Report Now. Report Effectively. Conceptualizing the Industry Practice for Cybercrime Reporting

Morvareed Bidgoli
PayPal, Inc.
Scottsdale, AZ, USA
mbidgoli@psu.edu

Bart P. Knijnenburg
School of Computing
Clemson University
Clemson, SC, USA
bartk@clemson.edu

Jens Grossklags
Department of Informatics
Technical University of Munich
Munich, Germany
jens.grossklags@in.tum.de

Brad Wardman
*P*ayPal, Inc.
Scottsdale, AZ, USA
bwardman@paypal.com

***Abstract*—Reporting plays a vital role in combatting cybercrimes. The data collected from cybercrime reporting can not only bolster the efforts of those on the responding end of such attacks (i.e., government, law enforcement agencies, and the technology industry), but also provide relevant prevention tips to computer users to help mitigate their cybercrime risk. Despite the importance of cybercrime reporting, we observe that many cybercrimes go unreported, which arguably can be due to an overall lack of effectiveness of currently existing cybercrime reporting mechanisms. This study aims to streamline cybercrime reporting processes at PayPal by proposing a design of an interactive customer-facing cybercrime reporting interface. The overall goals of the proposed design are to (1) appropriately triage reports both within the company and to relevant external entities and (2) to educate the customer base about cybercrimes and cybercrime reporting through helpful links. The proposed design was tested with 523 Amazon Mechanical Turk workers and was considered user-friendly and informative by our participants. Moreover, a statistical model demonstrated that aside from our proposed interface's usability, users' victimization, self-efficacy, and perception of cybercrimes' severity all had a positive effect on the likelihood to report a cybercrime. Our proposed design and evaluation have the potential to improve the efficiency and effectiveness of cybercrime reporting to corporations and government/law enforcement agencies.**

***Keywords*—cybercrimes, cybercrime reporting, user study, user interface design**

I. Introduction

Cybercrimes have proven to be a persistent threat to modern society [1], which is estimated to impose costs as high as $6 trillion annually through 2021 [7]. The Internet Crime Complaint Center (IC3), an official U.S. cybercrime reporting entity, received a total of 301,580 complaints totaling $1.42 billion in financial loss in 2017 [12]. However, for businesses the financial impact of cyber-related incidents is not the only concern, there is also the risk of losing sensitive customer data and diminished brand reputation [7]. Therefore, it is essential that businesses have the right contingencies in place to mitigate their cybercrime risk. One pivotal piece to combatting cybercrimes is having the proper avenues in place for victims to report them. Since there is so much valuable information to be gained from cybercrime report data, it is vital that a company collects this data not only to help ensure the security of their customers' accounts, but also as a means to know how to properly safeguard its business operations by properly allocating the right resources to do so.

Within the industry context, we have found that there are very few technology companies that provide customer-facing avenues to report cybercrimes. While companies such as Google allow for individuals to report phishing and malware websites, we do not observe many companies that allow for cybercrime-related incidents to be reported directly from a customer to a company through delineated reporting avenues like those that currently exist at PayPal.

In this paper, we propose and test an initial design of what a customer-facing cybercrime reporting interface would look like for industry companies like PayPal. Currently, PayPal provides customers two avenues to report cyber-related incidents that may have potentially compromised their accounts: speaking to a customer service representative over the phone or forwarding a phishing email to a designated email address. However, it is worth noting that these reporting avenues take some effort to find and there presently is no standalone webpage that provides relevant company specific information regarding cybercrime reporting; instead, we observe that much of this information is dispersed across many different pages on PayPal's online platform.

One key motivation behind proposing a customer-facing cybercrime reporting interface is that PayPal has had a history of reports that have been either misdirected (i.e., the phishing response team receives non-phishing related incidents) or that are simply unrelated to the company (e.g., incident reports involving other companies). For instance, between the months of January and April 2017, there were over 10,000 emails per month reported to their abuse mailbox that could not be properly diagnosed and handled by the company's automated system leading to the content being redirected to a human agent for analysis. One of the fundamental goals of our proposed cybercrime reporting interface design is to properly triage submitted reports. Arguably, this not only helps reduce agents' review times, but also ensures that incidents are properly reported to the relevant governmental/law enforcement agency when needed. With the added functionality of having a built-in triage for incoming reports, we foresee a number of positive outcomes such as:

- **More effective reporting** in terms of properly redirecting

unrelated reports to the relevant governmental/law enforcement agencies and the allocation of law enforcement resources to combat cybercrimes in the most sensitive areas,
- **Bolstering the company's cyber intelligence** through the extraction of Indicators of Compromise (IOCs) and prioritizing cybercrime event types, and
- **Educating users** on how to properly report a cybercrime to the company and how to leverage relevant online resources at their disposal for reporting cybercrimes that occur outside the company's purview.

This paper is structured as follows. We first discuss relevant related work, which specifically pertains to the topic of cybercrime reporting (Section II). Next, we detail the design of our study to evaluate our proposed cybercrime reporting interface (Section III) followed by the results of this study (Section IV). We mention the limitations of our study (Section V), discuss our findings (Section VI), and end with concluding remarks (Section VII).

II. Related Work

To our knowledge, our study is the first of its kind not only in trying to design and study a streamlined cybercrime reporting experience within the industry, but also in looking at the overall effectiveness of a cybercrime reporting interface. However, there is a rich, broader literature on cybercrime reporting.

In particular, there is an unfortunate yet well-documented history of cybercrimes going unreported, which is due to a number of reasons such as the victim believing the cybercrime they experienced lacked severity [19] [17], the victim being unaware that a cybercrime occurred [8] [19] [17], the victim feeling embarrassment over their victimization [8] [17], the victim experiencing self-blame over their victimization [9], the victim's belief that the reporting process is a "waste of time and effort" [9], and the victim's belief that there is a low likelihood that the cybercriminal will get caught [9]. In responding to these challenges, a key motivating factor of our study is to make the cybercrime reporting processes at PayPal more efficient because we believe that by creating a more streamlined cybercrime reporting experience more reporting will take place. Moreover, by properly directing reports through the correct avenues, reports will be better processed, which increases the likelihood of an adequate response as well as the correct accounting of the incident in the reporting system.

Cybercrimes can also go unreported due to a lack of reporting knowledge [3] [4], which can be attributed to the novelty of reporting mechanisms like the IC3 [16]. This problem is not restricted to cybercrime reporting studies, for instance, [5] and [10] have found that college students were not successful in reporting policy-related concerns (e.g., drug recalls) online to the appropriate government entities due to an overall lack of knowledge of government structure and policies.

In [18], seven organizations in technology-driven fields were examined for their ability to convey information to their customers regarding phishing attacks across three specific communication vectors: website content, customer phone support, and email reporting support. One of the authors' main suggestions is that organizations should provide helpful links to external educational content that also relays information about other cyber threats other than phishing through all communication vectors. Consequently, providing such information is a key facet of our proposed interface since we believe that it is important for companies to educate their customers about the many available cybercrime reporting resources including those that are external to the company.

III. Methodology

The overarching goal of our study is to explore the viability of a prototype of a cybercrime reporting interface that can bolster the overall efficiency of the state of cybercrime reporting at PayPal. Efficiency refers to properly triaging reports internally within the company's currently existing queues as well as externally in the event that an unrelated incident is reported.

While from a business standpoint there are countless benefits to such an initiative (e.g., reducing agent queues), we were also driven by properly representing the customers' interests in formulating our design, most notably in terms of its overall usability. Jakob Nielsen [11] outlines 10 usability heuristics for user interface design, a few of which we emphasized in our interface prototype:

- **Match between the system and the real world:** we clearly defined any technical terms that were mentioned (i.e., phishing) and to write in layman's terms whenever possible,
- **User control and freedom:** users are able to undo mistakes they make while progressing through our interface by pressing the back button found at the bottom of each page, and
- **Minimalist design:** we only included the pertinent information that the end user needed for progressing through our interface's pages to file a report.

The implementation of these heuristics will be further highlighted in the subsequent subsection (Section III-A) where we present a step-by-step description of key pages of our reporting interface. Our justification for testing our proposed design as a prototype, aside from being a cost-effective approach, is to test its overall functionality with a set of users in order to address any other future design improvements that need to be made before its final deployment [14].

In the following subsections, we will walk through the pages of our proposed design (Section III-A), the procedures that were implemented for testing our design using the task of hypothetically reporting an incident participants were randomly assigned to (Section III-B), the measurement properties of a series of questions we asked participants to answer after completing the task (Section III-C), and a theoretical model to help explain the factors that influence users' tendency to report cybercrimes in the context of the proposed interface (Section III-D).

A. *Proposed Interface Design*

We inspected existing cybercrime reporting mechanisms from the FTC and IC3 to inform our proposed interface design. The reasoning behind this was twofold: (1) we wanted an initial benchmark of how to design our own interface since no such interface currently exists in the industry and (2) we wanted to ensure that all important information is being asked in the event that a reported incident needs to be referred to external agencies such as the FTC and IC3. Our design is mainly informed by the FTC's Complaint Assistant. What we appreciated most about this design is that it has descriptions of the various categories of complaints consumers can file in order to ensure that the consumer properly selects a category. Moreover, there is a series of background questions that are asked prior to filing a report to detect whether there is a more effective way the consumer can file a report for the incident they experienced.

We created a fictitious online payments company called NQCPay and used this name throughout our reporting interface to avoid mentioning PayPal and associated brand effects. We used SurveyMonkey to build a prototype of our cybercrime reporting interface. Our interface has three different reporting avenues: email, web form, and phone. Figures 1-5 show screenshots of the pages of our cybercrime reporting interface. The exact reporting procedure a participant experiences depends on the scenario they were randomly assigned. Each participant viewed the interface homepage (see Figure 1). The purpose of the homepage was to not only welcome the user to the reporting interface, but also to provide a series of helpful links that they could access to learn more about cybercrimes. We decided to provide direct links to Google's Safe Browsing pages for phishing and malware in the event that a user experienced either incident.

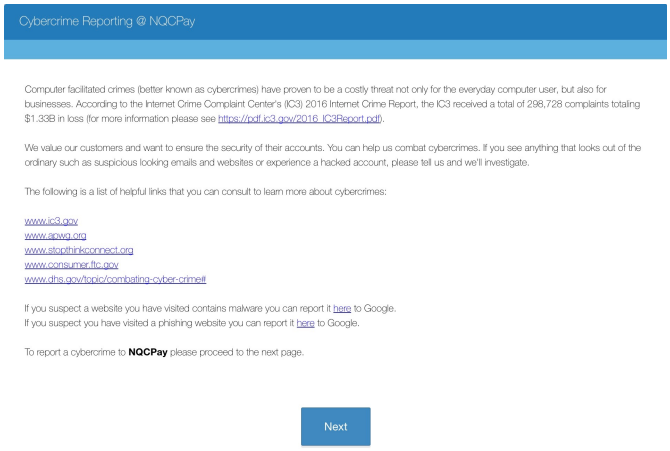

Fig. 1. Cybercrime reporting interface homepage

Once a participant clicks Next on the interface homepage, they proceed to a page where they are asked the following Yes or No question: *"Are you a NQCPay customer?"* This question effectively tackles instances where non-NQCPay customers would file a report through the NQCPay interface; this specific question addresses PayPal's persistent problem when reviewing incidents reported to its abuse mailbox. In the event a participant indicates that they are not a NQCPay customer, they are shown a page containing a series of external entities to which they can report their incident (see Figure 2). We believe that it is the responsibility of companies to educate users about where to report a cybercrime even if it is unrelated to the company. We argue that such facilities increase consumers' cybercrime reporting knowledge and in turn reduce under-reporting, which benefits not only the industry, but also the public as a whole in the long run. For non-NQCPay customers, the external triage page marks the end of their experience with our interface.

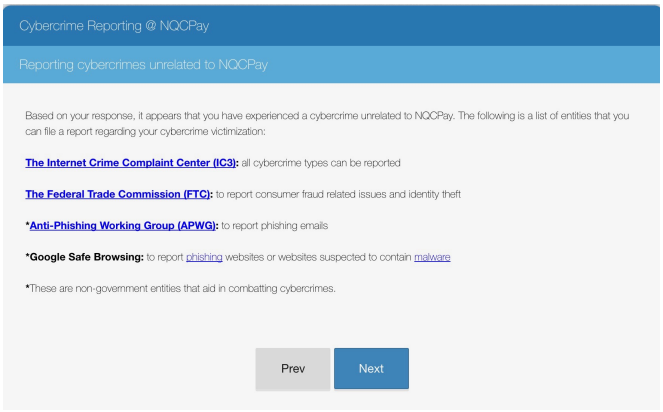

Fig. 2. External triage page (reporting cybercrime outside of NQCPay)

If a participant answers Yes to the question: *"Are you a NQCPay customer?"* then they will be prompted with the following Yes or No question: *"Do you believe your NQCPay account may have been compromised?"* This follow-up question distinguishes between choate or inchoate[1] cybercrimes and provides useful context for individuals working the backend of the interface in determining the priority level of the report. Inchoate cybercrimes should be reported just as much as choate cybercrimes since they help individuals who are responding to reports to better understand what types of cybercrimes exist and at what rate they are occurring. Bidgoli and Grossklags [3] found that cybercrime victims feel compelled to report inchoate cybercrimes for reasons such as catching the criminal, raising awareness to prevent it from happening to others, and providing useful information for law enforcement to act on.

Irrespective of whether a participant answers Yes or No regarding the potential compromise of their account, they will then be prompted with another Yes or No question: *"Did you experience phishing?"* A brief definition of phishing is also provided beneath the question. We chose to provide a definition of phishing since it is a technical term that not every computer user may be familiar with, which can greatly

[1]Legal terminology used to describe complete vs. incomplete crimes, respectively.

impact whether an incident will be properly reported. If a participant answers Yes, then they are directed to our internal triage page with instructions on how they can report their phishing-related incident to NQCPay via email (see Figure 3). This procedure is similar to how phishing-related incidents are currently reported to PayPal. The justification behind why PayPal collects phishing incident reports via email is twofold: (1) to mitigate the chance that a computer user may engage with URLs embedded within the emails in the process of filing a report and (2) to preserve the full URLs and headers found within the emails in order for proper takedowns to take place.

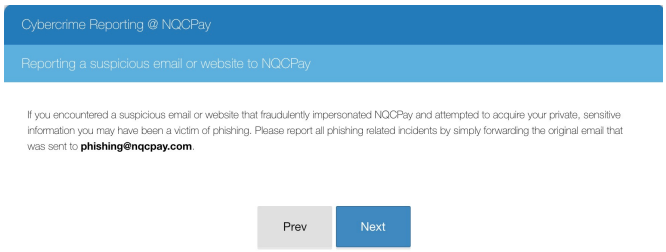

Fig. 3. Internal triage page (email avenue for phishing related incidents)

If a participant answers No to whether the incident they experienced was phishing then they will be asked whether they would prefer to report their non-phishing related incident by phone or via the web form. If a participant decides they would like to speak to a customer service representative, they are shown a page with the number to call (see Figure 4). If a participant decides they would like to fill out a web form instead then they will be shown a form to fill out (see Figure 5). We felt the need to incorporate this reporting avenue for non-phishing related incidents because customers may not feel as comfortable speaking to someone over the phone regarding their victimization. For example, [3] found that some cybercrime victims preferred filling out a web form versus speaking to someone over the phone because they can fill out a report on their own time and also think about how they want to fill out the report.

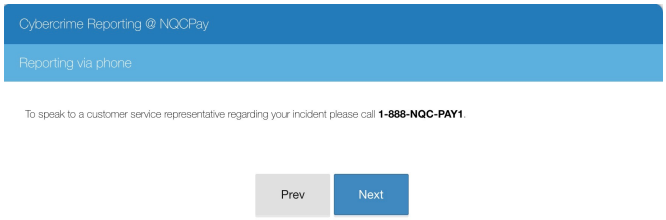

Fig. 4. Internal triage page (phone avenue for non-phishing related incidents)

B. Implementation

Amazon Mechanical Turk (AMT) was used to test the overall usability of the interface and its effectiveness in properly triaging reports. In order to participate in our study, an AMT

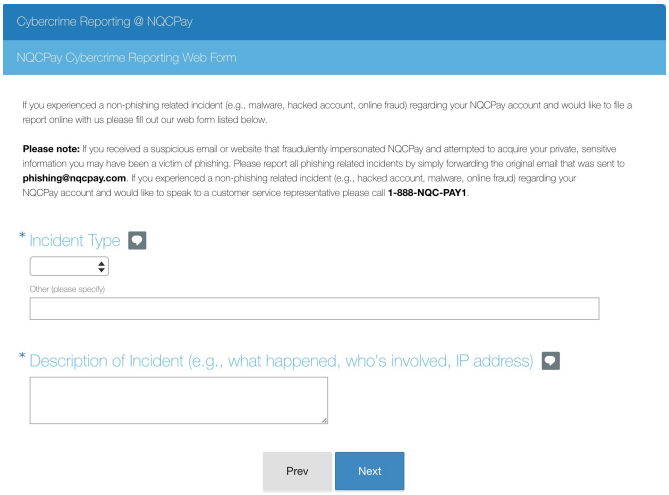

Fig. 5. Internal triage page (web form avenue for non-phishing related incidents)

worker had to be U.S. based and have a 95% or higher Human Intelligence Task (HIT) approval rate. We limited our participants to the U.S. since we are specifically focused on U.S. cybercrime reporting (i.e., many of the external cybercrime reporting entities we mention within our interface are U.S. based governmental agencies); moreover, we wanted to control for any potential cultural differences participants may have in how they perceive cybercrimes outside of the U.S. Additionally, workers with a reputation of 95% or higher have been shown to provide higher quality data [13]. Each participant was compensated $0.50 upon verification that they completed our HIT.

We used a scenario-based design to walk our participants through our proposed interface, which entailed a random assignment to one of ten cybercrime scenarios that each involved an incident that was or was not related to NQCPay. The NQCPay-related incidents that were used came directly from emails submitted to PayPal. Figures 6 & 7 are examples of related and unrelated incidents to PayPal, respectively. The NQCPay-related incidents consisted of phishing and malware incidents while the non-PayPal related incidents were either an online extortion or online scam. To reduce confusion, we specifically denoted whether the participant was an NQCPay customer or not, which would impact how they navigate through our interface. Additionally, for the majority of the cybercrime scenarios, we directly stated the type of cybercrime each participant was assigned to at the end of the scenario since we would later inquire about this information in the online survey portion of our study.

We piloted our proposed design internally at PayPal and with AMT workers to ensure that our study procedures were clear. The pilot run took place in mid-July 2017 for almost two weeks and involved 162 AMT workers. After suggested changes were made to our study, we ran a complete final run of our proposed design with workers from late July to early August 2017. A total of 648 workers participated, but only 523

participants were included in our final analysis because some workers did not fully complete our questions or had previously participated in our study.

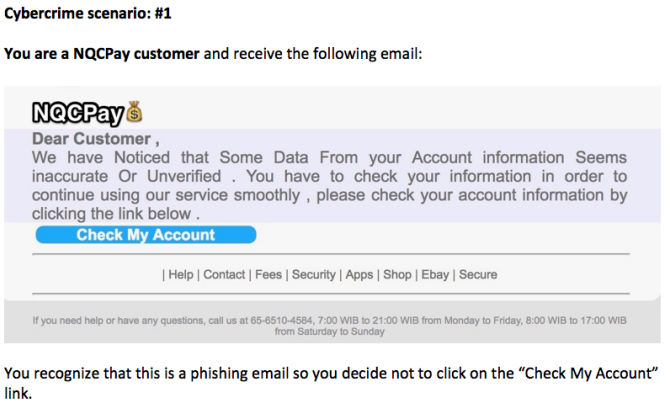

Fig. 6. PayPal related incident

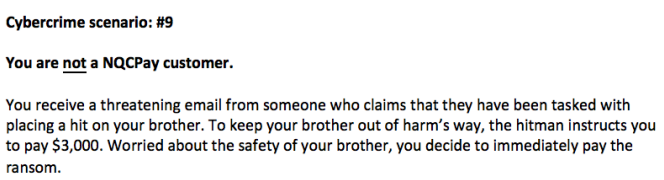

Fig. 7. Non-PayPal related incident

C. Measurement

After completing their task in the reporting interface, participants were asked questions to measure self-reported cybercrime victimization, self-efficacy regarding cybercrime reporting, perceived severity of cybercrimes, the usability of our interface, and their tendency to report future victimizations.

Victimization was treated as an index variable and a sum score was calculated for the six yes/no questions. The remaining questions, which were all measured on a 7-point scale, were subjected to a Confirmatory Factor Analysis (CFA). One item was dropped due to low communality. The factors, items, and loadings are reported in Table I and the inter-factor correlations and Average Variances Extracted (AVEs) are reported in Table II.

The CFA had a moderate fit ($\chi^2(203) = 873.5$, CFI = .941, TLI = .932, RMSEA = .080, 90% CI: [.074; .085]) and all factors showed convergent ($AVE > 0.5$) and discriminant ($\sqrt{(AVE)} >$ largest correlation with other factors) validity.

D. Theoretical Model

We have several hypotheses regarding the factors influencing users' tendency to report cybercrimes, which we present below. We start with hypotheses regarding users' personal characteristics, in this case, their past victimization and perceived self-efficacy. Research shows that cybercrime victims become more sensitized to the severity of cybercrimes [17] [19], thus, we hypothesize:

H1. Participants' past victimization is positively associated with their perception of the severity of cybercrimes.

Regarding self-efficacy, research shows that users who feel in control of their ability to deal with cybercrimes have less fear of cybercrimes, but are more likely to report them [4] possibly because they find the reporting mechanisms more

TABLE I
CONFIRMATORY FACTOR ANALYSIS (CFA) RESULTS FOR THE 7-POINT SCALE POST-REPORTING QUESTIONNAIRE ITEMS

Construct	Item	Load
Self-Efficacy	I feel that I am knowledgeable about cybercrimes.	0.800
	I know the effects cybercrimes can have on my life.	0.852
	I understand the differences between different types of cybercrimes.	0.814
	Sometimes I doubt whether I know enough about cybercrimes.	
	I don't understand most cybercrimes.	0.692
Severity	How harmful do you find phishing to be?	0.759
	How harmful do you find malware to be?	0.728
	How harmful do you find hacking to be?	0.732
	How harmful do you find identity theft to be?	0.916
	How harmful do you find credit card fraud to be?	0.723
	How harmful do you find other types of online fraud/scams to be?	0.782
Usability	The reporting interface was easy to use.	0.868
	Based on what I've seen, the reporting interface makes it convenient to report cybercrimes.	0.878
	The reporting interface taught me how to properly file a report regarding a cybercrime.	0.703
	I would like to use this interface frequently to report cybercrimes.	0.745
	I found the reporting interface unnecessarily complex.	0.720
	I would imagine that most people would learn to use this reporting interface very quickly.	0.830
Reporting	If you were a victim of phishing, how likely are you to report it to the appropriate entity?	0.715
	If you were a victim of malware, [etc.]?	0.675
	If you were a victim of hacking, [etc.]?	0.731
	If you were a victim of identity theft, [etc.]?	0.935
	If you were a victim of credit card fraud, [etc.]?	0.895
	If you were a victim of any other type of online fraud/scam, [etc.]?	0.755

TABLE II
AVERAGE VARIANCE EXTRACTED (AVE) AND INTER-FACTOR CORRELATIONS OF THE CFA RESULTS. THE DIAGONAL LISTS $\sqrt{(AVE)}$. VICTIMIZATION IS INCLUDED FOR COMPLETENESS

Factor	AVE	Correlation with			
		Self-efficacy	Severity	Usability	Reporting
Self-efficacy	0.627	0.792			
Severity	0.603	0.309	0.776		
Usability	0.630	0.390	0.457	0.794	
Reporting	0.624	0.357	0.629	0.443	0.790
Victimization	NA	0.142	0.147	0.101	0.125

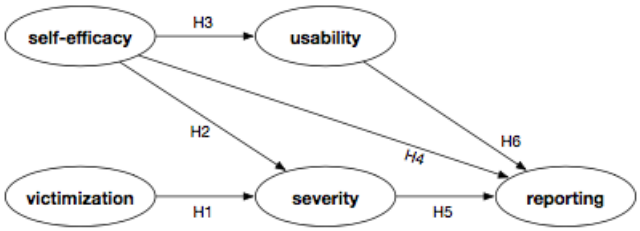

Fig. 8. Hypothesized effects on participants' tendency to report cybercrimes

usable (self-efficacy is linked to usability in the third iteration of the Technology Acceptance Model; [15]). Therefore, we hypothesize:

H2. Participants' cybercrime self-efficacy is negatively associated with their perception of the severity of cybercrimes.

H3. Participants' cybercrime self-efficacy is positively associated with their perception of the usability of our cybercrime reporting interface.

H4. Participants' cybercrime self-efficacy is positively associated with their tendency to report cybercrimes.

As previously mentioned, people who believe cybercrimes lack severity tend to underreport them [3] [4]. Likewise, users who understand the severity of cybercrimes are more likely to report [4]. Therefore, we hypothesize:

H5. Participants' perception of the severity of cybercrimes is positively associated with their tendency to report them.

Finally, the Technology Acceptance Model links usability to eventual system use [6], thus, we hypothesize:

H6. Participants' perception of the usability of our cybercrime reporting interface is positively associated with their tendency to report cybercrimes.

This final hypothesis is focal hypothesis to our theoretical model as it quantifies the effect of the usability of the reporting interface on users tendency to report cybercrimes. Fig. 8 gives an overview of the hypothesized effects.

IV. Results

In this section, we first provide the results of the overall success of the interface's triaging capabilities in terms of navigating participants to accurately file a report through our interface (Section IV-A). Next, we provide the results from our theoretical model, which notably covers the effect of our interface's usability on the likelihood a cybercrime report will be filed (Section IV-B). Lastly, we discuss participants' written feedback about our interface (Section IV-C).

A. Accuracy of Triage Queues

The main goal of our proposed design was to properly triage reports that PayPal receives both internally and externally. For eight of our ten cybercrime scenarios (six phishing incidents, two malware incidents), participants were specifically told they were NQCPay customers and they were supposed to internally report the incident to NQCPay. The intended way to report a phishing incident to NQCPay in our interface is by forwarding the phishing email to the appropriate email address.

TABLE III
Breakdown of participants' reporting preferences for phishing incidents (NQCPay-related scenarios)

Reporting Entity	Reporting Avenue	Number of Incidents Reporting
NQCPay	email	155/315 (49.2%)
NQCPay	web form	109/315 (34.6%)
NQCPay	phone	14/315 (4.4%)
Outside NQCPay	email	17/315 (5.4%)
Outside NQCPay	web form	17/315 (5.4%)
Outside NQCPay	phone	3/315 (1%)

TABLE IV
Breakdown of participants' reporting preferences for malware incidents (NQCPay-related scenarios)

Reporting Entity	Reporting Avenue	Number of Incidents Reporting
NQCPay	email	50/118 (42.4%)
NQCPay	web form	49/118 (41.5%)
NQCPay	phone	5/118 (4.2%)
Outside NQCPay	email	3/118 (2.5%)
Outside NQCPay	web form	10/118 (8.5%)
Outside NQCPay	phone	1/118 (1%)

If the participant was assigned a malware incident, they were provided one of two intended options to report: to speak to a customer service representative over the phone or fill out a web form. For the remaining two cybercrime scenarios (i.e., online extortion and online scam) participants were specifically told they were not NQCPay customers, thus, they were supposed to report their victimization to the relevant external entity.

Tables III & IV provide a breakdown of participants' preferences to report phishing and malware incidents that were to be reported to NQCPay, respectively. Please note that some cybercrime types appeared more often since there were more scenarios with that specific cybercrime.

Among the 315 phishing incidents that were randomly assigned to our participants, 155 incidents (49.2%) were reported as intended to NQCPay via email. Among the 118 malware incidents, 54 incidents (45.7%) were reported as intended to NQCPay via web form or phone. As for the accuracy of filing the two types of incidents externally to NQCPay, 52 out of 67 online extortion incidents (77.6%) and 19 out of 23 online scam incidents (82.6%) were reported as intended to the appropriate outside entity.

We conjecture that the resulting accuracy rates are lower than expected for several reasons. First, we simulated cybercrime victimization in each of the scenarios so participants may have not felt invested in the scenario assigned.

Second, since we utilized SurveyMonkey to host our interface, we did not have the capability to track a participant's actions when filing a report through our interface since all data that is collected on SurveyMonkey is simply based on self-reported data from participants; therefore, it is possible that participants may have simply misremembered who they reported their victimization to and/or the reporting method they selected. One way this issue can be mitigated in the future is by adding options such as "I would like to file via [reporting

avenue option of choice]" within the interface design to better track our participants' chosen reporting actions rather than simply basing it on their own recollections.

We would also like to note that some participants may have misunderstood what constituted "reporting via web form" since the entire reporting interface is online. We noted this issue during our pilot run and decided to change "web form" to "online report" in the survey portion of our study. However, it is still possible that a number of participants conflated the true meaning of what reporting via online report entailed. In reality, such a matter would not be a critical issue since individuals would directly report to the intended reporting avenue of their choice and not be asked to recall what they selected afterwards.

Third, participants may have misunderstood the cybercrime they were assigned to particularly where we did not specifically outline in the scenario what cybercrime took place. Incidents that were incorrectly filed externally were classified as such based on the fact that they were incorrectly filed to NQCPay rather than to a relevant external entity. The external reporting avenue itself was not measured for accuracy since there are different reporting avenues offered by external reporting entities. We conjecture that one reason why a computer user would want to report an incident to a company like PayPal may be because they are customers themselves or because they trust the company to be better equipped to handle such incidents than an external entity like a government/law enforcement agency.

Between the phishing and malware incidents that were randomly assigned to our participants, a total of 51 incidents were reported to an external entity. While for the purposes of our study such reports were not filed in the intended way, they technically would not have been considered misfiled since a cybercrime victim is free to report to whomever they wish. For example, if a NQCPay customer experienced a phishing incident they may want to file to an external entity that focuses on combatting phishing (i.e., APWG) instead of filing to NQCPay; in other cases, they may want to file both internally and externally to NQCPay while in our study they were limited to reporting to one entity.

Interestingly, among the 54 malware incidents that were reported as intended, 49 participants (90.7%) chose to report via web form instead of speaking to a customer service representative over the phone. Therefore, we believe that adding the web form option as an alternative reporting avenue for reporting non-phishing related incidents like malware is a good idea.

Lastly, most of the phishing and malware incidents (a little under 90%) were correctly filed to NQCPay; the inaccuracies came from selecting the wrong reporting avenue. Despite a number of participants not reporting phishing and malware incidents in the way we had intended, we believe the disparity may simply be based on participants' personal preference. For instance, nearly 40% of phishing incidents were filed via web form or phone rather than email while slightly over 40% of malware incidents were filed via email rather than web form or phone. This suggests that cybercrime victims may have

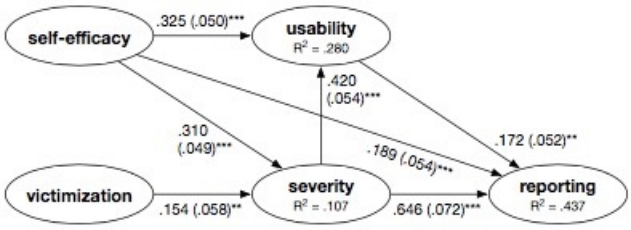

Fig. 9. The outcomes of the Structural Equation Model. Numbers on the arrows represent standardized regression coefficients (with standard errors), $** : p < 0.01$, $*** : p < 0.001$

different reporting preferences, which prior research has also found [3]. Therefore, we suggest that all cybercrime reporting entities including PayPal should consider offering multiple avenues to report, which can help mitigate the chance of reports not being filed if a victim does not feel inclined to report through the one avenue that is being offered.

B. Theoretical Model Results

The constructs of our CFA and the victimization index variable were subjected to Structural Equation Modeling (SEM) to test our research hypotheses. Modification indices of our initial structural model indicated a missing effect of severity on usability (modification index: $\chi^2(1)$ = 453.4). After adding this effect, our model showed a moderate fit ($\chi^2(224)$ = 897.2, CFI = .942, TLI = .934, RMSEA = .076, 90% CI: [.071; .081]). Fig. 9 shows the resulting model.

As hypothesized, participants' past victimization is positively associated with their perception of the severity of cybercrimes although the effect is small ($\beta = 0.154$, p = .008, H1 supported). Interestingly, participants' cybercrime self-efficacy is positively associated with their perception of the severity of cybercrimes ($\beta = 0.310$, $p < .001$, H2 not supported). That being said, self-efficacy is positively associated with participants' perception of the usability of our cybercrime reporting interface–a small to medium-sized effect–as hypothesized ($\beta = 0.325$, $p < .001$, H3 supported), and there is an additional indirect effect via severity due to a medium-sized effect of severity on usability ($\beta = 0.420$, $p < .001$). Self-efficacy is also positively associated with their tendency to report cybercrimes ($\beta = 0.189$, $p < .001$, H4 supported). And this small effect is amplified via partial mediation (via severity, usability, and both–the total effect is medium-sized).

Participants' perception of the severity of cybercrimes is positively associated with their tendency to report them and this is the strongest effect in our study (a medium-sized effect with $\beta = 0.646$, $p < 0.001$, H5 supported). Finally, participants perception of the usability of our cybercrime reporting interface is indeed positively associated with their tendency to report cybercrimes (a small effect with $\beta = 0.172$, $p = .001$, H6 supported). Thus, the usability of our reporting interface has a significant effect on reporting tendency, which validates our efforts to improve the usability of the reporting experience.

C. Qualitative Feedback

We gave participants the opportunity to provide written feedback about our cybercrime reporting interface. We extracted three key themes from the positive feedback we received from participants: our reporting interface is *user-friendly, informative,* and offers *multiple avenues to report.* Themes were derived from the propensity of key terms and descriptors that were used across the written feedback we received with the aid of textual analysis tools (e.g., word cloud) in order to mitigate any potential research bias. The written feedback was then appropriately grouped under one of the three themes mentioned. These themes reflect the set of features we aimed to achieve in creating our reporting interface. We briefly provide some of our own insights under each theme along with a sample of comments under each theme heading below. We would like to note that our contextualization of our participants' feedback is somewhat limited since we did not have the opportunity to further inquire about their opinions.

1) User Friendly.: We received feedback stating that our reporting interface was easy to navigate and understand. Arguably, our use of layman's terms throughout the interface contributed in part to our interface's user-friendly feel, which was corroborated by the following participants' feedback:

"[the interface] was user friendly and provided definitions for my alleged crime"

"It used simple language that was easy to understand and walked me through the process."

As highlighted by one of our participants, definitions were provided when technical terms were used (i.e., phishing). Again, our main justification for this was to control for users' potential lack of cybercrime knowledge, which could potentially lead to an incident being misreported.

Secondly, we also received positive feedback regarding the overall format of our reporting interface, which utilized a simple survey-based approach. We received comments like the following from participants regarding the simple Yes or No question format of our interface:

"It was easy to use, simple yes or no answers to click through."

"It was very easy to navigate using only the yes and no questions."

This particular format was viewed by some participants as "easy" and appears to reduce the burden of requiring the victim to decide on the appropriate reporting method for the incident they experienced as the following participants state:

"It was easy, step by step format that made me confident I was reporting it the correct way"

"I liked that the interface was easy to use and asked a series of questions to determine the most appropriate reporting avenue for my situation."

Moreover, when asked about their level of agreement with the following statement in our survey, *"The reporting interface was easy to use,"* an overwhelming majority of our participants agreed with this statement (i.e., 193 participants completely agreed (36.9%) and 220 (42.1%) participants agreed).

Lastly, a few participants were aware that the appropriate contingencies were in place if an individual incorrectly triaged themselves as evidenced by the following comments from our participants:

"i wasnt sure and when i picked the wrong thing, it told me where to go to it."

"Seemed simple enough to navigate and it seemed like it had redundancies built in so that even if you werent 100% sure of what to report, it would get you to the right place."

The most plausible scenario where an incorrect triage would likely arise is when an individual interacts with the web form, which provides a brief reminder on how to report phishing incidents and non-phishing related incidents if filling out a web form is not preferred (see Figure 5). We surmise that this would be useful in the event that an individual reaches the web form and wants to report a phishing incident to the company, which should have been done through the email reporting avenue instead.

2) Informative: One key facet of our reporting interface was the availability of resources to educate the user about cybercrimes; we used the homepage of the interface as the first opportunity to achieve this. Moreover, if a user wants to report an incident that is unrelated to the company then they should also be educated about the various external entities that can address the incident. This is represented by our external triage page (see Figure 2). The inclusion of this page is motivated by prior research that has shown that computer users lack general cybercrime reporting knowledge [3] [4]. We had a number of participants express their appreciation for the presence of such resources being mentioned within our interface:

"It provided links to useful websites, that I otherwise wouldnt have known."

"I like how it gave you options on which government agency to report to and their links, very helpful."

However, the key value of this information could not be better highlighted than by the following participant's comment:

"It actually routed me to the governmental website in question. Im literally about to file a complaint for a different issue Im having in a real life, because I didnt know the government had a page to report this until just now."

While we are pleased to have educated this participant on the availability of such crucial resources through our study, we are disheartened to hear the lack of awareness of their existence. Bolstering everyday computer users' cybercrime reporting knowledge is essential since reporting plays an important role in combatting cybercrimes and raising users overall cybercrime awareness.

3) Multiple Avenues to Report: Another key facet of our reporting interface was to provide individuals with multiple avenues to report their incidents to PayPal where possible; thus, we provided an additional avenue (i.e., a web form) to report non-phishing related incidents aside from the one already available at PayPal (i.e., calling a customer service representative). Our results do not tell us whether adding more reporting avenues for cybercrimes will encourage more reporting to take place. However, we find that preferences towards reporting avenues do exist, which is for instance highlighted by one participant stating that they *"like not having to speak*

with a person." This finding reflects the work done by Bidgoli and Grossklags [3], for example, who found that international college students who experienced online scams were evenly split on whether to report the cybercrime they experienced via phone or web form. Consequently, the existence of split preferences towards various reporting avenues sheds light on the inadequacies of existing governmental reporting entities such as the IC3, which only offers one method of reporting through a web form. Therefore, we suggest that any entity that handles cybercrime reports should consider incorporating multiple reporting avenues.

We were also interested in understanding what participants *disliked* about our cybercrime reporting interface as a means to make refinements to future iterations of our interface. The most prevalent negative feedback was that our design was overly simplistic, had poor aesthetics, or felt impersonal. Some of these problems can be overcome by making our interface look more aesthetically pleasing. Since we used SurveyMonkey to build a prototype of our reporting interface, we were limited to the built-in features that were offered by the platform to build the various pages of our design. Building a more professional-looking reporting interface within PayPal's platform would resolve these problems.

The remaining problems are related to users' uncertainty as to what happens after a report is filed. This is a fundamental problem of the cybercrime reporting process in general and contributes to cybercrimes going unreported. Research suggests that governmental cybercrime reporting entities like the IC3 can overcome this issue by creating case files that a victim can access to check the status of their report [2]. Similarly, one participant suggested adding a live chat feature for individuals who need help filing their report, which interestingly is a built-in feature of the FTC's Complaint Assistant. Ultimately, it will have to be at the discretion of the implementing organization to determine what the appropriate responses would be for the backend processes of the interface and whether the response would be automated, human driven, or a mixture of both.

V. Limitations

This study was funded and supervised by PayPal as an internship research project; as a result, there were specific deadlines the project was to meet in order to be executed in time. Thus, information such as the demographic composition of our participants could not be collected as a part of our survey since the appropriate company legal approvals to collect such data (which the company deems as sensitive) would not be received in a timely manner. Moreover, given our time constraints, the developed cybercrime reporting interface is a not fully functional mock-up (a weakness that was mentioned by some participants) and we used a cost-effective resource (i.e. SurveyMonkey) to realize our design conceptualization.

Secondly, the overall usability of our proposed interface design was only tested in two ways: (1) by asking a series of items regarding the overall usability of our reporting interface represented by one of the constructs we tested in our theoretical model (see Table I) and (2) by the written positive/negative feedback we received from our participants. Our design's overall focus was predominantly motivated and designed around properly triaging cybercrime reports internally and externally to PayPal. Future iterations of our study should employ commonly used usability testing techniques such as the think aloud protocol, which involves a more direct approach to understanding a user's thought process in approaching the task to file a report with our interface.

VI. Discussion

The results of our statistical model show users' victimization, self-efficacy, and perception of cybercrimes' severity all had a positive effect on the likelihood to report a cybercrime. Most notably, users' tendency to report cybercrimes was also influenced by the usability of our proposed interface. By utilizing a minimalist survey-based design that asks simple Yes or No questions, our interface not only lessens the burden of figuring out how to properly file a report, but also increases the chance that the report will be appropriately handled by the relevant responding entity whether that is the organization itself or an outside entity.

Moreover, we believe that offering multiple avenues to report cybercrimes empowers the victim to choose the avenue that they deem most appropriate. Currently existing cybercrime reporting interfaces do not provide this capability, thus, we recommend that they consider this in the future. Having multiple reporting avenues can increase the likelihood that cybercrimes will be reported.

Lastly, since education about how to protect against and report cybercrimes is lacking, we believe that the onus should be on the industry to educate their customer base and others about the propensity and severity of cybercrimes that could potentially affect them. A poignant place where this awareness can be spread is through reporting interfaces like our own, which can provide helpful links to resources that can properly educate those who were unaware of the existence of certain cybercrimes as well as those who are uncertain how certain cybercrimes can be reported to external entities such as the FTC and IC3.

VII. Conclusion

In this paper, we conducted a study to test a prototype for a streamlined cybercrime reporting interface that PayPal is considering to use in the future. The overall goal of this effort was to address the history it has with reports that have been misdirected within the company or that are unrelated to the company and need to be redirected to the appropriate external reporting entities.

Our statistical model finds that a usable reporting interface can increase users' tendency to report cybercrimes and the qualitative feedback we received regarding our interface indeed presented an overall positive theme of "user friendliness." However, the overall success of the reporting interface in the triage of reports was not as high as we had hoped. Different usability methodologies (e.g., the think aloud protocol) should

be administered to address design issues in the reporting interface that may have contributed to these lower than expected accuracy rates.

We hope that the results from our study will open a conversation within the industry and beyond about how cybercrime reporting should be addressed, most notably by introducing interactive, streamlined customer-facing reporting interfaces like the one proposed in this paper.

REFERENCES

[1] J. Balkin, J. Grimmelmann, E. Katz, N. Kozlovski, S. Wagman, and T. Zarsky. *Cybercrime: Digital cops in a networked environment*. NYU Press, 2007.

[2] M. Bidgoli and J. Grossklags. End user cybercrime reporting: What we know and what we can do to improve it. In *IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, pages 1–6. IEEE, 2016.

[3] M. Bidgoli and J. Grossklags. "Hello. This is the IRS calling.": A case study on scams, extortion, impersonation, and phone spoofing. In *2017 APWG Symposium on Electronic Crime Research (eCrime)*, pages 57–69. IEEE, 2017.

[4] M. Bidgoli, B. P. Knijnenburg, and J. Grossklags. When cybercrimes strike undergraduates. In *Electronic Crime Research (eCrime), 2016 APWG Symposium on*, pages 1–10. IEEE, 2016.

[5] F. Bridges, L. Appel, and J. Grossklags. Young adults' online participation behaviors: An exploratory study of web 2.0 use for political engagement. *Information Polity*, 17(2):163–176, 2012.

[6] F. Davis. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, pages 319–340, 1989.

[7] N. Eubanks. The true cost of cybercrime for businesses. https://www.forbes.com/sites/theyec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/#2ea09c774947. Jul 2017.

[8] M. D. Goodman and S. W. Brenner. The emerging consensus on criminal conduct in cyberspace. *International Journal of Law and Information Technology*, 10(2):139–223, 2002.

[9] W. Goucher. Being a cybercrime victim. *Computer Fraud & Security*, 2010(10):16–18, 2010.

[10] J. Grossklags, L. Appel, and F. Bridges. Young adults and online political participation: Search strategies and the role of social media. In *Proceedings of the 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times*, pages 302–306. ACM, 2011.

[11] J. Nielsen. 10 usability heuristics for user interface design. https://www.nngroup.com/articles/ten-usability-heuristics/. Jan 1995.

[12] F. B. of Investigation. 2017 Internet Crime Report. 2017.

[13] E. Peer, J. Vosgerau, and A. Acquisti. Reputation as a sufficient condition for data quality on Amazon Mechanical Turk. *Behavior Research Methods*, 46(4):1023–1031, 2014.

[14] K. Pernice. UX prototypes: Low fidelity vs. high fidelity. https://www.nngroup.com/articles/ux-prototype-hi-lo-fidelity/. Dec 2016.

[15] V. Venkatesh and H. Bala. Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences*, 39(2):273–315, 2008.

[16] D. S. Wall. Policing cybercrimes: Situating the public police in networks of security within cyberspace. *Police Practice and Research*, 8(2):183–205, 2007.

[17] D. S. Wall. Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law, Computers & Technology*, 22(1-2):45–63, 2008.

[18] B. Wardman, L. Kelly, and M. Weideman. Voice of the customer. In *eCrime Researchers Summit (eCRS)*, pages 1–7. IEEE, 2013.

[19] M. Yar. *Cybercrime and Society*. Sage, 2013.