ASSESSMENT SUMMARY

XXXXX

NUMBER

September 1, 2018

DATE

Phishing Campaign Assessment Summary

Office of Example

NCCIC

Phishing Campaign Assessment Details	
Customer Name	OFFICE OF EXAMPLE (EXAMPLE)
Customer POC	John Doe, Email@EXAMPLE.gov
NCATS Team Lead	Federal Lead, Email@hq.dhs.gov
Dates	June 4, 2018 to July 13, 2018
Test Location	DHS/NCATS Lab
Scope	1000 users within the following domain: @EXAMPLE.gov
Services	Phishing Campaign Assessment
NCATS ID	XXXXX

Revision History			
Version	**Date**	**Author**	**Notes**
1.0	06/04/2018	Federal Lead, DHS	First draft
1.1	07/02/2018	John Doe	Agency Review and Comment
2.0	07/16/2018	Federal Lead, DHS	Final Report

Table of Contents

Executive Report

This report provides the results for the Department of Homeland Security (DHS) National Cybersecurity Assessments and Technical Services- (NCATS) led Phishing Campaign Assessment (PCA) for OFFICE OF EXAMPLE (EXAMPLE). The PCA is a practical exercise intended to support and measure the effectiveness of security awareness training for information system users. The results of this PCA show the susceptibility of EXAMPLE personnel to social engineering attacks—specifically email phishing attacks—in which an adversary tricks an email user into clicking a malicious link to gain unauthorized network access. In the scenario that this PCA tested, the phishing attack bypassed technical controls that would normally detect and/or block malicious emails and links. The PCA, therefore, measured EXAMPLE's level of vulnerability to a successful phishing attack by targeted user click rates, click times, response rates, and response times, as shown in Table 1.

This report aims to enhance EXAMPLE's understanding of their information system users' cybersecurity behavior and to promote a more secure and resilient workforce.

Table 1: Targeted User Measurements

User Activity Metrics	Results
Total users targeted for phishing	1000
# of emails (phishing attempts) sent overall	2000 (*2 per user*)
# of clicked emails (successful phishing attempts) overall[1]	219 (*10.95% click rate*)
# of phished users overall[2]	203 (*20.3% of target population)*
# of user reports sent to helpdesk overall[3]	148 (*7.4% report rate*)
Ratio of reports-to-clicks	.68
Average time to first click[4,5]	0 hours 52 minutes 41 seconds
Average time to first report[6]	0 hours 30 minutes 25 seconds
Most successful phishing template	Level 6 "Updated Paycheck System Policy"

NCATS has provided this PCA to EXAMPLE at no cost and coordinated all activities—including planning and testing–with EXAMPLE's point of contact. EXAMPLE maintained control over the testing, including providing target email addresses, approving phishing email templates, approving testing timeframes, and adjusting mail security setting to ensure inbox access. This PCA was not intended to, and did not, test technical controls or electronic protections designed to block phishing attempts. This PCA spanned a six-week period and aimed to capture behavior-based metrics of EXAMPLE information system users' reaction to phishing emails of multiple complexity levels.

[1] Click rate is the total number of phishing emails that users clicked on divided by the total number of emails sent. Users had to click on the "malicious" link in the email in order to be counted as "phished."

[2] There were 203 users who clicked a "malicious" email link at least once by the end of the PCA out of the 1000 that were phished. There were 16 users who clicked in more than one campaign.

[3] Reporting rate is total number of user reports to the helpdesk divided by total phishing emails sent.

[4] Average time to first click and first report is calculated with geometric mean to compensate for a small sample size that is sensitive to being skewed by outliers.

[5] Click time is the time NCATS sent the emails minus the time user clicked the link within the email.

[6] Report time is the time NCATS sent the emails minus the time user alerts security office or helpdesk.

NCATS has established this voluntary service to help organizations

- support security awareness training efforts and
- decrease information system user vulnerability to phishing attempts.

Based on the assessment data, NCATS recommends implementing the following:

Table 2: Recommendations

Summary Recommendations
[Recommendation 1]
[Recommendation 2]
[Recommendation 3]

The remainder of this report provides findings and metrics of the NCATS phishing service for EXAMPLE.

EXAMPLE Methodology Specifics

NCATS used the methodology documented in Appendix A: Methodology to perform testing EXAMPLE. Specific phishing templates can be reviewed in Appendix C: Templates with corresponding complexity calculations. NCATS divided the 1000 email addresses that EXAMPLE provided into three groups. Group 1 had 333 addresses and received levels 1 and 4. Group 2 had 333 addresses and received levels 2 and 5. Group 3 had 334 addresses and received levels 3 and 6. See Table 3 for descriptions of email levels 1 – 6.

The assessment's goal was to capture the behavior-based responses of EXAMPLE to email phishing attempts; and the assessment operated under the scenario that no technical controls were able to detect, report, or stop the email phishing attempts. NCATS, as an external body conducting this PCA, did not have direct knowledge whether or not emails successfully arrived in targeted EXAMPLE user inboxes. To allow for a clear determination of click rates (email links clicked divided by emails sent), EXAMPLE or NCATS performed the following:

- EXAMPLE whitelisted the NCATS domain and IP address during the planning stage.
- EXAMPLE created specific mail receiving rules to permit the NCATS emails to land in user inboxes

Summary of Testing Activities and Results

This PCA concentrated on how phishing email complexity affected EXAMPLE user click behavior and response behavior. NCATS expects that a more complex and deceptive phishing email has a higher likelihood of being clicked and a lower likelihood of being reported. This assessment also gathered organizational emails through open-source intelligence techniques to determine EXAMPLE's potentially attackable online presence. See Appendix B: Detailed Results for detailed phishing and customer email data and Appendix C: Templates for a detailed explanation on complexity levels.

Over six weeks, EXAMPLE's targeted users received at least two phishing emails of increasing complexity. Levels 1 – 3 were "easier to detect" and levels 4 – 6 were "more difficult to detect," based on the number and type of indicators used. The table below summarizes the phishing templates used in this PCA.

Table 3: Email Template Overview

Level	Campaign	Description	Displayed Link
1	Store Error	Poorly worded email coming from a fake company describing a previous purchase error	*www[.]purchaseerror22992.com*
2	Urgent Software Update	Reasonably worded email from "IT Solutions Co" stating computer software is out of date	*www[.]immediateupdates.net*
3	Important Feedback Requested	Reasonably worded email from "HR Services" Requesting Feedback on a new program.	*www[.]requestedfeedbackprogram.com*
4	News Subscription Alert	Well-worded email from a local news source asking individuals to view news articles or requesting users unsubscribe if they wish.	*http[:]//www.localbreakingnews.biz/*
5	Upcoming Parking Program Survey	Well-worded, urgent email from "Human Resources" about a mandatory survey	*www[.]EXAMPLElink.net/SurveyID=18209/*
6	Updated Accounting System Policy	Well-worded, informational email from an internal financial office describing relevant accounting system updates	*www[.]sharepoint.EXAMPLE.com/accountingsystempolicy/*

Click Rate vs. Report Rate

One of the most common measures of an organization's susceptibility to phishing attacks is targeted-user click rates. If an actual phishing attack is able to bypass technical controls and arrive in a user's inbox, the human target must agree to click on the malicious link or attachment for the attack to be successful. In practical exercises such as this PCA, targeted-user click rates will fluctuate depending on the email complexity used in testing. Effective security awareness training, however, should result in a noticeable click rate decrease over time and to a level deemed acceptable based on the organization's risk management posture.

The counterpart to user click rates is the user-reporting rate, determined by the number of emails sent or calls to alert EXAMPLE's helpdesk during each campaign. Based on previous testing, NCATS recommends that organizations aim to have two people reporting the phishing attempts for every person that clicks. This ratio ensures that there is not only reporting coverage for the person clicking, but also redundant coverage in case the person who clicks the link does not report or does not realize they have been phished. Effective security awareness training should result in a noticeable report rate increase over time and to a level deemed acceptable based on the organization’s risk management posture.

In this report, the percentages shown by the user click rate and user report rate represent, respectively, the percentage of targeted people (determined by a unique email address) who have clicked at least once on a “malicious” link and those who reported a suspicious email. The number of unique clicks correlates to the number of end user devices potentially compromised in each campaign. The number of user reports correlates to the number of opportunities the EXAMPLE security team had to identify a potential breach and reduce its impact. Table 4 and Figure 1 summarize click and report rates.

Table 4: Unique User Click Rate and Report Rate Results

Level	Campaign	User Click Rate	Unique Clicks	User Report Rate	User Reports	Reporting Ratio
1	Store Error	3.60%	12	13.81%	46	3.83
2	Urgent Software Update	1.20%	4	4.20%	14	3.50
3	Important Feedback Requested	11.08%	37	9.58%	32	.86
4	News Subscription Alert	12.01%	40	11.41%	38	.95
5	Upcoming Parking Program Survey	11.11%	37	3.60%	12	.32
6	Updated Accounting System Policy	26.65%	89	1.80%	6	.07

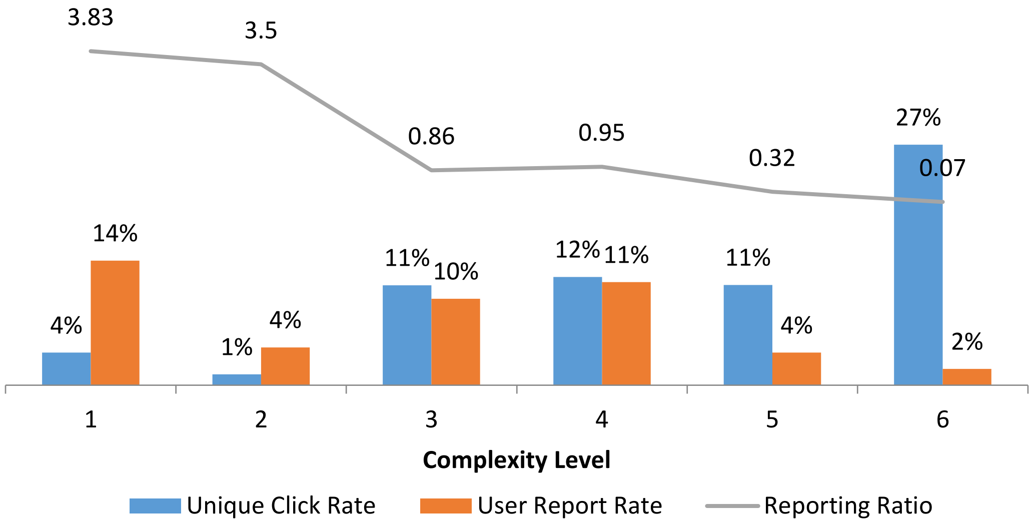


Figure 1: Unique User Click Rate vs. Report Rate per Level of Complexity.

Click Time vs. Report Time

To contain an attack, an organization's security team must be aware of the potential breach. In the scenario that this PCA tested, no technical controls were triggered during a phishing attack and the clock for a potential breach started once a targeted user clicked on a "malicious" link. Timely user reporting decreases the window of opportunity that an adversary has to access data or gain further network entry. Timely reporting also increases the opportunity the security team has to detect and respond to a potential breach. By educating users on how to both spot and promptly respond to phishing attempts, an organization can improve their anti-phishing defenses.

The following table details the time to first click and first report throughout the assessment and the lead or lag times for incident response measures to be activated (time elapsed represented in hours:minutes:seconds).

Table 5: Click Time vs. Report Time

Click Time vs. Report Time (HH:MM:SS)			
Level	**Time to First Click**	**Time to First Report**	**Time Gap (Lead or Lag)**
1	3:25:00	0:01:00	3:24:00 (LEAD)
2	1:19:00	5:03:00	20:16:00 (LEAD)
3	0:21:00	3:42:00	3:21:00 (LAG)
4	0:09:00	0:23:00	0:14:00 (LAG)
5	6:03:00	2:08:00	3:55:00 (LEAD)
6	0:01:00	0:04:00	0:03:00 (LAG)

The figure below shows the percentage of users who clicked during certain time intervals in the first 24 hours of a campaign. Overall, nearly 67 percent of all clicks occurred within one hour of receiving a phishing email. The median time to click was 2 hours, 4 minutes, and 37 seconds across all campaigns.

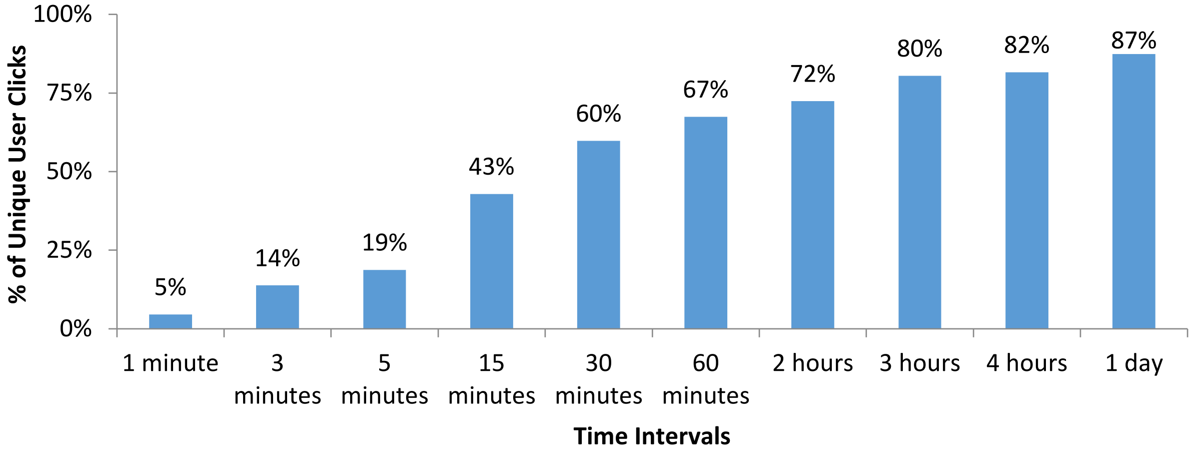


Figure 2: Timeline of Unique User Clicks Across All Levels

Figure 3 shows the amount of time for the first user to click on a link in an email from the time it was sent (elapsed time displayed as hours:minutes:seconds).

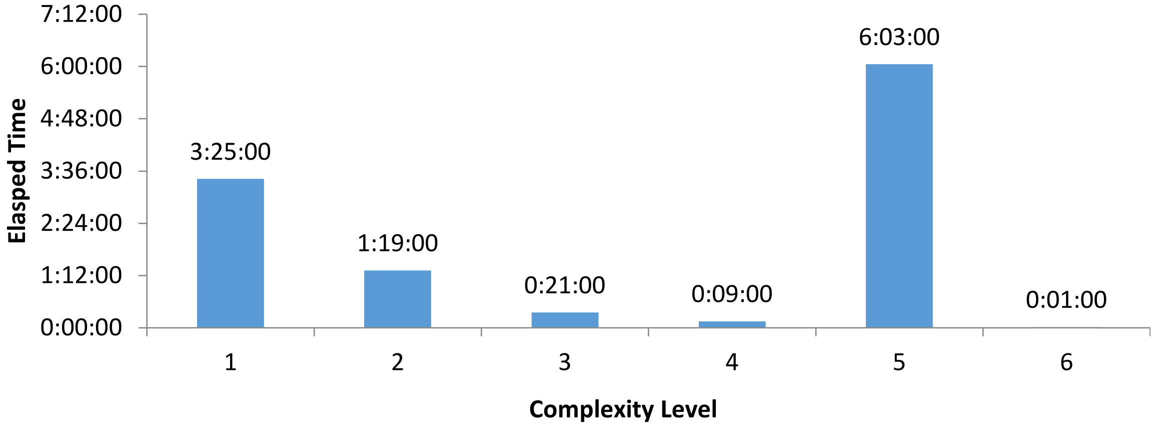


Figure 3: Time to First Click (HH:MM:SS)

Open-Source Intelligence Gathering

Information stored on the public Internet can be used to an adversary's advantage in planning for a cyber attack. An individual can perform passive reconnaissance (reviewing publicly available information) or active reconnaissance (direct interaction) to build a profile of their target and learn where potential weaknesses exist.

The following is a non-exhaustive list of information that may be found online and is not necessarily representative of the information found on the EXAMPLE website:

- employee information
  - names
  - emails
  - phone numbers
  - titles
  - addresses
  - usernames
- security policies
  - password complexity
  - physical security
- network information
  - IP ranges
  - domain names (naming convention)
- job announcements to identify technologies used within your organization
- user-generated content
  - company blogs
  - project presentations
  - whitepapers

For this PCA, NCATS looked for EXAMPLE email addresses publically available online. The following email addresses were discovered through passive reconnaissance and collected using open-source information gathering tools. The emails NCATS discovered were not used in this engagement unless previously provided by the technical POC. See Appendix B: Detailed Results for a complete enumeration of discovered emails.

Table 6: Email Reconnaissance Results

Item	Result
Email domain searched	EXAMPLE.gov
Date search performed	August 18, 2018 15:18 EST
# Unique email addresses found	25
# Matching list of user emails provided by EXAMPLE	7 (0.7%)

Based on previous testing, most of email addresses discovered during passive reconnaissance are sourced from organizational documents and presentations shared online. To limit the exposure of exploitable organizational information, NCATS recommends that employee names and emails be limited in use on websites and in reports or presentations stored on the public Internet. When announcing new products or updating online registrations, NCATS also recommends that organizations use generic distribution email address as opposed to specific employee names.

Closing

[Detailed Conclusion 1 – Assessment Summary]

[Detailed Conclusion 2 – Click Rates and Click Times]

[Detailed Conclusion 3 – Reporting Rates and Reporting Times]

[Detailed Conclusion 4 – Open Source Intelligence]

PCA is a young service with limited but meaningful data made available to EXAMPLE. NCATS hopes this data will be actionable and allow EXAMPLE to reduce some level of risk within their organization. As more PCAs are completed over time, statistical reporting will be enhanced and a non-attributable overview of phishing results will be collected as part of the NCATS annual service review.

As this new service continues to mature, NCATS looks forward to enhancing the PCA and building new test capabilities that include technical control checks. NCATS appreciates any comments to improve this report or service as a whole. For questions about this report or for future engagements with NCATS, please send an email to ncats_info@hq.dhs.gov.

Appendix A: Methodology

[Methodology details]

Appendix B: Detailed Results

Appendix B is a listing of detailed results collected throughout testing.

> **Sample Report Note:** *This section includes multiple detailed results, charts, and graphs. Although not all statistical data which is provided with an actual PCA is shown below, a few main charts are displayed to provide a sample.*

The table below shows a breakout of weekly click rates captured, and report rates EXAMPLE collected and submitted to NCATS through testing.

Table 7: Weekly Click and Report Results

Level	Campaign	Emails Sent	Total Clicks	Unique User Clicks	User Click Rate	User Reports	User Report Rate
1	Store Error	333	14	12	3.60%	46	13.81%
2	Urgent Software Update	333	8	4	1.20%	14	4.20%
3	Important Feedback Requested	334	42	37	11.08%	32	9.58%
4	News Subscription Alert	333	45	40	12.01%	38	11.41%
5	Upcoming Parking Program Survey	333	39	37	11.11%	12	3.60%
6	Updated Accounting System Policy	334	113	89	26.65%	6	1.80%

Figure 4 shows the comparison of unique clicks, total clicks, and reports per level of complexity.

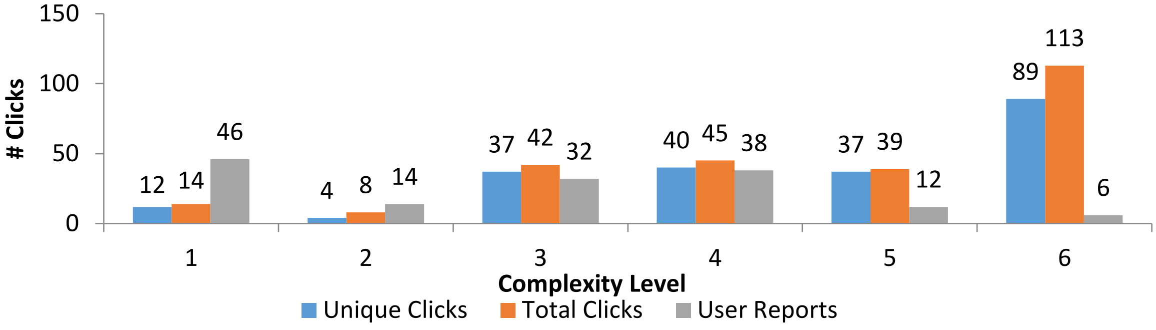


Figure 4: Unique Click, Total Click, and Report Results by Level

Sample Report Note: *For all assessments, additional results, charts, graphs, and figures include (but are not limited to):*

- *The number of users who clicked once, 2-3 times, 4-5 times, 6-10 times, and more than 10 times per campaign, broken down by complexity level.*
- *The time-related event log throughout testing, including time to first click, length of campaign (days), etc.*
- *The percentage of users who had clicked at least once by certain time intervals for each of the six complexity levels.*
- *The percentage of clicks for each tested complexity category and indicator. For example, in the behavior category, the fear indicator had an X percent unique click rate—or, X percent of all emails sent with a behavior - fear indicator were clicked at least once.*

The table below shows the number of unique email clicks, the percentage of total emails sent to office, and the percentage of all unique clicks gathered by the top clicking "Office" designations provided by EXAMPLE. All other offices are listed in the "Other" category.

Table 8: Unique Clicks per "Office"

Office	Office Count	Unique Office Clicks	Total Office Clicks	Percent of Office that Clicked	Percent of All Unique Clicks from Office
A	210	43	50	20.48%	19.63%
B	119	29	32	24.37%	13.24%
C	97	28	28	28.87%	12.79%
D	88	25	36	28.41%	11.42%
E	56	12	15	21.43%	5.48%
Other	430	82	100	19.07%	37.44%

Sample Report Note*: If specific "Office" or "Department" designations are provided, additional results, charts, graphs, and figures include (but are not limited to):*

- *The number of unique email clicks, the percentage of total emails sent to office, and the percentage of all unique clicks gathered by the top clicking "Office" designations provided by EXAMPLE.*
- *The numbers of clicks for each level belonging to the different "Office" designations.*
- *The percentage of each "Office" that clicked by level. The percentage is relative to individual "Office" totals and not a percentage of the whole of EXAMPLE. For example, X percent of Office A clicked on Level 2.*
- *The number of unique clicks (and percentage of unique clicks) by complexity level per "Office." For example, X percent of all clicks in Level 6 came from Office A.*

The table below is a detailed list of the email addresses ending in the provided domain(s) discovered through passive email reconnaissance along with source descriptions.

Table 9: Email Reconnaissance Results

#	Email	Email Source
1	ABC1@EXAMPLE.GOV	*[Source 1]*
2	ABC2@EXAMPLE.GOV	*[Source 2]*
3	ABC3@EXAMPLE.GOV	*[Source 1, 2]*
4	ABC4@EXAMPLE.GOV	*[Source 2]*
5	ABC5@EXAMPLE.GOV	*[Source 3]*
6	ABC6@EXAMPLE.GOV	*[Source 1,4]*

Table 10: Email Reconnaissance Source Descriptions

Source	Description
[Source 1]	*[Description 1]*
[Source 2]	*[Description 2]*
[Source 3]	*[Description 3]*
[Source 4]	*[Description 4]*

Appendix C: Templates

The phishing templates used throughout this service include six levels of varying complexity. Each level is based on a calculation of the factors designed to entice users to click on a malicious link. An explanation of the four factors used when determining an email's level of complexity can be found in *C1: Complexity*. The following defines key differences between each level:

[Level descriptions]

Appendix C2: Engagement Specific Templates

Below are the details about the templates used during PCA with EXAMPLE. The complexities are shown in the table below.

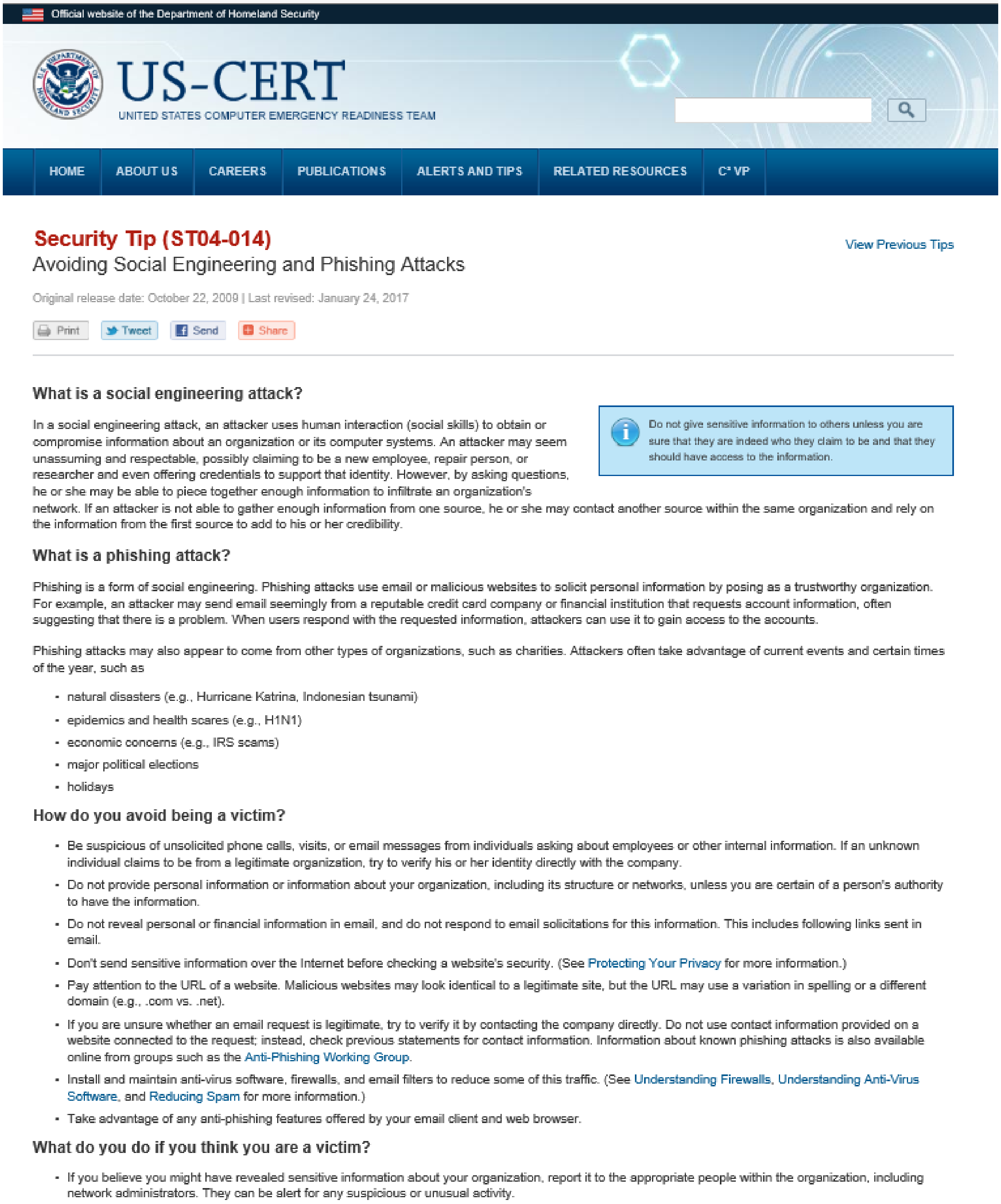
*[**Sample Report Note**: after an assessment, a text version or screenshot of each email template is provided below the table.]*

Table 11: EXAMPLE Phishing Email Template Complexity Rating Calculator

Phishing Email Template Complexity Rating Calculator			Store Error	Urgent Software Update	Important Feedback Requested	News Subscription Alert	Upcoming Parking Program Survey	Updated Accounting System Policy
Category	**Indicator**	**Ranking Scale**						
Appearance	Grammar	0=Poor, 1=Decent, 2=Proper	0	1	1	2	2	2
	Link Domain	0=Fake, 1=Spoofed/Hidden	1	0	0	1	0	1
	Logo/Graphics	0=Fake/None, 1=Spoofed/HTML	0	0	0	0	0	0
Sender	External	0=Fake/NA, 1=Spoofed	0	1	1	0	0	0
	Internal	0=Fake/NA, 1= Unknown Spoofed, 2= Known Spoofed	0	0	0	0	1	2
	Authoritative	0=None, 1=Corporate/Local/Mid-Level, 2=Federal/State/Upper-Level	0	0	0	0	1	0
Relevancy	Organization	0=No, 1=Yes	0	0	1	0	1	1
	Public News	0=No, 1=Yes	0	0	0	1	0	0
Behavior	Fear	No Score	X					
	Duty or Obligation	No Score		X	X		X	
	Curiosity	No Score			X	X		
	Greed	No Score						X
		Total	**1**	**2**	**3**	**4**	**5**	**6**

Appendix D: Landing/Redirect Page

[URL OF LANDING PAGE] **Example:** https://www.us-cert.gov/ncas/tips/ST04-014
[SCREEN SHOT OF LANDING PAGE] **Example:**



Security Tip (ST04-014)

Avoiding Social Engineering and Phishing Attacks

Original release date: October 22, 2009 | Last revised: January 24, 2017

What is a social engineering attack?

Do not give sensitive information to others unless you are sure that they are indeed who they claim to be and that they should have access to the information.

In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility.

What is a phishing attack?

Phishing is a form of social engineering. Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization. For example, an attacker may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.

Phishing attacks may also appear to come from other types of organizations, such as charities. Attackers often take advantage of current events and certain times of the year, such as

- natural disasters (e.g., Hurricane Katrina, Indonesian tsunami)
- epidemics and health scares (e.g., H1N1)
- economic concerns (e.g., IRS scams)
- major political elections
- holidays

How do you avoid being a victim?

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- Don't send sensitive information over the Internet before checking a website's security. (See Protecting Your Privacy for more information.)
- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group.
- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic. (See Understanding Firewalls, Understanding Anti-Virus Software, and Reducing Spam for more information.)
- Take advantage of any anti-phishing features offered by your email client and web browser.

What do you do if you think you are a victim?

- If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators. They can be alert for any suspicious or unusual activity.

Appendix E: Acronyms

DHS	Department of Homeland Security
NCATS	National Cybersecurity Assessments and Technical Services
NCCIC	National Cybersecurity and Communications Integration Center
PCA	Phishing Campaign Assessment
POC	Point of Contact
ROE	Rules of Engagement