State of California

Office of Information Security

Phishing Exercise

Standard

SIMM 5320-A

November 2021

REVISION HISTORY

REVISION	DATE OF RELEASE	OWNER	SUMMARY OF CHANGES
Initial Release	October 2020	Office of Information Security (OIS)	New Standard in support of SAM Section 5320-A, Phishing Exercise Standard.
Minor Update	November 2021	OIS	Provided additional phishing techniques and exercise planning coordination requirements.

TABLE OF CONTENTS

I. INTRODUCTION

Protecting state government from malicious email attacks requires the use of both technical measures and awareness from a security-focused workforce/staff. By providing regular simulated phishing exercises, Agencies/state entities can obtain a direct measurement of employee understanding as well as progress in user behavior. Phishing is the fraudulent attempt to obtain sensitive information, such as usernames, passwords, and credit card details, by disguising oneself as a trustworthy entity in an electronic communication, typically carried out by email spoofing or instant messaging, phishing often directs users to enter personal information at a fake website that matches the look and feel of the legitimate site. Since attachments and email replies are common user interactions employees are easily susceptible to phishing attacks and the various techniques. Phishing exercises in support of awareness and training are a critical component of a mature information security program and accordingly are included in State Administrative Manual (SAM) 5320. Continuous email phishing assessments of who is clicking on what and when can be effective by indicating patterns of phishing vulnerabilities within a department and identifying further awareness training needs. As a best practice, the frequency of agency/state entity phishing campaigns could be weekly, bi-weekly, or monthly and should accurately reflect the types of emails, campaigns, and other content such an employee is likely to see in the course of their employment. The content should also be designed to elicit a variety of agency/state entity specific information that could result in a loss or harm to the individual or the agency/state entity.

This Phishing Exercise Standard (SIMM 5320-A) establishes specific requirements for Agencies/state entities to coordinate phishing exercises with the California Department of Technology (CDT) Office of Information Security (OIS) and the California Cybersecurity Integration Center (Cal-CSIC), and other requirements for execution.

II. PHISHING TECHNIQUES

Seven key phishing techniques are commonly employed: 1) Link manipulation, 2) SMSishing, 3) Vishing 4) Website forgery 5) Pop-ups, 6) Video Teleconferencing (VTC) and collaboration platform phishing, and 7) Social Media.

1. Link manipulation consists of the following:

    a. Hidden URL- When a hacker hides the actual URL of a phishing website under plain text, such as “Subscribe”, “Submit” or “Click here”.
    b. Sub-Domains- Links can be altered and users will be directed to a sub-domain instead of the main-domain.
    c. URL Hacking- When a hacker buys domains with a variation in spellings of a popular domain, such as facebok.com, googlle.com, yahooo.com. Also referred to as typosquatting.
    d. Internationalized Domain Name (IDN) homograph attack- A link similar to an authentic link but contains characters and/or misspellings.

2. SMSishing events consist of the following:

a. Hacker will try to trick a victim into giving their private information via a text message.
b. Hacker will send a text and include a link that automatically downloads malware. An installed piece of malware can steal personal data such as banking credentials, tracking locations, or phone numbers from contact lists. The virus will then spread, and risk exponentially multiplies.

3. Vishing events consist of the following:
   a. Utilizing landline telephones/cell phones, vishing calls often appear to be coming from an official source, such as a bank or a government organization. These vishers even create fake Caller ID profiles (called 'Caller ID spoofing') which makes phone numbers seem legitimate.
   b. Vishers may also impersonate people through mimicking voices using artificial intelligence and trick victims into transferring money to them.

4. Website Forgery events consist of the following:
   a. Website spoofing occurs when a hacker creates a fake website that looks similar to a legitimate website that the user intends to access, and users may enter their sensitive information.
   b. Cross-site Scripting occurs when a hacker executes malicious script or payload into a legitimate web application or website through exploiting a vulnerability. Users click on links and request legitimate websites but also execute malicious script.

5. Pop-ups consist of the following:
   a. In-session phishing works by displaying a pop-up window during an online banking session, asking the user to retype his username and password as the session has expired.
   b. "Pop-up tech support" is when a user is browsing the internet and receives a pop-up message that the system is infected, and the user needs to contact the given number to obtain technical support via phone or email.
   c. The user enters his details, not expecting the pop-up to be a fraud as they had already logged into the bank's website.

6. VTC and collaboration platform phishing include but may not be limited to the following:
   a. Zoom Bombing-Occurs when unauthorized users invade video calls with inappropriate content for either humor or logistical disruption. The behavior has affected numerous institutions and organizations across the globe.
   b. Malicious Domain Registration- Popular video conferencing applications such as Zoom, Teams, and Google are seeing their names used by malicious actors to create newly registered fake domains. Thousands of new fake domains have been registered.
   c. Zoom Room Spoofing-Bad actors are inviting people to rooms organized for malicious purposes including malicious link sharing, credential harvesting, and dissemination of propaganda. Individuals are sent links to join malicious VTC and collaboration platform events.
   d. zWarDial tool-Automates enumeration of non-password protected meetings on

certain platforms and can test on average 110 meetings per hour with a success rate of close to 14%. The tool evades certain platforms attempts to block automated meeting scans that leverage the use of Tor and anonymous browsers. Certain platform's meeting searches are routed through multiple proxies and potentially exposes meeting room information without having to log in. Additional platform features and functionality may be vulnerable and not work as intended.

7. Social Media phishing consist of the following:
    a. Fake customer service accounts- Social media has changed the way customers interact with brands and they tend to go directly to a company's social media channels for customer support. Hackers have been quick to take advantage of this online relationship to launch fake accounts impersonating major brands. Research has found that 19% of social media accounts appearing to represent top brands were all fake.
    b. Fake comments on popular posts- A trending news story or popular post will tend to generate a lot of likes and comments. Hackers will take advantage of this large audience by adding their own comments to the posts with links to other attention-grabbing headlines. As soon as users click on the link, they will be directed to a phishing website or their computer will be infected with malware.
    c. Fake online discounts- It's hard to resist the lure of a cheap bargain online but these too good to be true offers usually are! The hackers will often create a fake page imitating a big brand name, then pretend to offer a real promotion. These scams are often set up specifically to harvest user data and will require the input of personal information.
    d. Fake trending videos- Hackers are adept at manipulating human behavior to launch scams. They will often use trending topics such as national disasters or sensationalist stories to entice people to click on a video. Upon clicking the link, users are told they need to download a plug-in before being able to view the video. Of course, this is nothing more than a ruse to get the user to download malicious software.

Social Media phishing is also a technique used by hackers to target end users via their own personal accounts, in addition to their agency/state accounts. Where employees of an agency/state entity are permitted to use or otherwise access their personal social media or webmail accounts while at work or otherwise connected to an agency/state system, they may be targeted by such hackers to gain information about or access to the individual or the agency/state IT infrastructure. Therefore, each agency/state entity that permits employees to use or otherwise access their personal social media or webmail accounts while at work should include enhanced training directed at an employee's use of social media and webmail while at work.

III. EXERCISE PLANNING

State entities are required to have a comprehensive phishing exercise plan. Prior to executing a phishing exercise, state entities are required to notify both CDT OIS and Cal-CSIC at least 72 hours (three business days) prior. The following are required elements of phishing exercise planning and plans.

A. Acquiring Products and Services for Exercise Simulation

Using the logos, trademarks, and domains of another company in a simulated phishing attack may open an agency/state entity to lawsuits from that company for trademark or copyright infringement. When conducting phishing exercises, some phishing products and solution providers include templates that use logos, trademarks and domains not owned by them and pass on any potential liability to the agencies/state entities through liability disclaimers. **To avoid such liability agencies/state entities should use prominent disclaimers informing users that the logos, trademarks and domains of companies are being used solely for training purposes.**

B. Validation of Domain Name

Validate ownership of all domain names to be used in the proposed phishing campaign Templates. Perform a domain lookup at the Internet Corporation for Assigned Names and Numbers (ICANN) website using https://lookup.icann.org/ to obtain ownership point of contact information and prevent disputes regarding the ownership and use of internet domain names.

Validate ownership of all ca.gov domain names using https://domainnamerequest.cdt.ca.gov/ that are to be used in proposed phishing campaign templates. Refer to SAM Sections 5195 and 5195.1 for Internet Domain Name Policy and Internet Domain Name Requirements. Validating domain name(s) ensures ownership to allow for proper exercise planning.

C. Plan Elements

Agency/state entities must have a complete exercise plan that includes, at a minimum, the following:

1. Use of fictional entity name(s), brand/logo(s), image(s), etc. Departments may mockup logos that closely resemble a legitimate brand/logo.
2. Pre- and post-exercise communication messages and protocols.
3. Information and phishing email content that reinforces the information/instructions a user will have received from awareness training, such as looking for poor grammar, typos, etc.
4. Pre and post exercise steps to control and properly manage the test. For example, controlling test emails from being forwarded outside of the test entity and ensuring their removal from employee email/shared email boxes once exercise is completed.
5. Advance notice to the business areas most likely impacted by the testing activity, such as IT help desk, entity Information Security Office, etc.
6. Segmented exercises that align with learner groups by functional role, when appropriate. A role-based approach will also minimize impact on day-to-day business activities and processes.
7. Assignment of observers/note takers for the testing activity or application logs to ensure the capture of various types of responses and lessons learned. Provide

learning and advice to users at the time of ‘clicking’. This may be in the form of redirection to advice pages (landing page) or online training modules (Learning Management System).

Phishing emails shall not use the following:

1. Inappropriate or sensitive material.
2. Political themes or legal or contractual issues.
3. Other state entity names or logos, union names or logos, or commercial brands and trademarks without express written approval from those entities.

D. Coordination

Coordination with departmental staff is required to ensure all phases of exercises are controlled and executed according to plan with minimal disruption and operational impact. At a minimum, phishing exercises shall provide for:

1. Advance coordination with the business areas most likely impacted when responding to the testing activity, such as IT help desk, entity ISO Office, etc.
2. Assignment of observers and note takers for the testing activity or application logs to ensure the capture of various types of responses and lessons learned.
3. Prior written approval from the agency/state entity AISO and ISO.
4. Prior written approval from CDT OIS for emails to be used.

E. Exercise Scoping and Control

Determine the scope of each email phishing exercise. Exercise scope may include email blasts to all employees in the department or targeted areas within specific organizational areas (i.e., Executive Management, Finance, Accounting, Human Resources, IT System Administrators, etc.). Pre- and post-exercises are required to control and properly manage the test. The following are the minimum scoping and control requirements.

1. Prepare pre- and post-exercise communication messages and protocols. This includes information that reinforces the information/instructions a user will have received from awareness training, such as looking for poor grammar, typos, etc.
2. Ensure department controls test emails from being forwarded outside the test entity and ensure their removal from employee email/shared email boxes once exercise is completed.
3. When appropriate, segment exercises and align with learner groups by functional role.
4. Use phishing emails that are a similar style of communication the department employees are familiar with that more accurately reflect the real threats users will be exposed to or experience.

F. Exercise Metrics

Phishing exercises must capture key metrics tracked during an email phishing exercise.

These include but are not limited to the following metrics:

1. Total number of users who opened the email.
2. Total number of users who “clicked on a link” within the email.
3. Total number of users who “clicked on the button” see a response.
4. Total number of users who entered credentials on the phishing site.
5. Total number of users who ran the malicious payload delivered via the phishing site.
6. Total number of users who completed the information described by the campaign.

G. Exercise Report

A summary report shall be created to assess campaign and provide comparable conclusions to assist in understanding the need for additional or special security training. At a minimum, the report shall provide for a weekly, bi-weekly, or monthly and year-over-year comparison of the following metrics to demonstrate awareness training program maturity and effectiveness.

1. Number and/or percentage of users who opened the email.
2. Number and/or percentage of users who clicked on a link within the email.
3. Number and/or percentage of users who entered credentials on the phishing site.
4. Number and/or percentage of users who ran the malicious payload delivered via the phishing site.
5. Number and/or percentage of users who completed the information described by the campaign.

IV. REQUIRED APPROVALS AND ADVANCED NOTIFICATIONS

Coordination with state oversight entities and all potentially impacted organizations must take place prior to phishing exercises. The following are the minimum required approvals that must be obtained and the advanced notifications that must be made prior to launching a phishing exercise.

1. Obtain prior written approval to use other state entity names or logos, union names or their logos, or commercial brands and trademarks from the respective state entity or organization.
2. Obtain prior written approval for any phishing exercise, and your phishing email templates, from your Information Security Officer (ISO) and Agency Information Security Officer (AISO).
3. Obtain written approval for any phishing exercise and your phishing email templates from CDT OIS. At least 72 hours (three business days) prior to an exercise, Agencies/state entities must notify the California Cybersecurity Integration Center (Cal-CSIC) via email at CalCSIC.SecurityAlerts@caloes.ca.gov and the California Department of Technology, Office of Information Security (CDT OIS) at security@state.ca.gov. The 72-hour (three business days) advanced notification must include the approved email(s) to be used. NEVER initiate a phishing exercise without first providing the required 72-hour (three business days) advance notification to Cal-CSIC and CDT OIS.

V. LINKAGE TO INCIDENT REPORTING AND RESPONSE LIFECYCLE

Phishing awareness and training are critical components of a mature information security program, but ensuring employees know what to do if they victim to a phishing scam is also critical. State entities must plan for the unique aspects of a phishing incident integrated with appropriate incident response. An agency/state entity's incident response plans and procedures must comport with SAM Sections 5330 and 5340, and SIMM 5340-A and 5340-C. Successful social engineering and phishing attacks must be one of the many likely scenarios addressed in the agency/state entity's incident reporting and response plans and procedures. As such, phishing exercises and the state department planning, execution, and response to those is a component of a department's incident reporting and response plans, as well as potentially its technology recovery plan.

Effective phishing incident response takes careful planning and most of all practice. Further, it requires organization, training of key personnel, and systematic procedures; therefore, conducting several exercises frequently are key requirements to properly assess your organization's readiness to an actual phishing incident. Listed below are the typical phases of the Phishing Incident Response lifecycle – the process of preparing for an incident, and then working through various stages to detect, analyze, contain, eradicate, recover, and apply the lessons learned.

1. Preparation

    a. Develop the incident reporting and response plan which comports with SIMM 5340-A.
    b. Identify the Information Security Officer (ISO) responsible and publish his/her contact and email with instructions for every staff member on reporting incidents.
    c. Ensure that staff members selected have received security awareness training, which includes how to detect and handle social engineering and phishing attacks.
    d. Prepare an internal escalation list (SIMM 5340-A), including names, contact information, and responsibilities for all staff involved in incident response and management.
    e. Create a methodology for users to inform ISO/Helpdesk immediately using email or phone about the incident.
    f. Maintain a list of contact information for external resources that may be involved in handling incident response for ready reference.
    g. A combination of phishing-aware users and a comprehensive technical strategy reduces the chance of a successful phishing attempt. Employ required mitigating controls, such as:
        i. Basic and role-based security awareness and training for all employees.
        ii. Ensuring all antivirus, anti-malware, personal firewalls, and browser anti-phishing controls are in place and up to date.

2. Detection

    a. Employees follow internal entity reporting policy and procedures.
    b. On receiving the information about an incident, the ISO/Helpdesk must receive all phishing email, including email headers or URLs from user. These emails, URLs and other information need to be an investigative priority.
    c. Entity ISO and/or Information Security Office is notified.
    d. Entity ISO reports incident to OIS/CHP CCIU through Cal-CSIRS (SIMM 5340-A) (FOR INTERNAL DEPARTMENTAL PHISHING EXERCISES DO NOT REPORT TO CCIU OR CAL-CSIRS UNLESS SCOPE OF PHISHING EXERCISE INCLUDES ADVANCED NOTICE AND COORDINATION WITH CDT-OIS).
    e. As standard practice, the entity needs to keep continuous watch on the following to enable rapid detection, containment, and response:
        i. Emails flagged by various filters.
        ii. Non-returnable and non-deliverable emails.
        iii. Consider adding a flag/tag to emails originating from domains external to the organization, warning the recipient to be extra vigilant when opening emails from this source. Example: Subject: [**External**] WARNING: This email originated outside of the xxx.gov email system! DO NOT CLICK links if the sender is unknown and never provide your User ID or Password.
        iv. Notification by third party (e.g., MS-ISAC) of suspicious email.
        v. Emails linked to internal and external URLs.
        vi. Notification from Security Operations Center, CDT OIS, and law enforcement agencies about emails.

3. Analysis

    a. The suspicious activity once detected and/or reported should be analyzed using available tools or external support.
    b. Once suspicious activity is confirmed to be an attack related to phishing, it should be categorized according to threat it poses to the organization.
    c. Use various means including logs and tools to gather information and analyze activity to determine the following:
        i. What systems and/or information assets have been exposed?
        ii. What protected information, if any, has been compromised?
        iii. What users, customers, public were/are likely to get exposed
        iv. Who might have launched the attack?
        v. Who has knowledge of this attack?
        vi. Worst case impact(s) on the system and/or information asset(s).
        vii. If this was or can be exploited for any criminal activity.
        viii. What time did the incident occur?

4. Containment

    a. Identify the system affected and how widespread the attack.
    b. Isolate the system including user device(s) or servers effected by the attack.
    c. Inform all users of the problems and immediate action needed to be taken by

them to contain the attack.

5. Eradication
    a. Use various tools to get the system free from the malware installed during the attack.
    b. Install patch, update rules, and modify content filter to avoid problem in future. Note: The image used to reimage device(s) may need to be updated before reimaging if it contains a vulnerability that was exploited in the attack.
    c. Test the system to ensure the problem does not occur again.
    d. Modify or change the affected system, site and/or network.
    e. Coordinate with SOC/IT Teams to initiate counter measures.
    f. Coordinate with any third-party to take down the site if required.
6. Recovery
    a. Update systems, firewalls, IDS's and remove temporary containment.
    b. Wipe and baseline the system.
    c. Update system with fresh signatures.
    d. Prepare detailed advisory and publicize it widely to avoid future attacks.
    e. Review the incident in detail.
    f. Update policy and processes.
    g. Document problem and actions taken including policy changes, process modifications and configuration changes.
    h. Prepare for new attacks.
7. Lessons Learned
    a. Incident Name
    b. Dates/Time and duration of the event
    c. Executive Summary
    d. Root cause of the incident (the technical details)
    e. Who has been disclosed on the details of the incident?
    f. What worked to assist identification, containment, and eradication?
    g. What improvements are recommended?
    h. What are next steps to mitigate against recurrence?

At a minimum, the agency/state entity conducting the phishing exercise shall plan and prepare for the following as part of its phishing exercise:

a. Communication/Inquiry to its designated Information Security Officer or Office.
b. Provide an internal incident report per its departmental reporting protocols or email from user that provides users information, date, and time of attack, and if user clicked on a link or provided any information, and what information was provided.

VI. DEFINITIONS

Phishing: Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising oneself as a trustworthy entity in an electronic communication. Typically carried out by email spoofing or instant messaging, it often directs users to enter personal information at a fake website that

matches the look and feel of the legitimate site.

Simulated Phishing: Simulated phishing are deceptive emails, like malicious emails, sent by an organization to their own staff to gauge a response to phishing and similar email attacks. The emails themselves are often a form of training, but such testing is normally done in conjunction with prior training; and often followed up with more training elements. This is especially the case for those who "fail" by opening any email attachments or clicking on any included web links - or if they were tricked into entering any credentials.

Social Engineering: Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. This differs from social engineering within the social sciences, which does not concern the divulging of confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

Phone phishing: Phone phishing (or "vishing") uses a rogue interactive voice response (IVR) system to recreate a legitimate-sounding copy of a bank or other institution's IVR system. The victim is prompted (typically via a phishing e-mail) to call in to the "bank" via a number (ideally toll free) provided to "verify" information. A typical "vishing" system will reject logins continually, ensuring the victim enters PINs or passwords multiple times, often disclosing several different passwords. More advanced systems transfer the victim to the attacker/defrauder, who poses as a customer service agent or security expert for further questioning of the victim.

Spear phishing: is a technique that fraudulently obtains private information by sending highly customized emails to a few end users. It is the main difference between phishing attacks because phishing campaigns focus on sending out high volumes of generalized emails with the expectation that only a few people will respond. On the other hand, spear phishing emails require the attacker to perform additional research on their targets to "trick" end users into performing requested activities. The success rate of spear-phishing attacks is considerably higher than phishing attacks with people opening roughly 3% of phishing emails when compared to roughly 70% of potential attempts. Furthermore, when users open the emails, phishing emails have a relatively modest 5% success rate to have the link or attachment clicked when compared to a spear-phishing attack's 50% success rate.

Whaling: Whaling refers to spear-phishing attacks directed specifically at senior executives and other high-profile targets. In these cases, 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 may be an executive issue such as a subpoena or customer complaint.

Clone phishing: is a type of phishing attack whereby a legitimate and previously delivered email containing an attachment or link has had its content and recipient addresses 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. It may claim to be a resend

of the original or an updated version to the original. Typically, this requires either the sender or recipient to have been previously hacked for the malicious third party to obtain the legitimate email.

Phishing kit: A phishing kit bundles phishing website resources and tools that need only be installed on a server. Once installed, all the attacker needs to do is send out emails to potential victims. Phishing kits, as well as mailing lists, are available on the dark web. A couple of sites, Phishtank and OpenPhish, keep crowd-sourced lists of known phishing kits. The availability of phishing kits makes it easy for cyber criminals, even those with minimal technical skills, to launch phishing campaigns.

Questions regarding this standard may be sent to:
California Department of Technology
Office of Information Security
Security@state.ca.gov