Enhancing Cybersecurity Awareness Training: A Comprehensive Phishing Exercise Approach

Michael J. A. Miranda

Division of Business Administration, University of Hawai'i at West O'ahu, HI
Email: mmirand1@hawaii.edu

[Abstract] Email communications is a critical service in nearly every aspect of business and personal activities. A person's email address is the online identity most relied upon for reliable and accountable communications. Banking, health and recreational activities conducted online in most cases depend on a person possessing and actively maintaining an email address. Unfortunately, email inherently possesses security shortcomings that enable malicious actors to commit fraud through phishing emails. Technology solutions do not entirely solve this issue, and the users themselves require training on how to identify and respond to suspected phishing emails. A structured and comprehensive phishing exercise training program can (1) reduce the probability of a cybersecurity compromise originating from fraudulent emails and (2) improve the overall cybersecurity posture.

[Keywords] cybersecurity, information security, email, phishing, social engineering

Introduction

Malicious actors successfully breach cybersecurity by tricking a person into providing the malicious actor unauthorized access to information, services and information technology infrastructure. By focusing on people and using techniques of social engineering, malicious actors can bypass the sophisticated and expensive cybersecurity technology implemented by businesses. The most widely used technique is sending fraudulent email to users that compel the user to take actions that lead to a compromise in cybersecurity. Generally, this technique is known as "phishing."

At 47 years old, email continues to play an essential role in online communications (Swatman, 2015). There were 3.7 billion email users in 2017 and will grow to 4.1 billion users by the year 2021 (The Radicati Group, Inc. [Radicati], 2017) despite the increased availability of additional collaboration and communication options, including chat, messaging, conferencing and workflow-based messaging (e.g., Slack[1], Microsoft Teams[2], Google Hangouts[3]). From a malicious actor's perspective, this user base is an attractive target that is relatively inexpensive to attack and easy to obfuscate the malicious actor's true identity. Although these new services have replaced, and improved workflows previously conducted by email, they have not replaced email as a means of reliable communication. To use many of these services, an email account is required as one's primary identity and means of communication with the service provider. Important notices about the service, billing statements, authentication verifications, and other relevant information are still transmitted to users by email. Therefore, email services will continue to be an authoritative means of business communications for many years to come (Radicati, 2017).

Email Remains Central to Our Digital Lives

Modern information technology (IT) applications and services are built to be accessed from anywhere and from nearly any platform (e.g., desktop, mobile, web) with users' email central to administration, including managing a user's authentication credentials. Application developers routinely provide support

[1] https://slack.com/
[2] https://products.office.com/en-us/microsoft-teams/group-chat -software
[3] https://hangouts.google.com/

for the major operating systems (Microsoft Windows, Apple macOS, Apple iOS, Google Android, Google Chrome and Linux) through native applications and web browser applications to reach as many users as possible to enable access from anywhere. For example, one can access the Gmail email service or Salesforce web application from nearly anywhere in the world and from any device.[4]

In this modern world where services can be bought and sold online without face-to-face or voice communications, credentials to those services are initially provisioned and managed through email. Signing up for a service online usually requires an email account as the primary username. If you forget your login or password to that service and need it to reset, email is usually the primary means of initiating a password reset. Also, critical notifications about the service, changes in the service agreement and other contractually binding agreements regarding digital services are commonly delivered and agreed to via email. Email remains a critical service that users (especially business users) regularly use and trust to conduct official business activity because:

- Most modern IT services exclusively rely on email to officially communicate with customers;
- Credential provisioning and management usually requires an email account as part of the process;
- Email is the most convenient method of aggregating communications with multiple services into a single identity;
- The barriers and overall cost to send and receive emails is very low, if not free; and
- An email address is perceived synonymously with a person's online identity.

These features of email that make them essential to businesses are the same reasons email is an attractive attack vector and target for malicious actors operating on the Internet. Email is the frontline where businesses and users need to defend themselves against malicious actors attempting to steal information, obtain access credentials and compromise infrastructure. If phishing results in stealing credentials, it is 400 times more likely that the victim's online identity will be hijacked compared to a random Google user (Thomas et al., 2017).

Exacerbating the risk, the Simple Mail Transfer Protocol (SMTP) standard that email relies on is "inherently insecure" (IETF 2008). "[I]t is feasible for even fairly casual users to negotiate directly with receiving and relaying SMTP servers and create messages that will trick a naive recipient into believing that they came from somewhere else. Constructing such a message so that the 'spoofed' behavior cannot be detected by an expert is somewhat more difficult, but not sufficiently so as to be a deterrent to someone who is determined and knowledgeable.

Consequently, as knowledge of Internet mail increases, so does the knowledge that SMTP mail inherently cannot be authenticated, or integrity checks provided, at the transport level" (IETF 2008). RFC-5321 on SMTP further enumerates several of the inherent security weaknesses in the email protocol and describes security controls to consider. End users are left with the responsibility to identify, report and respond appropriately to "spoofed" or phishing emails.

Objective

Organizations need to reasonably invest the resources in protecting the email service and reinforcing safe and secure usage. It is imperative that businesses train their employees on how to identify attempts by malicious actors to social engineer their way into accessing sensitive business data and information technology infrastructure through phishing. The objective of this document is to describe the fundamental components of a comprehensive program that trains, tests, measures and enhances an organization's

[4] Salesforce does offer the ability to restrict access to a customer's web application to certain IP addresses. See https://help.salesforce.com/articleView?id=admin_loginrestrict.htm&type=5, downloaded June 25, 2018.

cybersecurity to defend against phishing attacks. The recommended program is based on operational experience by the author developing, deploying and operating phishing training programs for government and private-sector organizations. It also guided by the best-practices recommended by the National Institute of Standards and Technology.

Phishing Training Program

Training on identifying and reporting phishing emails is a component of an organization's information security awareness training program. According to the National Institute of Standards and Technology (NIST) Cybersecurity Framework, informing, training and educating all users on cybersecurity awareness and related responsibilities is essential to cybersecurity risk management (NIST 2018). Also, training should be provided to new users and repeated periodically (NIST 2015). As recommended by NIST, organizations are encouraged to enhance the training by conducting exercises that simulate actual cyber-attacks (NIST 2015). Today, there are several open source and commercial tools readily available to send emails to simulate a phishing attack. Many organizations authorize the use of these tools to enhance cybersecurity training to launch phishing emails to generate a simple metric of the percentage of users that were fooled by the phishing email. Unfortunately, users and the organization may be failing to fully benefit from a phishing training exercise due to lack of a comprehensive program that addresses the entire lifecycle of phishing awareness training. A comprehensive program includes the following core activities:

1. Train on Phishing Detection and Incident Response
2. Obtain Leadership Approval
3. Develop the Training Exercise Scenarios
4. Select and Deploy the Phishing Tool
5. Implement and Test Exercise Scenarios
6. Develop and Implement Exercise Response
7. Initiate the Exercise
8. Report on the Metrics

Train on Phishing Detection and Incident Response

An organization and its users must be trained before you can test their abilities to detect and respond to phishing. The phishing exercise is not the training itself but a measure of the effectiveness of the provided training. It is also intended to reinforce concepts in the training material. The components of a security awareness training program can vary based on tailoring for the organization. For general guidance, see Building an Information Technology Security Awareness and Training Program, NIST 800-50, October 2003 (NIST 2003). Specific to phishing, the training should include the following:

- Indicators of fraudulent emails.
- The primary point of contact for phishing incident investigation and response (usually the information security team).
- Technical procedures on phishing incident investigation and response, including procedures addressing:
- Handling of email with suspected malware;
- Forensic investigation of emails, email clients (e.g., desktop, web and mobile applications), hosts, network traffic, logs and other data relevant to an email investigation; and
- Response actions to contain and eradicate the malicious activities and impacts of the phishing

email.

- This training may be more appropriate for the cybersecurity analysts, but a subset of training would be needed for users to identify phishing emails and how to report them to the analysts safely.
- Relevant data backup and recovery procedures.

Generally, this training should be given to all new employees upon hire and annually administered as part of an annual cybersecurity awareness training program. Phishing exercises should commence after training the organization and all targeted users.

Obtain Leadership Approval for the Exercise

Phishing exercises should be initiated only with the expressed consent of the leaders of the organization. When a user first experiences a phishing exercise, the first instinct of the user is to assume that any failure may impact their employment negatively in some way. Personnel issues arise that may lead to users questioning the authority and appropriateness of the exercise. Therefore, it is vital that the leadership approved the phishing training program and the exercise scenarios before starting. With this approval, all users and personnel involved in conducting the phishing exercise are fully aware of its appropriateness.

Develop the Training Exercise Scenarios

Tailor phishing email exercises to the line of business of the organization. While many phishing emails are sent to targets indiscriminately, those are more likely detected and deterred by automated email SPAM security tools. The most effective phishing emails are those that are tailored to be familiar to the activities of the targeted organization or user. For example, an energy sector employee would more likely respond to a phishing email relating to solar panels compared to a phishing email relating to swimming pool supplies.

There are other instances where events specific to the industry of the organization may be subjects of phishing emails. Therefore, the organization may want to develop exercise phishing emails specific to that event. Again, the energy sector may develop a phishing scenario mimicking an annual generator convention. A financial organization may develop a scenario relating to an annual auditors symposium.

Another consideration is to develop a scenario highlighting a specific and current risk observed on the computer network. For example, if the recent trend by attackers is to launch ransomware attacks, the organization may want to highlight this risk and develop a phishing email scenario that mimics a recent ransomware attack. By mimicking an active threat, an organization assesses the adequacy of current training while also reminding users to be vigilant in screening emails that may lead to the installation of ransomware.

Lastly, scenario development should also include determining the actions and metrics the organization wants to capture for future reporting. Examples include the following:

- The number of users that opened the phishing email.
- The number of users that clicked on the link in the phishing email.
- The number of users that sent an email response to the phishing email.
- The number of users per department that fell victim to the phishing email.
- The number of users that opened the attachment to the phishing email.

By developing these organization-specific scenarios, the organization clarifies its phishing exercise objectives and requirements.

Select and Deploy the Tool

With initial scenarios and requirements developed, the organization can begin evaluating tools to achieve the established objectives of the phishing training program. The nature of the scenario should dictate the features required for the tool. Information security requirements relating to data collection, storage and access also need to be considered. Although requirements may need to be adjusted based on tool capabilities generally, it is best to have a developed requirement list with the approval of leadership before deciding on a tool.

Implement and Test Exercise Scenarios

Build and test exercise scenarios after tool selection. Testing the exercise scenarios is vital to validate training and reporting objectives. Also, confirm that the exercise phishing emails are able to bypass current email and network security tools. Whitelisting phishing email servers or adjusting other mail transport configurations may be required. However, care must be taken to ensure any configuration changes do not inadvertently allow malicious phishing emails to bypass mail and network security controls.

Develop and Implement Exercise Response

Phishing exercise training must be appropriately handled to deconflict exercise phishing incidents from actual phishing incidents that engage incident response procedures. The purpose of this type of training is to assess the effectiveness of phishing training on users. Therefore, the exercise should not engage incident response procedures. An independent exercise response plan should be developed to handle phishing exercises. Critical components of the phishing exercise response plan include:

Phishing Exercise Email Marking - Every exercise phishing email should have a hidden marking indicating that it is an exercise email. The marking should also change periodically or with each phishing exercise. This marking will be used by incident handlers to confirm whether a reported phishing email is real or an exercise email. The marking could be a unique sequence of numbers, an image or hidden comments in HTML code. This marking should remain confidential among the personnel conducting the exercise and critical stakeholders in the exercise response plan.

Scripted Responses to Users - Responses to initial reports of the phishing exercise email should be scripted, but not reveal it is an exercise. Once users begin receiving exercise phishing emails, they will contact the information security team, the help desk or the IT manager to confirm the authenticity. The information security team, help desk, and IT manager should not initially inform a user that an email is an exercise email. The user may, in turn, warn other users to ignore the exercise email. At first, this seems like a good result. However, this does not meet the overall objective of assessing the effectiveness of the training on each employee since the other employees did not have an opportunity to review the exercise phishing email and apply their training. Therefore, another option is to provide a scripted response such as, "Thanks for referring this to us. Please send us a copy per our procedures. We will investigate and will contact you with an update." After the exercise is complete, inform users of the exercise phishing email and reemphasize the training objectives of that scenario.

Pre-Exercise Notifications - Before sending an exercise phishing email, brief cybersecurity incident handlers on the email contents and the exercise email marking. Since this is not an exercise of incident response, they need to be able to identify exercise phishing emails not requiring investigation resources. Examples of the stakeholders that need to be informed include:

- Help Desk Personnel
- Security Operations Personnel
- Department Managers

Initiate the Exercise

Initiate the phishing exercise after the exercise response plan is in place with concurrence and approval. One thing to consider is that users do not check and review email messages at the same time intervals. Therefore, the exercise should be planned to ensure the highest number of users will receive and open the exercise email within a short period. One recommendation for businesses operating during standard work hours Monday through Friday is to initiate the exercise on a Tuesday and to collect metrics for 72 hours. After which, the exercise phishing infrastructure can be taken down (e.g., fake websites, temporary domain names, metrics collection tools). After that date, cybersecurity analysts will know any new phishing emails like the exercise emails received or reported will require regular scrutiny and investigation.

Report on the Metrics

After the exercise window has ended, metrics should be compiled to determine the effectiveness of the organization's phishing training. Ascertain trends among the phishing exercises over time. The metrics and any newly identified phishing threats should also be used to develop new scenarios for the next exercise to meet training objectives. Furthermore, if some users repeatedly fall victim to the phishing exercise, consider additional training for those users or implementing technical security controls to address that heightened risk.

Conclusion

Email is an essential business communications tool. Consequently, deceptive phishing emails will continue to represent a significant threat to business and user data, services and information technology. By implementing a comprehensive phishing exercise training program (along with email security technology), the risks associated with that threat can be reasonably mitigated. The overall goal of the program is to go beyond merely catching users that click on fake emails. The imperfect human element in communications guarantees that a small percentage of users in the organization are always tricked into responding to a phishing email. Therefore, the goal is to minimize the size of that percentage through a methodical, consistent, structured and measurable phishing training program.

References

Internet Engineering Task Force (October 2008). RFC 5321, Simple Mail Transport Protocol, 75. Retrieved from https://tools.ietf.org/html/rfc5321

National Institute of Standards and Technology (October 1, 2003). Building an Information Technology Security Awareness and Training Program. Retrieved from Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf

National Institute of Standards and Technology (April 16, 2018). Framework for Improving Critical Infrastructure Cybersecurity version 1.1, page 31, PR-AT-1. Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

National Institute of Standards and Technology (January 22, 2015). Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53 Revision 4, AT-2, F-37 to F-38. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf

Swatman, Rachel (August 19, 2015). 1971. First Ever Email. Guinness World Records. Retrieved from http://www.guinnessworldrecords.com/news/60at60/2015/ 8/1971-first-ever-email-392973

The Radicati Group, Inc. (February 2017). Email Statistics Report, 2017-2021. Retrieved from https://www.radicati.com/wp/wp-content/uploads/2017/01/Email-Statistics-Report-2017-2021-Executive-Summary.pdf

Thomas, K., Li, K., Zand, A., Barrett, J., Ranieri, J., Invernizzi, L., …, Bursztein, E. (November 3, 2017). Data Breaches, Phishing, or Malware? Understanding the Risks of Stolen Credentials. Section 5.3. Retrieved from https://acmccs.github.io/papers/p1421-thomasAembCC.pdf