ASSESSMENT SUMMARY

Phishing Campaign Assessment
Cycle Report

PCA6304E61826057616CE957D16

Aug 31, 2022 DATE

Test Customer (TC)

If Test Customer wishes to create and distribute derivatives of this report (such as summaries of this report or Test Customer's commentary on the report's recommendations), Test Customer should (1) provide notice to CISA prior to distributing such derivatives; (2) clearly mark derivatives so that it is clear that Test Customer created them and so that they cannot be mistaken for official CISA documents; and (3) refrain from affixing the CISA logo or DHS seal to the derivatives, unless Test Customer has obtained written permission to do so from the CISA Office of External Affairs. [1]

[1] The unauthorized use of any Federal agency's seal is governed by the U.S. Code title 18 sections 506, 701, 709 and 1017. Requests to use the CISA logo or DHS seal should be directed to branding@cisa.dhs.gov, copying vulnerability_info@cisa.dhs.gov

ASSESSMENT SUMMARY

PCA6304E61826057616CE957D16

Phishing Campaign Assessment Cycle Report

Aug 31, 2022

Table of Contents

1. How to Use This Report

Welcome to your Phishing Campaign Assessment (PCA) cycle report. This document provides the results of the most recently completed email phishing campaign of Test Customer (TC)'s targeted users.

You may wonder what you're supposed to do with all this information. While it's not the Cybersecurity and Infrastructure Security Agency's (CISA) intent to prescribe a particular process for modifying or conducting your security training program, we hope you'll use this report to strengthen your security posture. Here's a basic flow:

1. **Look at the summary report card.** The report card contains high level results for this cycle and a quick comparison to the previous cycles. If this is your first report, you should note that the report card will initially lack historical data to make comparisons against, though that data will exist in your next report.
2. **Read the framework in which to understand results.** PCAs concentrate on how phishing email deception affects target user click behavior. CISA expects that a more deceptive phishing email has a higher likelihood of being clicked and a lower deception email has a lower likelihood of being clicked. CISA does not expect click rates for all deception levels to reach and sustain zero percent.
3. **Review the red flags and the sophisticated techniques ordered by click rate.** The indicators with click rates above your organization's average click rate are representative of the phishing elements that your targeted users are potentially less aware of and may benefit additional training on.
4. **See how performance has changed over time.** You should expect click rates and click times to fluctuate based on the deception level of the email templates used. Effective security awareness training, however, should result in a noticeable click rate decrease over time and to a level deemed acceptable based on your organization's risk management posture.
5. **Review the details of each campaign.** See examples of each phishing campaign used for this cycle and their click rate results to understand the context in which the red flags and sophisticated techniques were used.
6. **Compare click results to user reports of phishing.** If you have an established process for collecting reports of phishing, the attachments section provides Comma-Separated Values (CSV) files with the per-campaign click results you can use to compare to your internal statistics on user reports. A good initial goal for report rates is having two persons reporting the phishing attempts for every person that clicks in case the person who clicks the link does not report or does not realize they have been phished.
7. **Send an updated target list.** If you've experienced personnel changes since the start of this last cycle, send an updated email target list to vulnerability@cisa.dhs.gov prior to the start of your next phishing cycle on December 06, 2022.

If you have any questions about this report or feedback on how to improve the PCA service, email vulnerability@cisa.dhs.gov.

Test Customer

123 Main St
Brooklyn, NY 11207 USA
john.smith@inl.gov

TOTAL TARGETS
100

Cycle

Started
August 23, 2022

Ended
November 21, 2022

CHANGES

Current Cycle

Started August, 23, 2022
Ended November, 21, 2022

100 Targets, **100** Emails Successful

0 Emails Bounced

56 Total Clicks

56.0% Click Rate

Average First Click Time: **0 days, 0 hours, 5 minutes, 0 seconds**

Moderate Template With Most Clicks

Previous Cycle

Started, August 03, 2022
Ended, November 03, 2022

4 Targets, **2** Emails Successful

2 Emails Bounced

4 Total Clicks

200.0% Click Rate

Average First Click Time: **-20 days, 23 hours, 35 minutes, 31 seconds**

Moderate Template With Most Clicks

Click Rate

Overall Clicks
56.0%

LOW
Emails Sent 34
Unique Clicks 18
52.9%
-73.55%

MODERATE
Emails Sent 33
Unique Clicks 17
51.5%
+0%

HIGH
Emails Sent 33
Unique Clicks 21
63.6%
-36.4%

3. Framework

This section provides the framework in which to understand how email deception level may influence your email users' susceptibility to phishing attacks. At a high level, email phishing is a form of social engineering. In a social engineering attack, an attacker uses human interaction to obtain or compromise information about an organization or its computer systems. Phishing attacks use emails or malicious websites to solicit personal information or to get you to download malicious software by posing as a trustworthy entity.

The phishing emails in PCAs are modeled on real world phishing examples that contain links for targeted users to click. CISA expects that the more deceptive the email, the higher likelihood of being clicked. All PCA emails are coded with specific phishing indicators to determine the overall deception level:

- **Sophisticated techniques** are indicators used to increase the deception level by making an email appear normal, expected, and relevant to fool email recipients into acting before questioning or investigating the email's legitimacy.
- **Red flags** are indicators used to lower an email's deception level by undermining its legitimacy and arousing user suspicion by appearing unusual, out of place, or unfamiliar.

Deception levels range from low to high:

- **Low deception** emails are typically the easiest to detect and contain more red flags than sophisticated techniques.
- **Moderate deception** emails may initially appear legitimate due to sophisticated techniques but a similar number of red flags may arouse enough suspicion for the email recipient to reject the email as legitimate.
- **High deception** emails are typically the hardest to detect and contain more sophisticated techniques than red flags.

CISA does not expect click rates for all deception levels to reach and sustain zero percent. Effective security awareness training, however, should result in a noticeable click rate decrease over time and to a level deemed acceptable based on your organization's risk management posture.

CISA expects regular awareness training to be part of a multi-layered, anti-phishing strategy that at least also includes:

- **Established reporting processes.** Providing email users a simple means of reporting suspected phishing attacks decreases the window of opportunity for the attacker and increases the time your security team has to detect and respond to a potential breach.
- **Long and strong passwords.** Allowing network users to have a password manager to ensure they have unique, long, and strong passwords for each account.
- **Using multi-factor authentication (MFA).** Enabling MFA can help prevent adversaries from gaining access to your systems even if your password is compromised.
- **Installing and updating antivirus software.** Ensuring all your network connected devices are equipped with regularly updated antivirus software, firewalls, email filters, and antispyware to stop malicious activity when an email user does click a bad link.

4. Red Flags and Sophisticated Techniques

In general, CISA recommends that TC educate email users to be suspicious of any unsolicited or unexpected emails requiring the recipient to click on links, open attachments, or provide information for any reason. Adopting a baseline security posture for all emails meeting these conditions diminishes the click-inducing power of sophisticated phishing techniques and gives the email recipient more reason to scrutinize the email for potential red flags.

Specifically, CISA recommends that TC include in anti-phishing training and awareness efforts of the top 5 red flags and the sophisticated techniques outlined in the table below. Special attention should be paid to the indicators with click rates above this cycle's average click rate (56.0%) because they are representative of the phishing elements that TC targeted users are potentially least aware of and may benefit additional training on.

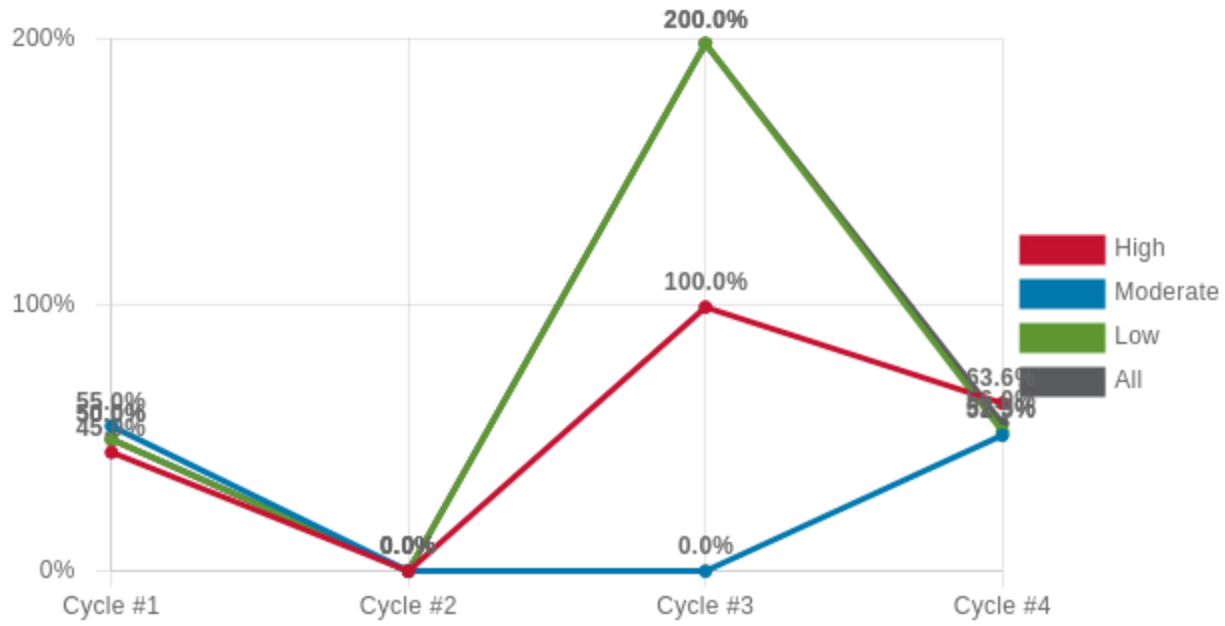
Rank	Indicator Name	Indicator Type	Current Click Rate	Previous Click Rate	Templates with this Indicator

5. Performance Over Time

The following table shows up to the previous 5 cycles and their corresponding start date, end date, target count, overall click rate, and overall time to first click. This can indicate whether overall trends are positive or negative.

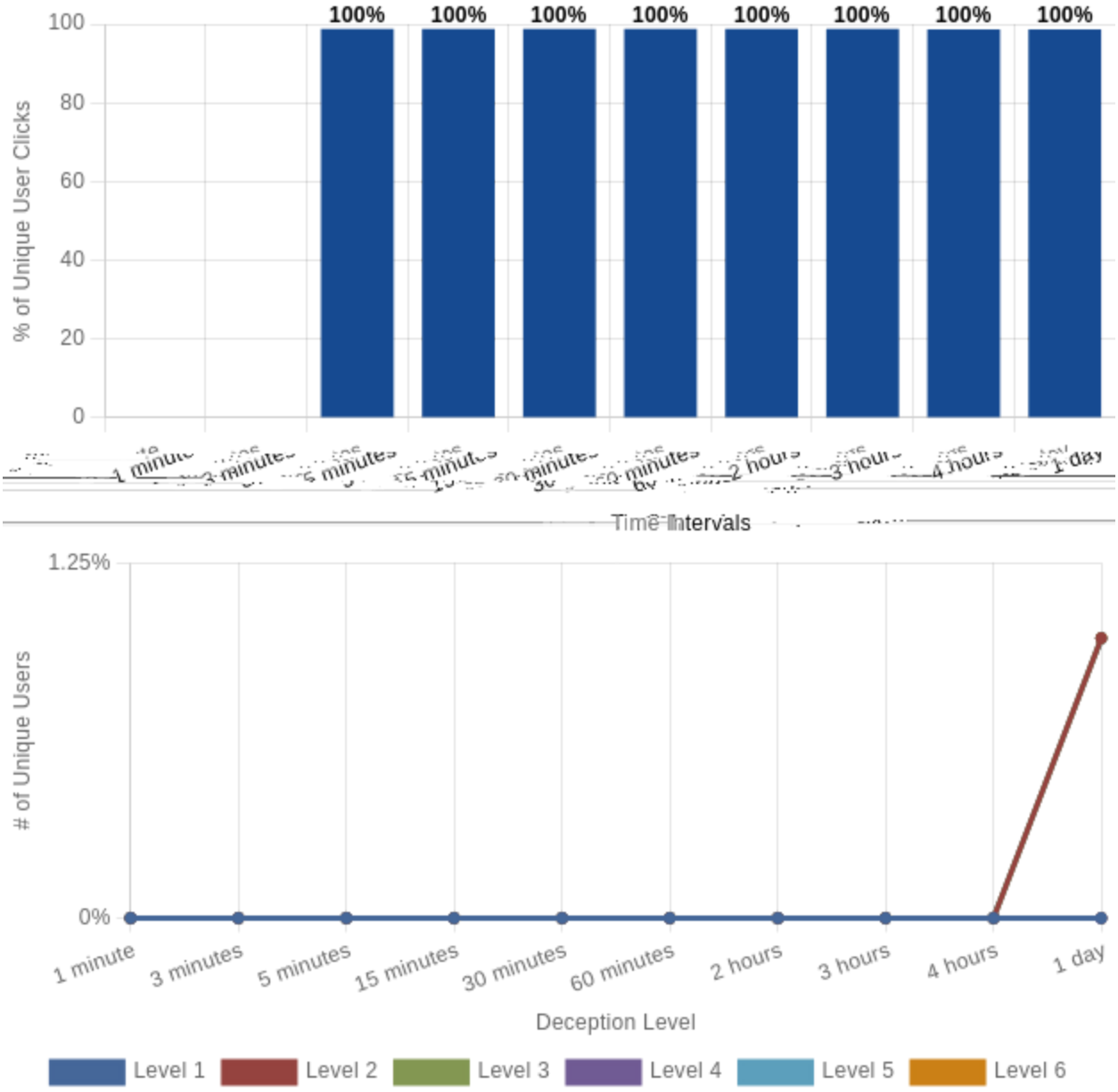
Cycle	Start Date	End Date	Targets	Click Rate	Click Time (HH:MM:SS)
Cycle #1	Aug 03, 2022	Nov 01, 2022	100	50.0%	00:00:05:00
Cycle #2	Aug 03, 2022	Nov 03, 2022	4	0.0%	00:00:00:00
Cycle #3	Aug 03, 2022	Nov 03, 2022	4	200.0%	-20:23:35:31
Cycle #4	Aug 23, 2022	Nov 21, 2022	100	56.0%	00:00:05:00

The following chart represents the average click rate across the three different deception levels (low, moderate, high). This is a good indication to see how click rates are improving based on the quality of the sent template.



6. Time Intervals

The figure below shows the percentage of users who clicked during certain time intervals in the first 24 hours of being sent a phish. Overall, nearly 100.0 percent of all clicks occurred within one hour of receiving a phishing email. The median time to click was 5 minutes.



7. Phishing Templates for this Cycle

Template #1 - Social Media Policy

Subject: Important Update to Social Media Policy
From: Social Media Compliance Team <SMCT@mg.inltesting.xyz>

All Staff:

In the coming weeks, new social media policies will be implemented that will affect all staff. Due to recent events in the news we are going to start blocking many of the popular social media sites for employees who do not need them for justified, business purposes.

We need your help to determine if you utilize social media and how you feel about this policy change. We have created a portal page on our internal network to get each employees usage of social media so we can determine which policy should be applied to your workstation. Please visit the Portal Page and complete this survey.

Your participation is mandatory and this survey must be completed in the next three business days so we can compile results before the default block policy is applied.

Thank you,
{{fake.first_name}}
Social Media Compliance Team

Deception Level:	High
Total Sent:	33
Unique Clicks:	21
Click Rate:	63.6%
Previous Cycle Click Rate for Level:	100.0%
CISA average click rate for level:	41.7%

Template #2 - Free iPad Giveaway

Subject: Free iPad Giveaway
From: Free Giveaways <info@mg.inltesting.xyz>

Want the new iPad Pro? I got mine free from this site here!!!!!

We would like to invite you to be part of a brand new pilot program to get our new product in the hands of users before official release. This assures that any issues or errors are fixxed before the release. If you are accept to participate in this program all we ask is that you submit a survey at
the end of the Pilot. You be able to keep iPad at the end for free!

Apples Customer Relationships Office Apples Campus, Cupertino, California 95114

Deception Level:	Low
Total Sent:	34
Unique Clicks:	18
Click Rate:	52.9%
Previous Cycle Click Rate for Level:	200.0%
CISA average click rate for level:	60.6%

Template #3 - Generic Test Template (Moderate)

Subject: Safelist Configuration Test
From: CISA <safelist-test@mg.inltesting.xyz>

{{target['email']}},

This is a test to verify your safelisting configuration. Please click the following link. You should see a "Don't Panic" Landing Page, or if it's outside of the testing timeline, you should see a generic "404 page not found" message.

{{url}}

Thanks,

CISA

Deception Level:	Moderate
Total Sent:	33
Unique Clicks:	17
Click Rate:	51.5%
Previous Cycle Click Rate for Level:	0.0%
CISA average click rate for level:	21.3%

Appendix A: Definitions

The following are definitions for terms found within the report.

- **Click Rate** is the total number of emails with "malicious" links that targets clicked at least once, divided by the total numbers of emails sent. Of the 100 emails sent, 56 users clicked the link at least once, an average click rate of 56.0%.
- **Click Time** is the time CISA sent the phishing email minus the time the user clicked the link within the email.
- **Average time to first click** is the average click time of the click time for each target that clicked a "malicious" link.

Appendix B: Red Flag Indicators

The following are definitions for **Red Flag** indicators.

- **Content irregularities -** Providing information throughout the message, in the display name, and the signature block that are inconsistent or contradictory.
- **Externally hosted resource -** Requiring the recipient to click an unfamiliar and externally hosted link when the message content is describing an internally hosted resource.
- **Generic greeting -** Not personally addressing the recipient for what looks to be a personalized message. A trusted organization will normally address the recipient by name and provide their contact information.
- **Generic signature -** Not providing organizationally relevant contact information in the signature block. A trusted organization or sender will typically provide their contact information or be verifiable through out-of-band information resources.
- **Generic terms -** Using generic phrases instead of known system names or office groups, and referencing topics and/or deadlines that cannot be verified by requesting confirmation from the related department points of contact or viewing website content.
- **Misplaced authority -** Using an authoritative tone but follows uncommon or unexpected business practices. Mature oganizations do not compel employees to circumvent established business process for the sake of speed or compliance.
- **Requirement to click -** Requiring the recipient to click a link to complete the request and not setting expectations as to where the link is hosted. A trusted organization would provide sufficient details about the request without requiring the recipient to follow links or download attachments if the message was unsolicited or unexpected.
- **Spelling and layout -** Unusually poor spelling and grammar in a supposedly automated message. Reputable institutions have dedicated personnel that produce, verify, and proofread customer correspondence.
- **Unfamiliar sender -** Using an unknown external sending address to send an internal message that should have come from the <<ORG DOMAIN>> or another known and trusted domain. Trusted organizations send from known domains or provide advance notice that a new domain will provide important communications to set expectations.
- **Unusual business process -** Citing non-compliance of a previously unknown requirement or document. A legitimate alert or notification would follow known processes, reference well-known requirements or documents, or be verifiable through trusted information resources.

Appendix C: Sophisticated Techniques

The following are definitions for **Sophisticated Techniques**.

- **Authoritative tone. -** Speaking from a place of power and stating that recipients are expected to respond may persuade the targeted user into clicking the link without first questioning it.
- **Context alignment. -** Attempting to appear organizationally relevant by speaking as a peer and work-related resources. Cybercriminals can use publically available information about organization's systems, personnel, leadership hierarchy, and tool sets to make their message look and feel legitimate.
- **Emotional triggers (CURIOSITY-QUESTIONS) -** Providing an opportunity to share opinions which may elicit feelings of curiosity on the types of questions asked. A cybercriminal may use a range of emotions to help persuade a user to click a link or open an attachment without examining it first.
- **Emotional triggers (FEAR/DUTY) -** Using a subject line or content that inspires feelings of fear or duty/obilgation to respond to motivate a response. A cybercriminal may use a range of emotions to help persuade a user to click a link or open an attachment without examining it first.
- **Emotional triggers (GREED) -** Offering opportunities for low effort financial gain that may trigger feelings of greed to motivate a response. A cybercriminal may use a range of emotions to help persuade a user to click a link or open an attachment without examining it first.
- **Spelling and layout -** Professional formatting and proper spelling and grammar to imitate reputable institutions that have dedicated personnel that produce, verify, and proofread correspondence.
- **Spoofed hyperlinks and websites. -** Hiding the externally-hosted link under hyperlinked text which requires the extra step of hovering over or long - pressing (on mobile phone) to investigate legitimacy. Additionally, cybercriminals may use a URL shortening service to hide the true destination of the link.

Appendix

Appendix E: Binding Operational Directive

Note to Customers on Binding Operational Directive (BOD) 22-01

November 3, 2021

Reducing the Significant Risk of Known Exploited Vulnerabilities

Pursuant to BOD 22-01 published on November 3rd, 2021, the Cybersecurity and Infrastructure Security Agency has developed and published a catalog of known exploited vulnerabilities.

While the BOD only requires action from federal civilian agencies, the catalog is provided for your awareness. CISA strongly recommends that private businesses and state, local, tribal, and territorial (SLTT) governments review and monitor the catalog and remediate the listed vulnerabilities to strengthen their security and resilience posture. Building collective resilience requires action across all stakeholders.

Thresholds and conditions for catalog updates:

CISA will update this catalog with additional exploited vulnerabilities as they become known, subject to an executive level CISA review and when they satisfy the following thresholds:

- The vulnerability has an assigned Common Vulnerabilities and Exposures (CVE) ID.
- There is reliable evidence that the vulnerability has been actively exploited in the wild.
- There is a clear remediation action for the vulnerability, such as a vendor provided update.

To report newly exploited vulnerabilities that are not in this catalog please email CISA Central at central@cisa.dhs.gov

For more information on this BOD please see cyber.dhs.gov - Binding Operational Directive 22-01 (https://cyber.dhs.gov/bod/22-01/)