From Victims to Defenders: An Exploration of the Phishing Attack Reporting Ecosystem

Zhibo Sun
Drexel University
Philadelphia, Pennsylvania, USA
zs384@drexel.edu

Faris Bugra Kokulu
Arizona State University
Tempe, Arizona, USA
fkokulu@asu.edu

Penghui Zhang
Arizona State University
Tempe, Arizona, USA
pzhang57@asu.edu

Adam Oest
Arizona State University
Tempe, Arizona, USA
aoest@asu.edu

Gianluca Stringhini
Boston University
Boston, Massachusetts, USA
gian@bu.edu

Tiffany Bao
Arizona State University
Tempe, Arizona, USA
tbao@asu.edu

Ruoyu Wang
Arizona State University
Tempe, Arizona, USA
fishw@asu.edu

Yan Shoshitaishvili
Arizona State University
Tempe, Arizona, USA
yans@asu.edu

Adam Doupé
Arizona State University
Tempe, Arizona, USA
doupe@asu.edu

Gail-Joon Ahn
Arizona State University
Tempe, Arizona, USA
gahn@asu.edu

ABSTRACT

Reporting phishing attacks can significantly shorten the time required to take down their operations and deter further victimization by the same phishing websites. However, little research has been conducted to understand the phishing reporting ecosystem and its effectiveness. In this paper, we comprehensively evaluate the phishing reporting ecosystem to identify the critical challenges people face and their concerns when reporting smishing, vishing, and phishing email attacks. First, we analyze the existing security advice and channels for reporting phishing attacks in both the public and private sectors. Then, we conduct a scenario-based experiment involving 89 participants to investigate what factors affect a participant's decision to report a phishing attack and what challenges they face in preparing the report. Third, we report phishing attacks ourselves and monitor the status of the reported phishing websites to empirically measure how reports are acted upon and how that affects the reported phishing websites. Finally, we propose approaches under five major concern categories to mitigate the challenges that we discover in the phishing reporting ecosystem.

CCS CONCEPTS

• **Security and privacy → Human and societal aspects of security and privacy**; **Usability in security and privacy**.

RAID 2024, September 30–October 02, 2024, Padua, Italy

ACM ISBN 979-8-4007-0959-3/24/09
https://doi.org/10.1145/3678890.3678926

KEYWORDS

Phishing Attack Reporting, Anti-phishing Strategies, Smishing, Vishing, Phishing Reporting Challenges

ACM Reference Format:
Zhibo Sun, Faris Bugra Kokulu, Penghui Zhang, Adam Oest, Gianluca Stringhini, Tiffany Bao, Ruoyu Wang, Yan Shoshitaishvili, Adam Doupé, and Gail-Joon Ahn. 2024. From Victims to Defenders: An Exploration of the Phishing Attack Reporting Ecosystem. In *The 27th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2024), September 30–October 02, 2024, Padua, Italy*. ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/3678890.3678926

1 INTRODUCTION

Phishing, one of the most prevalent types of cyber attacks [51], uses social engineering to lure victims into disclosing sensitive information such as Personally Identifiable Information (PII) or account credentials [8, 56]. The resulting impact can be crippling, leading to significant financial [22], political [32], and even national security [28] harm. Additionally, phishing occurrences are also *growing*: the FBI received more phishing complaints than any other type of cybercrime in 2022, increasing nearly eleven times compared to 2018 [13]. Moreover, phishing attacks have evolved beyond just email. In 2019, 84% of organizations faced smishing attacks (phishing over SMS), and 83% faced vishing (phishing over voice calls) [39].

Researchers have proposed many technical approaches for detecting phishing attacks [10, 12, 40, 55, 57], while numerous phishing messages still bypass detection systems and reach users. As a result, various awareness training frameworks have been developed to educate users, the weakest link in defending against phishing [3], how to recognize and avoid falling victim to phishing

attacks. Although these training programs have proven somewhat effective [5, 6, 10, 26, 30], the phishing websites themselves can remain active for hours or even days before being blocked, creating a window of opportunity for phishers to victimize less cautious users [4, 35].

To enhance the existing anti-phishing ecosystem and expedite the blacklisting of phishing websites, *manual reporting* of phishing attacks is an effective approach [37]. It alerts security teams about emerging phishing campaigns, facilitates the analysis of evasive phishing methods, and promotes proactive measures, mitigating potential damages.

However, the rate of phishing attack reporting is surprisingly low: Prior research has found that a typical phishing website will only be reported after 27 visits [35]. Moreover, 93% of employees did not report company-targeted phishing emails that they encountered in a phishing test [48], that 95% of phishing emails were not reported within one week after employees completed phishing awareness training [50]. Understanding the reasons behind the low rate of phishing reporting (and *increasing* this rate) is critical to ensure the efficacy of anti-phishing efforts across the ecosystem.

Why do many people not report the phishing attacks that they encounter? To answer this question, we conduct the first comprehensive evaluation of the current phishing reporting ecosystem to identify key challenges and concerns people face when reporting smishing, vishing, and phishing email attacks. We perform three studies to investigate the ecosystem from three different perspectives, from preparation to post-reporting: (1) what options the reporting ecosystem provides to individuals who wish to report phishing attacks (Study I), (2) what the actual experience is in preparing to report a phishing attack (Study II), and (3) what happens to phishing websites after reporting, and what feedback is conveyed to reporters (Study III). Additionally, we offer actionable suggestions to address current shortcomings in the phishing reporting ecosystem based on our findings. Note that we did not specifically explore spear-phishing because our research aims to investigate the challenges in the publicly accessible reporting ecosystem, rather than the likelihood of being fooled by phishing messages. We summarize our findings in the following paragraphs.

In Study I (§3), we summarize the search term patterns used to search reporting channels and apply 1,209 generated search terms to collect security advice most likely to be accessed by the general public provided by U.S. government agencies, nonprofit anti-phishing organizations, and Fortune 100 companies. We then conduct a qualitative analysis of the collected anti-phishing security advice and reporting channels to identify challenges associated with these reporting systems. For example, we discover that reporting to government entities may not be practical for resolving a reporter's problem because these entities do not act on individual cases.

In Study II (§4), we conduct a scenario-based experiment to study participants' experiences and investigate their key concerns when preparing to report phishing attacks. By answering three questions using both qualitative and quantitative analysis methods, we find that the concern of poor feedback or the lack of a clear outcome is the primary reason that discourages people from reporting phishing attacks to companies.

In Study III (§5), we launch synthetic phishing websites that mimic several companies' websites, report these "attacks," and monitor the status of the reported phishing websites to study the difficulty of reporting, the status of reported phishing websites, and responses from entities after reporting. We find that many companies that received our reports did *not* act on them: 28.5% of reported synthetic phishing websites were never accessed or scanned. Moreover, only 13.9% of all reported phishing websites were blocked.

Finally, by considering all findings, we propose mitigations under five areas of concern identified in the studies: *Reporting Outcome, Reporting Cost, Reporting Channel Choice, Reporting Criteria,* and *Personal Reason* (§6).

It is worth noting that reporting attacks to different entities (e.g., to the companies being impersonated versus to a government agency) can serve different purposes, and different philosophical stances exist on the value of these reporting channels. Our goal is not to evaluate or determine the most effective reporting entities, the reasons for reporting phishing attacks to particular entities, or the most effective reporting methods (e.g., reporting the malicious URL or phishing email) in this study, but to take the first step to shed light on this often-ignored section of the phishing defense pipeline within the current reporting ecosystem.

Contributions. This paper makes the following contributions:

- We conduct the first comprehensive evaluation of the phishing reporting ecosystem for smishing, vishing, and phishing email attacks.
- We identify challenges and concerns people face when preparing to report phishing attacks, which have been overlooked thus far.
- We evaluate the effectiveness of reporting phishing attacks and discuss the reporting aftereffects.
- We present approaches to mitigate the challenges identified in the phishing reporting ecosystem.

2 BACKGROUND AND RELATED WORK

Phishing is a social engineering attack [25, 33] that seeks to lure victims into disclosing their sensitive information by entering credit card numbers on fake websites, opening malicious attachments in phishing emails, and replying to phishing messages [8, 18, 51, 57]. Based on how phishing messages are delivered, there are three major types of phishing attacks: phishing email, smishing, and vishing attacks [56].

Phishing Email Attacks. Phishing email attacks are the most common type of phishing attack in which scammers send phishing messages through email to victims [51]. By taking advantage of various social engineering tactics, such as "urgency" [18], scammers deceive victims into logging in to a well-crafted fake webpage of a popular website, such as Facebook, to steal their account credentials.

Smishing Attacks. Smishing is a popular type of phishing attack [39], where phishing messages are delivered through a Short Message Service (SMS) on mobile devices [56]. Smishing attacks deceive people into performing similar actions to phishing email attacks by visiting a fake website, replying with sensitive information, or downloading a malicious mobile application. Due to the small size of the mobile device, it is difficult for people to check

whether a webpage is legitimate from URLs [42], and a study shows that 70% of people do not know of smishing attacks [39].

Vishing Attacks. By leveraging Voice over Internet Protocol (VoIP), scammers can deliver phishing messages through voice to socially engineer victims into disclosing their sensitive information, such as Social Security Numbers [44, 56]. Rather than directing victims to a fake webpage, scammers frequently provide a pretext that makes victims feel comfortable and obliged to divulge their confidential information [21, 41]. Additionally, researchers have shown that targeted vishing attacks are effective against real-world users [45].

Human-Centric Efforts on Anti-Phishing. Human subject research helps find effective defenses against phishing attacks [3]. Researchers explored authentic indicator designs to assist people in distinguishing phishing websites [12, 54, 55]. Moreover, human behaviors are studied in the context of phishing detection by analyzing people's neural activity [31], conceptual knowledge [7], and psychological factors that affect user decision-making [20]. Furthermore, researchers explore various phishing awareness training frameworks to educate people and decrease the likelihood of falling victim to phishing attacks [5, 6, 15, 30, 53].

Additionally, because reporting phishing attacks can shorten the time needed for detection and deter further victimization by the same phishing websites [35, 37], educating people to report phishing attacks is imperative. However, little effort is invested in this, resulting in a significantly low reporting rate (93% of employees did not report the phishing emails [48], and 95% of phishing emails were not reported within one week after phishing awareness training [50]). Although researchers investigated the reasons behind the low reporting rate using cognitive theory models [27], their study focuses on spear-phishing email attacks in business and lacks a comprehensive evaluation of the existing phishing reporting ecosystem. They do not disclose critical challenges people face or concerns when reporting phishing emails, smishing, and vishing attacks.

3 STUDY I: SURVEYING THE PHISHING REPORTING ECOSYSTEM

To investigate the phishing reporting ecosystem, we need to understand what mechanisms are offered to individuals seeking to report phishing attacks. To this end, we conduct a qualitative survey on the suggested security advice and the actual channels for reporting phishing attacks (phishing email, vishing, and smishing) from U.S. government agencies (Gov), nonprofit anti-phishing organizations (Org), and Fortune 100 companies, which are the top 100 companies in the United States.

3.1 Methodology

We first collected and analyzed security advice for reporting phishing attacks that can be found online. Next, we investigated reporting channels in Gov, Org, and companies identified from the security advice.

Identifying Search Terms. To collect security advice for reporting phishing attacks, which is more likely to be found and accessed by the public, from Gov, Org, and Fortune 100 companies, we recruited 175 US-based participants from Amazon Mechanical Turk (MTurk) [29, 38]. To have high-quality answers, we selected Master Workers as our participants [43].

> *Scenario:* suppose you are contacted by a **Phishing Text Message** that fraudulently claims to be from company **Apple** saying **"**We regret to inform you that your account has been restricted because of unusal activities. To continue using our services, please click the link to restore your account.**"**

Figure 1: Experimental scenario in Study I.

Table 1: Search terms in Study I (using Amazon as an example).

Search Type	Search Term Pattern	Example	Percentage
Non-targeted	Report *[PhishingAttackType]*	Reporting ***phishing email***	67.0%
	How to report *[PhishingAttackType]*	How can I report ***phishing email***	22.7%
	[PhishingAttackType]	***phishing phone call attacks***	10.3%
Targeted	*[CompanyName] [PhishingAttackType]*	***Amazon phishing email***	21.7%
	Report *[PhishingAttackType] [CompanyName]*	Reporting ***phishing email*** to ***Amazon***	57.1%
	[CompanyName] contact	***Amazon*** customer service	14.8%
	How to report *[PhishingAttackType] [CompanyName]*	how to report ***phishing emails*** to **emphAmazon**	6.3%

Users may give up their reporting attempt if they cannot locate the desired security advice in the first few search results, so understanding preferred search terms and search engines is crucial. Therefore, in the survey, participants were given a scenario, including a randomly assigned phishing attack type (e.g., phishing email attack, vishing, or smishing) and a company name (Figure 1), and answered four questions (Table 7 in Appendix B) to provide the search terms they would use while attempting to find phishing reporting tools on their search engine of choice.

After excluding 28 participants who provided low-quality answers, such as off-topic and irrelevant answers, we identified 286 search terms which we grouped into two categories: non-targeted search (without specific reporting targets in the search term, "Reporting phishing email") and targeted search (with specific reporting targets in the search term, "Amazon phishing"). We manually extracted search term patterns in each category (Table 1). By applying three types of phishing attacks (phishing email attack, smishing attack, and vishing attack) and Fortune 100 companies' names to the variables (*PhishingAttackType* and *CompanyName*) in search patterns, we generated a total of 1,209 possible search terms.

Fortune 100 Companies. We have opted to conduct our study on Fortune 100 companies due to their extensive customer reach, industry diversity, strong brand reputation, and robust anti-phishing resources. While this selection may not encompass the entirety of the phishing reporting landscape, it provides valuable insights from a corporate standpoint.

Selecting the appropriate companies presented challenges. We considered alternative options like industry-specific firms and high-traffic websites. Yet, we aim to study the overall reporting ecosystem, and attackers typically impersonate brands, not specific sites (e.g., mimicking Microsoft over Bing.com). Also, focusing solely on top phishing-targeted companies might miss some ecosystem intricacies. For example, individuals can still sometimes encounter

Table 2: Demographics and survey results in Study I (n=147).

	Variable	Metric	Percentage of Participants
Demographics	Age	18 – 29	9.5%
		30 – 49	76.9%
		50+	13.6%
	Gender	Female	46.3%
		Male	52.4%
		No Answer	1.4%
	Education	Up to Some College	23.1%
		Bachelor Degree	67.3%
		Advanced Degree	9.5%
Results.	Search Engine	Google	98.6%
		Bing	1.4%
		Yahoo!	0.0%
		Others	0.0%
	Max num of search results	Less than 10 search results	41.5%
		11 – 20 search results	51.7%
		21 – 30 search results	4.1%
		more than 30 search results	2.7%

phishing attacks masking as a well-known company in the healthcare industry but is not widely recognized by the general public, McKesson [47].

Fortune 100 companies often have many subsidiaries. We employed the following criteria to choose a brand that represents the company: (1) We choose the brand that shares the same name as the parent company. For instance, if a company like Amazon has subsidiaries such as Zappos and Ring, we will choose Amazon as our study brand. (2) We choose the US-based brand. For example, we study Walgreens for the Walgreens Boots Alliance. (3) If we cannot identify a brand for a particular company, we follow these steps: (a) apply the company name to the search term patterns identified in Study I to generate the search terms, (b) enter search terms in Google and collect the top 20 results, (c) if any of the US-based subsidiaries of the company appear in the results with reporting channel or phishing reporting advice, we will use that brand. If multiple brands appear, we will choose the one that provides a reporting channel. Otherwise, we will select the more recognizable brand for us.

Collecting Security Advice. We primarily collected security advice for reporting phishing attacks from official sources of Gov, Org, and companies because these entities are deemed authoritative.

Because *Google* was the most preferred search engine and 93.2% of participants would only read fewer than 20 search results before they stopped reporting based on our results (Table 2), we applied 1,209 search terms and scraped the top 20 results of each search from Google by running a scraper on five servers over two days. We then filter out web pages that are not from official websites by screening web pages whose TLDs are not "gov" or "org", and URLs are not affiliated with any company's domain. Lastly, we evaluated the remaining web pages manually to exclude irrelevant ones and ultimately identified 575 webpages containing reporting advice for phishing attacks from official sources.

Analyzing Security Advice. We analyzed the resulting security advice using a qualitative open coding process [24]. We first gathered the responses to one specific question we wanted to code in one place, and then two researchers reviewed each security advice in sets of 30 to build the coding book incrementally.

To measure the inter-coder reliability, the researchers reached a Krippendorff's α of 0.97, which is considered as a substantial agreement score [17] because of the simple and straightforward security advice on webpages. We provide our final codebook in Appendix A.

Phishing Reporting Channels. Two researchers independently examined all reporting channels identified from the analysis of security advice. To identify phishing reporting channels, we applied the following criteria: First, the reporting channels should be owned and operated by Gov, Org, or companies. Second, these reporting channels should be publicly accessible and dedicated to phishing reporting channels on their official websites (e.g., a dedicated phishing reporting email address or an online phishing reporting form). Thus, the contact information on their websites or their social networking accounts, which are not intended for use in reporting phishing attacks, was not included in the scope of the study, even though some people may go there to report phishing attacks.

Ethics. In close cooperation with our Institutional Review Board (IRB), we developed an experimental protocol that was approved for this study as it did not collect any Personal Identifiable Information (PII) about participants or pose any foreseeable risks to them.

Limitations. Although conducting experiments on MTurk is practical in cybersecurity research [43, 52] with high-quality results [9, 23], participants are generally younger and technical [49], which may affect the generalizability of the results. Additionally, we may miss some security advice on web pages not affiliated with a company's official website because one company may control multiple domains that we cannot fully enumerate. Moreover, solely based on the advice analysis, we cannot provide precise numbers regarding the scale of the challenges, such as the number of entities that do not provide feedback to reporters or resolve individual cases, as not every entity's advice will disclose such information. Therefore, it is important to note that these identified challenges (§3.3) indicate their presence in the corresponding sectors rather than existing in every entity investigated within those sectors.

3.2 Results

We present our analysis of security advice and the challenges we identified. Rather than criticizing specific entities, we examine the current state of the phishing reporting ecosystem and identify its critical challenges. Therefore, we anonymize names in this paper unless otherwise necessary. Considering the different interests in handling company-related phishing reports, we examine this from two perspectives: non-companies (Gov & Org) and companies.

3.2.1 Analysis of Phishing Reporting in Gov & Org. The analysis of security advice indicates that reporting channels exist in five main forms: email addresses, built-in functions of the software (e.g., clicking the "Report phishing button" in Gmail to report phishing emails), online complaint forms, SMS reporting numbers (e.g., forwarding a smishing message to 7726, which spells SPAM on a keypad), and talking with a person via phone call or live chat.

Table 3: Phishing reporting channels of different phishing attacks in Gov & Org and Company.

	Reporting Approach	Phishing Email	Smishing	Vishing
Gov & Org	Email (Forward the Message)	4	0	1
	Email (Send the Message as an Attachment)[a]	2	0	0
	Online Complaint Form	2	3	3
	Phone Call / Live Chat	0	1	1
	Built-in Function	0	0	0
	SMS Reporting Number	0	1	0
	Total	5	4	4
Company	Email (Forward the Message)	31	13	6
	Email (Send the Message as an Attachment)[a]	7	0	0
	Online Complaint Form	2	0	3
	Phone Call / Live Chat	5	2	2
	Built-in Function	6	2	1
	SMS Reporting Number	0	0	0
	Total	43	14	12

[a] Alternatively, forward the message with the email header information.

Table 4: Number of companies requesting to report to different Gov & Org reporting targets.

Reporting Target	Phishing Email (Victim[b])	Smishing (Victim[b])	Vishing (Victim[b])
FTC	19 (13)	14 (10)	15 (10)
FTC (spam@uce.com)[a]	9 (2)	1 (0)	2 (1)
CISA	2 (0)	1 (0)	0 (0)
IC3	6 (3)	5 (3)	5 (3)
FCC	0 (0)	0 (0)	1 (0)
SAGO	3 (1)	3 (1)	4 (1)
Police	4 (3)	2 (2)	4 (2)
SMS Reporting Num	0 (0)	3 (0)	0 (0)
APWG	7 (1)	2 (1)	2 (1)

[a] Alternative reporting approach of FTC.
[b] Number of companies request to report only when the reporter is a victim.

Additionally, we identified eight U.S. federal government sources and two anti-phishing organizations, which are Federal Trade Commission (FTC), Internal Revenue Service (IRS), Cybersecurity & Infrastructure Security Agency (CISA), FBI Internet Crime Complaint Center (IC3), Department of Homeland Security (DHS), Department of Justice (DOJ), Federal Communications Commission (FCC), Government Information and Services (USAGov), Anti-Phishing Working Group (APWG), and Phishing.org (PhishingOrg). In the rest of the paper, we focus on studying these Gov & Org that offer security advice for reporting phishing attacks because they are more likely to be accessed by the public.

We observed that Gov & Org offer security advice on reporting phishing attacks for specific types of phishing attacks because they all discuss how to report phishing email attacks, while four of them lack advice on smishing and vishing attacks. However, offering security advice does not imply providing reporting channels.

Table 3 shows the number of entities that have dedicated reporting channels for different types of phishing attacks. It can be seen that only half of the Gov & Org provide dedicated reporting channels for phishing email attacks, and four Gov & Org have channels for reporting smishing and vishing attacks. Moreover, we identified 12 primary reporting targets based on the security advice, which are *FTC, IRS, CISA, FCC, IC3, Police, State Attorney General's Office (SAGO), APWG, SMS Reporting Number (7726), Google, Impersonated Company*, and *Internet Service Provider (ISP)*.

3.2.2 Analysis of Phishing Reporting in Companies. Although Fortune 100 companies are more likely to have stronger motivations and resources (e.g., dedicated cybersecurity response teams), we could only identify 65 of them that provide security advice to guide their customers on how to report phishing attacks. Furthermore, only 44 of them provide reporting channels for phishing attacks, despite the fact that security advice from both the public and private sectors has strongly encouraged people to report attacks to impersonated companies. Additionally, we find that companies are more likely to be concerned about phishing email attacks (43 companies) than smishing (14 companies) and vishing (12 companies), based on the number of companies offering security advice for reporting phishing. A summary of these results can be seen in Table 3.

Moreover, we discovered very few companies with reporting channels for phishing emails (7 out of 43) that requested their reporters to provide the email header information while reporting phishing attacks. Compared with reporting channels offered by Gov & Org that often favor generic reporting methods due to their broad public reach, companies are more likely to provide a convenient reporting approach to the reporters by reporting through built-in functions in their software or applications.

Our analysis of the security advice from companies shows that companies request reporters to report phishing attacks to Gov & Org entities as well. Table 4 shows the number of companies requesting to report to different Gov & Org reporting targets. The FTC is the most often addressed reporting target because 19, 14, and 15 companies recommend the FTC for reporting phishing emails, smishing, and vishing, respectively.

Furthermore, we notice that the reporting advice given by companies frequently takes into account reporters' victim status, requesting them to report the attack to a specific target only when they fall victim to the attack. For example, 13 out of the 19 companies request their customers to report to the FTC only when they are victims of phishing email attacks (Table 4).

3.3 Challenges

In analyzing the security advice and reporting channels, we identified four General Challenges (GC) common to both the public and private sectors, one Challenge specific to Gov & Org (CGO), and two Challenges specific to Companies (CC).

GC_1: Email Phishing Reports Lack Critical Information. As shown in Table 3, only 40% and 16.3% of Gov & Org and Fortune 100 companies that have dedicated reporting channels for phishing email attacks request the reporters to provide the email header information. Lacking this critical information (e.g., the sender and recipient, timestamps, IP addresses) in the report might influence further actions against the phishing attacks, such as taking down mass email servers and pursuing phishers.

GC_2: Inconsistent Reporting Instructions in Different Reporting Channels. We notice that different reporting channels have inconsistent (even conflicted) security advice for reporting phishing attacks. This challenge might confuse reporters not only before reporting but also after reporting phishing attacks because they might not be sure whether or not they have reported to the

correct reporting channel through the right approach. In the meantime, we believe that this would potentially influence reporters' future reporting actions, such as they might not report new phishing attacks because they were told, "If you think you've received a phishing email, just delete it. There's no need to report it," by a company.

Conflicting Advice from Different Entities. Security advice in both the public and private sectors provides conflicting advice from different entities. For example, a Gov agency requests people to report to IC3 when they are victims ("If you are a victim of online crime, file a complaint with the Internet Crime Complaint Center (IC3)"), but another agency requests them to report to IC3 regardless of their victim status ("Always report a "phishing", whether or not you responded to that phishing e-mail or website").

Different Advice for Reporting Location. We also discover that security advice from many entities suggests people report through other methods than the reporting target requires. One of the most common cases is that some entities in both public and private sectors request reporters to report phishing attacks to a reporting email address of FTC (e.g., "fake email or text, you should report the incident to the Federal Trade Commission by forwarding it to spam@uce.gov."), which is different from the one requested on the FTC's official website, *"reportphishing@apwg.org."*

Advising Outdated Reporting Channels. We are surprised to note that security advice from both the public and private sectors suggests outdated reporting channels, such as a retired reporting email address. *"spam@uce.gov"* is the most commonly addressed one, which was retired in Nov 2019, but it was still recommended by many entities in 2022.

GC_3: Too many places to report. Security advice requests people to report the same phishing attack to multiple reporting targets. For example, an advice lists four places to report: APWG, the impersonated company, FTC, and IC3 ("Always report a "phishing" e-mail or website to the following groups, whether or not you responded to that phishing e-mail or website: Forward the e-mail to reportphishing@antiphishing.com ; Forward the e-mail to the "abuse" e-mail address at the company that is being spoofed (e.g., "spoof@ebay.com"); forward the e-mail to the Federal Trade Commission (FTC) spam@uce.gov and notify the Internet Crime Complaint Center (IC3) by filing a complaint on its website"). This might cause reporters to worry that reporting to some of the targets may not be effective.

GC_4: No feedback to reporters. In general, reporters may not receive any feedback except an autoreply to confirm the delivery of reports ("*Gov & Org AgnecyName* isn't able to give updates on reports that have been filed or respond to each report individually ..."). Therefore, reporters do not know whether their reports will be taken seriously, when the reported phishing website will be blocked or whether the criminals responsible for the attack have been identified. This might cause reporters to question whether reporting is meaningful and miss out on the opportunity to learn from the feedback.

CGO_1: Do not resolve an individual case. Reporters should not expect their problems solved by reporting the attacks to Gov & Org channels because they do not resolve individual cases ("We do not resolve individual complaints on these issues and you will not receive status emails about your complaint"). Therefore, people may wonder why they spend time reading confusing security advice, identifying reporting channels, and reporting attacks to multiple Gov & Org channels, which will actually not assist them in resolving their issues.

CC_1: No dedicated reporting channels. Our analysis shows that security advice strongly requests people to report phishing attacks to the impersonated companies (e.g., "Forward the e-mail to the "abuse" e-mail address at the company that is being spoofed"), however, fewer than half of Fortune 100 companies have reporting channels for phishing email attacks, and even fewer have reporting channels for smishing and vishing attacks (Table 3).

CC_2: Differently chosen reporting channels of Gov & Org. Additionally to requesting customers to report phishing attacks to them, companies also ask their customers to report to specific Gov & Org channels. Nevertheless, we observe that companies choose reporting channels differently, which might lead to confusion when reporting a future attack. For example, one company needs their customers to only report to the FTC ("fake email or text, you should report the incident to the Federal Trade Commission"), yet another company recommends reporting to IC3 and SAGO ("Consider contacting the Internet Crime Complaint Center or your state Attorney General's office").

4 STUDY II: LOCATING REPORTING CHANNELS

Given the available resources for phishing reporting, can users easily locate the channels for reporting phishing attacks? To answer this question, we conducted this study to analyze the real experience that people have when preparing to report phishing attacks by applying qualitative and quantitative analysis approaches.

4.1 Methodology

We developed a scenario-based human subjects experiment, in which we recruited participants to locate where to report a phishing attack based on a given scenario. Participants are asked to complete some post-task questions where we seek to collect their reporting experience, concerns, and comments on reporting phishing attacks. On average, participants took 15 minutes to complete the experiment and received fair compensation of $3, as only 4% of MTurk participants can earn more than $7.25/h [16].

Research Questions.

In this study, we will answer three research questions in this section while considering the findings discovered in Study I:

(1) Why do people not comply with the security advice to report phishing attacks?
(2) Would people follow the security advice to report the same phishing attack to multiple channels?
(3) What are participants' concerns and attitudes toward phishing reporting?

Study Overview

The online experiment consisted of six stages. Participants are first shown a phishing attack scenario with a random type of phishing attack, a company name, and a type of victim status after signing the consent form (Figure 2). Note that our objective is to examine the experience of preparing to report phishing attacks with the

Scenario: suppose you are contacted by a **Phishing Email** that fraudulently claims to be from company **Comcast** saying ``your account will expire in 24 hours, please click the link to update your password.''
In the attack, you are a **victim** (e.g., you have lost money or disclosed your credit card number or account password).

Figure 2: Experimental scenario in Study II.

assumption that the participants have already recognized the phishing attacks, so providing details about the attacks will not bias the results.

To proceed to the next stage, participants need to spend 20 seconds on the scenario introduction page to read the scenario carefully. To ensure that participants fully comprehend the scenario, they also need to answer attention-check questions (e.g., the type of phishing attack assigned in the scenario).

The second stage is the participants' action stage, in which participants search for the appropriate reporting channel if they want to report the attack or they can choose not to report it. Third, participants are asked to answer whether they have located the reporting channels or if they prefer not to report. Fourth, we ask participants to answer follow-up questions based on their task results. The follow-up questions are often open-ended questions, which allow participants to further elaborate on their previous answers, such as the failure reasons if they cannot locate the reporting channels (Q2 in Table 8 in Appendix C). Next, all participants are asked to answer questions pertaining to challenges identified in Study I, allowing us to gain further insights into their perspectives.

Finally, all participants take a post-task questionnaire and answer demographic and cybersecurity experience questions. Because of the complicated survey logical flow and more than 50 survey questions, we show the core questions in Table 8 in Appendix C and the completed questions in Appendix A.

We started our experiments on MTurk and stopped recruiting new participants after waiting for seven days without any applications for participation. After excluding low-quality and duplicated participants, we had 89 US-based participants for analysis.

Analyzing Participants' Answers. For all open-ended questions, we used similar analysis methods introduced in Section 3.1 to build a coding book: we first gathered the responses to each specific question in one place, and then two researchers reviewed each security advice in sets of 30 to build the coding book incrementally. The researchers reached an overall Krippendorff's α of 0.99. We provide our final codebook in Appendix A.

Ethics. Our institution's IRB approved this study because it does not collect any PII or present any foreseeable risks. Also, we strictly comply with the policy of MTurk to protect all participants' privacy.

Limitations. In addition to the limitations relating to the generalizability of findings based on the participants from MTurk discussed in Study I, the self-reported data and social-desirability biases might limit our results to a certain extent because the participants may not take the survey seriously. To this end, we presented the scenario for 20 seconds and added several attention-check questions

Table 5: Demographics and cybersecurity exp of participants in Study II (n=89).

	Variable	Explanation	Metric	Percentage of Participants
Demographics	Age	Participants' age	18 – 29	7.9%
			30 – 49	66.3%
			50+	25.8%
	Gender	Participants' gender	Female	57.3%
			Male	41.6%
			No Answer	1.1%
	Education	Participants' education level	Up to Some College	42.7%
			Bachelor Degree	43.8%
			Advanced Degree	13.5%
Cybersecurity Exp.	InterestSec	If the participant is interested in cybersecurity-related topics	No	19.1%
			Yes	78.7%
			No Answer	2.2%
	HaveSecExp	Whether the participant has the cybersecurity-related experience	No	71.9%
			Yes	28.1%
	KnowPhish	Whether the participant knows what the phishing attack is	No	5.6%
			Yes	94.4%
	PhishAttackedBefore	Whether the participant was ever attacked by phishing attacks	No	9.0%
			Yes	91.0%
	KnowCanReport	Whether the participant knows that there are channels for reporting phishing attacks	No	44.9%
			Yes	55.1%
	KnowWhereReport	Whether the participant knows where to report phishing attacks	No	51.7%
			Yes	48.3%
	ReportBefore	Whether the participant ever reported a phishing attack before	No	56.2%
			Yes	41.6%
			No Answer	2.2%

to ensure that participants understood the experiment. Additionally, we asked participants to provide more detailed information in the follow-up questions to validate their previous responses. For example, we asked the participants to provide the URLs of the webpages on which they found where to report the phishing attack (if they stated that they had discovered the reporting channels in the previous question). Although participants could only continue after understanding they could choose not to report a phishing attack (attention check), and there was an option stating "I don't want to report it" on their determination page, the potential biased scenario instruction of Study II, along with other factors such as financial incentives, a controlled environment, and self-selection bias of MTurk, may have contributed to the higher reporting rates.

Moreover, recruiting more participants would provide more reliable results, but we believe our results have provided insights into the ecosystem, and further analysis can be conducted in the future. Furthermore, we carefully reviewed all responses and eliminated all participants whose responses were not meaningful or of low quality. Additionally, we used browser cookies and manually reviewed all answers to prevent and eliminate repeat participants. We are aware that participants could misunderstand the scenario or the questions. Therefore, we conducted two pilot studies of five participants to refine our experimental design.

4.2 Results

In this study, we analyzed experiment results from 89 participants, and found that 15 of them decided not to report the phishing attacks, leaving 74 participants that attempted to report it. Also, 62 participants successfully identified the reporting channels. Table 5 shows the demographics and cybersecurity experience of the participants.

4.2.1 RQ1: Factors Hindering Phishing Reporting. Considering the advantages and security guidance regarding reporting phishing attacks, we delve into the factors that deter individuals from reporting such incidents. By analyzing the follow-up and post-task questions of non-reporting participants, we discovered four possible reasons that discourage them from reporting: *Reporting Cost, Reporting Outcome, Personal Reason,* and *Reporting Criteria.*

Reporting Cost. Participants believe that the high cost associated with reporting is the most primary reason (46.15%), such as the time spent searching for reporting channels was not worthwhile ("It simply isn't worth the time").

Reporting Outcome. Uncertain or even useless reporting outcomes dispelled participants' enthusiasm for reporting phishing attacks (38.46%) ("I've reported telemarketers before, but there really isn't a point").

Personal Reason. 30.77% of participants will not report phishing attacks for reasons that are subjective and unrelated to the reporting ecosystem from people's perspectives ("It's not my problem").

Reporting Criteria. Participants have their own reporting criteria (23.08%), and they would report the phishing attack only when the situation meets their criteria ("I would report something when I see it more than once").

Additionally, reporting phishing attacks to impersonated companies is critial [14] and highly valuable due to three primary reasons: (1) Companies can update their systems by analyzing delivered phishing messages and identifying advanced cloaking techniques; (2) Reporting alerts companies about emerging phishing campaigns, enabling them to prevent successful compromises and re-secure compromised accounts. (3) Multiple sources of reports aid companies in the early identification of phishing attacks.

Despite the importance of reporting, it is concerning that nearly half of the participants in the study would not comply with security advice to report phishing attacks to spoofed companies. Understanding the reasons behind this reluctance is essential to addressing and overcoming such barriers.

We analyzed these participants' answers and identified five primary reasons. For brevity, we show the primary reasons and corresponding concerns in Table 6, and the full table with typical comments on each concern in Table 9 in Appendix C. Note that a participant's comment may include several concerns, belonging to multiple categories.

As shown in Table 6, different from the previous finding, the *Reporting Outcome* is the most primary reason (53.19%) that discourages these participants from reporting to spoofed companies because participants believe that companies can do nothing (36.17%). Additionally, we discovered that 21.28% of participants think the spoofed companies are also victims of the attack, and they should not report the attack to these victims.

4.2.2 RQ2: Reporting to Multiple Channels. In Study I, we notice that security advice from both the public and private sectors requests people to report the same phishing attack to multiple channels (GC_3 in Section 3.3), while we noticed much different opinions about it in our pilot study. Hence, in this study, we intend to understand whether participants will follow this security advice.

In total, 85 participants responded whether they would report the attack to all the requested reporting channels, and 23 of them have cybersecurity experience. The result indicates that half of the participants (50.6%) would follow the security advice, and only a small part of participants (39.1%) with cybersecurity experience would comply with the advice.

Table 6: Why not report to companies.

Category	Concerns	Percentage of Participants
Personal Reason	Do not report to another victim	21.28%
	Not a big deal	4.26%
	I do not care	8.51%
	I just delete it	2.13%
	Total	36.17%
Reporting Criteria	Not a victim	8.51%
	Total	8.51%
Reporting Cost	It takes time and effort	10.64%
	Not necessary to report to multiple channels	2.13%
	Total	8.51%
Reporting Channel Choice	It's hard to find the channels	8.51%
	Prefer Gov reporting channels	14.90%
	Reporting to companies is not recommended.	2.13%
	Total	25.54%
Reporting Outcome	Companies can be aware of the attack without my report.	6.38%
	Companies can do nothing with it	36.17%
	Reporting to Gov channels is more effective.	10.64%
	Unexpected reporting consequence.	2.13%
	Total	53.19%

We further analyzed the participants' reporting channel preferences from their final comments, and we found that 55.2% of participants will report attacks to spoofed companies, and 51.7% of participants prefer the Gov channels because they think Gov channels are easy to find ("It was a simple google search that gave me the FTC"), and reporting to Gov is the most effective ("Reporting to some sort of legal authority seems to be the most effective way to go about getting some sort of resolution to the case because they have abilities to track the people"). However, the participants may not know that Gov channels do not resolve individual cases (CGO_1 in Section 3.3).

4.2.3 RQ3: Concerns and Attitudes. We summarized their comments and conducted sentiment analysis from two aspects: their attitudes towards phishing reporting and the ease of locating reporting channels.

We have 74 participants with quality comments, and their comments may belong to multiple topics. The qualitative analysis shows that the previously discussed five concern categories are also the major concerns in the final comments, which are *Reporting Criteria, Reporting Cost, Reporting Outcome, Reporting Channel Choice,* and *Personal Reason.* However, participants have two new concerns in *Reporting Outcome* and one additional concern in *Reporting Criteria* in addition to the concerns listed in Table 6.

There are three participants who do not believe Gov can handle phishing attacks ("The FTC seems to be in charge of fraud phone calls, but they cannot do much if the fraud originates outside of the

US") (*Reporting Outcome*). Also, participants complained that "zero" feedback after reporting because they do not know if the entities have received the reports ("But how do you make sure the company youre reporting to receives the report") or really care about the reports ("I don't think the FBI or any other government agency really cares about this kind of call because they are so common") (*Reporting Outcome*). Moreover, two participants stated they would not report unless they received multiple attacks ("I would only report that email if it happened frequently, if it was just once I would block it and delete it") (*Reporting Criteria*).

Additionally, we discovered that 32.4% of participants have limited knowledge of phishing reporting. 25.7% of participants did not know there were places to report phishing attacks ("I actually didnt know there were specific places to report it to"), and 2.7% of them were even unaware that they should report attacks to spoofed companies ("I was not aware companies wanted you to report").

In the sentiment analysis, we considered comments that clearly expressed participants' attitudes. For example, the comment "It simply isn't worth the time" expresses a negative attitude to reporting phishing attacks. We identified participants' attitudes toward phishing reporting from 43 participants, and nine of them (20.9%) had negative attitudes primarily due to the useless reporting outcome, high reporting cost, and the prevalence of phishing attacks.

Additionally, we observed that 36 participants expressed their attitudes towards the ease of finding reporting channels, and 13 of them (36.11%) had negative attitudes, as they explicitly stated their frustrating and disappointing experience in locating the channels because of the unclear or unavailable information online ("It was a bit frustrating because I thought a large company like *CompanyName* would have information fairly easy to find that either outlined routine frauds that people try with their company or a point of contact at their company that would debunk fake e-mails").

5 STUDY III: EFFECT OF PHISHING REPORTS

Our prior studies showed that participants believe reports are not acted upon and that this is a main factor demotivating people from reporting phishing. So, what will actually happen after reporting phishing attacks? Are participants' concerns justified? We conducted Study III to empirically evaluate what actually happens after a report is made. Note that the study aims to investigate the responses to the reports, rather than assess the detection capabilities.

5.1 Methodology

In this study, we focused on the website-based phishing attack because it is the major form of attack in both phishing emails and smishing attacks. By monitoring the status of the reported phishing sites, we will answer two research questions: (1) what happens to the reported phishing websites? and (2) what feedback will reporters receive after reporting?

We reported the phishing sites to companies and the public SMS reporting number (7726, or "SPAM"), rather than to Gov & Org channels, for several reasons: (1) to avoid potential legal implications of reporting to Gov channels, (2) because Gov channels do not resolve individual cases, (3) because concerns about the ability of companies to act on reported phishing attacks is a major reason that affects participants' reporting decisions, and (4) because there is already prior research conducted to analyze the blocklisting time of phishing sites after reporting to Gov & Org channels [34]. Moreover, we strictly follow the reporting targets' instructions, providing only the requested information, such as forwarding suspicious emails without additional messages.

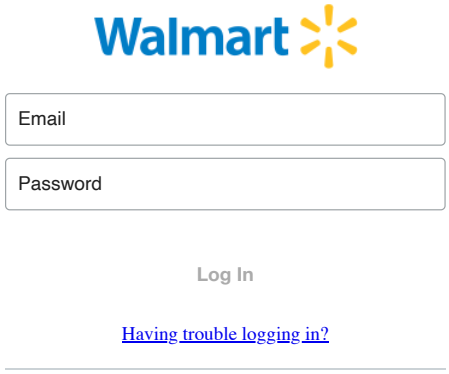

Figure 3: A screenshot of an experimental phishing website.

Designing Phishing Websites. In this study, we built phishing websites impersonating companies with their brand logos and reported them to the corresponding companies (Figure 3). There are two critical factors we need to consider while designing phishing websites. First, we need to ensure no risks to the public, and that the existence of this phishing website does not affect the companies' reputation (in case our phishing websites are visited accidentally). Therefore, our phishing website URL consisted of a domain and a randomly generated ID, such as `https://domain/?id=randomID`, and a blank webpage on all other webpages. Moreover, our domain names were also randomly generated, including three words and a four-digit number, such as "kellyjuniorconsultant6407.com", which is unlikely to be visited accidentally. Furthermore, our phishing websites would only log that input was submitted but would not record what was typed. Through these approaches, we can ensure that only reporting targets who receive our reports have access to the phishing sites, and that our experimental phishing websites pose a minimal risk to the general public.

Second, we also need to determine the status of phishing websites correctly. To this end, we applied six methods: (1) Our phishing websites do not use advanced cloaking techniques such as the *Bot Detection* [57] to ensure that these websites would not bypass companies' anti-phishing systems. (2) We did not reuse any domains because we observed that Google Safe Browsing (GSB) blocked the entire domain (e.g., https://domain) each time rather than the specific phishing URL (e.g., https://domain/?id=randomID) during our pilot tests. Therefore, using one domain per phishing website allows us to correctly determine the time it takes for the report to be blocked. Also, we used acme.sh to issue certificates to all experimental phishing websites. (3) We informed the domain registrar and the hosting service provider about our research in advance to ensure that the phishing could remain online without interruptions. (4) We logged all visit activities to the phishing websites. (5) We

checked the status of the reported phishing websites every five minutes using the GSB blocklisting service because major browsers have adopted the GSB blocklist service (e.g., Chrome, Safari, Firefox), protecting 81.74% of desktop users as of July 2021 [1]. (6) We ran a separate server to hold the brand logos of all companies and logged access activities to validate the phishing website visits.

Reporting to Companies. We reported phishing sites to 39 Fortune 100 companies through two reporting approaches: the email reporting address, and the online complaint form. Also, we use different email addresses to report the phishing attacks to avoid being blocked.

There are four points we need to clarify: (1) we did not report attacks through built-in functions because these companies also have other reporting channels, and our research focuses on publicly available reporting channels instead of specific companies' software; (2) we attempted to report phishing attacks to two companies through phone calls but never had the opportunity to provide the phishing website addresses since we were told that we simply needed to delete the messages. Hence, we did not conduct further analysis on the phone call reporting method. (3) We noticed some companies' reporting channels (email addresses) could not be found anymore, and some companies changed their security advice (e.g., changing their advice to "delete the phishing emails") when we started this study, so we were unable to report the phishing messages to all 43 companies, shown in Table 3; (4) we did not report attacks to Google because reporting to GSB was already studied by prior research [34], and we used the GSB blocklist service to monitor the status of the reported phishing websites regularly.

We reported 518 phishing websites to 37 companies through their email reporting addresses (including forwarding the message to 30 companies and forwarding the message with the email header information to seven companies) and 28 phishing websites to two companies through complaint forms in two months. Due to the possibility that companies may perform differently on weekdays and weekends, we did not report them all at once but rather reported them every other day between 11 am and 1 pm PDT. Therefore, it took 14 days for companies to receive reports from Monday through Sunday per month.

Reporting to 7726 (SPAM). Forwarding phishing messages to a specific SMS reporting number, 7726—which spells SPAM—is the most common and widely recommended way to report smishing attacks because individuals can report the messages regardless of the brand or operating system of their mobile phones. Our study adhered to this common practice, leaving built-in reporting as a prospective topic for future studies.

We launched phishing websites of all Fortune 100 companies, no matter if they have security advice, because this reporting channel can be used to report smishing attacks involving any company. By using an online SMS sending provider, we sent 100 phishing messages to our phones and forwarded them to 7726 in seven days.

Ethics. As previously discussed, we carefully designed all experiments to minimize risks to the public and impacts on the companies' reputations by only exposing the phishing websites to the companies and through their dedicated secure reporting channels. We took down these phishing websites at the end of the study. Due to the purpose of our research, we did not inform the involved companies beforehand. We used companies' names, brands, and logos on our phishing websites, which is a common practice used in prior research [11, 34, 36, 46]. We only reported 14 times to each company within two months (an average of 1.75 reports per week) to limit the overhead on these companies' normal operations. We believe that such a slight impact on companies' normal operations is worthwhile because (1) these companies may receive a large number of phishing reports every day, and (2) our study will positively impact the phishing reporting ecosystem.

Prior to launching synthesized attacks, we obtained approval from our university's IRB. We also informed the hosting service provider and domain registrar and acquired their consent. Additionally, we requested them to continually contact us if they receive reports about our phishing websites, following their standard operations protocol. Furthermore, we disclosed our findings to the companies involved.

Limitations. If reporting targets forward the reported phishing websites to other blocklisting services, then we may mistakenly determine that those phishing websites are not blocked. However, considering the popularity of GSB, its broader coverage, and its faster speed in comparison to other blacklists [34], we believe using GSB can still provide valuable insights into the blocklisting status of the reported phishing websites. Although each company was reported 14 times in the experiment, a larger number of reporting times might produce more reliable results. However, we believe our results provide insights into the current ecosystem, and future work can conduct longitudinal measurements of the response time of each company.

Additionally, company policies on reporting phishing websites to blocklists might affect our results. For instance, companies might not blocklist a phishing website if they only receive one report. However, we seek to study the overall effectiveness of reporting phishing websites, and this type of root cause analysis would be interesting for future research. There could exist possible collaborations between companies and host providers or registrars. Yet, two factors suggest the collaboration in this study is very limited: (1) In a pilot study where we reported phishing to 10 companies without informing the hosting or registrar provider, just one provider replied for one phishing site, and (2) We requested the registrar and hosting provider keep our study confidential. And one company repeatedly contacted the hosting provider, implying limited data sharing during our study. Moreover, our experiment does not disclose how reports are analyzed, and we will leave this to future research since it is not the purpose of this work. In our study, we reported smishing attacks to 7726 through a single US cellular carrier, which may not necessarily reflect the performance of all cellular carriers in handling such reports. Additionally, the reporting ecosystem could be exploited through the submission of fake reports. However, this research aims to uncover the critical challenges when reporting phishing attacks. Therefore, the adversary attack analysis is left to future work.

5.2 Results

We discuss our analysis results from three perspectives: the difficulty of reporting, the status of reported phishing websites, and contacts after reporting.

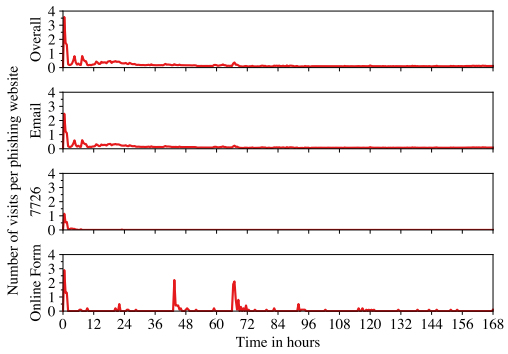

Figure 4: Website visits per phishing website over time in different reporting channels in one week.

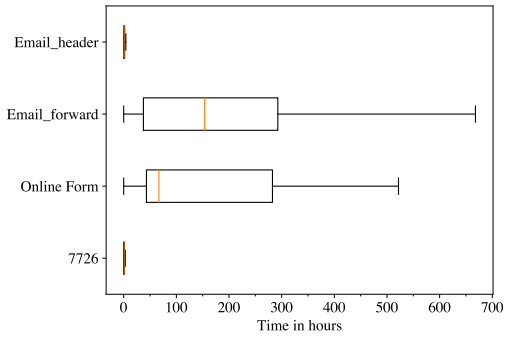

Figure 5: The time of website visit in different reporting approaches.

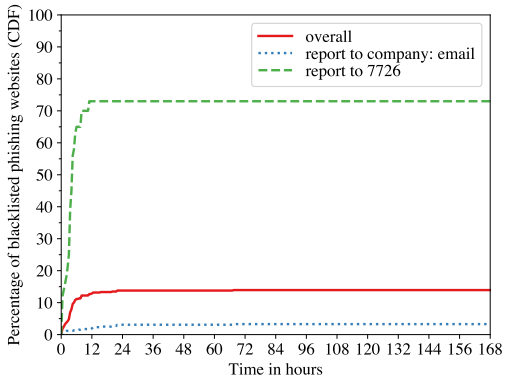

Figure 6: The growth of blocked phishing websites over time after reporting.

5.2.1 Difficulty of Reporting. The process of reporting phishing websites is not as seamless as we had anticipated, and we encountered two primary problems. First, we observed that the IP address of a reporter's email server must be reputable. We rented a virtual machine from a hosting provider with a shared IP address and configured it to serve as the reporter's email server in the pilot test. When we attempted to use it to report the phishing websites, reports could not be delivered to 14 of the companies. As a result, we used a reputable email service to report all our phishing reports.

Second, we also encountered a dilemma because two companies asked us to forward phishing emails while they blocked any suspicious emails, including the phishing reporting emails ("A signature was detected that could either be a virus, or a spam score over the maximum threshold"). Hence, we have to modify the phishing URLs by using the "URL Defanging" strategy [19] to convert them into an obfuscated format (e.g., `hxxps://abc[.]com`) before reporting them.

5.2.2 Status of Phishing Websites. We seek to empirically understand the status of the phishing websites after reporting. To do so, we answer two research questions: (1) did companies access the reported phishing websites? and (2) were the reported phishing websites blocked?

Accessing the Phishing Websites. Because of the design of the experimental phishing website, the phishing website addresses are only known to us and the reporting targets (companies and 7726 reporting channel). Therefore, we can accurately determine reporting target visits by analyzing the server logs. After excluding our IP addresses, we discovered that companies did not access every reported phishing website: 184 reported phishing websites of 29 companies (including six companies that require email header information) were never accessed. Moreover, ten companies never visited any of the reported phishing websites.

Figure 4 shows the number of visits per phishing website over time within one week. The top figure shows the overall website visit of all reported phishing websites. The other three figures show the website visits of phishing websites reported through different reporting channels. As shown in Figure 4, in general, phishing websites that have website visits are very likely accessed within 24 hours. Moreover, phishing websites reported through 7726 were visited concentrated within 7 hours than those reported through the online complaint forms.

Figure 5 shows the time of reported phishing website visits in different reporting approaches. We discovered that in the case of reporting to companies (through emails and online complaint forms), companies that request email header information in their reports access the phishing websites much sooner (a median of 0.82 hours) than other companies. However, it is worth noting that accessing the reported phishing websites earlier *does not mean* that these companies would blocklist the phishing websites earlier—we observed that a few of their phishing websites were blocked in the experiment. Moreover, reporting to 7726 has a similar performance to reporting by forwarding phishing messages with email header information, with a median of 0.84 hours.

Blocklisting Phishing Websites. By monitoring the status of reported phishing websites using GSB, we discovered that only 13.9% of all reported phishing websites were blocked. Moreover, reporting to 7726 is more likely to get the phishing websites blocked (73.0%) than using the email reporting channels (3.3%).

Furthermore, we observed that 98.9% of blocked phishing websites were blocked within 22 hours after reporting (Figure 6). Additionally, we discovered that phishing websites that were reported through online complaint forms were never blocked, and reporting

through 7726 can get phishing websites blocked faster (a median of 3.6 hours) than through email reporting channels (a median of 7.9 hours).

5.2.3 Contact after Reporting. We received contact and feedback after reporting from the perspective of two roles: the phishing attack reporter and the hosting owner.

Contact with Reporters. Table 10 in Appendix D shows the four types of replies we received from companies, which are *(i) Autoreply: confirm reports are received; (ii) Autoreply: no further feedback; (iii) Reply: confirm the reported message is malicious;* and *(iv) Reply: request more information.* By applying qualitative analysis of the replies, this study verified three of the participants' concerns identified in Study II, discouraging them from reporting phishing attacks to companies.

The first concern is that reporters would be unsure if companies received their reports because we received replies from 19 (51.4%) companies, including 15 companies' auto-replies, and replies from analysts in 5 companies. Second, reporters do not know whether reporting phishing attacks makes any difference. We received no replies indicating whether the phishing websites had been taken down or blocked. Moreover, three companies' auto-replies explicitly notified us that we would not receive any other responses from them. Third, our study confirms participants' view that some companies may not care about the reports enough because only four companies sent us emails informing us that the messages reported were phishing messages, and one company's analyst contacted us for more information regarding this matter. Moreover, these companies did not reply to every reporting email.

We also observed that it is possible that some of our reports have not been reviewed by the appropriate individuals or have not been carefully reviewed because they mistakenly think we have difficulties logging rather than reporting a phishing attack ("I am sorry to hear of the difficulty you experienced while visiting our website"). Furthermore, some companies might fail to maintain their email reporting channels properly, leading to the mailbox being unable to receive new reports ("The recipient's mailbox is full and can't accept messages now. Please try resending this message later").

For reporting through online complaint forms and the SMS reporting number (7726), we only received auto-replied SMS from 7726 requesting us to provide the phone numbers that sent the phishing messages and did not receive any other messages from the companies or 7726.

Contact with the Hosting Owner. As the hosting owner, we were contacted 14 times regarding 12 phishing websites impersonating seven companies through emails by the hosting service provider, domain registrar, and companies. Additionally, companies and security companies that assist those companies in dealing with phishing attacks are more likely to report the phishing websites to the hosting service provider, which we were contacted by the most frequently (11 times).

We observed that sometimes companies also report the domain registrar for the same phishing website (twice) after reporting to the service provider. Additionally, security companies directly contacted us through our anonymized contact information associated with the phishing domains (twice).

We understand that companies may not blocklist the phishing websites to allow hosting service providers and domain registrars to investigate the phishing websites. However, we discovered that two companies did not follow up on the status of their reported phishing websites after reporting because GSB did not blocklist these phishing websites. It is necessary to clarify that the domain registrar and hosting service provider did not take down our phishing websites because we informed them of our security research in advance. However, there are many "phishing friendly" hosting service providers [2] in the wild. Hence, companies should check the status of their reported phishing websites after reporting.

Moreover, we did not receive any contacts regarding the mass phishing email server or the server that hosts the brand logos of companies used by our phishing websites.

5.2.4 Responsible Disclosure. Following the study, we summarized our findings and disclosed them to the Fortune 100 companies that received our phishing reports via email. Except for the auto-reply emails from 13 companies, we did not receive any further responses from any companies within three weeks.

6 RECOMMENDATIONS

The findings in each of our studies are related to each other. For example, lack of feedback (Study I) is also a major concern in reporting outcomes (Study II and Study III). Therefore, it is likely that Gov, Org, and companies can apply measures to mitigate the challenges identified in the phishing reporting ecosystem and improve end-users' ability and enthusiasm to participate in the fight against phishing attacks.

We categorized all the findings into five concern categories identified from participants in Study II: *Reporting Outcome, Reporting Cost, Reporting Channel Choice, Reporting Criteria,* and *Personal Reason.* We present our recommended mitigation approaches under these five concern categories.

Mitigation Approaches for Reporting Outcome. The outcome of a report is people's primary concern, and it affects their decision on whether or not to report and where to report phishing attacks. Based on our analysis in Study II, we believe that providing feedback to reporters is an effective way to mitigate these concerns. To reduce security analysts' workloads, reporting targets can automate contacts in three steps: (1) send automatic replies confirming the reports have been received and listing actions that would be taken upon receiving the reports, (2) send automated notifications if the reported website is marked malicious, (3) send notifications if the reported phishing site has been blocked.

Additionally, all reported phishing attacks should be taken seriously. If phishing reports are randomly sampled, and not all are acted upon, it would give rise to further victimization by the same phishing websites and result in reporters believing that their reports are worthless. Moreover, reporting targets should report the phishing attacks to hosting service providers and domain registrars in addition to the blocklisting services (e.g., GSB). Meanwhile, they should follow up on the reported phishing websites to ensure these websites are blocked. Furthermore, unexpected messages or consequences (e.g., mistakenly blocking reporters' accounts) will discourage people from continuing to report phishing attacks.

Mitigation Approaches for Reporting Cost. The high cost of reporting phishing attacks impacts people's decisions on whether or not to report phishing attacks, resulting in negative attitudes toward reporting phishing attacks. Considering all the identified findings, we believe reporting targets should provide consistent security advice and reporting channels, which are properly maintained, publicly accessible, and easy to locate. This way, people can report phishing attacks seamlessly without confusion or significant effort (e.g., reports can be easily delivered).

One possible mitigation approach is having one dedicated Gov entity, such as the FTC, responsible for all phishing attack reports. This approach would allow for updated and consistent security advice that would allow all parties, such as companies, to follow the latest authoritative information (e.g., avoiding providing a retired reporting email address) and provide consistent security advice. Also, this approach can reduce people's effort in deciding whether or not to report the same attack to multiple channels or where to report in addition to the spoofed companies.

Moreover, according to our results, high time costs and efforts in locating companies' reporting channels are the primary reasons why people fail to report phishing attacks. Companies should also establish dedicated channels for reporting smishing, vishing, and phishing email attacks to respond rapidly to phishing attacks that may harm their customers and reputations because Gov & Org reporting channels will not resolve individual cases.

Mitigation Approaches for Reporting Channel Choice. Individuals have varying preferences when preparing for reporting phishing attacks. Considering that Gov & Org would not resolve individual cases and the different purposes for reporting, the mitigation approach addressed previously in *Mitigation Approaches for Reporting Cost* can mitigate the concerns in this part. Moreover, we suggest that the reporting targets state whether they will resolve individual cases in obvious places (e.g., not in the Q&A section), as we observe that 32.4% of participants have limited knowledge of phishing reporting, and some of them believe that reporting to Gov is an effective way to resolve their cases.

Mitigation Approaches for Reporting Criteria and Personal Reason. People's insufficient awareness and perception of reporting phishing attacks and *Reporting Cost* are the major causes of these two concern categories. Therefore, besides applying *Mitigation Approaches for Reporting Cost*, educating people on the significance of reporting is an effective way to mitigate these concerns. For example, the training materials should introduce how reporting benefits the reporters (e.g., re-securing their compromised accounts) and other parties, besides educating how to recognize phishing attacks.

7 CONCLUSION

In this paper, we conduct three studies to comprehensively evaluate the phishing reporting ecosystem to identify the critical challenges people face and their concerns when reporting smishing, vishing, and phishing email attacks.

Based on our results, we believe that the phishing reporting ecosystem deserves further attention from the research community. Phishing reporting is one of the few areas where end users—who often bear the brunt of the harm of phishing attacks—can actively fight against phishing. These end users can make a real difference in the fight against phishing. However, the phishing reporting ecosystem should be improved, as we outline in this paper. Hopefully, we can work toward research that empowers end users to help stem the tide of phishing in the future.

ACKNOWLEDGMENTS

We thank our shepherd, and the anonymous reviewers for their helpful suggestions. This work was supported by the National Science Foundation grants CNS-1942610, CNS-2127232, CNS-2346845, CNS-2419829, CICI-2232911 and DGE-1663651. Additionally, this work is sponsored by, and related to, Department of Navy award N00014-23-1-2563 issued by the Office of Naval Research. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of any funding agencies.

REFERENCES

[1] 2021. Browser Market Share. https://netmarketshare.com/browser-market-share.aspx
[2] Greg Aaron, Lyman Chapin, David Piscitello, and Colin Strutt. 2020. Phishing Landscape 2020: A Study of the Scope and Distribution of Phishing. (2020).
[3] Islam Abdalla Mohamed Abass et al. 2018. Social Engineering Threat and Defense: A Literature Survey. *Journal of Information Security* 9, 04 (2018), 257.
[4] Bhupendra Acharya and Phani Vadrevu. 2021. PhishPrint: Evading Phishing Detection Crawlers by Prior Profiling. In *Proceedings of the USENIX Security Symposium (USENIX)*.
[5] Nalin Asanka Gamagedara Arachchilage and Melissa Cole. 2011. Design a Mobile Game for Home Computer Users to Prevent from "Phishing Attacks". In *Proceedings of the IEEE International Conference on Information Society (i-Society)*.
[6] Nalin Asanka Gamagedara Arachchilage and Steve Love. 2013. A game design framework for avoiding phishing attacks. *Computers in Human Behavior* 29, 3 (2013), 706–714.
[7] Nalin Asanka Gamagedara Arachchilage and Steve Love. 2014. Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior* 38 (2014), 304–312.
[8] Hugo Bijmans, Tim Booij, Anneke Schwedersky, Aria Nedgabat, and Rolf van Wegberg. 2021. Catching Phishers By Their Bait: Investigating the Dutch Phishing Landscape through Phishing Kit Detection. In *Proceedings of the USENIX Security Symposium (USENIX)*.
[9] Michael Buhrmester, Tracy Kwang, and Samuel D Gosling. 2011. Amazon's Mechanical Turk: A new source of inexpensive, yet high-quality data? *Perspectives on Psychological Science* 6, 1 (2011), 3–5.
[10] Anthony Carella, Murat Kotsoev, and Traian Marius Truta. 2017. Impact of security awareness training on phishing click-through rates. In *Proceedings of the IEEE International Conference on Big Data (BigData)*.
[11] Yan Chen, Fatemeh Mariam Zahedi, Ahmed Abbasi, and David Dobolyi. 2021. Trust calibration of automated security IT artifacts: A multi-domain study of phishing-website detection tools. *Information & Management* 58, 1 (2021), 103–394.
[12] Lorrie Faith Cranor, Serge Egelman, Jason I Hong, and Yue Zhang. 2007. Phinding Phish: An Evaluation of Anti-Phishing Toolbars. In *Proceedings of the Symposium on Network and Distributed System Security (NDSS)*.
[13] FBI. 2023. 2022 Internet Crime Report. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
[14] Federal Trade Commission. 2024. Phishing. https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/phishing
[15] Dorota Filipczuk, Charles Mason, and Stephen Snow. 2019. Using a game to explore notions of responsibility for cyber security in organisations. In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*.
[16] Kotaro Hara, Abigail Adams, Kristy Milland, Saiph Savage, Chris Callison-Burch, and Jeffrey P Bigham. 2018. A data-driven analysis of workers' earnings on Amazon Mechanical Turk. In *chi*.
[17] Andrew F Hayes and Klaus Krippendorff. 2007. Answering the Call for a Standard Reliability Measure for Coding Data. *Communication Methods and Measures* 1, 1 (2007), 77–89.
[18] Jason Hong. 2012. The State of Phishing Attacks. *Commun. ACM* 55, 1 (2012), 74–81.
[19] IBM. 2021. Email Security – Defanging URLs. https://www.ibm.com/docs/en/rsoa-and-rp/32.0?topic=SSBRUQ_32.0.0/com.ibm.resilient.doc/install/resilient_install_defangURLs.htm

[20] Markus Jakobsson. 2007. The Human Factor in Phishing. *Privacy & Security of Consumer Information* 7, 1 (2007), 1–19.

[21] Keith S Jones, Miriam E Armstrong, McKenna K Tornblad, and Akbar Siami Namin. 2020. How social engineers use persuasion principles during vishing attacks. *Information & Computer Security* 29, 2 (2020), 314–331.

[22] Tom Huddleston Jr. 2019. How this scammer used phishing emails to steal over $100 million from Google and Facebook. https://www.cnbc.com/2019/03/27/phishing-email-scam-stole-100-million-from-facebook-and-google.html

[23] Aniket Kittur, Ed H Chi, and Bongwon Suh. 2008. Crowdsourcing user studies with Mechanical Turk. In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*.

[24] Faris Bugra Kokulu, Ananta Soneji, Tiffany Bao, Yan Shoshitaishvili, Ziming Zhao, Adam Doupé, and Gail-Joon Ahn. 2019. Matched and Mismatched SOCs: A Qualitative Study on Security Operations Center Issues. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*.

[25] Katharina Krombholz, Heidelinde Hobel, Markus Huber, and Edgar Weippl. 2015. Advanced social engineering attacks. *Journal of Information Security and applications* 22 (2015), 113–122.

[26] Ponnurangam Kumaraguru, Justin Cranshaw, Alessandro Acquisti, Lorrie Cranor, Jason Hong, Mary Ann Blair, and Theodore Pham. 2009. School of Phish: A Real-World Evaluation of Anti-Phishing Training. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*.

[27] Youngsun Kwak, Seyoung Lee, Amanda Damiano, and Arun Vishwanath. 2020. Why do users not report spear phishing emails? *Telematics and Informatics* 48 (2020), 101–343.

[28] Wired Magazine. [n. d.]. Researchers Uncover RSA Phishing Attack, Hiding in Plain Sight. https://www.wired.com/2011/08/how-rsa-got-hacked/

[29] William Melicher, Blase Ur, Sean M Segreti, Saranga Komanduri, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2016. Fast, lean, and accurate: Modeling password guessability using neural networks. In *Proceedings of the USENIX Security Symposium (USENIX)*.

[30] MJ Miranda. 2018. Enhancing Cybersecurity Awareness Training: A Comprehensive Phishing Exercise Approach. *International Management Review* 14, 2 (2018), 5–10.

[31] Ajaya Neupane, Md Lutfor Rahman, Nitesh Saxena, and Leanne Hirshfield. 2015. A multi-modal neuro-physiological study of phishing detection and malware warnings. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*.

[32] CBS News. [n. d.]. The phishing email that hacked the account of John Podesta. https://www.cbsnews.com/news/the-phishing-email-that-hacked-the-account-of-john-podesta/

[33] Adam Oest, Yeganeh Safaei, Adam Doupé, Gail-Joon Ahn, Brad Wardman, and Kevin Tyers. 2019. PhishFarm: A Scalable Framework for Measuring the Effectiveness of Evasion Techniques Against Browser Phishing Blacklists. In *Proceedings of the IEEE Symposium on Security and Privacy*.

[34] Adam Oest, Yenganeh Safaei, Penghui Zhang, Brad Wardman, Kevin Tyers, Yan Shoshitaishvili, Adam Doupé, and Gail-Joon Ahn. 2020. PhishTime: Continuous Longitudinal Measurement of the Effectiveness of Anti-phishing Blacklists. In *Proceedings of the USENIX Security Symposium (USENIX)*.

[35] Adam Oest, Penghui Zhang, Brad Wardman, Eric Nunes, Jakub Burgis, Ali Zand, Kurt Thomas, Adam Doupé, and Gail-Joon Ahn. 2020. Sunrise to Sunset: Analyzing the End-to-end Life Cycle and Effectiveness of Phishing Attacks at Scale. In *Proceedings of the USENIX Security Symposium (USENIX)*.

[36] Justin Petelka, Yixin Zou, and Florian Schaub. 2019. Put Your Warning Where Your Link Is: Improving and Evaluating Email Phishing Warnings. In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*.

[37] PhishMe. 2017. *Phishing Defense Guide 2017.* Technical Report.

[38] Angelisa C Plane, Elissa M Redmiles, Michelle L Mazurek, and Michael Carl Tschantz. 2017. Exploring user perceptions of discrimination in online targeted advertising. In *Proceedings of the USENIX Security Symposium (USENIX)*.

[39] Proofpoint. 2020. *2020 State of the Phish: An in-depth look at user awareness, vulnerability and resilience.* Technical Report.

[40] Stuart Schecter, Rachna Dhamija, Andy Ozment, and Ian Fischer. 2007. The Emperor's New Security Indicators: An evaluation of website authentication and the effect of role playing on usability studies. In *Proceedings of the IEEE Symposium on Security and Privacy*.

[41] Keyur Shah, Tanushree Shenvi, Karan Desai, Reshad Asrani, and Varun Jain. 2015. Phishing: An Evolving Threat. *International Journal of Students' Research in Technology & Management* 3, 1 (2015), 216–222.

[42] Hossain Shahriar, Tulin Klintic, Victor Clincy, et al. 2015. Mobile Phishing Attacks and Mitigation Techniques. *Journal of Information Security* 6, 03 (2015), 206.

[43] Zhibo Sun, Adam Oest, Penghui Zhang, Carlos E Rubio-Medrano, Tiffany Bao, Ruoyu Wang, Ziming Zhao, Yan Shoshitaishvili, Adam Doupé, and Gail-Joon Ahn. 2021. Having Your Cake and Eating It: An Analysis of Concession-Abuse-as-a-Service. In *Proceedings of the USENIX Security Symposium (USENIX)*.

[44] Huahong Tu, Adam Doupé, Ziming Zhao, and Gail-Joon Ahn. 2016. SoK: Everyone Hates Robocalls: A Survey of Techniques against Telephone Spam. In *Proceedings of the IEEE Symposium on Security and Privacy*.

[45] Huahong Tu, Adam Doupé, Ziming Zhao, and Gail-Joon Ahn. 2019. Users Really Do Answer Telephone Scams. In *Proceedings of the USENIX Security Symposium (USENIX)*.

[46] Enis Ulqinaku, Hala Assal, AbdelRahman Abdou, Sonia Chiasson, and Srdjan Capkun. 2021. Is Real-time Phishing Eliminated with FIDO? Social Engineering Downgrade Attacks against FIDO Protocols. In *Proceedings of the USENIX Security Symposium (USENIX)*.

[47] Cornell University. [n. d.]. NEW SUMMER EMPLOYMENT OFFER FOR STUDENTS BY MCKESSON CORPORATION. Retrieved Aug 10, 2018 from https://it.cornell.edu/phish/6315

[48] USPS Office of Inspector General. 2015. Information Security Awareness Training and Phishing. https://www.uspsoig.gov/sites/default/files/document-library-files/2015/IT-AR-16-001.pdf

[49] Tavish Vaidya, Daniel Votipka, Michelle L Mazurek, and Micah Sherr. 2019. Does Being Verified Make You More Credible? Account Verification's Effect on Tweet Credibility. In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*.

[50] Verizon. 2019. *2019 Data Breach Investigations Report.* Technical Report.

[51] Verizon. 2021. *2021 Data Breach Investigations Report.* Technical Report.

[52] Ben Weinshel, Miranda Wei, Mainack Mondal, Euirim Choi, Shawn Shan, Claire Dolin, Michelle L Mazurek, and Blase Ur. 2019. Oh, the Places You've Been! User Reactions to Longitudinal Transparency About Third-Party Web Tracking and Inferencing. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*.

[53] Zikai Alex Wen, Zhiqiu Lin, Rowena Chen, and Erik Andersen. 2019. What. hack: Engaging anti-phishing training through a role-playing phishing simulation game. In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*.

[54] Emma J Williams and Danielle Polage. 2019. How persuasive is phishing email? The role of authentic design, influence and current events in email judgements. *Behaviour & Information Technology* 38, 2 (2019), 184–197.

[55] Min Wu, Robert C Miller, and Simson L Garfinkel. 2006. Do Security Toolbars Actually Prevent Phishing Attacks?. In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*.

[56] Ezer Osei Yeboah-Boateng and Priscilla Mateko Amanor. 2014. Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices. *Journal of Emerging Trends in Computing and Information Sciences* 5, 4 (2014), 297–307.

[57] Penghui Zhang, Adam Oest, Haehyun Cho, Zhibo Sun, RC Johnson, Brad Wardman, Shaown Sarker, Alexandros Kpravelos, Tiffany Bao, Ruoyu Wang, Yan Shoshitaishvili, Adam Doupé, and Gail-Joon Ahn. 2021. CrawlPhish: Large-scale Analysis of Client-side Cloaking Techniques in Phishing. In *Proceedings of the IEEE Symposium on Security and Privacy*.

A CODEBOOK AND SUPPLEMENTARY MATERIAL

The codebooks and questionnaires are available at https://github.com/phishing-reporting/phishing-reporting.

B APPENDIX FOR STUDY I

Table 7: Survey questions in Study I.

ID	Question	Answer Options
Q1	Suppose you decide to report the phishing attack and need to find where to report it. Please tell us what search term(s) you may use based on your scenario?	Short answer
Q2	Suppose you decide to report the phishing attack to the company, please tell us what search term(s) you may use based on your scenario?	Short answer
Q3	Which search engine will you use?	(i) Google; (ii) Bing; (iii) Yahoo! (iv) Other
Q4	If you select "Other," please tell us what search engine you will use.	Short answer
Q5	We understand that many people may stop reporting after reading a few search results if they do not find the reporting advice or reporting channels they need. If so, how many search results may you review before you stop reporting? (The number of search results displayed on each page depends on your monitor settings and approximately ten results (excluding Ads) per page.)	(i) less than 10 search results; (ii) 11 – 20 search results; (iii) 21 – 30 search results; (iv) more than 30 search results

C APPENDIX FOR STUDY II

Table 8: Core survey questions in Study II.

ID	Question	Answer Options (Next Question)
Q1	Have you found where to report the phishing attack based on the assigned scenario?	(i) Yes (Q5); (ii) No (Q2); (iii) I don't want to report it (Q4)
Q2	What makes you believe you cannot find where to report this *Phishing Attack Type* that fraudulently claims to be from *CompanyName*?	Short answer (Q3)
Q3	If you cannot find where or how to report it, what will you do? Can you briefly explain the reason?	Short answer (Q6)
Q4	What makes you decide to stop reporting this *Phishing Attack Type* that fraudulently claims to be from *CompanyName*?	Short answer (Q14)
Q5	How did you identify where to report the phishing attack?	(i) Search online (Q7); (ii) Ask someone (Q11); (iii) I have experience on it and know the answer (Q12); (iv) Others (Q13)
Q6	How did you try to identify where to report the phishing attack?	(i) Search online (Q10); (ii) Ask someone (Q11); (iii) I have experience on it and know the answer (Q12); (iv) Others (Q13)
Q7	Please enter the website address (URL) where you found the information about where and how to report this *Phishing Attack Type* that fraudulently claims to be from [CompanyName]. (If there are more than one, please use semicolons ";" to separate)	Short answer (Q8)
Q8	Based on the information you found, where and how are you requested to report this phishing attack?	Short answer (Q9)
Q9	Do you plan to report to all the requested channels you just found?	i) Yes (Q10); (ii) No (Q10); (iii) I don't want to report it (Q10)
Q10	How did you search for where to report the phishing attack in your scenario? Please list all search terms you tried. (If there are more than one, please use semicolons ";" to separate)	Short answer (Q14)
Q11	Who did you ask and what did you ask? (If there are more than one, please use semicolons ";" to separate)	Short answer (Q14)
Q12	When and Where did you get this experience and knowledge?	Short answer (Q14)
Q13	Which "Other" ways did you use to search for where to report the attack? (If there are more than one, please use semicolons ";" to separate)	Short answer (Q14)
Q14	If you are requested to report the phishing attack to multiple reporting channels (e.g., FTC, IC3, impersonated company, internet service provider, and APWG), will you do that? Can you explain the reason?	Short answer (Q15)
Q15	Do you plan to report the phishing attack to the impersonated company, *CompanyName*?	i) Yes (Q17); (ii) No (Q16)
Q16	Why don't you plan to report to the company?	Short answer (Q17)
Q17	Your feelings, thoughts, and suggestions about finding where and how to report the attack are of great significance to the study of the current reporting ecosystem. We really appreciate your being able to leave some comments at the end.	Short answer

Table 9: Why not report to companies (Question 2) in Study II with Quotes.

Category	Concerns	Quote	Percentage of Participants
Personal Reason	Do not report to another victim	Because the phishing attack is not really Apple, it's pretending to be Apple.	21.28%
	Not a big deal	It's not a huge deal	4.26%
	I do not care	Because I really do not care. It is Valero's problem, not mine	8.51%
	I just delete it	I'm not sure if it really even is a phishing attack. I would probably just delete the email.	2.13%
	Total		36.17%
Reporting Criteria	Not a victim	Since I wasn't an actual victim, I didn't feel the need to report it.	8.51%
	Total		8.51%
Reporting Cost	It takes time and effort	Not worth the time or effort	10.64%
	Not necessary to report to multiple channels	The other reports are sufficient.	2.13%
	Total		8.51%
Reporting Channel Choice	It's hard to find the channels	Because I was not able to find out the procedure for doing do.	8.51%
	Prefer Gov reporting channels	I would rather report it to the FTC in this case, and let them handle it.	14.90%
	Reporting to companises is not recommended.	Reporting to the company was not one of the recommended actions listed.	2.13%
	Total		25.54%
Reporting Outcome	Companies can be aware of the attack without my report.	They (companies) probably already know about it from other individuals.	6.38%
	Companies can do nothing with it.	They (companies) don't have anything to do with it. They have no power to stop it from happening.	36.17%
	Reporting to Gov channels is more effective.	I would think reporting it to legal authorities would be more effective to get some sort of resolution.	10.64%
	Unexpected reporting consequence.	Because my previous experiences reporting the impersonated company (when I did NOT respond to the phishing email, didn't lose anything) just got my account flagged as a security problem – had a hard time doing any business after that. Response was like another attack.	2.13%
	Total		53.19%

D APPENDIX FOR STUDY III

Analysis shows that only five companies sent the reported phishing websites to GSB for blocklisting. Figure 7 shows the blocklisting time of phishing websites in different companies (Co.) and reporting channels in general, excluding outliers of blocklisting times calculated by using quantile ranges. It shows that the blocklisting time varies across companies, and even the same company would have significantly different performance, such as *Co.3* in Figure 7. After studying the blocked phishing websites of *Co.3*, we think the reporting time could be the reason for the delay in blocklisting because we reported one phishing website on Friday, and the company blocked it on Monday.

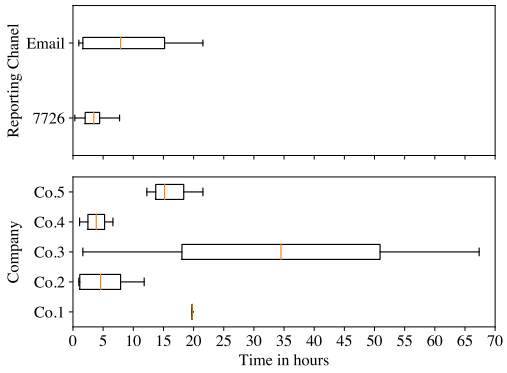

Figure 7: The blocklisting time of phishing websites in Study III.

Table 10: Contacts after reporting in Study III.

Reply Type	Quote	Num of Companies
Autoreply: confirm reports are received	Thank you for forwarding this information to us. You are correct in assuming this may be part of an attempted scam. We are aware that individuals may inappropriately use the *CompanyName* name or its services to perpetuate fraudulent activities. We appreciate you alerting us to this latest incident.	15
Autoreply: no further feedback	Thank you for forwarding your suspicious message. Please be aware that you will not receive any other response besides this automated email.	3
Reply: confirm the reported message is malicious	We appreciate you alerting us of this scam and fraudulent email. Please be advised that the referenced email address is not affiliated with *CompanyName*. We urge you to block and delete from your email account records for your protection and security.	4
Reply: request more information	Please contact me regarding the tech scam email that you recently reported on *CompanyName*. I have a few follow-up questions regarding your report.	1