Conducting an Email Phishing Campaign

WMISACA/Lansing IIA Joint Seminar
May 26, 2016

William J. Papanikolas, CISA, CFSA
Sparrow Health System
Estimated cost of cybercrime to the world economy in 2015 was $450 billion dollars
90 -95% of all successful cyber-attacks begin with a phishing email
Estimates indicate that around 156 million emails are sent each day
  ➢ 16 million make it through the filters
  ➢ 800,000 of them are not only opened, but the phishing links are clicked
  ➢ Estimates indicate that those who clicked the links, 80,000 share compromising information
Each quarter 250,000 new phishing URL’s are identified

The information above is from the KnowBe4 Whitepaper – The Phishing Breakthrough Point
Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

Phishing emails may contain links to websites that are infected with malware.

Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies.
Hello!
As part of our security measures, we regularly screen activity in the Facebook system. We recently contacted you after noticing an issue on your account.

Our system detected unusual Copyrights activity linked to your Facebook account, please follow the link below to fill the Copyright Law form:

http://www.facebook.com/application_form

Note: If you don't fill the application your account will be permanently blocked.

Regards,

Facebook Copyrights Department.
What to Look for in a Potential Phishing Email

- **Spelling and bad grammar.** Cybercriminals are not known for their grammar and spelling. Professional companies or organizations usually have a staff of copy editors that will not allow a mass email like this to go out to its users. If you notice mistakes in an email, it might be a scam.

- **Beware of links in email.** If you see a link in a suspicious email message, don't click on it. Rest your mouse (but don't click) on the link to see if the address matches the link that was typed in the message. In the example below the link reveals the real web address, as shown in the box with the yellow background. The string of cryptic numbers looks nothing like the company's web address. Links might also lead you to .exe files. These kinds of file are known to spread malicious software.

```
https://www.woodgrovebank.com/loginscript/user2.jsp

```
- **Threats.** Have you ever received a threat that your account would be closed if you didn't respond to an email message? The email message shown above is an example of the same trick. Cybercriminals often use threats that your security has been compromised.

- **Spoofing popular websites or companies.** Scam artists use graphics in email that appear to be connected to legitimate websites but actually take you to phony scam sites or legitimate-looking pop-up windows.

- Cybercriminals also use web addresses that resemble the names of well-known companies but are slightly altered.
• **Phishing** - An attempt to acquire information such as user names, **passwords**, and credit card details by masquerading as a trustworthy entity in an **electronic communication**

• **Spear Phishing** - Attempts directed at specific individuals or companies. Attackers may gather personal information about their target to increase their probability of success. This technique is, by far, the most successful on the internet today, accounting for 91% of attacks.

• **Clone Phishing** - A type of phishing attack whereby a legitimate, and previously delivered, email containing an attachment or link has had its content and recipient address(es) taken and used to create an almost identical or cloned email. The attachment or link within the email is replaced with a malicious version and then sent from an email address spoofed to appear to come from the original sender.
Types of Phishing

• **Whaling** - Several recent phishing attacks have been directed specifically at senior executives and other high profile targets within businesses, and the term *whaling* has been coined for these kinds of attacks. In the case of whaling, the masquerading web page/email will take a more serious executive-level form. The content will be crafted to target an upper manager and the person’s role in the company. The content of a whaling attack email is often written as a legal subpoena, customer complaint, or executive issue. Whaling scam emails are designed to masquerade as a critical business email, sent from a legitimate business authority. The content is meant to be tailored for upper management, and usually involves some kind of falsified company-wide concern. Whaling phishermen have also forged official-looking FBI subpoena emails, and claimed that the manager needs to click a link and install special software to view the subpoena.
• A malicious attachment can install spyware or malware on the user’s computer. These attacks can be designed to steal information such as passwords, usernames, credit card numbers or other sensitive information entered into website or store on the user’s hard drive. The malware could also be used as a launching point for attackers to infiltrate your network
• A malicious link, if clicked, could lead to many different types of attacks on a user. The resulting web page link could leverage browser exploits to install spyware or malware on the user’s system. These exploits could easily be used as launching points for attackers to infiltrate your network and possibly compromise your security.
• Users may be prompted for their username and password on a site that may closely resemble their own. If the user enters their credentials on this site, an attacker may be able to use them to log into externally facing VPN or Remote Desktop servers.
• Negative publicity, leading to both long and short term loss of corporate reputation.
• Direct IT costs to locate the source of data loss.
• Breaching both regulatory and legal requirements, such as the Sarbanes-Oxley Act, and state breach notification laws that exist in 17 U.S. states.
To reduce the threat of spear phishing, security awareness and training to all employees is key.

Through the use of training memos, in-person demos and awareness campaigns, ensure the leaders of your organization know the risks of falling for a phishing attack, as well as the signs of an attack in process. Inform them to never click on a link in an email, chat session, blog or other medium. Eliminating this one action severely reduces the success of a spear phishing attack. They should also be instructed to be careful of unsolicited messages, especially ones containing public information about them. Teach them the risks, as well as how to prevent phishing attacks.

Ensure all antivirus, antimalware, personal firewalls and browser antiphishing controls are in place and up to date.

A combination of phishing-aware users and a comprehensive technical strategy reduces the chance of a successful phishing attempt.
• **Primary Objective** – Evaluate the level of risk that phishing poses to your organization as it relates to your organization’s security awareness.

• **Specific Objectives:**
  • Conduct a round of an email phishing attack against a defined set of employees
  • Test employee response and email policy adherence
  • Identify areas of weakness as it relates to your employees’ ability to identify phishing emails.
  • Create reporting that provides a summary of the employee responses to phishing emails and potential impacts.
• Create and host a phishing site that has the same look and feel of your organization’s site.
• Purchase a plausibly named domain.
• Create an email message (campaign) that instructs the employee to follow a link to the external domain.
• Determine what emails (blast or targeted) that will be used in the assessment.
• Send the phishing emails to all selected email addresses.
• Track the activity of the users that interact with the email and visit the phishing site.
• Conduct an assessment using resources in your organization
• Contract with a vendor to perform the Email Phishing Assessment
Develop a campaign that will have the same look and feel as a legitimate organization email.

Campaign examples include:

Example #1
In order to protect employee data, your organization is furthering security initiatives by conducting a brief information security survey to ensure employee awareness of our current security policies and best practices. Feedback will be gathered via a web-based survey to confirm the importance of each operational area's information systems, data, and business processes (i.e., information assets). We will use this feedback to ensure that we are applying appropriate controls to help protect these assets.

Each person who completes the survey will be entered in a drawing to win a $50 gift card.

Please complete the brief survey located at the following link:
<href=link_to_phishing_site>

The survey should take less than five minutes to complete, and your feedback will remain anonymous.

Thank you for your assistance in this important matter.
Example #2
This is an automated message from the Human Resources Department to inform you that a pending harassment complaint. Please click the following link to log in and view the details:
<href=link_to_phishing_site>

Example #3
Marketing is conducting a brief survey to determine the effectiveness of our communication programs. Feedback will be gathered via a web-based survey. We will use this feedback to ensure that we are addressing all Caregiver communication requirements.
Each person who completes the survey will be entered in a drawing to win a $50 gift card.
Please complete the brief survey located at the following link:
<href=link_to_phishing_site>
The survey should take less than five minutes to complete, and your feedback will remain anonymous.
Thank you for your assistance in this important matter.
• Email Blast – Send phishing emails to all employees in the organization.
• Targeted – Send phishing emails to employees in the following departments:
  • Executive Management
  • Finance (Accounting, Accounts Payable and Payroll)
  • Human Resources
  • IT Administrators
  • Supply Chain
  • Other departments that have access to the organization’s assets
• Frequency
  • “Blast” to all employees in the same time frame (1 – 2 hours) depending on the size of the population.
  • Staggered – to all employees or targeted employees over the course of a week or month. This potentially eliminates employees tipping-off other employees of the campaign.

Scope of the Email Phishing Assessment
Conducting an Email Phishing Campaign
Key metrics tracked during an email phishing attack include:

- Users who opened the email.
- Users who clicked on a link within the email.
- Users who entered credentials on the phishing site.
- Users who ran the malicious payload delivered via the phishing site.
- Users who completed the information described by the campaign.
• The phishing email is sent to the selected employees (either blast or staggered).
• The employee may or may not open the email. If the email is opened they will see the campaign message and be asked to click on a link to continue to process.
• If the employee clicks the link that will be taken to a website where they will be asked to entered their credentials (Username and Password).
• After entering their credentials they will be asked to click a “submit” button that will load the payload.
• The payload will display a screen that will ask for information specific to the campaign, the employee will enter the information and click “submit”.
• phising attempt, but a fake phishing attempt as a educational tool. The message will also include educational information regarding phishing.
• After clicking submit the employee will receive a message indicating they have been “phished”. The message will indicate that this was not a real phishing attempt, but a fake phishing attempt as an educational tool. The message will also include educational information regarding phishing.
An Email Phishing Summary Report should be created showing the following metrics:

- Users who opened the email.
- Users who clicked on a link within the email.
- Users who entered credentials on the phishing site.
- Users who ran the malicious payload delivered via the phishing site.
- Users who completed the information described by the campaign.
• Continual Awareness Training is key to mitigating email phishing attempts.
• Continual email phishing assessments on who is clicking what and when can effectively indicate patterns of phishing vulnerabilities within an organization.
• Clear communication with employees regarding IT update or HR processes can play a vital role in preventing misunderstandings and blocking phishing attempts based on generic organization email themes.
“The adage is true that the security systems have to win every time, the attacker only has to win once.”

- Dustin Dykes, CISSP
  Founder Wirefall Consulting
Conducting an Email Phishing Campaign