

# SMILE4VIP: Intervention to Support Visually Impaired Users Against Phishing

1<sup>st</sup> Mark Bohlender  
Karlsruhe Institute for Technology  
Karlsruhe, Germany  
mark.bohlender@student.kit.edu

2<sup>nd</sup> Raphael Morisco  
Karlsruhe Institute for Technology  
Karlsruhe, Germany  
raphael.morisco@kit.edu

3<sup>rd</sup> Mattia Mossano  
Karlsruhe Institute for Technology  
Karlsruhe, Germany  
mattia.mossano@kit.edu

4<sup>th</sup> Thorsten Schwarz  
Karlsruhe Institute for Technology  
Karlsruhe, Germany  
thorsten.schwarz@kit.edu

5<sup>th</sup> Melanie Volkamer  
Karlsruhe Institute for Technology  
Karlsruhe, Germany  
melanie.volkamer@kit.edu

**Abstract**—Phishing is an ever increasing danger that threaten both sighted and visually impaired users. Yet, most of the research in this field focuses on sighted users, even though visually impaired people are equally threatened by phishing attacks. To help visually impaired people detect phishing attacks, we propose here an initial version of a novel tool, *SMILE4VIP*. *SMILE4VIP* builds on the results obtained by other tools with sighted users, and adapt their solutions to visually impaired people. We ran a preliminary online feedback study with  $N = 4$  visually impaired participants to investigate their thoughts on both our tool and our study design. Although the tool was well received, we received several interesting feedback on both the tool and the study itself. We plan to implement the feedback on both, and then run a larger scale user study to determine the effectiveness of *SMILE4VIP*.

**Index Terms**—assistive technology, anti-phishing, phishing intervention

## 1. Introduction

Phishing was the most reported and expensive cyber security threat of 2023, according to the Federal Bureau of Investigation [9]. This is not surprising, as the latest Anti-Phishing Working Group’s report [4] declared 2023 to be the worst year on record for phishing.

To answer this danger, researchers proposed numerous solutions, from awareness measures (e.g., [14], [24]–[26], [28]) to support tools (e.g., [3], [15], [19], [22]). Yet, Yu et al. [27] show that past research focused on sighted users. This is a problem, given that *visually impaired people* (VIP) are also targeted by phishing attacks.

Moreover, beyond the obvious issue that any anti-phishing tool based on visual cues (e.g., icons and banners) would not work with VIP, there is also to consider how VIP interact with the virtual environment. Namely, they use *screen-readers*, technologies that read the screen through a voice synthesizer (aka, *Text-to-Speech*, or TTS, e.g., Apple “VoiceOver” [5], Google “TalkBack” [10], Microsoft “Narrator” [13]). The problem is that TTS are not focused on security: for example, screen readers can only read the URL behind

a link if the link uses special HTML elements (e.g., those from the ARIA initiative [7]). Yet, a common way to detect phishing is by checking the URL behind a link, namely the domain and top-level domain part of it. Any accessible anti-phishing tool aimed at VIP, then, cannot be based on visual cues and must work with screen readers.

There have been some proposals aimed at VIP in the past, but they all fall short of accessing the URL behind a link. Sonowal [21] proposes an email filter (SPEDAS) that rejects emails based on how close the TTS pronunciation of URLs is to legitimate URLs. Although it reached 83% accurate phishing detection, it does not address TTS issues reading URLs. Yu et al. [27] compare Google Gmail phishing warnings with some of their own design optimized for use with TTS. They showed that their proposal is more effective than the Gmail warnings. Yet, they still do not consider the URL behind a link.

We believe a different approach is possible: start from tools developed for sighted users, and adapt them to VIP and TTS. Namely, we find two interventions especially promising: *SMILE* [6], [15] and *TORPEDO* [20], [22], [23]. An overview of both is in Section 2.

Our proposal, called *SMILE4VIP*, adds *TORPEDO* risk level assessments to an email subject line, avoiding relying on tooltips and other visual cues, and applies *SMILE* modifications to the email links, allowing TTS access to the URL behind the link. It also produces auditory alerts, to further differentiate between risk levels. *SMILE4VIP* is meant as an add-on for the Thunderbird email client, with the potential to adapt it to other clients in the future. *SMILE4VIP* is described in Section 3.

We conducted a first feedback online study with four VIP to achieve two goals: first, receive their thoughts on our intervention. Second, determine if our design was a viable solution for online studies with VIP. The latter point is quite salient: both *SMILE* and *TORPEDO* were evaluated with online user studies, but this is not a viable solution for *SMILE4VIP*, as VIP cannot judge screenshots or other animated mock-ups. Hence, we designed an online study that could be completed by VIP. A detailed overview of the study is in Section 4.

We plan to follow-up on this initial study by implementing the changes proposed by the participants in *SMILE4VIP*, and evaluate it in a large scale user study.

## 2. Background

This section briefly describes TORPEDO and SMILE.

### 2.1. TORPEDO

TORPEDO [20], [22], [23] presents users with a tooltip next to any link hovered with the mouse, as per Petelka et al. [19] suggestion.

The tooltip uses URL highlighting to increase the visibility of the domain part of the URL. For example, the URL “https://www.example.com/path” would be shown as “https://www. **e x a m p l e . c o m** /path.” Further, its border is color-coded on the risk level of the link currently hovered. The risk level itself is determined by following a set of checks: first, TORPEDO compares the domain of the URL behind the link with an allow-list of safe URLs based on the ALEXA Top visited web sites. Then, it checks an allow-list of domains previously checked and visited by the user. Finally, TORPEDO checks the URL for potentially dangerous characteristics, e.g., non-ASCII characters, use of IP address, and mismatch between link anchor text and actual URL. These steps allow TORPEDO to distinguish between three risk levels:

- **Low risk** - URL part of the allow-lists. Green (Alexa list) or blue (visited and checked) border.
- **Unknown risk** - URL not part of the allow-lists. Gray border.
- **Unknown with indicators of high risk** - URL not part of the allow-lists and contains dangerous characteristics. Gray border with triangular sign with exclamation mark in the upper-left corner.

The tooltip also contains a brief explanation of the potential dangers of clicking a link, with text tied to the risk level. Examples of the levels are in the Appendix.

The add-on disables the link for a short period (default, 3 seconds) to force users to inspect the link before clicking, giving them some time to check the URL. This is done because previous results show that time friction might increase users’ phishing detection [19]. Further, TORPEDO resolves short URLs and redirection URLs, showing the hidden destination URL to users.

Volkamer et al. [22] show that TORPEDO significantly improves phishing email detection, reaching 85.17% correct phishing detection versus 43.31% without it.

Unfortunately, TORPEDO relies on visual cues to convey its warnings, e.g., different colors, tooltips, URL formatting. This would not work for VIP, as any visual cue would not be perceived. Furthermore, TORPEDO works through a tooltip. Tooltips as a whole, if not programmed using specific HTML elements (e.g., `aria-describedby` [16]), are not accessed nor read by TTS. Even when accessible HTML elements are used, the TTS must be able to recognize them, which is not always the case (e.g., NVDA only does so if enabled by the user [18]). Still, as previous work on sighted people shows that they need help to read and understand URLs (e.g., [1], [2], [8], [29]), we believe a tool like TORPEDO would be helpful to VIP too. Namely, we believe that the different risk levels can be communicated in ways that allow VIP to access them through TTS, for example, as text in the subject of an email.

### 2.2. SMILE

SMILE [6], [15] replaces the anchor of email links with *SMILE-strings*, i.e., domain and top-level domain of the URL behind the links. For example, the URL “https://www.example.com/path” would be shown as “example.com.” Users can then check if they would be taken to the legitimate website or elsewhere.

The program identifies four link types and apply different substitutions to each one:

- **Image** - Link anchored to an image. SMILE-string added above the image, between square parenthesis, preceded by “Image link.”
- **URL-like** - Link anchored to URL-like text, e.g., “example.com.” SMILE-string replaces the anchor, between square parenthesis.
- **Misc** - Link anchored to generic text, e.g., “Click here.” SMILE-string replaces the anchor, between square parenthesis, preceded by the original text.
- **Area** - Various links anchored to an image. SMILE-strings added above the image, between square parenthesis, preceded by “Area link.”

Examples of the substitutions are in the Appendix. Besides the above, SMILE handles non-ASCII characters by replacing them with Punycode, and IP addresses by applying a URL-like substitution with the full IP address. It also resolves short URLs and redirection URLs.

Beckmann et al. [6] show that SMILE significantly improves phishing emails detection to 71.7% compared to 50% without it.

When considering how VIP interact with links (see Section 1), the SMILE-strings should make links easily readable by TTS, increasing phishing detection. Yet, SMILE does not offer the analysis support of TORPEDO. This is a limitation, because we mentioned before that VIP likely needs as much support reading and understanding URLs as sighted users (see Section 2.1). Hence, we believe that combining SMILE with a TORPEDO-like risk analysis that considers the specific needs of VIP would lead to a tool better capable of supporting them.

## 3. SMILE4VIP Description

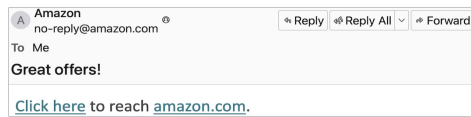
SMILE4VIP aims at supporting VIP detection of phishing emails. Examples of how a modified email would look like is in Figure 1. Namely, its focus is on phishing emails not identified by email filters and delivered to the users’ inbox. SMILE4VIP works independently of the TTS used, i.e., any TTS should potential work with it.

Client wise, SMILE4VIP is meant to be used in Mozilla Thunderbird, with adaptations to other clients as potential future work. The description of why we chose Thunderbird is in Section 4.1.2.

Like TORPEDO (Section 2.1), SMILE4VIP uses risk levels, albeit, differently than the former, the latter does not display them for each link contained, but rather for the entire email. Namely, the highest risk level among the links (evaluated with the same rules as TORPEDO) determines the email overall risk level.

The warning to notify users of the risk level is not added to the email text, but rather to the subject line. The design idea is to modify the subject so that VIP can

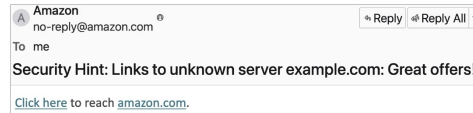
### Unmodified



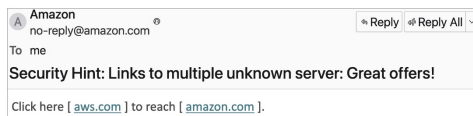
### Legitimate Single Domain



### Phishing Single Domain



### Legitimate Multiple domains



### Phishing Multiple domains



Figure 1. Example showing SMILE4VIP case dependent modifications. From the top: the email as it looks without SMILE4VIP; the email if both links lead to the same domain, legitimate on the left, phishing on the right; the email if the first link leads to a domain and the second link to a different domain, legitimate on the left, phishing on the right.

decide whether they want to examine the email further (i.e., read it aloud) or not. In case all links point to the same domain, then the domain is added to the subject line and the email text is left unchanged. If more than one unknown domain is present, SMILE4VIP applies SMILE substitutions (Section 2.2) to the links to show domain and top-level domain as anchor text. We chose to only use SMILE substitutions in this case to limit the impact of our tool on VIP reading strategies. Furthermore, to ensure that the risk level warning is noticed, SMILE4VIP plays an acoustic alert using Auditory Icon or Earcon for the Unknown Risk level.

SMILE4VIP distinguishes between two risk levels:

- **Low Risk:** All URLs are on the allow-list. Email unmodified, and no warning added to the subject.
- **Unknown Risk:** At least one URL not on the allow-list. Two sub-cases distinguished:
  - All URLs lead to one unknown web server. An auditory alert is played and the sentence: “Security Hint: Links to unknown server example.com:” added before the subject.
  - The URLs lead to various unknown web servers. An auditory alert is played, the sentence: “Security Hint: Links to multiple unknown servers:” added before the subject, and SMILE substitutions applied to the links.

SMILE4VIP resolves the destination URL of known short URL / redirection URL services, as done by both TORPEDO and SMILE. The destination URL is then used to determine the risk level.

The text added to the subject can be shortened by the users, if desired, e.g., reducing it to “Server example.com unknown”. Like TORPEDO, the allow-list is not static, and the users can add or remove entries through the

settings. For instance, a company can classify commonly used domains or servers as low risk, reducing the number of emails classified as unknown.

After installation, users receive a brief introduction to SMILE4VIP functionalities. Namely, that: (1) the warning means the security checks cannot assess the email risk, and the user must decide themselves, (2) the warning does not indicate legitimacy or phishingness, only potential risk, and (3) how to determine whether an email with a risk level warning is legitimate or not (i.e., a brief awareness intervention).

In summary, SMILE4VIP not only combines features of TORPEDO and SMILE, but refines and adapts them to create an accessible solution tailored to VIP.

## 4. Feedback Study

This section describes the methodology of our feedback study and its results.

### 4.1. Methodology

Our goal is twofold: first, get feedback on SMILE4VIP from VIP, and collect initial hints on its effectiveness. Second, determine if our study design is a viable option to run online user studies with VIP.

The recruitment for our study was done informally through contact with VIP that cooperated in the past with one of the authors. They were invited via email as volunteers, with no compensation for their help.

No control group was recruited. TTS cannot read URL behind links and most anti-phishing recommendations are aimed at sighted users. Hence, a group without SMILE4VIP could only guess the legitimacy of an email. The results of the follow-up study will be compared with those of TORPEDO and SMILE to determine if VIP achieve similar levels of phishing detection.

**4.1.1. Study Design.** The feedback study itself is implemented in SoSci Survey, chosen for two reasons: first, it abides to the GDPR rules. Second, it has a built-in accessible version, making the use by VIP more easy.

The study starts with an informed consent on the rights of the participants and information on the protection of their data. We then inform the participants of the task we ask them to complete and show them an introduction to SMILE4VIP. This introduction contains the same information as the one shown after the tool installation (see Section 3).

Following the introduction, the participants are asked to download a portable version of the Thunderbird client, with 48 pre-archived emails, some modified to simulate how they would look after SMILE4VIP is applied, and others not. Further information on the mock-up used in the study is in Section 4.1.2.

The participants then see a scenario: they are Martin, and their friend Thomas forwards them emails he thinks might be interesting without checking their legitimacy. The next 48 pages (one per email) have two questions each: a binary question regarding the legitimacy of the corresponding email, and a five-point Likert scale to express how sure participants are of their answer.

Then, we ask the participants eleven questions on their impression of our tool, if they have feedback on it, and if they have feedback on the study design itself. These questions can be found in the Appendix.

In the end, we ask our participants some demographics questions, and thank them for their help.

**4.1.2. Thunderbird Mock-up and Study Emails.** We prepared a portable version of Mozilla Thunderbird [11] to allow participants to go through the study. We chose Thunderbird for several reasons. First and foremost, this allows participants to use the TTS already installed on their machines, avoiding them having to learn how to use a different set-up. Furthermore, this allowed us to see if SMILE4VIP can work with different TTS or whether some might cause problems to it. The second reason why we chose this Thunderbird version is that it does not collect nor leave behind personal information. Finally, there were several reasons related to the study design itself. Thunderbird Portable, like its non-portable version, let us easily prepare the emails to judge through the ThunderHTMLedit add-on.<sup>1</sup> This add-on allowed us to modify the HTML source code of every email directly in the compose window. We could then store the modified emails inside Portable Thunderbird itself, and deliver everything in a single compressed archive to the participants. The participants only had to click a link in the user study, download the archive, extract it, and Portable Thunderbird would simply work as if they installed non-portable Thunderbird. Once the study was over, each participant could simply move the archive and Portable Thunderbird in the trash bin.

To create the emails themselves, we did not use real world phishing emails to avoid exposing our participants to unnecessary danger if they clicked on the links. Instead, we modified legitimate emails by changing the URL behind the links. Specifically, we collected several

newsletters and advertisement email, until we reached the intended 48 emails, making sure to have no more than 4 emails from the same sender. We determined to need 48 emails based on a categorization of the features we wanted to evaluate. These features were: 1) being low risk or unknown risk, 2) linking to a single domain or multiple domains, 3) being legitimate or phishing, and 4) which among three phishing tricks was used (described later). This initially led to 24 distinct emails ( $2 * 2 * 2 * 3 = 24$ ). However, we also wanted to be sure that the specific email used did not influence the participants, e.g., because they knew the provider. Hence, we used two emails for each feature, leading to the total of 48.

As mentioned, the phishing URLs contained one out of three phishing tricks: 1) a random domain different from the legitimate one; 2) an attack where one URL character is changed but similar, e.g., from “galeria.de” to “qaleria.de”; 3) an inversion of two characters of the URL, e.g., from “aldi-sued.de” to “adli-sued.de.”

Regarding the emails distribution, we assumed that approximately 20% of all emails (9.6, rounded-up to 10) contained links leading to more than one domain. Table 1 shows the final distribution of the emails. Note, no phishing case is considered as Low Risk. As phishing domains are usually not among the top visited websites, and therefore not part of SMILE4VIP allow-list, they are normally evaluated as Unknown Risk.

## 4.2. Results

We present here our participants’ feedback on the two primary facets of the study: tool support and study design.

**4.2.1. Demographics.** As mentioned in section 4.1, we adopted an informal recruitment methodology of known VIP. Namely, we contacted  $N = 60$  VIP through emails. Of the initial VIP contacted,  $N = 6$  started the survey, but only  $N = 4$  completed it. Demographics information of these four participants are in Table 2. Our results are based on the answers of these four VIP.

**4.2.2. Feedback - Tool Support.** Regarding SMILE4VIP effectiveness, our participants correctly distinguished legitimate from phishing emails 74.58% of the time on average. This detection rate would set SMILE4VIP at a similar effectiveness level as SMILE, but lower than TORPEDO. Yet, participants were not particularly sure of their choices, with an average of 3.52 on a five-point Likert scale. We want to stress, though, that these are merely preliminary results, and a larger study is required.

The quantitative results are somewhat mirrored in our participants’ feedback, with several pointing out that SMILE4VIP helped them in their task. In particular, they found the subject line warnings helpful, and they might recommend SMILE4VIP to other VIP. Yet, one participant was considerably less enthusiastic about our intervention, stating that they could not determine if it helped them or not. This too is mirrored in the quantitative data, given that the same participant was also the one with the lowest correct distinction rate, only reaching an average of 52% correctly distinguished emails. Still, even this participant mentioned that they would recommend SMILE4VIP.

1. Unfortunately, ThunderHTMLedit is no longer available.

TABLE 1. DISTRIBUTION OF STUDY EMAILS.

	Low risk		Unknown risk		Total
	Single domain	Several domain	Single domain	Several domains	
Legitimate	10	2	10	2	24
Phish - Random	-	-	6	2	8
Phish - Similarity	-	-	6	2	8
Phish - Inversion	-	-	6	2	8
Total	10	2	28	8	48

TABLE 2. DEMOGRAPHICS OF THE PARTICIPANTS.

	Partic. 1	Partic. 2	Partic. 3	Partic. 4
Gender	Male	Male	Male	Male
Age Group	20-39	20-39	60+	20-39
Previous Phishing Info	No	No	No	No
Industry Experience	No	No	No	Yes
Screen Reader	JAWS	JAWS	NVDA	NVDA
Visual Impairment	Blind	Blind	Blind	Blind
Thunderbird Experience	Yes	No	No	Yes

On the side of which improvements the participants would like to see, the most mentioned one was a more granular information on the link analysis. Namely, that *per-link* indicators of legitimacy would be welcomed, i.e., a risk level analysis of every link alongside the overall email risk analysis in the subject line. Also welcomed would be the possibility to query WHOIS for further information on the domain (e.g., ownership, length of existence, etc.) At the same time, shorter text in the subject line for the email overall analysis would also be a welcomed improvement.

**4.2.3. Feedback - Study Design.** On the topic of the user study itself, there was a more varied feedback.

Most notably, there were complains about the number of emails used, and some technical limitations of Portable Thunderbird. The latter, more specifically, pertained the lack of ability to check the full email header. Also the scenario was somewhat criticized as unusual. In particular, because subscription to newsletters is a personal choice, it would be strange for someone else to forward such a considerable number of them to a friend.

A more worrisome criticism was that one participant had difficulties enabling the accessible version of the questionnaire. This is not an acceptable limitation, given that all participants are likely to require such function.

On a different note, we asked the participants if they tried to visit any of the link of the study, and only one of them did so. Nonetheless, this can be potentially dangerous, in the event that any of the made-up domains becomes dangerous during the questionnaire period.

## 5. Future Works

This section describes our future work, how to integrate the feedback, and which modifications we have planned for the large scale study.

## 5.1. Implementation of the Feedback on SMILE4VIP

Based on the feedback we obtained during this first study, we plan to expand the planned functionalities of SMILE4VIP. Namely, it seems sensible to add the possibility of *per-links* analysis, i.e., showing the risk level of each link when selected, alongside the email overall risk level, i.e., the estimated risk of the email as a whole in the subject line. More technically, our initial idea is to add information on each link risk level to the body of the email through the `aria-describedby` [16] or the `aria-details` [17] attributes. This should allow TTS access to the information on the risk level on request, without interfering with the normal email reading strategies of the users. Similarly, we plan to set the shorter subject lines modifications as default, and leave the longer ones as an optional, more verbose option.

Regarding the WHOIS inquiry, this might be more difficult, both technically and ethically. On the technical side, since the introduction of the GDPR in 2018, WHOIS information has not been reliable, as any registrar could ask for their information to be scraped from the website (as mentioned in ICANN Governmental Advisory Committee [12]). Hence, WHOIS information might not lead to any benefit. Furthermore, accessing external services like WHOIS might introduce a privacy trade-off that users are unaware of. Thus, further deliberation is required to determine if this is acceptable or not.

Something that could not receive feedback is the auditory warnings. This because we used a mock-up of SMILE4VIP and the function was not present. We plan to add it and in the next iteration of study.

## 5.2. Ideas for the Improvements to the Study Design, for Conducting a Large-scale Study, and for Reaching Out to VIP

Regarding the questionnaire itself, the first thing we will address is the non-functioning accessible version. We will check if this was due to a misconfiguration on our part, or the problem originated in SoSci Survey itself.

Furthermore, we plan to address the complains regarding the scenario by proposing a more realistic one, e.g., avoiding or reducing the number of newsletters and introducing more common emails such as delivery notices.

In light of the very low turn-out in the feedback study phase, we will also revisit our recruitment strategies. Besides the obvious solution of monetary compensation (which we plan to implement), another potential option is to collaborate with a VIP association to provide credibility to our intentions. The familiarity of VIP with such

organizations might help not only with recruitment, but also to spread knowledge of our security tool.

## 6. Conclusion

We set out to receive feedback on a novel support tool aimed at helping visually impaired people to detect phishing attacks through emails, SMILE4VIP. We designed and run an online user study with visually impaired people to receive feedback on both a mock-up of our tool and our study design. Our results show that SMILE4VIP seems a promising solution. We now plan to create a working version of our tool and study more thoroughly its effectiveness. In this regard, we plan to include the participants' feedback in our study design, and then run a larger scale study with a working version of SMILE4VIP.

## References

- [1] Sara Albakry, Maria K. Wolters, and Kami Vaniea. What is this url's destination? empirical evaluation of users' url reading. In *Conference on Human Factors in Computing Systems*, CHI '20, page 1–12, Honolulu, US, 2020. ACM.
- [2] Mohamed Alsharnouby, Furkan Alaca, and Sonia Chiasson. Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, 82:69–82, 2015.
- [3] Kholoud Althobaiti, Kami Vaniea, and Serena Zheng. Faheem: Explaining URLs to People Using a Slack Bot. In *Symposium on Digital Behaviour Intervention for Cyber Security*, AISB '18, pages 1–8, Liverpool, GB, 2018. Edinburgh Research Explorer.
- [4] Anti-Phishing Working Group. Phishing Activity Trends Report. Technical Report 4th Quarter 2023, APWG, 2024.
- [5] Apple. Vision, 2024. <https://www.apple.com/accessibility/vision/>.
- [6] Christopher Beckmann, Benjamin Berens, Niklas Kühl, Peter Mayer, Mattia Mossano, and Melanie Volkamer. Design and Evaluation of an Anti-Phishing Artifact Based on Useful Transparency. In *Workshop on Socio-Technical Aspects in Security*, STAST '22, Copenhagen, DK, In Press. Springer.
- [7] World Wide Web Consortium. Providing accessible names and descriptions, 2023. <https://www.w3.org/WAI/ARIA/apg/practices/names-and-descriptions/>.
- [8] Rachna Dhamija, J. Doug Tygar, and Marti Hearst. Why phishing works. In *Conference on Human Factors in Computing Systems*, CHI '06, page 581–590, Montréal, CA, 2006. ACM.
- [9] Federal Bureau of Investigation. 2023 Internet Crime Report. Technical report, FBI, 2024.
- [10] Google. Get started on android with talkback, 2024. <https://support.google.com/accessibility/android/answer/6283677?hl=en>.
- [11] John T. Haller. Thunderbird, Portable Version, 2024. [https://portableapps.com/apps/internet/thunderbird\\_portable](https://portableapps.com/apps/internet/thunderbird_portable).
- [12] ICANN Governmental Advisory Committee. WHOIS and Data Protection.
- [13] Microsoft. Complete guide to narrator, 2024. <https://support.microsoft.com/en-us/windows/complete-guide-to-narrator-e4397a0d-ef4f-b386-d8ae-c172f109bdb1>.
- [14] Gaurav Misra, Nalin Asanka Gamagedara Arachchilage, and Shlomo Berkovsky. Phish Phinder: A Game Design Approach to Enhance User Confidence in Mitigating Phishing Attacks. In *Symposium on Human Aspects of Information Security & Assurance*, HAISA '17, pages 41–51, Adelaide, AU, 2017.
- [15] Mattia Mossano, Benjamin Berens, Philip Heller, Christopher Beckmann, Lukas Aldag, Peter Mayer, and Melanie Volkamer. SMILE - Smart eMail Link Domain Extractor. In *Computer Security. ESORICS 2021 International Workshops*, SPOSE '21, pages 403–412, Online, 2022. Springer.
- [16] Mozilla Foundation. aria-describedby, 2024. <https://developer.mozilla.org/en-US/docs/Web/Accessibility/ARIA/Attributes/aria-describedby>.
- [17] Mozilla Foundation. aria-details, 2024. <https://developer.mozilla.org/en-US/docs/Web/Accessibility/ARIA/Attributes/aria-details>.
- [18] NV Access. NVDA 2023.3.4 User Guide, 2023. <https://www.nvaccess.org/files/nvda/documentation/userGuide.html#AdvancedSettings>.
- [19] Justin Petelka, Yixin Zou, and Florian Schaub. Put Your Warning Where Your Link Is: Improving and Evaluating Email Phishing Warnings. In *Conference on Human Factors in Computing Systems*, CHI '19, pages 1–15, Glasgow, GB, 2019. ACM.
- [20] Research Group Security, Usability, and Society. TORPEDO - Add-on to support users in detecting phishing e-mails, 2024. <https://secuso.aifb.kit.edu/english/TORPEDO.php>.
- [21] Gunikhan Sonowal. A Model for Detecting Sounds-alike Phishing Email Contents for Persons with Visual Impairments. In *Conference on e-Learning*, eConf '20, pages 17–21, Sakheer, BH, 2020. IEEE.
- [22] Melanie Volkamer, Karen Renaud, and Benjamin Reinheimer. TORPEDO: TOoltip-poweRed Phishing Email DetectiOn. In *ICT Systems Security and Privacy Protection*, SEC '16, pages 161–175, Ghent, BE, 2016. Springer.
- [23] Melanie Volkamer, Karen Renaud, Benjamin Reinheimer, and Alexandra Kunz. User experiences of TORPEDO: TOoltip-poweRed Phishing Email DetectiOn. *Computers & Security*, 71:100–113, 2017.
- [24] Melanie Volkamer, Karen Renaud, Benjamin Reinheimer, Philipp Rack, Marco Ghiglieri, Peter Mayer, Alexandra Kunz, and Nina Gerber. Developing and Evaluating a Five Minute Phishing Awareness Video. In *Trust, Privacy and Security in Digital Business*, TrustBus '18, pages 119–134, Regensburg, DE, 2018. Springer.
- [25] Rick Wash and Molly M. Cooper. Who Provides Phishing Training? Facts, Stories, and People Like Me. In *Conference on Human Factors in Computing Systems*, CHI '18, pages 1–12, Montréal, CA, 2018. ACM.
- [26] Zikai Alex Wen, Zhiqiu Lin, Rowena Chen, and Erik Andersen. What.Hack: Engaging Anti-Phishing Training Through a Role-Playing Phishing Simulation Game. In *Conference on Human Factors in Computing Systems*, CHI '19, pages 1–12, Glasgow, GB, 2019. ACM.
- [27] Yaman Yu, Saidivya Ashok, Smirity Kaushik, Yang Wang, and Gang Wang. Design and Evaluation of Inclusive Email Security Indicators for People with Visual Impairments. In *Symposium on Security and Privacy*, SP '23, pages 2885–2902, San Francisco, US, 2023. IEEE.
- [28] Tianjian Zhang. Knowledge Expiration in Security Awareness Training. In *Conference on Digital Forensics, Security and Law*, ADFSL '18, pages 197–212, San Antonio, US, 2018. Embry-Riddle Aeronautical University.
- [29] Sarah Zheng and Ingolf Becker. Presenting suspicious details in user-facing e-mail headers does not improve phishing detection. In *Symposium on Usable Privacy and Security*, SOUPS '22, Boston, US, 2022. USENIX.

## Appendix

### TORPEDO Risk Level Screenshots

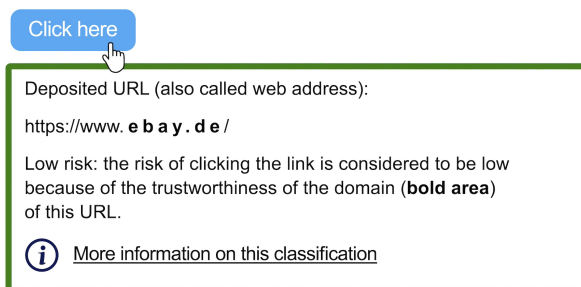


Figure 2. TORPEDO's low risk from the built-in list. Example from the TORPEDO tutorial.

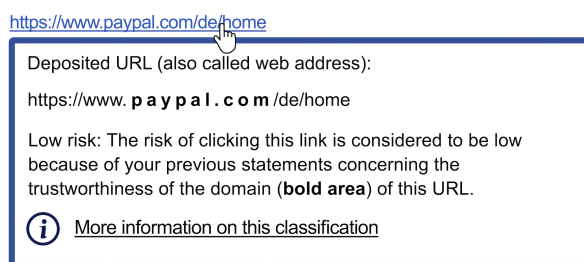


Figure 3. TORPEDO's low risk from the user-defined allow-list. Example from the TORPEDO tutorial.

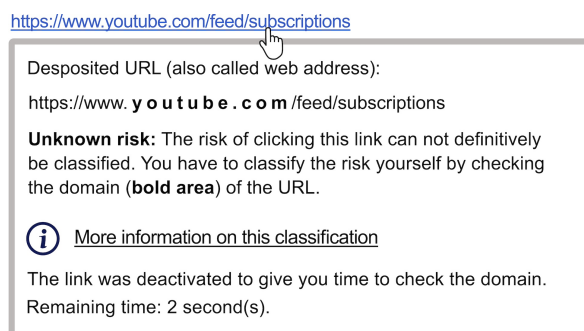


Figure 4. TORPEDO's unknown risk. Example from the TORPEDO tutorial.

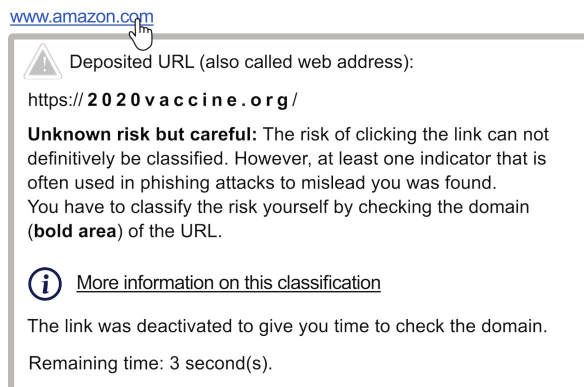


Figure 5. TORPEDO's unknown risk with indicator. Example from the TORPEDO tutorial.

## SMILE Substitutions Table







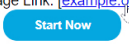

	Image Type		URL-Like		Misc		Area Map
	Generic	Button-like	Generic	Button-like	Generic	Button-like	
<i>Unmodified</i>			Register now at <a href="https://example.com/register">https://example.com/register</a>		Register now and secure benefits.		
<i>Artifact</i>	Image Link: [example.org] 	Image Link: [example.org] 	Register now at [example.com]	[example.org]	Register now [example.com] and secure benefits.	Start Now [example.org]	Area Link: [example1.com] Area Link: [example2.com] 

Figure 6. Before and after applying SMILE substitutions. From Mossano et al. [15]

## Questions Asked after Phishing Detection Task

- 1) How did you go about deciding whether it was a phishing email or not?
- 2) To what extent has the SMILE4VIP tool helped you with your decision?
- 3) Which existing function would you change in the SMILE4VIP tool and what would you change?
- 4) What other function would you like to see in SMILE4VIP?
- 5) Have you tried to open a link by clicking on it or by manually copying and pasting it into a browser? (Response options: "I have tried clicking on a link", "I have tried copying and pasting a link", "I have tried both options" or "I have tried neither option")
- 6) Do you think that SMILE4VIP makes it easier for you to recognize phishing emails with dangerous links than without the tool? Please explain why.
- 7) Do you believe that you can recognize phishing emails with dangerous links more quickly with SMILE4VIP than without the tool? Please explain why.
- 8) Do you believe that SMILE4VIP can ensure a higher phishing detection rate in business e-mail traffic? Please explain why.
- 9) Would you recommend SMILE4VIP to a friend with a severe visual impairment or blindness? Possible answers: "Yes", "No" or "Maybe."
- 10) Would you recommend SMILE4VIP to a friend without severe visual impairment or blindness? Possible answers: "Yes", "No" or "Maybe"
- 11) You can send us any further comments here.