be psychologically manipulative or exploit emotions of the recipient
    - May contain "insider" knowledge (e.g., job functions, work relationships, current projects, etc.)
  - Deceit and trickery is key (e.g., below threshold of average human perception)

Psychology of Phishing

- Victim's perspective
  - Victim may comply with request that appears to come from an authority figure
  - Victim's decision making may be influenced by authority, time pressure, and tone of message
  - Victim may be deceived into thinking that the message comes from a trusted source (e.g., corporate logo and name)
  - No matter how savvy you are, you can be a victim
    - Some individuals are more susceptible than others
- Who is more susceptible to phishing?
  - Individuals who:
    - Have a strong commitment to the organization
    - Exhibit agreeableness
    - Obey the chain of command

Anatomy of a Phishing Attack

1. Identify the target
    a. Who to target? What to target? E-mail addresses? Harvested? Purchased lists from third parties?
2. Craft the message
    a. Message content designed so victim takes some action (e.g., open an attachment, click on malicious links, respond to message)
    b. General phishing message: one size fits all
    c. Spear-phishing or whaling message: tailor it to the victim
    d. Generate malicious payload (as applicable)
3. Deliver the message
    a. Send the message to the victim; the sender often has a spoofed email address

Anatomy of a Phishing Attack

4. Deception of the victim
    a. Recipient of the delivered message is deceived into taking the intended action or providing the desired information
5. Action or disclosure by victim
    a. Victim performs the intended action or provides the information
6. Action by attacker
    a. Attacker uses collected information or the result of the victim's action for his or her end (e.g., financial or otherwise)

New Phishing Techniques

- Hijacking of email threads with attacker masquerading as a trusted colleague, friend, or family member
  - You may be tricked into opening a malicious attachment (you may be less wary, thinking that you are communication with someone you know)
- "Lookalike" domain names [phishing websites may have these phony names]
  - Typejacking attack: www.examp1e.com
  - Homograph attack: www.dịsh.com
- Dynamic data exchange (DDE) attacks
  - Malicious calendar invites (may result in code execution if a victim opens or cancels an invite)

New Phishing Techniques

- Artificial intelligence enabled spear-phishing attacks
  - Fully automated spear-phishing system that creates tailored tweets based on user's interests (high click rate, according to researchers)
  - Fully automated spear-phishing system that includes automatic construction and communication of a spear-phishing message tailored to the victim with information that is unique to the individual

Mitigating Phishing Attacks

- Increase your situational awareness
- “Study up” on the latest phishing techniques
- Participate in information sharing with colleagues
- “Test” your workforce on the ability to detect phishing attempts (simulated phishing)
- Keep metrics re: phishing “click rate”
  - See what is working & not working
  - Set a goal; give it “teeth”
- Implement basic and advanced security controls (defense in depth with human & technical controls)
  - Evolve both human and technical controls (nothing stays the same, including with phishing)
- Reward good behavior and novel ways at anti-phishing defense

Security Awareness Tips

- Provide security awareness training of your workforce with greater frequency (once a year training is the norm in healthcare!)
- Provide regular tips to the workforce on combatting phishing
- Raise the collective phishing IQ of everyone (not just IT)
  - Provide education & training
  - Adopt awareness initiatives: Data Privacy Day, National Cyber Security Awareness Month
- Train workers to be suspicious (look for mistakes or discrepancies in messages, watch out for **o**dd letters, etc.)
- Train workers to be cautious (especially for messages that ask for personal, confidential, proprietary, or sensitive information)
- Train workers to trust their instincts and common sense
- Verify suspicious emails with the sender (via out of band communication)
- Never click links unless you are sure where they lead

Questions

Lee Kim, JD, CISSP, CIPP/US, FHIMSS

lkim [at] himss [dot] org

https://www.linkedin.com/in/leekim

@lkimcissp [Twitter]