





# Literature Review: Misconceptions About Phishing

Mattia Mossano<sup>(✉)</sup>  and Melanie Volkamer<sup></sup>

Karlsruhe Institute of Technology, Karlsruhe Kaiserstraße 12,  
76131 Karlsruhe, Germany  
{mattia.mossano,melanie.volkamer}@kit.edu

**Abstract.** Phishing is a danger to both private users and businesses. Industry and academia have proposed several approaches to deal with this threat, many of which developed with a supposedly human-centric design. Yet, to our knowledge, there is no research focused on the misconceptions that users might have on phishing. This glaring gap is a problem, as previous research has shown that not engaging with the mental model of users can lead to lack of effectiveness of an approach in the real world. To address this gap, we conducted a systematic literature review starting from papers published at CHI in the last ten years, and expanding to other venues through a backward and a forward search based on the initial relevant CHI papers. We identified 15 misconceptions about phishing in 21 papers that researchers should address in their solutions to enhance the effectiveness of their approaches.

**Keywords:** phishing misconception · literature review · awareness

## 1 Introduction

The Federal Bureau of Investigation’s report on cyber security threats [15] declared phishing as the most problematic and expensive security threat of 2023. This is hardly surprising, given that the Anti-Phishing Working Group [6] declared 2023 as the worst year on record for phishing.

There is a lot of research on anti-phishing solutions, both on the side of awareness measures (e.g., [25, 47–50]) and as support tools (e.g., [5, 27, 36, 46]). Yet, although most of them claim to have been developed in a human-centric approach, we were surprised that, to our knowledge, researchers have not systematically investigated existing (anti-)phishing related misconceptions. The problem with this gap is that, to induce behavioral changes, one step (among others, e.g., see Beyer et al. [8]) is to address the underlying mental model<sup>1</sup> of the target group (as shown in Bada et al. [7]). Therefore, addressing relevant misconceptions is essential to increase the effectiveness of security awareness measures, as argued in Mayer and Volkamer [24]. However, current anti-phishing solutions,

<sup>1</sup> In our work we call “misconception” any mental model that is not inline with reality.

especially awareness measures, do not engage the misconceptions of users [8], but rather focus on providing information and coping techniques.

If the underlying misconceptions are not addressed, an anti-phishing awareness measure might be effective in a study setting, but not in the real world. For example, the participants might trust that email filters will block all phishing attacks, and not analyze emails as they did in the study setting.

To address this, we started by conducting a literature review that identifies (anti-)phishing related misconceptions in the ACM Conference on Human-Factors in Computer Systems (CHI) literature from the past ten years, following a similar approach to Mayer and Volkamer [24], who identified password misconceptions. We then expanded to other venues through a backward and a forward search based on the initial relevant CHI papers. We initially focused on CHI as it is ranked as an A\* conference according to CORE [10] and has a track on usable security. We found 21 relevant papers and 15 misconceptions about phishing<sup>2</sup> that should be addressed by anti-phishing awareness measures.

## 2 Methodology

The goal of this paper is to start addressing a glaring gap in the anti-phishing field of research, i.e., the lack of understanding regarding users' misconceptions about phishing. We started by focusing our investigation on works published in CHI, due to its strong presence in the anti-phishing community and it being rated A\*. Correspondingly, we used the ACM Digital Library to find relevant papers<sup>3</sup>, and further limited the search by defining as interval the years 2013–2023.

Regarding the keywords used, as suggested in Kitchenam [21] and done in Mayer and Volkamer [24], we started from two main terms (i.e., “misconception” and “phishing”), and deduced other keywords from fitting synonyms. Specifically, we deduced two set of keywords: 1) *phish\**, *malicious message*, *fraudulent message*, and 2) *misconception*, *misunderstanding*, *misperception*, *flawed perception*, *flawed understanding*. Every term in set 1 was then paired with each term in set 2 with the AND Boolean operator. For example, the pairs of *phish\** resulted in: *phish\** AND *misconception*, *phish\** AND *misunderstanding*, *phish\** AND *misperception*, *phish\** AND “*flawed understanding*”, and *phish\** AND “*flawed perception*”.

We queried the ACM Digital Library (with the aforementioned constraints) with each keywords pair singularly. The results were then exported as BibTex files, and stored using ReadCube's Papers v.4.37.2374 on an Apple MacBook Pro 2019 with MacOS Sonoma v.14.4. In cases where the entire proceedings of a specific year were returned as result, we opened the proceedings web page in Microsoft Edge v.124.0.2478.51, expanded every track, and used the browser search function with each keyword one at a time. We then exported the papers

<sup>2</sup> Some papers had more than one misconception, and some misconceptions were identified by more than one paper.

<sup>3</sup> <https://dl.acm.org/conference/chi>, accessed last on 06.05.2024.

in a BibTex file and added them to the database. After merging repeated results, we found 69 papers in total.

The second phase of a literature review is usually excluding papers by going over title and abstract. However, it might be that the misconceptions were only a secondary product of the research presented in a paper, e.g., mentioned by users who were asked to judge messages for phishing and reported in the results, but not relevant to answer the main research question. Hence, misconceptions might not have been mentioned in either title or abstract, but still be present in the paper text. For this reason, we decided to go over each one of the 69 papers and search their text with each one of our keywords one at a time. When a passage surrounding a keyword seemed promising, i.e., seemed as if describing a participant's misconception about phishing, we then jumped to that point and investigated further, e.g., by back-tracking to the beginning of that section. We did so for each of the 69 papers and we identified 14 relevant CHI papers.

We then expanded our search to other venues through a backward and a forward search based on the 14 relevant CHI papers. For the backward search, we identified three papers, and investigated them following the same methodology described before. Unfortunately, none of them contained any misconception. Regarding the forward search, we used the ACM Digital Library to find papers that cited the 14 relevant CHI ones. In total, 269 papers from various venues referred to at least one of the 14 relevant CHI papers. We collected these 269 papers, and investigated them following the same methodology described before, finding other 7 relevant papers. Hence, in total, we identified 21 relevant papers.

### 3 Results

Based on the 21 relevant publications found, we collected 15 misconceptions about phishing. Note that some papers had more than one misconception, and that some misconceptions were identified by more than one paper. Note further that these misconceptions are not limited to specific vectors of delivery (e.g., emails), but rather they cover various aspects related to phishing. Here, we list the misconceptions, explain their meaning, and where each one was found. We will then discuss them in Sect. 4.

*1. Strong Passwords are Enough to Protect from Phishing.* Some participants<sup>4</sup> think that using a strong password is a sufficient security practice to be safe from phishing. Although strong passwords are clearly important for security, there seems to be the misconception that such a solution would keep safe from every security threat. Unfortunately, this is not the case: a strong password is effective only when it is a secret that needs to be guessed by an attacker. However, one of the goals of phishing is tricking users into revealing their credentials, password included. In such instances where an attacker would succeed, even a strong password would be worthless, given that the attacker could simply enter it, without having to spend time guessing. Found in: [44].

<sup>4</sup> We use “participants” when talking of the people in the study where the misconception was found, and “users” when referring to people in general.

2. *If a Website is Known to the User or Looks Official it is Safe to Enter Credentials.* Several participants think that a familiar-looking website, especially when it has an official-looking layout, is always safe to enter their credentials on. This seems to come from a misconception regarding how websites are created, namely, not knowing that anyone can simply copy the layout and logos of a website. Therefore, users that are unaware of this possibility would be tricked into revealing their credentials. This is especially problematic because it is trivial for an attacker with some HTML knowledge to “clone” a website and make it look official. Found in: [19,38,41].

3. *SPAM and Phishing Messages are the Same.* This misconceptions is due to a confusion in the technical terminology used by experts and awareness measures alike. Normally, SPAM is defined as unwanted messages that are sent without consent (according to the National Institute of Standards and Technology [32]). These does not need to be phishing attacks, but can merely be undesired advertisement. Yet, many participants conflate SPAM with phishing. This is problematic, as some measures to defend against SPAM (e.g., SPAM filters) are not sufficient to protect from phishing (e.g., emails getting through the filters). It is also problematic because a user might think that reporting phishing is as simple as adding it to their SPAM folder, when in reality there are dedicated channels for reporting phishing attacks (e.g., “Action Fraud” in the UK [31]). Found in: [37].

4. *Technical Solutions (e.g., Filters, Anti-virus) Always Protect from Phishing.* Several participants believe that either anti-virus, email filters, or other technical solutions (e.g., Mimecast/Proofpoint security solutions) are capable of blocking 100% of attacks, so they can safely click on any link and be protected anyway. Although partially true, in the sense that older attacks and phishing websites are usually blocked by either email filters or browser filters, this is not the case for new phishing campaigns. For example, zero-hour attacks or lateral movement attacks (i.e., accessing the network through stolen credentials to disseminate further phishing attacks [26]) cannot be easily prevented by technical solutions. Found in: [39,43].

5. *Cybersecurity Warnings Always Identify Phishing or Anyway Dangerous Messages.* So far, the misconceptions came from lack of understanding or excessive trust in technical solutions. Misconception 5, however, rises from a somewhat opposite situation, as it originates from an excess of caution. Namely, participants interpret every warning related to emails as a sign that the email is malicious and dangerous. Yet, this is not the case, as it might be a false positive. For example, a mailing list re-distributing a signed email could brake the original digital signature (i.e., as if part of a man-in-the-middle attack), even if legitimate. This happens due to the sender address, i.e., the mailing list address, being different from the one on the digital signature certificate, i.e., the user’s address sending the email to be distributed. Found in: [20].

6. *Opening Attachments from Seemingly Legitimate Emails without Further Inquiry is not Dangerous.* This is somewhat related to misconception 2: participants believe that, as long as an email looks legitimate and the sender is known, it is fine to open any attachment delivered by it. As in the case of websites, users do not understand that an email can be made to look however the sender wants. However, there is also another misconception at play, here: users do not understand that the sender of an email is not a definitive proof of legitimacy, as it can be spoofed. Hence, although similar to misconception 2, there is a further dimension to misconception 6 that needs to be addressed. Found in: [52].

7. *If a URL Shows HTTPS it Means that it is Safe to Click on the Link.* This misconception comes from a misunderstanding of what the S in “HTTPS” stands for. Namely, many participants interpret it as a sign that the URL is safe to be visited, when in reality, all it shows is that the connection between two servers is encrypted. This, however, does not assure the identity of the destination server’s owner, who can be someone other than the impersonated identity. Found in: [18, 19, 22, 34, 39, 40, 42].

8. *If a Voice Over IP Call Shows a Registered Caller ID, the Identity of the Caller is also Verified.* This misconception is a relatively niche case. Since 2020, the United States of America TRADE Act mandate every voice network provider to adopt the STIR/SHAKEN framework [16]. In short, the framework is meant to stop robocalls from spoofing legitimate numbers. This is achieved by asking every service using Voice Over IP to verify the identity of numbers’ owners. One solution proposed to convey the information that a number is verified is to show a message on the device of the receiver such as “Caller Verified.” The problem is that such messages only mean that the number and its owner are verified, not the specific caller. However, participants interpret these messages as a verification of the identity of the caller. Found in: [14].

9. *If a Familiar Name is in the URL then the URL is Safe.* The misconception originates from the misunderstanding of the structure of URLs. Participants think that, as long as the name of the legitimate entity is anywhere in the structure of the URL shown, it means that the URL will take them to the entity’s legitimate website. However, the reality is that only the domain and top-level domain are important to identify where a URL would take once clicked. Specifically, an attacker can write anything they want as subdomains or in the path of a URL, but the URL will always take to their website, not the legitimate entity’s one. Found in: [3]

10. *If the Sender of a Message is Someone from the Social Circle of the User, the Message is Trustworthy.* The misconception originates from the belief that a sender address is a reliable indicator of the sender identity. Participants thought that, as long as they recognize the name of the sender as someone in their social circle, then the message is legitimate. However, it has been shown in the past

that senders can be spoofed, indifferently from the platform used (e.g., social networks [9], phone number [30], email address [35]). Hence, users should be careful even if a message seems to be from someone they know. Found in: [2].

*11. Enabling Anti-tracking in the Smartphone Options Protects from Phishing.* Some smartphones have built-in technologies aimed at protecting users from trackers, e.g., blocking apps from tracking them when not in use. Participants believe that this could somehow protect them also from phishing, which is clearly not true, as these technologies would not stop malicious emails from arriving. Furthermore, these technologies would also not stop users from releasing their sensitive information to others, as they are not meant for that. Found in: [17].

*12. Blocking Cookies Protect from Phishing.* Similarly to misconception 10, participants believe that blocking cookies can protect them from phishing. However, as for the case of the anti-tracking function in smartphones, blocking the leak of data by trackers is not the same as blocking the willing (albeit tricked) release of sensitive data. Found in: [17].

*13. There is no Difference Between the Text of a Link and Its URL.* Participants has a misconception regarding the difference between the anchor of a link (e.g., the text used) and the URL behind it (i.e., the actual destination). This lead to several insecure practices, like copy pasting the link text to check its legitimacy and, once it returns the expected legitimate website, use the original link, in effect reaching a different website. This is a clear misunderstanding of how links and URLs works, as an attacker can use any anchor text for their link, meaning that only checking the URL is a secure way to analyze a link before clicking it. Found in: [13].

*14. Reporting Phishing is not a User's Duty.* This misconception was found in the business context, but it can be applied also to the private one. Participants believe that reporting phishing is not important, and that it is not up-to-them to do so. However, as mentioned before, reporting is one of the main defenses against new phishing campaigns, and quick reporting can block an attack before it does too much damage. Hence, it is important to stress that every user should report phishing attacks when they discover them, highlighting the proper channels to do so. Found in: [23].

*15. Clicking on a Dangerous Link Always Infects the Device.* This misconception is different from the others, as it does not always make a user vulnerable. Participants think that clicking on a link always leads to the infection of the device. However, clicking a link rarely causes automatic download and installation of dangerous programs. A case in which this misconception makes users vulnerable is the “Pegasus” spyware software, who would infect a device without any action from its victims (as described in Norton [33]). Yet, this was directed towards high value targets (e.g., journalists), so normal users should not be concerned. Still, although this is a misconception, we discuss in Sect. 4 how we believe that

preventing users from clicking on dangerous links is always a better solution. Found in: [19].

## 4 Discussion

We will now discuss the implications of the misconceptions in Sect. 3. We grouped the misconceptions according to similarity, e.g., URL related misconceptions are described in Sect. 4.3. At the beginning of each sub-section we state which misconceptions it covers, and then proceed to discuss them.

### 4.1 Lack of Technical Knowledge

Several misconceptions (i.e., misconceptions 2, 4, 5, 6, and 9) highlight a lack of knowledge from users regarding the technical side of phishing. This is to be expected, as not everyone is technologically savvy enough to understand the technical implications of phishing attacks. Yet, these misconceptions must be addressed. To clarify, what we are proposing is not to make an expert of every user, as that would be an absurd expectation, and contrary to what has been the goal of usable security from its inception (see, e.g., Adams and Sasse [1]). Still, there are ways to address these misconceptions without resorting to technically descriptions. For example, instead of describing how an attacker can clone emails and web pages through HTML or JavaScript coding, an awareness measure can simply state that attackers can copy the look and logos of an email or a web page to make them look official, avoiding technical details.

Misconceptions 2, 6, 9, and 10 highlight a lack of understanding that a message or a webpage could look official, without it being legitimate. These misconceptions are dangerous, as without preparation users might trust a message or a webpage on looks alone. It is important that researchers focus their measures on the security indicators that cannot be spoofed by attackers, e.g., the URL, be it in a web address bar or, especially, in the URL behind a link. It is also important to clearly communicate to users that looks can be deceiving, and that they should not trust something simply because it looks legitimate.

Misconceptions 4 and 5, instead, highlight an excessive trust in technological solutions as the be-all and end-all answer to phishing. It is a known fact that technical solutions (e.g., email filters) cannot stop 100% of the phishing attacks (as shown in, e.g., Das et al. [11]). The over-reliance on technical solutions should be discouraged, because, even if these technologies are extremely useful, it is always important that users' pay attention before clicking a link or answering an email. Hence, it is required that researchers clearly states to users that their input is and (likely) will always be an important part of their defenses against phishing attacks.

### 4.2 Users' Confusion

Several misconceptions (i.e., misconceptions 1, 3, 5, 7, 8, 11, and 12) highlight the confusion of users regarding multiple aspects of the terminology and the significance of warnings.

Misconception 3 shows that users often use the terms SPAM and Phishing interchangeably. However, this is a dangerous practice, as it might lead to misunderstanding of awareness measures and secure behavior. This is a grave misunderstanding, as actions taken to avoid SPAM emails and actions that protect from phishing are not equally effective. For example, moving an email in the SPAM folder does not have the same effect as reporting an email as a phishing attempt. If an IT department gets a report of a phishing attempt, different mechanisms are enacted to protect every employee from them, which is something that would not happen for SPAM emails, given that something that is considered SPAM by one user might be interesting for another (e.g., newsletters). It is important that awareness measures and (potentially) email clients clearly states the distinction between SPAM and phishing emails.

Misconceptions 1, 11, and 12 shows how users confuse tracking protection (privacy related) with phishing protection (security related), and how they believe security to be all-encompassing. This is unfortunate, as it leads to the belief that email clients, browsers, and smartphones devices can autonomously protect them from phishing, which is clearly not true (as stated above regarding technology over-reliance). It is also unfortunate that it is not clear how different aspects of security does not necessarily influence one another. It is important that researchers clearly state the boundaries of the solutions they propose. This will give users a better understanding of what they can solve with certain actions and what they would not cover with them. For example, specify that strong passwords are important, but that they only work if not revealed to others. It might also be relevant to mention the difference between privacy and security, as these are often portrayed as one and the same, when in reality there are differences (e.g., a security solution might be privacy invasive, e.g., VPN services that log users' online traffic).

Another point which is somewhat tied to security misunderstanding is the one shown in misconceptions 5, 7, and 8. It is important that warnings and security indicators are clearly explained to users, to highlight their meaning and avoid over-cautiousness or misinterpretations. In this case, researchers should also highlight the limitations of their proposals to users, so that they are aware of what a certain warnings can tell them and what they should avoid assuming based on what they see (e.g., that an encrypted communication is inherently secure).

### 4.3 URL Analysis

It is not surprising that four out of the fourteen misconceptions (i.e., misconceptions 7, 9, 13, and 15) are related to URLs, given that previous research highlighted the lack of understanding users have on them (e.g. [3,4,12,51]). This reinforces the need of user support that previous works have mentioned (e.g., [28,29]). Especially important is the description of how to properly check the URL of a link (misconception 12), as this is a foundational knowledge that must be clear to users, to avoid them believing they are acting securely when they are not.

Nonetheless, misconceptions 7 and 9 are tied to others already discussed, i.e., that links can be deceiving and the explanation of what security indicators means. Hence, it might be possible to address them alongside other clarifications to provide a more holistic understanding and avoid security fatigue, i.e., ignoring some security recommendations due to the number of them that have been given (as described in Stanton et al. [45]).

Another important aspect is in regard of misconception 15. Although it is true that clicking on a link does not necessarily lead to malware being installed, we think that suggesting to users only high value targets should be a concern about this is counter-productive. If a user believes themselves to be not important enough to be targeted, they might act more recklessly. Furthermore, it might be that attackers adapt to this lack of cautiousness and start using more programs like the cited “Pegasus” spyware, to take advantage of the reduced attention paid to them. However, these are all hypotheticals, and more research is required before a clear answer is given.

#### 4.4 Reporting Phishing

Misconceptions 3 and 14 show how users under-estimate the importance of reporting phishing attacks. This is a serious lack in the anti-phishing awareness, as early reporting is one of the most important defenses against phishing. As mentioned for misconception 3, phishing reports allow security experts to take measures to reduce its impact on other users. It is therefore very important that researchers take care of highlighting how significant of a contribution each phishing report can be for the overall security of every user.

#### 4.5 Overall Message

So far we highlighted how each misconception should be addressed, and is important in its own right. Yet, some are more impactful than others, e.g., misconception 12 is more relevant than misconception 8, as the first is impacting every link analysis, while the latter is only important in a very specific case.

Unfortunately, it is difficult to foresee which misconceptions would be more important than others in every context. For example, even if misconception 13 is very dangerous, it might not be relevant in awareness measures that only cover vishing (i.e., phishing through phone calls).

To this end, we want to stress that, although we think every misconception we found should be addressed, each awareness measure must be tailored to the population it targets and its context of use. Researchers should therefore exercise caution and address only those misconceptions that are relevant for their population and context, to avoid causing security fatigue in the users.

#### 4.6 Limitations

Our work has some limitations. The first and most clear one is that our results started by only considering papers published in CHI between 2013 and 2023.

We made this decision as CHI is one of the highest rated conferences in the field of usable security, and further expanded our search to other venues through a backward and forward search. Still, we might have missed relevant papers that were not cited in or referenced the initial 14 CHI papers. Nonetheless, we believe our research is still significant, if nothing else, as a starting point to expand the research in an aspect of phishing so far not considered. Another limitation is that our choice of keywords might have missed some relevant papers due to the use of different terminology. Unfortunately, there is no standard terminology for misconceptions. However, considering that we also included several synonyms, we think that our work gives at least a good initial overview of the current literature from CHI on misconceptions about phishing. This being said, we did not cover every synonym of “phishing” and “misconception”, which might have caused us to miss some relevant papers. Still, as we used strong synonyms of the original terms, we believe our work gives a good overview of those papers that considered misconceptions about phishing. A different limitation is that we did not use an accepted framework for our methodology (e.g., PRISMA<sup>5</sup>). This was a conscious choice on our part, as we based our review on Mayer and Volkamer [24]. As it was our intention to conduct a comparable work as theirs, we decided that following a similar methodology was a requirement.

## 5 Conclusion and Future Work

Phishing continues to be a threat to both users and businesses. There is an abundance of approaches aimed at dealing with it, from awareness measures to technical solutions. Yet, although many of these solutions are presented as human-centric, to our knowledge none effectively engage with the misconceptions of users. Previous research shows that this lack of engagement is a problem, as addressing users’ misconceptions is a mandatory step towards secure behavior.

In our work, we present the results of a literature review aimed at identifying misconceptions about phishing. We started from papers accepted and published in the proceedings of the ACM Conference on Human-Factors in Computer Systems (CHI) in the last ten years, and then expanded to other venues through a backward and forward search based on the initial relevant CHI papers. We found 15 of misconceptions about phishing in 21 papers, spanning from “simple” terminological misunderstanding to others due to the users’ lack of technical knowledge. We believe it is imperative that researchers address these misconceptions in their approaches, to avoid the risk of over-estimating the effectiveness of their solutions in thwarting phishing attempts. We believe this to be an important step towards supporting users defending themselves from phishing, and achieving a long lasting effect on their behavior.

As future work, we plan to further expand our literature review to other venues to search for papers not cited by or that referenced CHI works. This has a two-folds goal: first, to see if there are further misconceptions that we have not yet identified. Second, we want to find further evidences of those misconceptions

<sup>5</sup> <https://www.prisma-statement.org/>.

that we have already collected. Furthermore, we want to develop a framework to design awareness measures that includes the misconception aspect of the users' knowledge. This will allow us to provide an effective tool to experts from industry and academia alike, enabling them to create solutions effective in both study settings and the real world.

**Acknowledgments.** This work was supported by funding from the project “Engineering Secure Systems” of the Helmholtz Association (HGF) [topic 46.23.01 Methods for Engineering Secure Systems] and by KASTEL Security Research Lab.

## References

1. Adams, A., Sasse, M.A.: Users are not the enemy. *Commun. ACM* **42**(12), 40–46 (1999). <https://doi.org/10.1145/322796.322806>
2. Ahmad, R., Terzis, S.: Understanding phishing in mobile instant messaging: a study into user behaviour toward shared links. In: *Human Aspects of Information Security and Assurance, HAISA 2022*, pp. 197–206. Springer, Cham (2022). [https://doi.org/10.1007/978-3-031-12172-2\\_15](https://doi.org/10.1007/978-3-031-12172-2_15)
3. Albakry, S., Vaniea, K., Wolters, M.K.: What is this URL’s destination? empirical evaluation of users’ url reading. In: *Conference on Human Factors in Computing Systems, CHI 2020*, pp. 1–12. ACM, New York (2020). <https://doi.org/10.1145/3313831.3376168>
4. Alsharnouby, M., Alaca, F., Chiasson, S.: Why phishing still works: user strategies for combating phishing attacks. *Int. J. Hum Comput Stud.* **82**, 69–82 (2015). <https://doi.org/10.1016/j.ijhcs.2015.05.005>
5. Althobaiti, K., Vaniea, K., Zheng, S.: Faheem: explaining urls to people using a slack bot. In: *Symposium on Digital Behaviour Intervention for Cyber Security, AISB 2018* pp. 1–8. Edinburgh Research Explorer, Liverpool, GB (2018)
6. Anti-Phishing Working Group: Phishing Activity Trends Report. Tech. Rep. 4th Quarter 2023, APWG (2024). [https://docs.apwg.org/reports/apwg\\_trends\\_report\\_q4\\_2023.pdf](https://docs.apwg.org/reports/apwg_trends_report_q4_2023.pdf)
7. Bada, M., Sasse, A.M., Nurse, J.R.C.: Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *arXiv* (2019). <https://doi.org/10.48550/arxiv.1901.02672>
8. Beyer, M., Ahmed, S., Doerlemann, K., Arnell, S., Parkin, S., Sasse, A., Passingham, N.: Awareness is Only the First Step. White paper (2015)
9. Bilge, L., Strufe, T., Balzarotti, D., Kirda, E.: All your contacts are belong to us: automated identity theft attacks on social networks. In: *Conference on World Wide Web, WWW 2009*, pp. 551–560. ACM, New York (2009). <https://doi.org/10.1145/1526709.1526784>
10. CORE: Icore conference portal (2024). url=<https://portal.core.edu.au/conf-ranks/11/>
11. Das, A., Baki, S., Aassal, A.E., Verma, R., Dunbar, A.: SOK: A Comprehensive Reexamination of Phishing Research from the Security Perspective. *arXiv* (2019). <https://doi.org/10.48550/arxiv.1911.00953>
12. Dhamija, R., Tygar, J.D., Hearst, M.: Why phishing works. In: *Conference on Human Factors in Computing Systems, CHI 2006*, pp. 581–590. ACM, New York (2006) <https://doi.org/10.1145/1124772.1124861>
13. Distler, V.: The influence of context on response to spear-phishing attacks: an in-situ deception study. In: *Conference on Human Factors in Computing Systems, CHI 2023*, pp. 1–18. ACM, New York(2023). <https://doi.org/10.1145/3544548.3581170>

14. Edwards, G.W., Gonzales, M.J., Sullivan, M.A.: Robocalling: stirred and shaken! - an investigation of calling displays on trust and answer rates. In: Conference on Human Factors in Computing Systems, CHI 2020, pp. 1–12. ACM, New York (2020). <https://doi.org/10.1145/3313831.3376679>
15. Federal Bureau of Investigation: 2023 Internet Crime Report. Tech. rep., FBI (2024). [https://www.ic3.gov/Media/PDF/AnnualReport/2023\\_IC3Report.pdf](https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf)
16. Federal Communication Commission: TRACED Act Implementation (2024). <https://www.fcc.gov/TRACEDAct>
17. Frik, A., Kim, J., Sanchez, J.R., Ma, J.: Users' expectations about and use of smartphone privacy and security settings. In: Conference on Human Factors in Computing Systems, CHI 2022, pp. 1–24. ACM, New York (2022). <https://doi.org/10.1145/3491102.3517504>
18. Hadan, H., Serrano, N., Camp, L.J.: A holistic analysis of web-based public key infrastructure failures: comparing experts' perceptions and real-world incidents. *J. Cybersec.* **7**(1), tyab025 (2021). <https://doi.org/10.1093/cybsec/tyab025>
19. Herbert, F., et al.: A world full of privacy and security (mis)conceptions? findings of a representative survey in 12 countries. In: Conference on Human Factors in Computing Systems, CHI 2023, pp. 1–23. ACM, New York (2023). <https://doi.org/10.1145/3544548.3581410>
20. Jeong, R., Chiasson, S.: 'Lime', 'open lock', and 'blocked': children's perception of colors, symbols, and words in cybersecurity warnings. In: Conference on Human Factors in Computing Systems, CHI 2020, pp. 1–13. , ACM, New York (2020). <https://doi.org/10.1145/3313831.3376611>
21. Kitchenham, B.: Procedures for Performing Systematic Reviews. Keele University, Keele, GB, Tech. rep. (2004)
22. Krombholz, K., Busse, K., Smith, M., von Zeszschwitz, E.: If HTTPS were secure, i wouldn't need 2fa-end user and administrator mental models of HTTPS. In: IEEE Symposium on Security and Privacy, IEEE S&P 2019, pp. 246–263. IEEE, New York (2019). <https://doi.org/10.1109/sp.2019.00060>
23. Marin, I.A., Burda, P., Zannone, N., Allodi, L.: The influence of human factors on the intention to report phishing emails. In: Conference on Human Factors in Computing System, CHI 2023, pp. 1–18. ACM, New York (2023). <https://doi.org/10.1145/3544548.3580985>
24. Mayer, P., Volkamer, M.: Addressing misconceptions about password security effectively. In: Workshop on Socio-Technical Aspects in Security and Trust, STAST 2017, pp. 16–27. ACM, New York (2018). <https://doi.org/10.1145/3167996.3167998>
25. Misra, G., Arachchilage, N.A.G., Berkovsky, S.: Phish Phinder: a game design approach to enhance user confidence in mitigating phishing attacks. In: Symposium on Human Aspects of Information Security & Assurance, HAISA 2017, pp. 41–51, Adelaide, AU (2017)
26. MITRE AT&CK&CK: Internal Spearphishing (2024). <https://attack.mitre.org/techniques/T1534/>
27. Mossano, M., et al.: SMILE - Smart eMail link domain extractor. In: Computer Security. ESORICS 2021 International Workshops, SPOSE 2021, pp. 403–412. Springer, Online (2022). [https://doi.org/10.1007/978-3-030-95484-0\\_23](https://doi.org/10.1007/978-3-030-95484-0_23)
28. Mossano, M., Kulyk, O., Berens, B.M., Häußler, E.M., Volkamer, M.: Influence of URL formatting on users' phishing URL detection. In: European Symposium on Usable Security, EuroUSEC 2023 pp. 318–333. ACM, New York (2023). <https://doi.org/10.1145/3617072.3617111>
29. Mossano, M., Vaniea, K., Aldag, L., Düzgün, R., Mayer, P., Volkamer, M.: Analysis of publicly available anti-phishing webpages: contradicting information, lack of concrete advice and very narrow attack vector. In: European Symposium on

- Security and Privacy Workshops, EuroUSEC 2020, pp. 130–139. IEEE, New York (2020). <https://doi.org/10.1109/EuroSPW51379.2020.00026>
30. Mustafa, H., Xu, W., Sadeghi, A.R., Schulz, S.: You can call but you can't hide: detecting caller ID spoofing attacks. In: Conference on Dependable Systems and Networks, IEEE DNS 2014, pp. 168–179. (2014). <https://doi.org/10.1109/DSN.2014.102>
  31. National Fraud & Cyber Crime Reporting Center: Report a phishing attempt (2024). <https://www.actionfraud.police.uk/report-phishing>
  32. National Institute of Standards and Technology: spam | Glossary (2024). <https://csrc.nist.gov/glossary/term/spam>
  33. Norton: What is Pegasus spyware + how to remove it from your mobile device? (2023). <https://us.norton.com/blog/emerging-threats/pegasus-spyware>
  34. Okuda, T., Chiba, N., Akiyama, M., Fukunaga, T., Suzuki, R., Kanda, M.: Brand validation: security indicator to better indicate website identity. In: HCI for Cyber-security, Privacy and Trust, HCI- CPT 2021, pp. 432–447 (2021). [https://doi.org/10.1007/978-3-030-77392-2\\_28](https://doi.org/10.1007/978-3-030-77392-2_28)
  35. Opazo, B., Whitteker, D., Shing, C.C.: Email trouble: secrets of spoofing, the dangers of social engineering, and how we can help. In: Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery, ICNC-FSKD 2017, pp. 2812–2817 (2017). <https://doi.org/10.1109/FSKD.2017.8393226>
  36. Petelka, J., Zou, Y., Schaub, F.: Put Your Warning Where Your Link Is: improving and evaluating email phishing warnings. In: Conference on Human Factors in Computing Systems, CHI 2019, pp. 1–15. ACM, Glasgow, GB (2019). <https://doi.org/10.1145/3290605.3300748>
  37. Rader, E., Munasinghe, A.: "Wait, do i know this person?": understanding misdirected email. In: Conference on Human Factors in Computing Systems, CHI 2019, pp. 1–13. ACM, New York (2019). <https://doi.org/10.1145/3290605.3300520>
  38. Reeder, R.W., Felt, A.P., Consolvo, S., Malkin, N., Thompson, C., Egelman, S.: An Experience sampling study of user reactions to browser warnings in the field. In: Conference on Human Factors in Computing Systems, CHI 2018, pp. 1–13. ACM, New York (2018). <https://doi.org/10.1145/3173574.3174086>
  39. Reynolds, J., et al.: Measuring identity confusion with uniform resource locators. In: Conference on Human Factors in Computing Systems, CHI 2020, pp. 1–12. ACM, New York (2020). <https://doi.org/10.1145/3313831.3376298>
  40. Ruoti, S., Monson, T., Wu, J., Zappala, D., Seamons, K.: Weighing context and trade-offs: how suburban adults selected their online security posture. In: Symposium on Usable Privacy and Security, SOUPS 2017. USENIX, Berkeley, CA, US (2017). <https://doi.org/10.5555/3235924.3235942>, <https://www.usenix.org/system/files/conference/soups2017/soups2017-ruoti.pdf>
  41. Sarker, O., Jayatilaka, A., Haggag, S., Liu, C., babar, M.A.: A multi-vocal literature review on challenges and critical success factors of phishing education, training and awareness. *J. Syst. Softw.* **208**(111899), 1–25 (2024). <https://doi.org/10.1016/j.jss.2023.111899>
  42. Seamons, K.: Privacy-Enhancing Technologies, pp. 149–170. Springer, Cham (2022). [https://doi.org/10.1007/978-3-030-82786-1\\_8](https://doi.org/10.1007/978-3-030-82786-1_8)
  43. Sharif, M., et al.: A field study of computer-security perceptions using anti-virus customer-support chats. In: Conference on Human Factors in Computing Systems, CHI 2019, pp. 1–12. ACM, New York (2019). <https://doi.org/10.1145/3290605.3300308>

44. Shay, R., Ion, I., Reeder, R.W., Consolvo, S.: My religious aunt asked why i was trying to sell her viagra: experiences with account hijacking. In: Conference on Human Factors in Computing Systems, CHI 2014, pp. 2657–2666. ACM, New York (2014). <https://doi.org/10.1145/2556288.2557330>
45. Stanton, B., Theofanos, M.F., Prettyman, S.S., Furman, S.: Security Fatigue. *IT Professional* **18**(5), 26–32 (2016). <https://doi.org/10.1109/mitp.2016.84>
46. Volkamer, M., Renaud, K., Reinheimer, B.: TORPEDO: tooltip-powered phishing email detection. In: Hoepman, J.-H., Katzenbeisser, S. (eds.) SEC 2016. *IAICT*, vol. 471, pp. 161–175. Springer, Cham (2016). [https://doi.org/10.1007/978-3-319-33630-5\\_12](https://doi.org/10.1007/978-3-319-33630-5_12)
47. Volkamer, M., et al.: Developing and evaluating a five minute phishing awareness video. In: Furnell, S., Mouratidis, H., Pernul, G. (eds.) TrustBus 2018. *LNCS*, vol. 11033, pp. 119–134. Springer, Cham (2018). [https://doi.org/10.1007/978-3-319-98385-1\\_9](https://doi.org/10.1007/978-3-319-98385-1_9)
48. Wash, R., Cooper, M.M.: Who provides phishing training? facts, stories, and people like me. In: Conference on Human Factors in Computing Systems, CHI 2018, pp. 1–12. ACM, Montréal, CA (2018). <https://doi.org/10.1145/3173574.3174066>
49. Wen, Z.A., Lin, Z., Chen, R., Andersen, E.: What.Hack: engaging anti-phishing training through a role-playing phishing simulation game. In: Conference on Human Factors in Computing Systems, CHI 2019, pp. 1–12. ACM, Glasgow, GB (2019). <https://doi.org/10.1145/3290605.3300338>
50. Zhang, T.: Knowledge expiration in security awareness training. In: Conference on Digital Forensics, Security and Law, ADFSLS 2018, pp. 197–212. Embry-Riddle Aeronautical University, San Antonio, US (2018)
51. Zheng, S., Becker, I.: Presenting suspicious details in user-facing e-mail headers does not improve phishing detection. In: 18th Symposium on Usable Privacy and Security, SOUPS 2022, USENIX, Berkeley, CA, US (2022). <https://www.usenix.org/conference/soups2022/presentation/zheng>
52. Zou, Y., Roundy, K., Tamersoy, A., Shintre, S., Roturier, J., Schaub, F.: examining the adoption and abandonment of security, privacy, and identity theft protection practices. In: Conference on Human Factors in Computing Systems, CHI 2020, pp. 1–15. ACM, New York (2020). <https://doi.org/10.1145/3313831.3376570>

**Open Access** This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

