# State of California

# Office of Information Security

# Phishing Exercise

# Standard

# SIMM 5320-A

October 2020

## REVISION HISTORY

| REVISION | DATE OF RELEASE | OWNER | SUMMARY OF |
|---|---|---|---|
| **Initial Release** | **October 2020** | **Office of Information Security (OIS)** | **New Standard in support of SAM Section 5320-A, Phishing Exercise Standard** |

## 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. 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.

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

Five key phishing techniques are commonly employed: 1) Link manipulation, 2) SMSishing, 3) Vishing 4) Website forgery, and 5) Pop-ups.

1. Link manipulation consists of the following:

    a. Hidden URL. Most state entities will utilize link manipulation for their phishing exercise and hide 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.

## 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 prior. The following are required elements of phishing exercise planning and plans.

### A. Validation of Domain Name

Validate ownership of all 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.

## B. 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 ISO 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.

## C. Coordination

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

1. Advance notice to the business areas most likely impacted by 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.

## D. 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.

## E. 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.

## F. 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 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 advanced notification must include the approved email(s) to be used. NEVER initiate a phishing exercise without first providing the required 72-hour 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 fall 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 (SAM 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 handing 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 PHISHING EXERCISES SIMULATE THIS ONLY 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. Notification by third party (e.g. MS-ISAC) of suspicious email.
iv. Emails linked to internal and external URLs.
v. 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.

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

## APPENDIX A

Using the logo of another company in a simulated phishing attack may open a customer to lawsuits from that company for trademark or copyright infringement. To assist the state entities, avoid copyright and trademark liabilities when conducting phishing exercises. Some phishing product and solution providers include templates that use domains not owned by them and liability disclaimers in the use of those. Refer to Appendix A as an example. The following is an example of product liability disclaimers seen in product and solution provider tools. KnowBe4 Site

KnowBe4
Human error. Conquered.

**PRODUCTS & SERVICES**

Trademark Issues

*This webpage/discussion has been prepared for general information purposes only to permit you to learn more about KnowBe4 and our products and services. KnowBe4 is not a law firm. The information presented is not legal advice, is not to be acted on as such, may not be current, and is subject to change without notice. None of our customer service representatives are lawyers and they also do not provide legal advice. Although we go to great lengths to make sure our information is accurate and useful, we recommend you consult a lawyer if you want legal advice. No attorney-client or confidential relationship exists or will be formed between you and KnowBe4 or any of our representatives.*

Trademark and Copyright - Issues- Updated 3.27.2017

**The misunderstanding**: Using the logo of another company in a simulated phishing attack will open a customer to lawsuits from that company for trademark or copyright infringement.
**The truth**: The crux of a trademark infringement claim is whether there is consumer confusion as to the source of a product or service. When KnowBe4's customers incorporate another company's logo in a simulated phishing email, that logo is not used in a way that confuses customers into believing that their goods or services originate with, are related to, or are sponsored by the company whose logo is displayed. KnowBe4's customers are not branding goods or services with anyone else's logo; rather they are engaged in security awareness training. Potential confusion is mitigated by a corrective landing page and/or instructional video that launches at the conclusion of a simulated phishing attack, advising users to be more wary of phishing scams. KnowBe4 includes sample language at the bottom of its "OOPS - corrective landing page" reinforcing that any third party logo is for illustrative or instructional purposes only and there is no affiliation or relationship between the mark owner and KnowBe4 or KnowBe4's customer. Customers should not omit this important information when customizing landing pages.

From a copyright perspective, incorporating a third-party logo in a simulated phishing email serves an entirely new, transformative purpose, and as such, constitutes a fair use. The logo is employed in a different manner (unrelated to the offering or sale of goods or services) and for a different purpose (aimed at security awareness and educating the public about how to avoid phishing scams). This transformative use does not undermine the copyright holder or any market that the copyright holder would reasonably exploit.