



# Better Together: The Interplay Between a Phishing Awareness Video and a Link-centric Phishing Support Tool

Benjamin Maximilian Berens  
Benjamin.Berens@kit.edu  
Karlsruhe Institute of Technology  
Karlsruhe, Germany

Mattia Mossano  
mattia.mossano@kit.edu  
Karlsruhe Institute of Technology  
Karlsruhe, Germany

Florian Schaub  
fschaub@umich.edu  
University of Michigan  
Ann Arbor, MI, USA

Melanie Volkamer  
melanie.volkamer@kit.edu  
Karlsruhe Institute of Technology  
Karlsruhe, Germany

## ABSTRACT

Two popular approaches for helping consumers avoid phishing threats are phishing awareness videos and tools supporting users in identifying phishing emails. Awareness videos and tools have each been shown on their own to increase people's phishing detection rate. Videos have been shown to be a particularly effective awareness measure; link-centric warnings have been shown to provide effective tool support. However, it is unclear how these two approaches compare to each other. We conducted a between-subjects online experiment ( $n=409$ ) in which we compared the effectiveness of the NoPhish video and the TORPEDO tool and their combination. Our main findings suggest that the TORPEDO tool outperformed the NoPhish video and that the combination of both performs significantly better than just the tool. We discuss the implications of our findings for the design and deployment of phishing awareness measures and support tools.

## CCS CONCEPTS

• Security and privacy → Human and societal aspects of security and privacy.

## KEYWORDS

anti-phishing, online study, phishing awareness.

### ACM Reference Format:

Benjamin Maximilian Berens, Florian Schaub, Mattia Mossano, and Melanie Volkamer. 2024. Better Together: The Interplay Between a Phishing Awareness Video and a Link-centric Phishing Support Tool. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24)*, May 11–16, 2024, Honolulu, HI, USA. ACM, New York, NY, USA, 60 pages. <https://doi.org/10.1145/3613904.3642843>

## 1 INTRODUCTION

Email-based phishing attacks remain a big issue both in the private and the business contexts [38, 46, 51]. The goal of phishing emails

is either to learn sensitive data, such as passwords, or to install malware on the user's device [42]. To reach their goals, phishers often craft emails to look legitimate (e.g., by simply copying content from legitimate emails [10, 41]), with the intent to get their victim to click on a phishing link, which may be disguised behind an action button or image. While there have been significant advances in automatically detecting and filtering certain phishing attacks, it is not possible to detect 100% of phishing emails automatically [4, 63]. Thus, it is vital to strengthen users' ability to be aware of and check for essential indicators of phishing in emails that reach their inboxes. While many indicators could be considered (such as sender's address and grammar), the most reliable one, and the only one applicable to sophisticated phishing emails, is the URL behind a link. Thus, it is important to check the URL before clicking a link.

Two approaches to minimize the risk of falling for phishing emails have been studied extensively in the past: (1) *phishing awareness* measures, including games (e.g., [8, 48, 58]), videos (e.g., [24]), training (e.g., [17]), and other readable materials (e.g., [26, 28, 57]). Furthermore, (2) *phishing support tools* providing additional information at the client-side, i.e., either showing warnings and/or passive security indicators in email environments, (e.g., [7, 40, 54]). Another option is to act once users have clicked on a link by displaying warnings and/or passive security indicators in web browsers (e.g., [2, 21]). Most of the developed measures have been shown to significantly improve individuals' phishing detection rate. For phishing awareness, *videos* seem to be most promising, as the time needed to spend on the measure is much shorter compared to others, without reducing its effectiveness [56]. For phishing support tools, prior work has shown that providing support in the email environment with *link-centric warnings* is most promising, as the support is provided *in situ* when users consider clicking on a link [40].

While both phishing videos and phishing support tools have been studied extensively, little is known about (1) their interplay in helping users recognize phishing attacks, (2) what their comparative strengths and weaknesses are with regard to phishing URL's recognition, and (3) whether these two approaches create redundancy or their combined use yields additional benefits.

To provide answers to these questions, we conducted a between-subjects online experiment ( $n=409$ ) to comparatively evaluate a specific state-of-the-art phishing awareness video and a specific state-of-the-art support tool with link-centric phishing warnings,



This work is licensed under a Creative Commons Attribution International 4.0 License.

CHI '24, May 11–16, 2024, Honolulu, HI, USA

© 2024 Copyright held by the owner/author(s).

ACM ISBN 979-8-4007-0330-0/24/05

<https://doi.org/10.1145/3613904.3642843>

as well as their combination. More concretely, we evaluated the NoPhish video, which has been shown to increase the phishing detection rate [56] (increase from 42.6% to 86.9%); and the TORPEDO link-centric warnings approach, that has also been shown to increase the phishing detection rate [54] (increase from 43.31% to 85.17%). While each measure has been evaluated on its own in prior work, respective results are difficult to compare due to different evaluation approaches. In contrast, our study uses a consistent evaluation methodology to test these two measures individually and in combination against a range of URL manipulations common in phishing attacks. Additionally, our work addresses some limitations in prior work. For instance, Petelka et al. [40] did not study false positive rates by showing a warning for a benign link, but we do so. While the NoPhish video had already been evaluated in the past [56], that prior study was limited in that participants were only shown static screenshots, and the URL behind links was directly visible. Instead, our study design is more realistic, by studying interactions with phishing emails in a more dynamic environment similar to a email client, where hovering was necessary to see the URL behind a link. Furthermore, for the TORPEDO tool, we assess the effect of the different risk levels of the support tool on both phishing and legitimate detection rates.

Our results suggest that, (1) when used on their own, the TORPEDO tool outperforms the NoPhish video. (2) The combination of TORPEDO's link-centric warnings and the NoPhish video performed significantly better than the TORPEDO tool on its own and all other conditions tested. (3) Our findings confirm prior results for the NoPhish video [56] and the TORPEDO link-centric warnings [54], i.e., we confirm that both significantly improve phishing detection rates compared to baseline groups representing the status quo in current web browsers/email clients (i.e., the URL is displayed in the status bar and a simple tooltip, respectively). Yet, in contrast to the prior evaluations, the high internal validity of our results helps to compare the different groups with each other. This suggests that, without any of the measures, participants struggle to differentiate between phishing and legitimate examples.

Our results demonstrate that, even though effective on their own, combining link-centric phishing warnings, as offered by TORPEDO, with a phishing awareness video, such as NoPhish, appears to be beneficial in helping users to both understand phishing risks, and to more accurately interpret warning content. Furthermore, our findings indicate that showing URL information only in the status bar, as is common in many browsers and some email clients, is highly ineffective with regard to the detection of phishing links/emails. Our results suggest that browsers and email clients need to start providing more useful information directly at links to curb phishing risks, beyond showing only a simple tooltip with the plain URL.

## 2 RELATED WORK

Two common approaches for addressing email-based phishing attacks or to minimize the chance of falling for them are phishing awareness video and phishing support with warnings.

### 2.1 Phishing Awareness Videos

Various types of phishing awareness measures have been proposed and shown to significantly improve people's ability to detect

phishing attempts, including games [16, 18, 34, 39, 48, 58], videos [1, 24, 56, 61], workshops [43, 62], and other readable materials, e.g., e-learning materials [37, 57].

Particularly promising phishing awareness measures are videos, which have been shown to increase users' engagement and attention compared to text-only methods [25]. Abawajy [1] identifies both games and videos as more effective compared to text-based awareness. However, videos tend to be less time consuming compared to games. Compared to workshops, which Stockhardt et al. [50] found to be more effective than games and readable materials, videos have the advantage that no presenter is required, making their consumption more flexible and much less time-consuming. Hamdani et al. [25] also found that their participants preferred either videos or infographics. For all these reasons we decided to focus on videos for our comparison between phishing awareness measure and phishing support tools.

### 2.2 Phishing Support Tools

Various types of phishing support with warnings have been proposed and shown to be effective in increasing phishing email detection rates, both when shown before or after clicking a link.

Among the many security warning research results that any phishing support with warnings approach should take into account, the main ones are:

(1) avoid warning fatigue by showing too many similar warnings [2]; (2) provide sufficient information to help users understand the risk level, and to make an informed decision on how to continue [2, 6, 29]; (3) active warnings are more effective than passive ones in (potentially) critical situations [21].

More specific warning types related to emails have also been proposed, such as including a link-centric warning before clicking a link (i.e., a special tooltip being displayed once users hover over a link with the mouse) [40, 54], or the use of chatbots to help users decide whether a link is a phishing attempt [7]. For example, Mossano et al. [36] proposed to extract the domain name of every link in an email and replace the link text in the email with the extracted domain/top-level-domain combination. They showed that this method is more effective than the status quo in both web browsers and many email clients, i.e., showing the URL behind links in the status bar when hovering the link with the mouse. Petelka et al. [40] comparatively evaluated the effectiveness of banner warnings, link-centric warnings, and browser warnings (i.e., after clicking an email link) and found that link-centric warnings are the most effective ones. Other studies have focused on warnings shown in the web browser after the link was clicked, such as [2, 21]. However, a concern with this approach is that the warning is only shown after a user has made the decision to open the webpage.

Volkamer et al. [54, 55] showed that TORPEDO effectively supports users in detecting phishing emails without the need to click on links, thus reinforcing this behavior.

Combining both the literature on phishing awareness measures and phishing support tools, there is a variety of sources on different measures and different tools to help users. But the two have so far been considered separately and both still had room for improvement: the participants with the NoPhish video only achieved a phishing detection rate of 86.9% [56], with those of TORPEDO

reaching 85.17% [54]. Moreover, the risk levels of TORPEDO have not been evaluated in detail and their benefit remains unclear. Therefore, it is necessary to compare these approaches against each other, especially with regard to manipulation strategies that may either lay within their strengths or not be addressed at all. More about the research questions based on this gap in Section 4.1.

### 3 STUDIED PHISHING INTERVENTIONS

The goal of our study is to better understand how phishing awareness videos and link-centric phishing warnings compare, given that they both have been shown to be effective on their own. Rather than designing our own videos and warnings, we chose to evaluate existing state-of-the-art approaches. Namely, we compare the performance of a specific video-based phishing awareness measure, the *NoPhish* video [56], and a specific link-centric phishing support tool, *TORPEDO* [54, 55]. We chose a one-time video and a link-centric phishing support tool because they are common phishing education approaches that can both be deployed at scale and be easily employed in combination. There are other awareness measures, such as more extensive training's/workshop/games (see Section 2.1), but we wanted two measures with comparable deployment (e.g., time needed to complete or resources needed to implement them).

In this section, we discuss our selection rationale, and describe both the approaches and the implementations used.

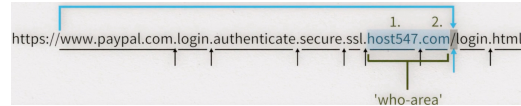
#### 3.1 Phishing Awareness: NoPhish Video

**3.1.1 Selection Criteria.** As the phishing awareness video we chose the 'NoPhish video.' It is a state-of-the-art video that is freely available on YouTube,<sup>1</sup> goes beyond general explanations of phishing, and was shown to be effective in the past [43, 56]. Furthermore, the video is not specifically aimed at the business context, but rather at the general public. This allows us to integrate it into an online survey without requiring modifications or further information that would be available to employees of a specific business. Thus, we decided to choose the NoPhish video for our comparison with link-centric phishing warning support.

**3.1.2 Description.** The NoPhish video is about 5 minutes long. It starts with a general introduction to phishing risks and potential consequences when falling for a phish, i.e., stolen sensitive data such as credentials (e.g., bank access details) and/or download of malware (e.g., ransomware, keyloggers). Moreover, it points out that phishing links are not only sent via email, but also through other vectors, e.g., social networks.

The video further explains that the URL behind the link is most important to check, and where to find it (status bar or tooltip). It also explains how to check URLs, including that the domain name (called *who-area* in the video) is the most important part and how to find it (see Figure 1).

The video then gives two tips on spotting commonly used tricks. The first tip explains that misleading information can be added either in the path or as subdomain and that it is important to only focus on the *who-area* (see Figure 1). The second tip shows that domains can look similar to legitimate ones (e.g., tvtwitter.com, with



**Figure 1: Domain-top-level-domain combination (i.e., who-area) as shown in the NoPhish video [56].**

two v instead of w) and that it is important to carefully check each character of a URL.

#### 3.2 Support Tool: TORPEDO Warnings

**3.2.1 Selection Criteria.** TORPEDO warnings [54] is a prominent link-centric phishing warning system. TORPEDO is the shortcut for TOoltip-poweRed Phishing Email DetectiOn. Volkamer et al. [54, 55] showed that the TORPEDO warnings effectively supports users in detecting phishing emails.

TORPEDO incorporates multiple insights from prior security warning research: (1) warning fatigue, as described in [2], is addressed by TORPEDO warnings as different risk levels, resulting in different warning messages, in line with proposals from [23]; (2) as recommended by prior research [2, 6, 29], the TORPEDO warnings provide information to help users understand the risk level of a link/URL and how to decide whether it would be safe to click on the link or not; (3) TORPEDO leverages prior findings that active warnings [21] are more effective than passive ones by, depending on the risk level, introducing a delay before the link becomes clickable to ensure users cannot miss the warning; (4) when displaying a URL, TORPEDO uses domain highlighting which has been shown to effectively support users in detecting phishing URLs [30]. Furthermore, it is publicly available as a browser extension<sup>2</sup>, so it can easily be used in a user study. For all these reasons, we decided to use the TORPEDO warnings approach for our comparative analyses.

**3.2.2 Description.** TORPEDO assumes that obvious phishing emails are being blocked by automatic detection tools and focuses on supporting users in checking link URLs for emails in the user's inbox. We used TORPEDO in version 1.7.1 (for Google Chrome) in our study, which has the following features: it shows a tooltip whenever the user hovers over a link. The tooltip adapts to the estimate risk. All tooltips display the URL behind a link text, formatted to highlight the domain-top-level-domain combination (i.e., called 'who-area' in the NoPhish video, see Figure 1). Depending on the risk level, the design of the warning differs and the link is (or is not) deactivated for some seconds to provide a cooldown [55]. TORPEDO includes a tutorial, shown once the add-on is installed. The tutorial explains that a tooltip appears when the user hovers with the mouse cursor over the link. It explains that the tooltip content varies based on the link's determined risk level, with explanations and visual examples for each. The tutorial further illustrates how the tooltip highlights a URL domain/top-level-domain-combination. The tutorial, in particular, also explains the different risk levels. For the translated tutorial see the Figure 8 in the appendix. TORPEDO distinguishes the following three risk levels (see Figure 2 for an overview):

<sup>1</sup>Volkamer et al.'s video is available on YouTube in English <https://www.youtube.com/watch?v=1phRPBijFoo> and in German <https://www.youtube.com/watch?v=JYu07OcFzew>.

<sup>2</sup><https://chrome.google.com/webstore/detail/torpedo-browser/cjglnlkhmaffelpeagnmgimhjhdjomi?hl=en>

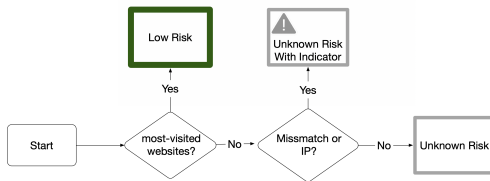


Figure 2: TORPEDO scheme for the study.

**Low Risk:** If the URL’s domain-top-level-domain combination is on the list of most-visited websites in the user’s country (and/or context), or if the user has visited this domain-top-level-domain combination at least twice in the past (referred to as *history case*), the phishing risk is considered “low.” The link-centric tooltip is displayed in the first case with a green frame (see Figure 5 for an example) and with a blue one in the second case. The tooltip contains relevant explanation in either case. In our study, we only consider the most-visited case (green), as we did not want to ask our participants for access to their browsing history.

**Unknown Risk With Indicator:** If TORPEDO does not know the domain-top-level-domain combination (yet) and detects potential URL-related phishing tricks, then a warning triangle is included in the link-centric tooltip, the tooltip is informing the user to carefully check the URL and (i.e., not clickable) to give users time to check the link before they click it (see Figure 7 for an example TORPEDO tooltip). TORPEDO currently supports various URL-related phishing tricks. For this study are relevant the mismatch (where a mismatch between the domain-top-level-domain combination of the link text and the link’s URL is detected) and the IP (where an IP is used to make the URL not readable for humans)<sup>3</sup>. Note, the TORPEDO developers argue to use a gray design (and no red one) as there are only indications towards phishing, but no definitive proof. A mismatch could be introduced by accident or there is a legitimate reason to use an IP address. Thus, the user needs to decide on the URL risk based on their knowledge of the context.

**Unknown Risk:** If the risk level is not “low” (i.e., the URL domain-top-level-domain combination is not in the two lists considered as low risk) and not classified as “unknown risk with indicator”, it is “unknown” (see Figure 2). The tooltip of the unknown risk case has a gray frame. The message to the user is that they should check the URL and in particular the URL domain-top-level-domain combination (see Figure 6 for an example). The link is deactivated for three seconds to give users time to check whether it is a phishing link or not before they click it. Note, both results are possible for the unknown risk case.

## 4 METHODOLOGY

We designed our study to comparatively assess the effects of the NoPhish video, as a current example of an effective phishing awareness measure, and TORPEDO, as a state-of-the-art link-centric phishing warning support tool, as well as the combination of both.

<sup>3</sup>Additional supported tricks are not included as they could not be compared in a fair way to the NoPhish video. For a complete list we refer the reader to <https://secuso.aifb.kit.edu/english/TORPEDO.php>.

### 4.1 Research Questions & Hypotheses

We designed our study to answer five research questions. We describe each of these research questions with the corresponding hypotheses in the following.

The first two research questions act as prerequisites needed for the further comparisons. These prerequisites ensure that the interventions used in the study achieve similar results as in the past, thereby being comparable against each other and combined. From previous literature we know that both the video [56] and the link-centric warning [54] significantly improve the phishing detection rate. Yet, our study is the first to directly compare their baseline performance on the same tasks against a control group.

**RQ-1:** Does the NoPhish video provide a positive effect compared to the control groups with respect to users’ ability to distinguish phishing and legitimate emails as shown in [56]?

**H<sub>0-RQ1</sub>:** The NoPhish video does not affect the ability of participants to distinguish phishing and legitimate emails.

**RQ-2:** Do the studied TORPEDO warnings provide a positive effect compared to the control groups with respect to users ability distinguish phishing and legitimate emails as shown in [40, 54]?

**H<sub>0-RQ2</sub>:** The TORPEDO warnings does not affect the ability of participants to distinguish phishing and legitimate emails.

Moving on from the prerequisites, our goal is two-folds: (1) to assess whether either the NoPhish video or TORPEDO warnings performs clearly better when comparing against each other, and (2) if their combination leads to greater, synergistic effects than each intervention on its own. In contrast to prior studies, we conducted a more detailed analysis, including an analysis of trends for different phishing tricks, where these phishing tricks represent a variety of different methods to manipulate the URL (see Section 4.4.1). Thereby, our first main research question is:

**RQ-3:** Is there a preferable option between the studied NoPhish video and the studied TORPEDO warnings in terms of the ability to distinguish phishing and legitimate emails? Such a comparison is new and can provide more reliable results, rather than comparing plain results from different studies, that might also differ in factors such as the introduction to the task or the used examples.

**H<sub>0-RQ3</sub>:** There is no difference between NoPhish video and TORPEDO warnings in the ability of participants to distinguish phishing and legitimate emails.

Coming to the second main research question, participants in studies with either the NoPhish video and TORPEDO warnings achieved good results with regard to phishing and legitimate detection rate, although between 10% to 15% of examples were still not identified correctly. Yet, the optimal result in a study setting should be close to 100%, as it is likely to see a drop in correctly identified messages in the real world. This because, security (i.e., checking for phishing emails) is not the primary task of users. As participants with either the NoPhish video and TORPEDO warnings separately did not achieve such an ideal detection rate, the question arose if a combination of both could bring it closer to the optimum. Therefore,

our second main research question is:

**RQ-4:** Does combining the NoPhish video and TORPEDO warnings provide an additional benefit regard people’s ability to distinguish phishing and legitimate emails, compared to using each of them on their own?

**H<sub>0-RQ4</sub>:** The use of a combination of NoPhish video and TORPEDO warnings does not affect the ability of participants to distinguish phishing and legitimate emails compared to only NoPhish video or only the TORPEDO warnings.

The fifth research question was formulated to control for the effect of the TORPEDO tutorial. Users in the real world may skip reading the tutorial of the TORPEDO warnings, and we wanted to isolate the effects of using TORPEDO without the tutorial.

**RQ-5:** What is the effect of reading the tutorial to the ability to distinguish phishing and legitimate emails when introducing the studied TORPEDO warnings?

**H<sub>0-RQ5</sub>:** The subtraction of the tutorial from the TORPEDO warnings does not affect the recognition rate of participants.

## 4.2 Study Groups

We included two control groups in our study because there are two status quos worth comparing against, namely a link’s URL is shown in the *status bar* (this is the status quo in most web browsers as well as the Thunderbird email client) or in a plain *tooltip* (this is the status quo in Microsoft Outlook and in Apple Mail).

**Status Bar.** For this group, when a user hovers with the mouse cursor on a link, the URL is displayed in a status bar in the bottom left corner of the screen.

**Tooltip.** For this group, when a user hovers over a link, a simple tooltip with the URL appears next to the link after a short delay. We designed the tooltip in our study like the one from MS Outlook, i.e., in addition, to the URL the following sentence was shown: "Click or tap to follow the link"; and the URL is displayed without special formatting (e.g., highlighting is not used). Similar to MS Outlook, the URL is also displayed in the status bar.

To answer research questions RQ-1 and RQ-3, we use the following two study groups:

**NoPhish Video + Status Bar.** Same as the ‘Status Bar’ group, but participants view the NoPhish video first, before judging emails.

**NoPhish Video + Tooltip.** Same as the ‘NoPhish Video + Status Bar’ group, but participants view the NoPhish video first, before judging emails.

The following study group is required to answer research questions RQ-2 and RQ-3:

**TORPEDO Warnings.** This group judges the emails with the TORPEDO warnings. Participants first view the TORPEDO tutorial before judging the emails.

We use the following study group to answer research question RQ-4:

**NoPhish Video + TORPEDO Warnings.** Same as the ‘TORPEDO Warnings’ group, but participants first view the NoPhish video, then the tutorial, then they judge the emails..

The following study groups are required to answer research question RQ-5:

**TORPEDO Warnings Without Tutorial.** This group judges the emails with the TORPEDO warnings, but they are not shown the TORPEDO tutorial.

**NoPhish Video + TORPEDO Warnings Without Tutorial.** Same as the ‘NoPhish Video + TORPEDO Warnings’ group, but they are not shown the TORPEDO tutorial.

## 4.3 Study Design

We conducted a between-subjects online experiment. Participants were randomly assigned to study groups. We used the online study platform SoSci Survey to collect the data, as they are compliant with the European Data Protection Regulation (GDPR). An overview of the various steps is depicted in Figure 3. The various steps are:

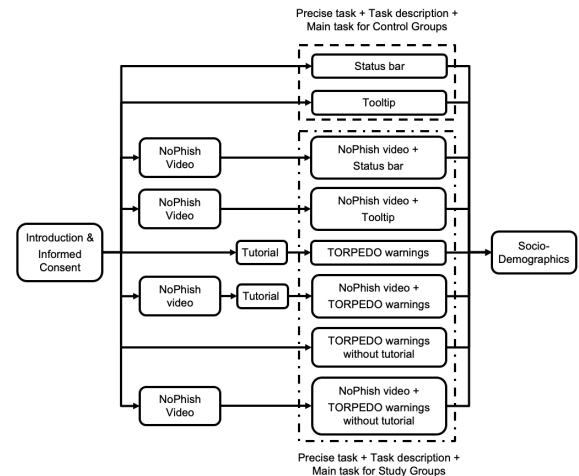


Figure 3: Overview of Study.

**General Introduction & Informed Consent.** First, participants were informed about the general purpose of the study and what rights they had while participating. This included that the data would be collected anonymously, and no personally identifiable information would be collected. In addition, the study could be discontinued at any time, and accordingly, their data erased. The participants were then asked to give their consent. The phishing awareness video groups were informed that they would watch a video next, and that they would be asked to answer questions about it afterwards. They were also asked to turn on the sound.

All participants received the notice that there is an example to practice the interaction (*interaction exercise*) with emails before the actual tasks start. All participants received the information that afterwards they would be asked to classify 16 emails as either legitimate or phishing, and that the study would end with socio-demographic questions.

**NoPhish Video.** The groups NoPhish Video + Status Bar, NoPhish Video + Tooltip, TORPEDO Warnings *Without Tutorial* and NoPhish

Video + TORPEDO Warnings saw the five-minute long NoPhish video [56] about phishing messages and phishing links at this point (see more about the video in Section 3.1). On this page they started the video by themselves. Afterwards, participants were asked in which way they watched the video. There were different choices (once completely without pause(s), several times the complete video, once entirely and then again single parts, once completely, but with pause(s), not at all or other:). This was followed by four attention questions about the video. These questions were necessary to evaluate the effect of the video, making sure that participants at least had a basic understanding of the content. The added questions were introduced after the pilot test conducted before the main study. Also because of the pilot study, we moved the task description with the instruction to turn on the audio from the beginning of the study to right before the video. Participants had to answer three of the four questions correctly in order to continue.

**Tutorial.** At this point, the two groups with the TORPEDO warnings and tutorial saw a page with the tutorial (see Figure 8). Participants in these groups were then asked three questions about the tutorial (e.g., how many risk levels are being distinguished), which served as attention check questions.

**Practice Task.** For all groups, a practice task followed. Participants were told about the form in which links can be hidden in the emails. They were also told that clicking on links was disabled as part of the study. Then, the participants were shown an example email and were asked to count the number of links in it to familiarize themselves with the environment. Participants who failed this task were excluded from the rest of the study.

**Task Description.** Here, participants saw a more detailed task description. We used a role-playing approach for the main task similarly to previous research on phishing [5, 20, 59] and other security contexts [44]. Previous research has shown that there might be a slight decrease in the participants' cautiousness during a study task using a role-play scenario [45]. Yet, [45] also mention that the role-play approach provides benefits with respect to the subjective plausibility of the examples. The messages can be tailored to the selected persona, increasing the examples plausibility without requiring knowledge of the study sample (e.g., the name or the services known by a participant). This increased plausibility is especially important when studies are focusing on other factors than the plausibility itself. So, right before the evaluation of emails started, we provided them with a scenario description: they are Martin Müller with the email address martin.mueller.77@gmail.com. In addition, all services used in the study should be considered known and used by Martin Müller.

**Main Task: Evaluating Emails.** Each participant then saw 16 screenshots of emails in the Gmail environment, displayed in random order. Each screenshot was presented on a separate page with a question (This email is a... phishing email or legitimate email). As we only used email screenshots, we implemented an event function when participants hovered over the link, which then displayed the URL in the status bar, the simple tooltip or, depending on the assigned group, the corresponding link-centric warning. The group assignment (as an intervention) represents the independent variable. Our dependent variable was the participant's *decision whether an example is phishing or legitimate*.

Participants in the TORPEDO warnings groups were informed that this was a fictitious update to the Chrome browser.

**Socio-Demographics.** The study ended with demographic questions, asking the participant's gender, age (in age ranges), and level of education. Participants were also asked about issues with color perception. This is an essential factor, especially for the TORPEDO warnings intervention groups – although none of the used color constellations is known to be easily mistaken (green and gray).

**Thanks and Payment.** The study ended with thanking participants and providing their code for payment.

#### 4.4 E-Mail Screenshots

An essential part of the email screenshots used in the study are the URLs as main indicator to distinguish between phishing and legitimate example. Thus, before explaining how the emails themselves were selected, we first describe the URL manipulation strategies we included in the study. Note, for all eight groups, the URL is always (additionally) visible in the status bar.

**4.4.1 URL Manipulation Strategies.** There are various ways to trick users when it comes to URLs behind links. Prior work [16, 30, 43, 52, 54] that studied the effect of either the NoPhish video or TORPEDO warnings on their own used different URL manipulation categories, making comparisons of the two approaches based on the prior findings difficult. Especially strategies based on the tooltip being a mismatch to the actual URL are rarely used, even though they can be hard to spot and are easy to create (as the domain can be completely random and, therefore, is not detected easily by companies themselves). And as both the phishing awareness video and phishing support with warnings address this strategy, we used the following URL manipulation strategies (see Table 1 for the full details of the literature and corresponding manipulation strategies):

**Table 1: Overview of the different manipulation strategies across different papers. An “x” signals that the mentioned literature included the manipulation strategies.**

Literature	Obfuscate	Mislead	Mangle	Delusive Mismatched URL
[30]	x	x	x	
[43]	x	x	x	x
[53]	x	x	x	
[60]	x	x	x	
[50]	x		x	
[48]	x	x		
[16]	x	x		
[37]		x	x	
[27]				x
[47]		x	x	x

**Obfuscate:** An arbitrary domain name or IP address is used to hide the destination. The URL lacks a connection to the faked sender of the email content.

**Mislead:** The name of the impersonated company is used either in the subdomain area or in the path following the domain.

**Mangle:** The brand name is used in the domain, but with small, difficult to spot changes to it. For example, the order of two characters is switched (e.g., mircosoft) or characters are substituted with similar looking ones (e.g. arnazon instead of amazon).

**Delusive Mismatched URLs:** The link text resembles a URL. This URL matches the domain-top-level-domain combination of the actual company, while the URL behind this link directs users to the phisher’s server (see Figure 7).

Both the phishing awareness video as well as the TORPEDO warnings address all four phishing URL manipulation strategies. Note: the video used was neither tailored to the examples nor to the interface used for the study (link to video from the study: <https://www.youtube.com/watch?v=JYu07Ocfzew>).

**4.4.2 Actual Emails Used in the Study.** All manipulation strategies were covered at least twice in the study, requiring 16 emails. For an overview see Table 8 (note as the study was conducted in Germany, the emails were in German language). Similar to previous studies, we aimed for the same amount of phishing and legitimate emails, and used two examples per manipulation strategy. On the one hand, this helped reduce the probability that a single error by the user, e.g., maybe due to the organization used, could cause wrong conclusions on a type of manipulation strategies. On the other hand, we limited it to two examples per manipulation strategy to not make the number of examples disproportionately large.

We used real-world emails from well-known companies as the basis for our screenshots. These emails were sent as we use them except that we manipulated the link depending on the strategy for the specific example - - so all other aspects of the email were 100% legitimate. They all include a call to action which is common in phishing studies/attacks [40, 54, 56]. The companies were chosen because of their high popularity in Germany, so that users would not consider an email suspicious just because they were unfamiliar with the company. We also wanted to eliminate the influence of company reputation from the decision and used both a phishing and a legitimate example for each company. In pilot tests we found that using the same email twice, with a legitimate and a phishing URL, influenced the decision depending on which case was seen first. Therefore, we decided to use two different emails from the same company to create a legitimate and a phishing example for it.

For the TORPEDO warnings groups, we had to decide which emails would appear as low risk, as unknown risk, and which as unknown risk with indicator. We equally distributed these levels among the examples (see Table 8). Note that there was also one benign email with unknown risk with indicator as a false positive, as non-phishing mismatched URLs can appear in real world emails.

## 4.5 Limitations

Our study has several limitations that we factored into our design decisions. Priming participants to check URLs was a necessary trade-off for several reasons. Despite being a limitation, it does not affect the internal validity, as every group underwent the exercise. Thus, the influence should be consistent across all groups. Checking URLs was crucial to assess the effectiveness of the phishing awareness video and support tool, as observed effects could be attributed to these interventions. Previous research [3] suggests that, although people look at URLs, they often struggle to read them correctly, so we did not expect priming to significantly impact groups beyond directing their attention.

However, our findings may have limited external validity, as participants likely paid closer attention to link URLs than they

would in real-life scenarios, setting a ceiling for attention to URLs. Real-world performance may differ. Still, our findings offer valuable insights into the relative effectiveness of the interventions tested.

Security was the main task for participants, so performance may decline when transferred to real-world settings. However, our goal was a controlled comparison of different groups, necessitating a clearly formulated task without major external influences. Future field studies could repeat various comparisons, such as the time between watching the NoPhish video and judging screenshots.

We employed a study environment with email screenshots, which may differ from an actual email program. To mitigate this, we allowed for real interaction with emails, unlike prior studies using static screenshots. We also included screenshots of the entire environment, with URLs requiring mouse hovering for visibility.

Additionally, we acknowledge other factors within examples beyond the manipulation strategies used, such as time pressure. Inducing actual time pressure in our online study with no participant-owned accounts is challenging, but should be evaluated in future studies. However, not all phishing or legitimate emails contain time pressure, as it is primarily a tactic used by phishers. As our examples were based on copied legitimate emails, our results shed light on the effectiveness of such examples.

## 4.6 Ethics & Data Protection

Each participant gave their consent in the beginning of the study on the Sosci Survey platform. We also informed them that they could withdraw their consent at any time during the study, e.g., by not continuing the study or by informing the study administrator without giving any reason. The ethical requirements of our university and common established ethical guidelines were met by informing participants of the nature of the study on the first page, and informing them of their rights on the second page (informed consent). For those who were told that there was an update to their browser (which was the phishing support tool functionality) we had a debriefing after they finished the study part to tell them about the actual add-on and the possibility to download it. We received IRB/ERB approval from our university to conduct the study.

## 4.7 Recruitment

We recruited participants using the panel service “Clickworker.” The only criteria were being 18 years or older and speaking German. The recruitment message did not mention either security nor phishing to lessen the self selection bias - simply stating: “Participate in a study about User Experience with E-Mail interfaces.” According to Cohen [19], without sufficient information a medium effect size helps to not over- or underestimate the expected effect size. Therefore, we decided to plan for medium effect size  $f = 0.25$ . We assumed to use a ANOVA for independent groups, for the test strength analyses with G\*Power. In addition to the effect size, we set the test power to 0.95 and the alpha error to 0.05. Based on these numbers, we calculated a required sample size of 360 participants. To avoid falling below this limit due to exclusions, we set the participant number to 430.

Based on pre-tests, we expected the study to be finished in 30 minutes. We wanted to pay the participants at or above minimum wage. Since participants were randomly assigned to groups we

chose the longest group time to determine payment for all participants. We used the latest (December 2021) German minimum wage standard [11] of 9,82€ rounded up to 10€. Given that the study lasts about 30 minutes we compensated participants with 5€.

#### 4.8 Data Analysis Approach

Phishing detection is not just about catching all phishing messages/links. Scaring people excessively could make them view every message/link as phishing, leading to rejecting many legitimate messages by mistake. This could cause other problems, such as missing critical messages or using it as an excuse for not responding promptly.

Signal Detection Theory (SDT) [49] has proven effective in assessing phishing prevention performance. Several studies have used SDT in the context of phishing [12–15, 22, 31–33, 35, 48].

In SDT, Sensitivity ( $d'$ ) gauges the ability to distinguish between a stimulus and noise. A higher Sensitivity value indicates better discrimination. In our study the maximum value, 3.38, represents perfect identification of phishing or legitimate examples. Criterion ( $C$ ) measures the tendency to favor one decision over another, irrespective of the actual example. A neutral Criterion is ideal, indicating no bias toward stimulus or noise. Deviations from neutrality suggest a propensity toward one or the other.

To analyze SDT hypotheses, we employ a single ANOVA for both sensitivity and criterion. Significant improvements in Sensitivity confirm hypotheses, while Criterion should ideally remain near zero without significant trends.

Our analysis begins with assumption checks, including outlier analysis and tests for normality and homogeneity of variances. For the latter, we use Levene's test and employ the Welch one-way ANOVA for significant results. Detection rates for phishing and legitimate examples are reported for different phishing tricks, cases, and specific email examples.

Especially for Criterion results, ANOVA findings are interpreted alongside descriptive values to assess alignment with research questions. Each research question analysis includes ANOVA for sensitivity and both ANOVA and descriptive statistics for Criterion.

#### 4.9 Data Cleaning & Sample

We recruited participants based on our power analysis (see Section 4.7). Participants were assigned randomly to conditions at the beginning. Participant numbers vary due to dropouts and data cleaning (see below). A total of 420 participants completed the online study. We performed the following data cleaning steps: (1) We excluded one participant due to the answers showing straightlining. The participant had 100% legitimate email identification and 0% phishing email identification respectively; i.e., they selected legitimate for all emails. (2) For the analysis of the signal detection theory we calculated outliers and excluded those that violated the maximum of 1.5x interquartile range (IQR). This led to excluding 10 participants (four from TORPEDO Warnings and six from NoPhish Video + TORPEDO Warnings).

We ended up with 409 participants for the final analysis: Status Bar: 58, NoPhish Video + Status Bar: 49, Tooltip: 53, NoPhish Video + Tooltip: 47, TORPEDO Warnings *Without Tutorial* : 58,

NoPhish Video + TORPEDO Warnings *Without Tutorial*: 42, TORPEDO Warnings: 63 and NoPhish Video + TORPEDO Warnings: 39. (Further details on the sample in Appendix A.2).

## 5 RESULTS

This section starts with a summary of the results. The in-depth sections with the detailed analyses are linked accordingly.

Up front, both the NoPhish video and the TORPEDO tool groups performed better than the current status quo ones with regard to distinguishing between phishing and legitimate examples (see Section 5.1.1). When comparing both measures against each other, the TORPEDO tool group performed better than the video one. Yet, the combination group performed better than both the NoPhish video and the TORPEDO tool on their own. Furthermore, the groups with the tutorial performed better than the groups without. Hence, the overall best performing group was the one with the combination of the two measures and the tutorial. Nonetheless, most of the groups had troubles detecting the “Mangle” manipulation strategy (see Section 5.2). Finally, we found that TORPEDO's risk levels provided a benefit to the participants, especially alongside the tutorial or even the phishing awareness video (see Section 5.3).

Our overall results for correct answers per group and phishing type are shown in Table 2. For testing the hypotheses, we start off by reporting the overall results of one-way ANOVAs for sensitivity/criterion with groups as a factor. The result from the ANOVA are then split into separate parts to fit the different research questions. Each research question will feature those post-hoc tests that are needed for the related hypotheses with adjustment for multiple testing. We also provide boxplots for the groups with their mean value (see Figure 4) or for all the different comparisons between groups (see Table 9 in the appendix).

The ANOVA shows a significant difference for the sensitivity between groups ( $p < 0.0001$ ) with  $F(7,401) = 50.867$ ,  $\omega^2 = 0.46$ . For the criterion there is a significant difference between groups ( $p < 0.0001$ ) with  $F(7,401) = 16.062$ ,  $\omega^2 = 0.20$ . The results of the post-hoc tests can be found in Table 9.

### 5.1 Hypotheses Testing

We first discuss our findings regarding those research questions that are used as prerequisites, confirming that the effectiveness of the individual interventions demonstrated in previous studies on the phishing awareness video [56] and phishing support with warnings [54] holds in our setting too, i.e., that each measure significantly increases the effectiveness in distinguishing between phishing and legitimate examples.

**5.1.1 Effectiveness of individual intervention.** The test of the individual interventions starts with RQ1 on the effect of the phishing awareness video.

*RQ-1 - NoPhish video effect:* we can confirm the results from previous literature that the phishing awareness video ( $d'_{status}=1.87$  and  $d'_{tooltip}=2.12$ ) has a positive effect compared to the control groups ( $d'_{status}=1.01$  and  $d'_{tooltip}=1.13$ ) in our study. There is a significant improvement for the sensitivity  $d'$ . For the criterion  $C$  there is a significant difference, ending closer to zero, which is the overall goal (see Section 4.8). As we wanted to have the sensitivity



maximal large and the criterion minimal close to zero, our results show that the groups with NoPhish video are significantly better than both control groups. *Thus, we can reject the null hypothesis  $H_{0-RQ1}$  that the NoPhish video does not affect the sensitivity.* Hence, we conclude that the NoPhish video performed better than the control groups, positively answering RQ-1.

*RQ-2 - TORPEDO warnings effect:* We can confirm the results from previous literature that the TORPEDO warnings ( $d' = 2.51$ ) have a positive effect. There is a significant improvement for the sensitivity  $d'$ . For the criterion  $C$  there is no significant difference, all three groups being similarly distant from zero. As we wanted to have the sensitivity maximal large and no significant worsening of the criterion away from zero, our results show that the group with TORPEDO warnings performed significantly better than both control groups. *Thus, we can reject the null hypothesis  $H_{0-RQ2}$  that the TORPEDO warnings do not affect the sensitivity.* Hence, we conclude that the TORPEDO warnings group performed better than the control groups, positively answering RQ-2.

Thereby, the prerequisite of both interventions performing better than the control groups was met. This also holds true for phishing tricks that have not been tested in the previous studies, such as the mismatch trick (more in Section 5.2).

**5.1.2 Effectiveness comparing interventions and combining interventions.** After confirming that the interventions still achieved significantly better results on their own compared to the control groups, the next step was to compare the two interventions against each other, as well as assessing the effect of their combination. We also investigated the effect of the tutorial on the phishing support with warnings.

*RQ-3 - NoPhish video vs. TORPEDO warnings:* we can state that the TORPEDO warnings outperform the NoPhish video. There is a significant improvement for the sensitivity ( $d' = 2.51$ ) for TORPEDO warnings compared to the NoPhish Video + Status Bar ( $d' = 1.87$ ) and NoPhish Video + Tooltip ( $d' = 2.12$ ). For the criterion  $C$  there is no significant difference between the NoPhish Video + Status Bar and TORPEDO warnings and a significant difference between NoPhish Video + Tooltip and TORPEDO warnings. As our main goal was to have the sensitivity significantly improve and NoPhish Video + Tooltip and TORPEDO warnings having different directions of their tendency for  $C$  with the first trending into selecting more phishing and the second trending into selecting for legitimate - the significant difference needs to be looked into more closely for interpretation.

*Thus, we can reject our null hypothesis  $H_{0-RQ3}$  that there is no difference between TORPEDO warnings and NoPhish video for the sensitivity.* We conclude that the TORPEDO warnings performed better than the NoPhish video group.

*RQ-4 - combined NoPhish video and TORPEDO warnings effect:* we can state that the NoPhish video + TORPEDO warnings ( $d' = 2.92$ ) outperforms both the NoPhish video ( $d' = 2.12$ ) and TORPEDO warnings ( $d' = 2.51$ ). There is a significant improvement for the sensitivity  $d'$  for NoPhish video + TORPEDO warnings compared to NoPhish video. For the criterion  $C$  there is no significant difference between the NoPhish video + TORPEDO warnings and NoPhish Video + Status Bar and NoPhish Video + Tooltip, with all of them being

relatively close to zero. As our main goal was to have the sensitivity significantly improve and no significant worsening of the criterion away from zero, our results show that the NoPhish video + TORPEDO warnings group is significantly better than both control groups with NoPhish video. *Thus, we can reject the null hypothesis  $H_{0-RQ4}$  that the NoPhish video + TORPEDO warnings improves the detection rate.*

From the results of the last two hypotheses, one can see that the combination of NoPhish video and TORPEDO warnings performed clearly better than just using one or the other.

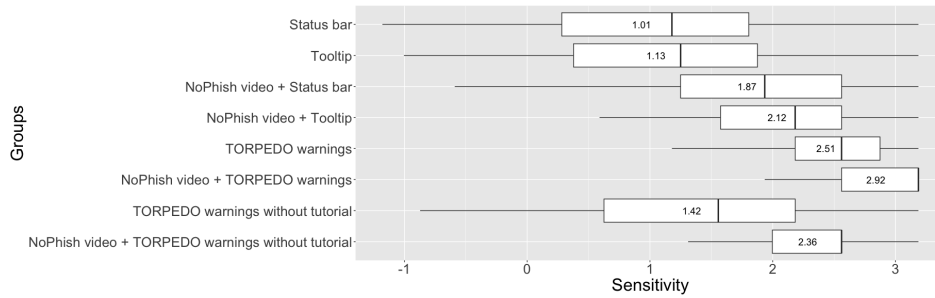
*For the fifth hypothesis - tutorial effect:* we can state that the TORPEDO warnings without the tutorial ( $d' = 1.42$ ) performs worse than the TORPEDO warnings ( $d' = 2.66$ ) and that it does not provide a benefit to the NoPhish video ( $d' = 2.12$ ) groups anymore. There is a significant difference for the sensitivity  $d'$  for TORPEDO warnings and TORPEDO warnings without tutorial and no significant difference for TORPEDO warnings without tutorial and any of the control groups. For the criterion  $C$  there is no significant difference between the TORPEDO warnings and TORPEDO warnings without tutorial and a significant difference between TORPEDO warnings without tutorial and the NoPhish Video + Status Bar respectively the NoPhish Video + Tooltip. As for sensitivity the TORPEDO warnings without tutorial is worse than the TORPEDO warnings and it's worse for the criterion compared to the control groups with NoPhish video, our results show that the TORPEDO warnings without tutorial performs worse than the others. *Thus, we can reject the null hypothesis  $H_{0-RQ5}$  only for the TORPEDO warnings comparison - but in a way that it worsens the detection rate.*

## 5.2 Effectiveness against different phishing tricks

This subsection deals with the effectiveness of the different interventions in relation to the phishing tricks, phishing examples and legitimate examples respectively. For the full overview of all results for the phishing tricks and phishing examples, see Table 3 and for the legitimate examples see Table 4.

### Phishing tricks:

First, we discuss the observed trends for the different manipulation strategies (for more details see Table 2). The status quo (status bar or tooltip) only achieved between 60% to 70% correct responses against three manipulation strategies ("Obfuscate", "Mislead" and "Special Link Manipulation"). The fourth manipulation strategy, "Mangle," achieved a value of around 20% to 25%. Adding the video to the status quo lead to an increase of about 25% to 50% ("Mangle" from 25.47% to 75.53% for the tooltip group), whereas "Mangle" remained at 55.10% for the video group with the status bar. With values above 80%, the other three manipulation strategies performed much better, with the tooltip group having 100% correct answers for the "Delusive Mismatched URLs." For those groups with the TORPEDO warnings, the "Mangle" manipulation strategy achieved the worst rates, with only 32.76% for the TORPEDO warnings without tutorial, and 53.97% for the TORPEDO warnings. The other strategies mostly achieved values of at least over 70%. The NoPhish video + TORPEDO warnings group achieved values of at least 90% for all four strategies, with two times 100% for "Mislead" and "Delusive Mismatched URLs". In contrast, the TORPEDO



**Figure 4: Boxplot for sensitivity of all groups with the mean values rounded to two digits. The sensitivity ranges from -3.38 to +3.38.**

**Table 2: Overview of the percentage of correct answers for the groups overall, phishing examples, legitimate examples and manipulation strategies. Grp1 = Status bar, Grp2 = Tooltip, Grp3 = NoPhish video + Status bar, Grp4 = NoPhish Video + Tooltip, Grp5 = TORPEDO warnings, Grp6 = NoPhish video + TORPEDO warnings, Grp7 = TORPEDO warnings without tutorial, Grp8 = NoPhish video + TORPEDO warnings without tutorial.**

Manipulation strategy	Grp1	Grp2	Grp3	Grp4	Grp5	Grp6	Grp7	Grp8
Obfuscate	65.52	66.98	89.8	94.68	93.65	96.15	71.55	94.05
Mislead	62.93	61.32	86.73	92.55	96.03	100.00	71.55	96.43
Mangle	19.83	25.47	55.1	75.53	53.97	92.31	32.76	75.00
Delusive Mism. URL	68.97	72.64	94.9	100	98.41	100.00	75.86	100
Phish	54.31	56.6	81.63	90.69	85.52	97.12	62.93	91.37
Legit	81.68	83.73	83.67	81.91	98.41	97.44	86.21	89.29
Overall	68	70.17	82.65	86.3	91.96	97.28	74.57	90.33

**Table 3: Overview of the percentage of correct answers for the phishing examples. Grp1 = Status bar, Grp2 = Tooltip, Grp3 = NoPhish video + Status bar, Grp4 = NoPhish Video + Tooltip, Grp5 = TORPEDO warnings, Grp6 = NoPhish video + TORPEDO warnings, Grp7 = TORPEDO warnings without tutorial, Grp8 = NoPhish video + TORPEDO warnings without tutorial.**

Name	Manipulation strategy	Grp1	Grp2	Grp3	Grp4	Grp5	Grp6	Grp7	Grp8
P1	Obfuscate	86.21	81.13	93.88	100.00	100.00	100.00	87.93	100.00
P2	Obfuscate	44.83	52.83	85.71	89.36	87.30	92.31	55.17	88.10
P3	Mislead	56.90	60.38	93.88	100.00	98.41	100.00	74.14	100.00
P4	Mislead	68.97	62.26	79.59	85.11	93.65	100.00	68.97	92.86
P5	Mangle	20.69	24.53	59.18	74.47	69.84	94.87	37.93	80.95
P6	Mangle	18.97	26.42	51.02	76.60	38.10	89.74	27.59	69.05
P7	Delusive Mism. URL	67.24	71.70	93.88	100.00	96.83	100.00	79.31	100.00
P8	Delusive Mism. URL	70.69	73.58	95.92	100.00	100.00	100.00	72.41	100.00

warnings without tutorial group only achieved the lowest from all four TORPEDO groups, i.e., around 70% for “Obfuscate”, “Mislead” and “Delusive Mismatched URLs.” Overall, the NoPhish video + TORPEDO warnings group performed the best among all groups. Comparing the tutorial groups with those without, the first always performed better. Similarly, the TORPEDO group performed better than the current status quo with both status bar or tooltip.

#### Phishing examples:

The results of all phishing examples for all eight groups can be found in Table 3. Starting again with the current status quo (status bar or tooltip), they achieved scores for the phishing examples ranging from only 18.97% to 86.21%. On average, the tooltip group performed slightly better than the status bar one. Yet, looking at the specific examples, the performance was mostly similar, with sometimes one being higher than the other. Mostly, the phishing examples showed similar trends for the detection rate within the manipulation strategy. But there were also differences. For instance, P1 and P2 had a huge difference of around 30% for status bar (P1 = 86.21%, P2 = 44.83%) and tooltip (P1 = 81.13%, P2 = 52.83%). The gap

was smaller for all the other groups, except for TORPEDO warnings without tutorial (P1 = 87.91%, P2 = 55.17%). Additionally, P5 and P6 had very similar results for seven out of eight groups, with the only exception being the TORPEDO warnings group (P5 = 69.84%, P6 = 38.10%). Overall, most of the phishing examples based on a manipulation strategy performed similarly within the same group. The only major difference was that the example with an IP address for the status quo achieved worse detection rates compared to the random URL one.

#### Legitimate examples:

Differently than the phishing examples (see Table 4), the legitimate examples can only be categorized in limited fashion. The examples L7 and L8 (see Table 8 for details) had a typo in the link-text, comparable to the phishing examples with “Delusive Mismatched URLs.” Therefore, those examples could be categorized as “legitimate with a small error,” with the other legitimate example being fully legitimate. Generally, the legitimate examples mostly achieved higher scores than the phishing ones for their respective group. Interestingly, L1 scored lower for the status quo groups with video

**Table 4: Overview of the percentage of correct answers for the legitimate examples. Grp1 = Status bar, Grp2 = Tooltip, Grp3 = NoPhish video + Status bar, Grp4 = NoPhish Video + Tooltip, Grp5 = TORPEDO warnings, Grp6 = NoPhish video + TORPEDO warnings, Grp7 = TORPEDO warnings without tutorial, Grp8 = NoPhish video + TORPEDO warnings without tutorial.**

Name	Grp1	Grp2	Grp3	Grp4	Grp5	Grp6	Grp7	Grp8
L1	74.14	77.36	61.22	61.70	98.41	97.44	86.21	80.95
L2	82.76	84.91	95.92	95.74	100.00	94.87	82.76	92.86
L3	94.83	94.34	100.00	93.62	100.00	100.00	93.10	100.00
L4	93.10	84.91	85.71	93.62	98.41	97.44	89.66	97.62
L5	87.93	90.57	81.63	89.36	100.00	100.00	94.83	95.24
L6	94.83	86.79	100.00	93.62	100.00	100.00	94.83	100.00
L7	62.07	71.70	71.43	63.83	95.24	94.87	79.31	85.71
L8	63.79	79.25	73.47	63.83	95.24	94.87	68.97	61.90

than the equivalents without video. In contrast, the four groups with the TORPEDO warnings performed better on this example than the status quo, both with and without video. The difference between the legitimate examples for the TORPEDO groups with tutorial was shallow, and only in the range of 5% from the worst to the best example. For the other six groups, i.e., the status quo with and without video, and the TORPEDO warnings without tutorial, the differences were higher and tended to be in the range of 20 to almost 40% (NoPhish video + status bar or NoPhish video with TORPEDO warnings without tutorial). Across all groups, it is also noticeable that L1 performed worse on average, alongside L7 and L8 (which both have spelling mistakes in the link text), with just under 80% across all groups. For example, only L7 and L8 performed worse across all groups.

To summarize, it can be said that the manipulation strategy “Mangle” stood out in the phishing category. Both the manipulation strategy and the single examples from this strategy were the most difficult ones to detect across all the phishing examples. It is also noticeable that the selected phishing examples produced similar results for the respective manipulation strategy. When comparing the results of the video groups with those of the TORPEDO groups, it is noticeable that the differences in the phishing category were similar – except for the combination of both, which outperformed all groups. In contrast, the TORPEDO groups achieved significantly better results than the video groups, particularly for legitimate messages.

### 5.3 Effectiveness of different risk levels

Furthermore, we evaluated the effect of the TORPEDO warnings’ different risk levels as they have different designs and texts. For both the phishing and legitimate examples with the different frame colors and classification the average number of correct answers is displayed in Table 8. For the fraudulent examples with the gray frame color there was not much difference between those with and without an indicator. For all four TORPEDO groups those examples scored higher ranging from very similar for the TORPEDO warnings without tutorial group (96.92% to 97.95%) to the biggest difference for the TORPEDO warnings group (80% to 94.29%). For the legitimate examples it was the opposite as those examples with an indicator scored lower than those without an indicator. All four groups achieve values above 80% up to 97.46% for the legitimate examples with an indicator. As expected for the phishing examples the indicator lead to a higher detection rate and for the legitimate examples the detection rate decreased for those with an indicator.

However, especially the group NoPhish video + TORPEDO warnings performed at a nearly optimal level for both those examples with indicator and those without. The TORPEDO warnings group at least for the legitimate examples performed on a similar level and only scored lower for those phishing examples without an indicator. So a possible negative effect of the indicator in the direction of a lower rate for legitimate examples with an indicator could not be found. Overall all risk level especially when the tutorial and phishing awareness video are provided lead to very good values of phishing detection. Only for the group TORPEDO warnings the gray risk level without an indicator lead to around 15 to 20% lower rates of such phishing examples.

## 6 DISCUSSION

Our findings provide important insights regarding the interplay and effectiveness of a specific phishing awareness video and a link-centric warning tool. As such, our findings may not directly generalize to other phishing awareness measures and other forms of phishing support. Nevertheless, we believe they still meaningfully contribute to the research on phishing awareness measures and support tools.

*NoPhish Video or TORPEDO warnings.* Starting with the results for the prerequisites, they showed that the NoPhish video improved the detection rate significantly for the status quo (RQ-1) as did the TORPEDO warnings (RQ-2). Thus, the prerequisites are met, as both interventions on their own performed better than the status quo with either a single status-bar or a combination of a tooltip with a status-bar. So, even though participants might be more aware of the URL and it’s importance for phishing due to the interaction with the practice task, this did not lead to an improvement in their ability to distinguish between phishing and legitimate examples, as evidenced by the lower performance in the control groups. At least, not to such an extent that the improvement provided by either intervention is negated in some way. Additionally, the TORPEDO warnings performed better compared to the NoPhish video (RQ-3). So, when someone would have the resources to only introduce one of the two interventions, our results suggest that the TORPEDO warnings or a similar phishing support tool would be the better option overall.

*Combination of Awareness + Support Tools.* However, the results for RQ-4 clearly indicate that the combination of the NoPhish phishing awareness video and the TORPEDO warnings is more effective in supporting users in their ability to distinguish between phishing and legitimate examples compared to each intervention on its own.

**Table 5: Overview of % correct answers for the different risk level of TORPEDO Warnings. For explanation of the risk level see Section 3.2.2.**

	Legitimate			Phish	
	Low (green)	Unknown without indicator (gray)	Unknown with indicator (gray with warning triangle)	Unknown without indicator (gray)	Unknown with indicator (gray with warning triangle)
TORPEDO warnings	98.41	99.47	97.46	80.00	94.29
NoPhish video + TORPEDO warnings	97.95	97.44	96.92	96.92	97.95
TORPEDO warnings without tutorial	88.97	89.08	82.07	59.31	69.31
NoPhish video + TORPEDO warnings without tutorial	92.86	95.24	86.67	88.57	92.86

To further improve the situation, in future work the NoPhish video and the TORPEDO warnings could be integrated more. Note, the NoPhish video was not designed with the studied TORPEDO warnings in mind, but was rather meant to improve phishing awareness for the status quo, i.e., URLs displayed in simple tooltips and/or status bars. Based on the results for RQ-5, it is also apparent that TORPEDO warnings should be combined with the tutorial, in particular to explain the meaning of the unknown risk level, and to explain that unknown risk with indicator does not necessarily mean it is a phishing link, but rather than caution is warranted. Our findings also suggest that the TORPEDO warning design for this case could be improved further.

*Difference of Manipulation Strategies.* There are different manipulation strategies, with substantial differences between NoPhish video and TORPEDO warnings. For example, in Mangle, there is a difference of 53.97% correct answers (TORPEDO warnings) to 75.53% correct answers (NoPhish video). Likewise, there is a difference of 98.41% correct answers (TORPEDO warnings) to 81.91% correct answers (NoPhish video) for legitimate examples.

Identification of the manipulation strategies of the mangle type seems to benefit from a combination of the NoPhish video and TORPEDO warnings. This might be, on the one hand, because there are several such examples in the NoPhish video and it explains several times that it is important to check character by character. On the other hand, this might be due to how the URL is displayed in the studied TORPEDO warnings approach. While we saw a huge performance difference for the mangle type compared to the status quo (from 20% status bar, 25% tooltip to 92% when combining the NoPhish video and TORPEDO warnings), the 85% is still the lowest compared to the other manipulation strategies.

As future work, it is worth studying different ways to display the URL in the TORPEDO warnings to find the optimal one with respect to this type.

*Status quo (status bar and tooltip).* Our results contribute further evidence that developers of email clients and web browsers should rethink how they display information on URLs behind links. Using the status bar as a display format for the URL causes problems – on average, only 54% of the phishes were detected in the groups without additional link-centric warnings. Thus, our findings demonstrate the need for browsers and email clients to provide link-centric information that actively helps users scrutinize a link URL, e.g., by highlighting the domain and indicating mismatches between link-text and URL. Furthermore, the idea of TORPEDO [54] to have different risk levels is worth implementing as, on the one hand, the links with low risk level can be decided quickly and, on the other hand, the results in Table 8 show that it is possible to

explain to users false positives for the unknown with indicator risk level.

*Comparing results to previous studies.* The results from this study suggest an even better result for the combined approach with TORPEDO warnings and the NoPhish video ( $d' = 2.92$ ) compared to previous studies (analyzing the sensitivity from SDT) like Reinheimer et al. [43] for their instructor-based training ( $d' = 2.13$ ) and for their video reminder ( $d' = 1.80$ ), Sheng et al. [48] for their phishing game ( $d' = 2.02$ ), and Berens et al. with their online course [9] ( $d' = 2.66$ ).

*Takeaways for the design of link-centric warnings.* Although we looked at a specific phishing support tool, our findings still provide insights for the design of phishing warnings. One of the significant takeaways, especially in the context of link-centric warnings, is that even when such warnings include textual content to describe the current situation, a tutorial can be helpful and should be offered. Both groups with the tutorial performed significantly better than their counterpart without one. So, at least in a situation when multiple categorizations akin to TORPEDO’s risk levels are used, it might be helpful to directly give the users an overview of the possible categorizations. While users might also be able to learn about categorizations and their functionality over time, and might eventually catch up with those that have received an overview at the beginning, our findings suggest that this effect would be delayed. Furthermore, such a catch up effect would need to be further investigated.

*Takeaways for the design of phishing awareness videos.* Our findings also provide insights for the design of phishing awareness videos. It is particularly striking that both video groups in our study did not perform well for the “Mangle” manipulation strategies (55.1% and 75.53%). These results are comparable with earlier results from more complex measures, such as an Android game (approx. 30%) [16] or e-learning (70.83%) [9]. So, there’s a need to investigate more effective ways of helping users recognize this phishing trick, similarly to successful awareness measures for other phishing tricks. Various effects could play a role here, which should be investigated in more details. Explanations need to consider the effect that people do not read words letter by letter. For example, more concrete examples could be shared to demonstrate how easy it is to overlook such small changes.

## 7 CONCLUSION

Phishing awareness measures and warnings have been extensively studied, but little is known about how they work together in aiding

users to recognize phishing attacks. To address this gap, we conducted an online experiment comparing the NoPhish video [56] and the TORPEDO warnings [54]. We chose these interventions because they both focus on users considering the URL before clicking and have individually been shown to have positive effects on phishing detection rates. Our findings confirm previous research [40, 54, 56] that both the phishing awareness video and the link-centric warning significantly improve phishing detection compared to baseline groups representing traditional web browser/email client practices. However, we also found that TORPEDO warnings outperform the NoPhish video, and combining TORPEDO warnings and NoPhish video yields the best results. Our results highlight the necessity for both warnings and educational videos, with the video ideally preceding the warnings. Browsers and email clients should provide more informative URL details directly within links. Additionally, it's beneficial to move beyond simple tooltips, such as those in MS Outlook and Apple Mail, and consider more expressive link-centric warnings, as studied here.

## ACKNOWLEDGMENTS

This work has been partially supported by Google through a Faculty Research Award and this work was partially funded by the Topic Engineering Secure Systems, subtopic 46.23.01 Methods for Engineering Secure Systems, of the Helmholtz Association (HGF) and supported by KASTEL Security Research Labs, Karlsruhe.

## REFERENCES

- [1] Jemal Abawajy. 2014. User preference of cyber security awareness delivery methods. *Behaviour & Information Technology* 33, 3 (2014), 237–248. <https://doi.org/10.1080/0144929X.2012.708787> arXiv:<https://doi.org/10.1080/0144929X.2012.708787>
- [2] Devdatta Akhawe and Adrienne Porter Felt. 2013. Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness. In *22nd USENIX Security Symposium (USENIX Security 13)*. USENIX Association, Washington, D.C., 257–272. <https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/akhawe>
- [3] Sara Albakry, Kami Vaniea, and Maria K. Wolters. 2020. What is This URL's Destination? Empirical Evaluation of Users' URL Reading. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (Honolulu, HI, USA) (CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–12. <https://doi.org/10.1145/3313831.3376168>
- [4] Abdullah Alnajim and Malcolm Munro. 2009. An Anti-Phishing Approach that Uses Training Intervention for Phishing Websites Detection. In *6th International Conference on Information Technology: New Generations*. IEEE, Las Vegas, NV, USA, 405–410.
- [5] Abdullah Alnajim and Malcolm Munro. 2009. An Evaluation of Users' Anti-Phishing Knowledge Retention. In *2009 International Conference on Information Management and Engineering*. IEEE, Kuala Lumpur, Malaysia, 210–214. <https://doi.org/10.1109/ICIME.2009.114>
- [6] Kholoud Althobaiti, Nicole Meng, and Kami Vaniea. 2021. I Don't Need an Expert! Making URL Phishing Features Human Comprehensible. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (<conf-loc>, <city>Yokohama</city>, <country>Japan</country>, </conf-loc>)* (CHI '21). Association for Computing Machinery, New York, NY, USA, Article 695, 17 pages. <https://doi.org/10.1145/3411764.3445574>
- [7] Kholoud Althobaiti, Kami Vaniea, and Serena Zheng. 2018. Faheem: Explaining URLs to people using a Slack bot. In *Symposium on Digital Behaviour Intervention for Cyber Security (AISB)*. Edinburgh Research Explorer, Liverpool, UK, 1–8.
- [8] Nalin Asanka Gamagedara Arachchilage, Steve Love, and Konstantin Beznosov. 2016. Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior* 60 (2016), 185–197.
- [9] Benjamin Berens, Mattia Mossano, and Melanie Volkamer. 2022. Phishing awareness and education – When to best remind?. In *Symposium on Usable Security and Privacy (USEC) (Symposium on Usable Security and Privacy (USEC), Vol. USEC)*. Internet Society, San Diego, CA, USA, 1–15.
- [10] Vaishnavi Bhavsar, Aditya Kadlak, and Shabnam Sharma. 2018. Study on Phishing Attacks. *International Journal of Computer Applications* 182, 33 (2018), 27–29. <https://doi.org/10.5120/ijca2018918286>
- [11] Statistisches Bundesamt. 2022. Mindestlohn. [https://www.destatis.de/DE/Themen/Arbeit/Verdienste/Mindestloehne/\\_inhalt.html](https://www.destatis.de/DE/Themen/Arbeit/Verdienste/Mindestloehne/_inhalt.html)
- [12] Casey Canfield, Alex Davis, Baruch Fischhoff, Alain Forget, Sarah Pearman, and Jeremy Thomas. 2017. Replication: Challenges in Using Data Logs to Validate Phishing Detection Ability Metrics. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, Santa Clara, CA, 271–284. <https://www.usenix.org/conference/soups2017/technical-sessions/presentation/canfield>
- [13] Casey Canfield, Baruch Fischhoff, and Alex Davis. 2015. Using Signal Detection Theory to Measure Phishing Detection Ability and Behavior. In *Poster Abstr. SOUPS 2015*. *Poster Abstr. SOUPS 2015* 3, 3, 1–2.
- [14] Casey Canfield, Baruch Fischhoff, and Alex Davis. 2016. Quantifying Phishing Susceptibility for Detection and Behavior Decisions. *Human Factors: The Journal of Human Factors and Ergonomics Society* 58 (2016), 1158–1172. <https://doi.org/10.1177/0018720816665025>
- [15] Casey Inez Canfield and Baruch Fischhoff. 2018. Setting Priorities in Behavioral Interventions: An Application to Reducing Phishing Risk. *Risk Analysis* 38 (2018), 826–838. <https://doi.org/10.1111/risa.12917>
- [16] Gamze Canova, Melanie Volkamer, Clemens Bergmann, and Benjamin Reinheimer. 2015. NoPhish App Evaluation: Lab and Retention Study. In *USEC. Internet Society, San Diego, CA, USA*, 1–10.
- [17] Lennon YC Chang and Nicholas Coppel. 2020. Building cyber security awareness in a developing country: lessons from Myanmar. *Computers & Security* 97 (2020), 101959.
- [18] Gokul CJ, Sankalp Pandit, Sukanya Vaddepalli, Harshal Tupsamudre, Vijayanand Banahatti, and Sachin Lodha. 2018. PHISHY - A Serious Game to Train Enterprise Users on Phishing Awareness. In *Proceedings of the 2018 annual symposium on computer-human interaction in play companion extended abstracts (Melbourne, VIC, Australia) (CHI PLAY '18 Extended Abstracts)*. Association for Computing Machinery, New York, NY, USA, 169–181. <https://doi.org/10.1145/3270316.3273042>
- [19] Barry H Cohen. 2008. *Explaining psychological statistics*. John Wiley & Sons, Hoboken, New Jersey.
- [20] Julie S. Downs, Mandy Holbrook, and Lorrie Faith Cranor. 2007. Behavioral Response to Phishing Risk. In *Proceedings of the Anti-Phishing Working Groups 2nd Annual ECrime Researchers Summit (Pittsburgh, Pennsylvania, USA) (eCrime '07)*. Association for Computing Machinery, New York, NY, USA, 37–44. <https://doi.org/10.1145/1299015.1299019>
- [21] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. 2008. You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (Florence, Italy) (CHI '08)*. Association for Computing Machinery, New York, NY, USA, 1065–1074. <https://doi.org/10.1145/1357054.1357219>
- [22] Iain Embrey and Kim Kaivanto. 2023. Many phish in the C: A coexisting-choice-criteria model of security behavior. *Risk analysis* 43, 4 (2023), 783–799.
- [23] Adrienne Porter Felt, Robert W. Reeder, Alex Ainslie, Helen Harris, Max Walker, Christopher Thompson, Mustafa Emre Acer, Elisabeth Morant, and Sunny Consolvo. 2016. Rethinking Connection Security Indicators. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, Denver, CO, 1–14. <https://www.usenix.org/conference/soups2016/technical-sessions/presentation/porter-felt>
- [24] Vaibhav Garg, Jean Camp, Lesa Mae, and Katherine Connelly. 2011. Designing risk communication for older adults. In *Symposium on Usable Privacy and Security (SOUPS)*. Citeseer, Citeseer, Pittsburgh, PA USA, 20–22.
- [25] Kamran Javed Hamdani and Muhammad Ijaz E Mustafa. 2021. *Effectiveness of Online Anti-Phishing Delivery methods in raising Awareness among Internet Users*. Master's thesis. Luleå University of Technology, Department of Computer Science, Electrical and Space Engineering.
- [26] Ponnuram Kumaraguru, Justin Cranshaw, Alessandro Acquisti, Lorrie Cranor, Jason Hong, Mary Ann Blair, and Theodore Pham. 2009. School of Phish: A Real-World Evaluation of Anti-Phishing Training. In *Proceedings of the 5th Symposium on Usable Privacy and Security (Mountain View, California, USA) (SOUPS '09)*. Association for Computing Machinery, New York, NY, USA, Article 3, 12 pages. <https://doi.org/10.1145/1572532.1572536>
- [27] Ponnuram Kumaraguru, Yong Rhee, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. 2007. Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System. In *CHI*. ACM, New York, NY, USA, 905–914. <https://doi.org/10.1145/1240624.1240760>
- [28] Elmer Lastdrager, Inés Carvajal Gallardo, Pieter Hartel, and Marianne Junger. 2017. How Effective is Anti-Phishing Training for Children?. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, Santa Clara, CA, 229–239. <https://www.usenix.org/conference/soups2017/technical-sessions/presentation/lastdrager>
- [29] Peter Likarish, Donald E Dunbar, Juan Pablo Hourcade, and Eunjin Jung. 2009. BayeShield: conversational anti-phishing user interface.. In *SOUPS*, Vol. 9. ACM, Mountain View, CA, USA, 1–1.

- [30] Eric Lin, Saul Greenberg, Eileah Trotter, David Ma, and John Aycok. 2011. Does Domain Highlighting Help People Identify Phishing Sites?. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (<conf-loc>, <city>Vancouver</city>, <state>BC</state>, <country>Canada</country>, </conf-loc>) (CHI '11). Association for Computing Machinery, New York, NY, USA, 2075–2084. <https://doi.org/10.1145/1978942.1979244>
- [31] Jaclyn Martin. 2017. *Something Looks Phishy Here: Applications of Signal Detection Theory to Cyber-Security Behaviors in the Workplace*. Ph.D. Dissertation. University of South Florida.
- [32] Jaclyn Martin, Chad Dubé, and Michael D Coovert. 2018. Signal Detection Theory (SDT) Is Effective for Modeling User Behavior Toward Phishing and Spear-Phishing Attacks. *Human Factors: The Journal of Human Factors and Ergonomics Society* 60 (2018), 1179–1191. <https://doi.org/10.1177/0018720818789818>
- [33] Christopher B Mayhorn and Patrick G Nyeste. 2012. Training users to counteract phishing. *Work (Reading, Mass.)* 41 Suppl 1 (2012), 3549–52. <https://doi.org/10.3233/wor-2012-1054-3549>
- [34] Gaurav Misra, Nalin Asanka Gamagedara Arachchilage, and Shlomo Berkovsky. 2017. Phish Phinder: A Game Design Approach to Enhance User Confidence in Mitigating Phishing Attacks. arXiv:1710.06064 [cs.CR]
- [35] María M Moreno-Fernández, Fernando Blanco, Pablo Garaizar, and Helena Matute. 2017. Fishing for phishers. Improving Internet users' sensitivity to visual deception cues to prevent electronic fraud. *Computers in Human Behavior* 69 (2017), 421–436. <https://doi.org/10.1016/j.chb.2016.12.044>
- [36] Mattia Mossano, Benjamin Berens, Philip Heller, Christopher Beckmann, Lukas Aldag, Peter Mayer, and Melanie Volkamer. 2022. SMILE - Smart eMail Link Domain Extractor. In *Computer Security. ESORICS 2021 International Workshops*. Springer International Publishing, Cham, 403–412.
- [37] Stephan Neumann, Benjamin Reinheimer, and Melanie Volkamer. 2017. Don't Be Deceived: The Message Might Be Fake. In *Trust, Privacy and Security in Digital Business*. Springer International Publishing, Cham, 199–214.
- [38] Federal Bureau of Investigation. 2023. *Intrnet Crime Report 2022*. Technical Report. Federal Bureau of Investigation. [https://www.ic3.gov/Media/PDF/AnnualReport/2022\\_IC3Report.pdf](https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf)
- [39] Adebukola S. Onashoga, Oluwafolake E. Ojo, and Oluwadamilola O. Soyombo. 2019. Securix: a 3D game-based learning approach for phishing attack awareness. *Journal of Cyber Security Technology* 3, 2 (2019), 108–124. <https://doi.org/10.1080/23742917.2019.1624011> arXiv:https://doi.org/10.1080/23742917.2019.1624011
- [40] Justin Petelka, Yixin Zou, and Florian Schaub. 2019. Put Your Warning Where Your Link Is: Improving and Evaluating Email Phishing Warnings. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) (CHI '19). Association for Computing Machinery, New York, NY, USA, 1–15. <https://doi.org/10.1145/3290605.3300748>
- [41] Daniel Pienta, Jason Bennett Thatcher, and Allen C Johnston. 2018. A Taxonomy of Phishing: Attack Types Spanning Economic, Temporal, Breadth, and Target Boundaries. In *Workshop on Information Security and Privacy* (San Francisco, CA, US) (WISP 2018, Vol. 1). Association for Information Systems, Atlanta, GA, US, 1–18. <https://aisel.aisnet.org/wisp2018/19>
- [42] Rebecca Smith. 2016. How a U.S. utility Got Hacked. <https://www.wsj.com/articles/how-a-u-s-utility-got-hacked-1483120856> accessed: 21.01.2022.
- [43] Benjamin Reinheimer, Lukas Aldag, Peter Mayer, Mattia Mossano, Reyhan Duezgüen, Bettina Lofthouse, Tatiana von Landesberger, and Melanie Volkamer. 2020. An investigation of phishing awareness and education over time: When and how to best remind users. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, Berkeley, CA, US, 259–284. <https://www.usenix.org/conference/soups2020/presentation/reinheimer>
- [44] Scott Ruoti, Jeff Andersen, Scott Heidbrink, Mark O'Neill, Elham Vaziripour, Justin Wu, Daniel Zappala, and Kent Seamons. 2016. "We're on the Same Page": A Usability Study of Secure Email Using Pairs of Novice Users. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) (CHI '16). Association for Computing Machinery, New York, NY, USA, 4298–4308. <https://doi.org/10.1145/2858036.2858400>
- [45] Stuart E. Schechter, Rachna Dhamija, Andy Ozment, and Ian Fischer. 2007. The Emperor's New Security Indicators. In *2007 IEEE Symposium on Security and Privacy (SP '07)*. IEEE, Berkeley, CA, USA, 51–65. <https://doi.org/10.1109/SP.2007.35>
- [46] SecureList. 2023. *Spam and Phishing in 2022*. Kaspersky. Retrieved 12.12.2023 from <https://securelist.com/spam-phishing-scam-report-2022/108692/>
- [47] Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Faith Cranor, and Julie Downs. 2010. Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Atlanta, Georgia, USA) (CHI '10). Association for Computing Machinery, New York, NY, USA, 373–382. <https://doi.org/10.1145/1753326.1753383>
- [48] Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. 2007. Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish. In *Proceedings of the 3rd Symposium on Usable Privacy and Security* (Pittsburgh, Pennsylvania, USA) (SOUPS '07). Association for Computing Machinery, New York, NY, USA, 88–99. <https://doi.org/10.1145/1280680.1280692>
- [49] Harold Stanislaw and Natasha Todorov. 1999. Calculation of signal detection theory measures. *Behavior Research Methods, Instruments, & Computers* 31, 1 (1999), 137–149.
- [50] Simon Stockhardt, Benjamin Reinheimer, Melanie Volkamer, Peter Mayer, Alexandra Kunz, Philipp Rack, and Daniel Lehmann. 2016. Teaching Phishing-Security: Which Way is Best? *IFIP SEC 471* (2016), 135–149. [https://doi.org/10.1007/978-3-319-33630-5\\_10](https://doi.org/10.1007/978-3-319-33630-5_10)
- [51] Verizon. 2022. *Data Breach Investigations Report*. Technical Report. Verizon.
- [52] Melanie Volkamer, Karen Renaud, and Paul Gerber. 2016. Spot the phish by checking the pruned URL. *Information and Computer Security* Volume 24 (2016), 372–385. <https://doi.org/10.1108/ics-07-2015-0032>
- [53] Melanie Volkamer, Karen Renaud, and Paul Gerber. 2016. Spot the phish by checking the pruned URL. *Information and Computer Security* 24, 4 (2016), 372–385. <https://doi.org/10.1108/ICS-07-2015-0032>
- [54] Melanie Volkamer, Karen Renaud, and Benjamin Reinheimer. 2016. TORPEDO: TOoltip-poweRed Phishing Email DetectiOn. In *IFIP SEC*. Springer, Springer International Publishing, Cham, 161–175.
- [55] Melanie Volkamer, Karen Renaud, Benjamin Reinheimer, and Alexandra Kunz. 2017. User experiences of TORPEDO: TOoltip-poweRed Phishing Email DetectiOn. *Computers & Security* 71 (2017), 100–113. <https://doi.org/10.1016/j.cose.2017.02.004>
- [56] Melanie Volkamer, Karen Renaud, Benjamin Reinheimer, Philipp Rack, Marco Ghiglieri, Peter Mayer, Alexandra Kunz, and Nina Gerber. 2018. Developing and Evaluating a Five Minute Phishing Awareness Video. *Trust, Privacy and Security in Digital Business (TrustBus)* 11033 (2018), 119–134. [https://doi.org/10.1007/978-3-319-98385-1\\_9](https://doi.org/10.1007/978-3-319-98385-1_9)
- [57] Rick Wash and Molly M. Cooper. 2018. Who Provides Phishing Training? Facts, Stories, and People Like Me. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) (CHI '18). Association for Computing Machinery, New York, NY, USA, 1–12. <https://doi.org/10.1145/3173574.3174066>
- [58] Zikai Alex Wen, Zhiqiu Lin, Rowena Chen, and Erik Andersen. 2019. What.Hack: Engaging Anti-Phishing Training Through a Role-Playing Phishing Simulation Game. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) (CHI '19). Association for Computing Machinery, New York, NY, USA, 1–12. <https://doi.org/10.1145/3290605.3300338>
- [59] Min Wu, Robert C. Miller, and Simson L. Garfinkel. 2006. Do Security Toolbars Actually Prevent Phishing Attacks?. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Montréal, Québec, Canada) (CHI '06). Association for Computing Machinery, New York, NY, USA, 601–610. <https://doi.org/10.1145/1124772.1124863>
- [60] Aiping Xiong, Robert W. Proctor, Weining Yang, and Ninghui Li. 2017. Is Domain Highlighting Actually Helpful in Identifying Phishing Web Pages? *Human Factors* 59, 4 (2017), 640–660. <https://doi.org/10.1177/0018720816684064>
- [61] Takashi Yamanoue, Michio Nakanishi, Atsushi Nakamura, Izumi Fuse, Ikuya Murata, Shozo Fukada, Takahiro Tagawa, Tatsumi Takeo, Shigeto Okabe, and Tsuneo Yamada. 2005. Digital Video Clips Covering Computer Ethics in Higher Education. In *Proceedings of the 33rd Annual ACM SIGUCCS Conference on User Services* (Monterey, CA, USA) (SIGUCCS '05). Association for Computing Machinery, New York, NY, USA, 456–461. <https://doi.org/10.1145/1099435.1099536>
- [62] Tianjian Zhang. 2018. Knowledge Expiration in Security Awareness Training. *Conference on Digital Forensics, Security and Law (ADFSL)* 2 (2018), 197–212.
- [63] Yue Zhang, Jason I. Hong, and Lorrie F. Cranor. 2007. Cantina: A Content-Based Approach to Detecting Phishing Web Sites. In *Proceedings of the 16th International Conference on World Wide Web* (Banff, Alberta, Canada) (WWW '07). Association for Computing Machinery, New York, NY, USA, 639–648. <https://doi.org/10.1145/1242572.1242659>

## A APPENDICES

### A.1 TORPEDO Risk Level Screenshots

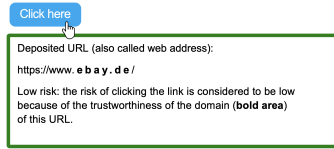


Figure 5: TORPEDO’s low risk level warning.

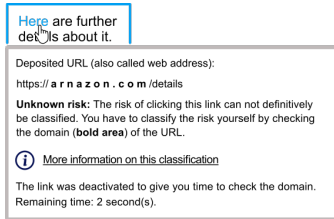


Figure 6: TORPEDO’s unknown risk warning.

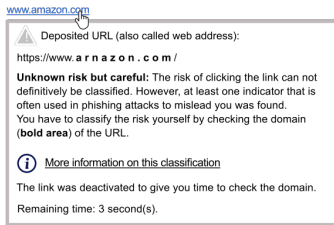


Figure 7: TORPEDO’s unknown risk warning with indicator.

### A.2 Socio-demographics

For the age (see Table 6) and gender (see Table 7) we see a general trend of mostly participants from 20 to 40, with some older participants distributed across groups and a trend towards more male than female participants. 187 participants were university graduates and only 37 had an occupation linked to IT.

Table 6: Age distribution

Group	Age range in years										
	18-19	20-24	25-29	30-34	35-39	40-44	45-49	50-54	55-59	60-64	>65
ST	1	10	8	13	8	6	2	4	4	1	1
AW + ST	3	4	14	8	6	3	2	2	4	3	0
TT	2	7	8	7	8	7	7	2	1	3	1
AW + TT		7	7	7	5	5	4	1	6	1	2
- awareness, + tutorial	4	8	16	17	4	3	5	2	4	0	0
- awareness, - tutorial	3	6	10	9	15	4	4	6	1	0	0
+ awareness, - tutorial	0	5	11	10	4	5	3	2	1	1	0
+ awareness, + tutorial	1	3	7	6	6	7	2	4	2	1	0

**Table 7: Gender distribution across the different groups.**

Group	Male	Female	Diverse or Not Specified
Status Bar	39	19	0
Tooltip	32	21	0
NoPhish Video + Status Bar	27	22	0
NoPhish Video + Tooltip	37	10	0
TORPEDO Warnings	31	31	1
TORPEDO Warnings Without Tutorial	41	16	1
NoPhish Video + TORPEDO Warnings Without Tutorial	21	21	0
NoPhish Video + TORPEDO Warnings	26	12	1

### A.3 Overview of the factors creating the phishing and legitimate examples

**Table 8: Overview of the manipulation strategies matched to the companies and the TORPEDO warnings risk levels. (1) Link text in email: <https://brief.gmmx.net/AGB>. (2) Link text in email: <https://www.paypall.com/gutschein>. (3) Link text in email: <https://premium.gmx.de/speichervoll>. (4) Link text in email: <https://www.paypal.com/>. As of 22.02.2024, the URLs have been checked and pose no risk. No guarantees can be given for the future.**

Name	Company	Manipulation Strategies	URL	Risk level
L1	Amazon	Legitimate	<a href="https://packet.amazon.de/paketverfolgung">https://packet.amazon.de/paketverfolgung</a>	low
L2	Lufthansa	Legitimate	<a href="https://www.lufthansa.com/buchungsanzeige">https://www.lufthansa.com/buchungsanzeige</a>	unknown
L3	Google	Legitimate	<a href="https://www.google.com/neuesgeraet">https://www.google.com/neuesgeraet</a>	low
L4	LinkedIn	Legitimate	<a href="https://video.linkedin.com/kurs">https://video.linkedin.com/kurs</a>	unknown
L5	DHL	Legitimate	<a href="https://mailing.dhl.de/wunschort">https://mailing.dhl.de/wunschort</a>	unknown
L6	Netflix	Legitimate	<a href="https://www.netflix.com/neuepreise">https://www.netflix.com/neuepreise</a>	low
L7	GMX	Legitimate	<a href="https://bestaetigung.gmx.de/AGB_1">https://bestaetigung.gmx.de/AGB_1</a>	low
L8	PayPal	Legitimate	<a href="https://www.paypal.com/gutschein_2">https://www.paypal.com/gutschein_2</a>	unknown with indicator
P1	Amazon	Obfuscate	<a href="https://telefon.host745.com/hinzufuegen">https://telefon.host745.com/hinzufuegen</a>	unknown
P2	Lufthansa	Obfuscate	<a href="https://87.147.12.250/buchungsänderung">https://87.147.12.250/buchungsänderung</a>	unknown with indicator
P3	Google	Mislead	<a href="https://www.google.com.megahoust.ru/sicherheitscheck">https://www.google.com.megahoust.ru/sicherheitscheck</a>	unknown
P4	LinkedIn	Mislead	<a href="https://login.linkyzt.com/www.linkedin.com/profil">https://login.linkyzt.com/www.linkedin.com/profil</a>	unknown
P5	DHL	Mangle	<a href="https://account.dlh.com/zustellung">https://account.dlh.com/zustellung</a>	unknown
P6	Netflix	Mangle	<a href="https://www.netflx.com/neuerlogin">https://www.netflx.com/neuerlogin</a>	unknown
P7	GMX	Delusive Mism. URL	<a href="https://premium.host547.ru/speichervoll_3">https://premium.host547.ru/speichervoll_3</a>	unknown with indicator
P8	PayPal	Delusive Mism. URL	<a href="https://www.hokpurt.ru/AGB_4">https://www.hokpurt.ru/AGB_4</a>	unknown with indicator

### A.4 Extended ANOVA Tests Table

**Table 9: Overview hypotheses for sensitivity ( $d'$ ) and criterion ( $C$ ). Significance with '\*\*\*\*\*' < 0.0001, '\*\*\*\*' = 0.0001, '\*\*\*' = 0.001, '\*\*' = 0.01 and 'ns' = not significant. The third column per value always contains the level of significance found comparing the groups with a Game-Howell correction for multiple testing.**

Group 1	Group 2	Sensitivity $d'$			Criterion $C$		
		Group 1	Group 2	sig.	Group 1	Group 2	sig.
Status bar	Phishing Awareness Video + Status bar	1.01	1.87	****	0.41	0.03	***
Tooltip	Phishing Awareness Video + Tooltip	1.13	2.12	****	0.4	-0.13	****
Status bar	Phishing Support Tool	1.01	2.51	****	0.41	0.27	ns
Tooltip	Phishing Support Tool	1.07	2.51	****	0.4	0.27	ns
Phishing Awareness Video + Status bar	Phishing Support Tool	1.87	2.51	****	0.03	0.27	ns
Phishing Awareness Video + Tooltip	Phishing Support Tool	2.12	2.51	***	-0.13	0.27	***
Phishing Awareness Video + Status bar	Phishing Awareness Video + Phishing Support Tool	1.87	2.92	****	0.03	0.01	ns
Phishing Awareness Video + Tooltip	Phishing Awareness Video + Phishing Support Tool	2.12	2.92	****	-0.13	0.01	ns
Phishing Support Tool	Phishing Awareness Video + Phishing Support Tool	2.51	2.92	****	0.27	0.01	****
Phishing Support Tool	Phishing Support Tool without tutorial	2.51	1.42	****	0.27	0.37	ns
Phishing Awareness Video + Status bar	Phishing Support Tool without tutorial	1.87	1.42	ns	0.03	0.37	*
Phishing Awareness Video + Tooltip	Phishing Support Tool without tutorial	2.12	1.42	ns	-0.13	0.37	****



## A.5 TORPEDO Tutorial

In this study, you will assess emails in the Chrome web browser. These are emails that Martin Müller found in his Gmail account. Martin Müller already has a new update of the Chrome browser. The goal of this update is to help users distinguish between phishing emails and legitimate emails. As in the video you saw, you can still check the URL in the status bar at the bottom left of the screen. The new tooltip also supports you with even more functionality in detecting legitimate or phishing emails.

In the following we will briefly explain how this support works:  
When you touch a link in the email with your mouse, one of three dialogs appears.  
All dialogs contain the domain. The domain is also called the who area. The domain is the most important area of a URL (also called web address) when it comes to phishing email detection.

The domain is marked in **bold** in the following example URL:

<https://www.mail.google.de/dshf0qdfqfssxcidsfhqiodhufqifhqd/index.php>

So in the dialog, the URL would be displayed and the domain **google.de** would be highlighted in bold.

Which of the three dialogs is displayed depends on the risk level:

1. Green – the risk of clicking the link is rated as low. The reason is that the domain is part of a list of most visited websites of all internet users in Germany.

In the following example "Click here" is the link.

Click here

Deposited URL (also called web address):  
<https://www.ebay.de/>

Low risk: the risk of clicking the link is considered to be low because of the trustworthiness of the domain (**bold area**) of this URL.

(a) Link-Centric Warning Tutorial Part1.

3. Grey – the risk of clicking the link is rated as unknown. In these cases, you must check the domain yourself to find out whether the link will lead to a phish-attack or not. To avoid rash clicking, the link is deactivated for three seconds.

The following section contains one **phishing** and one **legitimate** example.

**Example 1:** Imagine you open an email. The design of the email and the sender make it look like clicking the link will open a New York Times website with the subject covid-19.

In this example "Here" is the phishing link since you are not forwarded to the New York Times.

Here are further details about it.

Deposited URL (also called web address):  
<https://2020coronaviruspandemic.com/>

**Unknown risk:** The risk of clicking this link can not definitively be classified. You have to classify the risk yourself by checking the domain (**bold area**) of the URL.

The link was deactivated to give you time to check the domain.  
Remaining time: 2 second(s).

**Example 2:** Imagine you open an email. The design and the sender suggest that clicking the link would lead to a website of the RWTH-Aachen. In this case <https://www.rwth-aachen.de/> is the legitimate link because the domain belongs to the RWTH Aachen.

<https://www.rwth-aachen.de/>

Deposited URL (also called web address):  
<https://www.rwth-aachen.de/>

**Unknown risk:** The risk of clicking this link can not definitively be classified. You have to classify the risk yourself by checking the domain (**bold area**) of the URL.

The link was deactivated to give you time to check the domain.  
Remaining time: 2 second(s).

(b) Link-Centric Warning Tutorial Part2.

Figure 8: Link-Centric Warning Tutorial Part1 and Part2.

4. Grey with warning symbol – The risk of clicking this link is rated as unknown. The warning symbol is displayed since at least one indicator that is often used in phishing attacks was found. However, it does not necessarily mean that it is a phishing URL. Legitimate emails may contain these indicators as well. You must check yourself whether the link leads to a website that might perform a phishing attack or not. As in case 3 clicking is deactivated for 3 seconds to avoid rash clicking of the link.

The following examples will show one **phishing** and one **legitimate** link with a warning symbol due to an identified indicator. The indicators are that the link text does not match the domain of the link.

**Example 1:** Imagine you open an email. The email looks like it came from amazon and contains links to the website of amazon.

In this example [www.karlsruhe.de](http://www.karlsruhe.de) is the phishing link. The dialogue shows that the link does not lead to the domain karlsruhe.de. The warning symbol appears because the domain of the link text does not match the domain of the deposited link.

[www.karlsruhe.de](http://www.karlsruhe.de)

⚠ Deposited URL (also called web address):  
<https://2020vaccine.org/>

**Unknown risk but careful:** The risk of clicking the link can not definitively be classified. However, at least one indicator that is often used in phishing attacks to mislead you was found. You have to classify the risk yourself by checking the domain (**bold area**) of the URL.

The link was deactivated to give you time to check the domain.  
Remaining time: 3 second(s).

**Example 2:** Imagine you open an email. The design and the sender suggest that clicking the link would lead to a website of the RWTH-Aachen.

In this example [www.rwth-aachen.de](http://www.rwth-aachen.de) is a legitimate link. The warning symbol is displayed since the link text does not match the domain of the deposited link: the link text contains a typo. Aachen is spelled with two "n" instead of just one. Typos happen in emails. Since the domain of the deposited link is from the RWTH Aachen this is *not* a phishing attack.

(a) Link-Centric Warning Tutorial Part3.

[www.rwth-aachen.de](http://www.rwth-aachen.de)

⚠ Deposited URL (also called web address):  
<http://www.rwth-aachen.de/>

**Unknown risk but careful:** The risk of clicking the link can not definitively be classified. However, at least one indicator that is often used in phishing attacks to mislead you was found. You have to classify the risk yourself by checking the domain (**bold area**) of the URL.

The link was deactivated to give you time to check the domain.  
Remaining time: 3 second(s).

(b) Link-Centric Warning Tutorial Part4.

Figure 9: Link-Centric Warning Tutorial Part3 and Part4.

## A.6 Redacted Online Survey Version without any Logo from Organizations

0% ausgefüllt

### Einverständniserklärung zur Teilnahme an der Studie

Die Richtlinien der Deutschen Forschungsgemeinschaft (DFG) sehen vor, dass sich die Teilnehmenden an empirischen Studien explizit und nachvollziehbar einverstanden erklären, dass sie freiwillig an der Forschung teilnehmen. Aus diesem Grund möchten wir Sie bitten, sich die vorliegende Einverständniserklärung aufmerksam durchzulesen.

### Erhebung und Nutzung der Daten

Ich erkläre mich freiwillig dazu bereit, an der Online-Studie teilzunehmen. Ich habe zur Kenntnis genommen, dass ich meine Teilnahme jederzeit ohne Angabe von Gründen abbrechen kann. Bitte beachten Sie, dass Sie im Fall, dass Sie abbrechen, nicht für die Teilnahme bezahlt werden können. Während der Studie wird es zu keinen physischen Sicherheitsrisiken kommen. Die Antworten, die Sie im Rahmen der Studie eingeben, werden aufgezeichnet. Es werden keine weiteren Daten erhoben. Die aufgezeichneten Daten werden im Rahmen der Datenanalyse anonymisiert ausgewertet und weiterverarbeitet sowie veröffentlicht. Hierbei wird es nicht möglich sein, die Quelle der Information zurückzuverfolgen.

### Speicherung und Löschung personenbezogener Daten

Ich wurde darüber informiert, dass meine personenbezogenen Daten anonymisiert gespeichert werden, und dass ich bis zum vollständigen Ausfüllen der Umfrage meine Einwilligung in die Speicherung dieser Daten zurückziehen kann, ohne dass mir dadurch Nachteile entstehen. Hierzu können Sie die Umfrage einfach abbrechen. Nach Empfehlung der DFG (Empf. 7, Sicherung guter wissenschaftlicher Praxis) werden die im Rahmen des Forschungsprojekts erhobenen Daten und Untersuchungsergebnisse bis zu zehn Jahre lang aufbewahrt.

Die Entscheidung für die Genehmigung der Verwendung und Verbreitung Ihrer Informationen ist vollkommen freiwillig.

1. Wenn Sie zustimmen, an dieser Studie teilzunehmen, wählen Sie bitte Option 1:

- Ich bin damit einverstanden, an dieser Studie teilzunehmen
- Ich möchte nicht an dieser Studie teilnehmen

Weiter

**Aufgabenbeschreibung:**

Zu Beginn bekommen Sie eine kurze Einführung in die Studie.

Dann sehen Sie ein 5-minütiges Video, welches Sie über Phishing informiert.  
Dafür ist es wichtig, dass Sie ihren **Ton** einschalten!  
Das Video ist wichtig für die spätere Aufgabe.

Anschließend sehen Sie 1-2 E-Mails und werden gebeten, zu zählen wie viele Links enthalten sind. Dabei muss mindesten eine der beiden Fragen richtig beantwortet werden, damit Sie weiter an der Studie teilnehmen können.

Im dritten Teil sehen Sie 20 E-Mails, die Sie als legitim oder Phishing klassifizieren sollen.

Nach dem Bearbeiten der Aufgabe stellen wir Ihnen einige Fragen zu der Aufgabe und Ihrer Person.

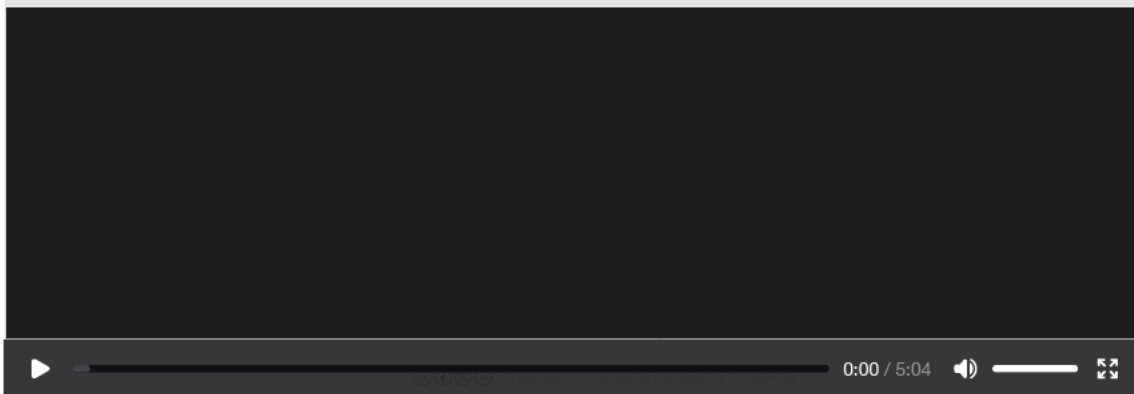
Erwartungsgemäß lässt sich die Studie mit einer Bearbeitungszeit von **30 Minuten** absolvieren.

[Weiter](#)

Bitte schauen Sie sich dieses Video in Ruhe an.

Nachdem erstmaligen Durchlauf des Videos erscheint der "Weiter"-Button.

Video 2  
Gefährliche Links erkennen



Nachdem das Video nun abgelaufen ist und bevor Sie nun fortfahren, hätten wir noch eine Frage an Sie.

Wie oft haben Sie sich das Video angeschaut?

- Einmal komplett ohne Pause(n)
- Mehrere Male das komplette Video
- Einmal komplett und dann nochmal einzelne Teile
- Einmal komplett, aber mit Pause(n)
- Gar nicht

Sonstiges:

Weiter

---

7% ausgefüllt

Phishing-Angriffe finden nur per E-Mail statt.

- Richtig
- Falsch

Securepay24 wurde als Beispiel verwendet.

- Richtig
- Falsch

DHL wurde als Beispiel verwendet

- Richtig
- Falsch

„Achte auf den gefälschten Wer-Bereich“ ist in dem Video ein genannter Tipp.

- Richtig
- Falsch

Weiter

Im Rahmen dieser Studie werden Sie E-Mails in dem Chrome Web-Browser beurteilen. Es sind E-Mails, die Martin Müller in seinem Gmail Account vorgefunden hat. Martin Müller hat bereits ein neues Update des Chrome Browsers. Ziel dieses Updates ist es, dass die Nutzer bei der Unterscheidung zw. Phishing E-Mails und legitimen E-Mails unterstützt werden.

Wie in dem von Ihnen gesehenen Video, können Sie auch weiterhin in der Statusleiste am unteren Linken Bildschirmrand die URL überprüfen. Der neue Tooltip unterstützt Sie dazu mit noch weiterer Funktionalität bei der Erkennung von legitimen bzw. Phishing E-Mails.

Im Folgenden erklären wir Ihnen kurz wie diese Unterstützung funktioniert:

Wenn Sie mit der Maus einen Link in der E-Mail berühren, erscheint einer von drei Dialogen.

Alle Dialoge enthalten die Domain. Die Domain wird auch Wer-Bereich genannt. Die Domain ist der wichtigste Bereich einer URL (auch Webadresse genannt), wenn es um die Erkennung von Phishing E-Mails geht.

Die Domain ist in der folgenden Beispiel-URL **fett** markiert:

<https://www.mail.google.de/dshfgfgdfgspddsfhgiodhfgdfghgd/index.php>

Im Dialog würde also die URL angezeigt und die Domain **google.de** fett markiert.

Welcher der drei Dialoge angezeigt wird, hängt davon ab, welches Risikolevel vorliegt:

1. **Grün** - das Risiko des Klickens auf den Link wird als **gering eingestuft**. Der Grund hierfür ist, dass die Domain in einer Liste der meistbesuchten Webseiten aller Internetnutzer in Deutschland vorkommt.

In dem folgenden Beispiel ist "Hier klicken" der Link.

Hier klicken

Hinterlegte URL (auch Webadresse genannt):  
<https://www.ebay.de/>

Geringes Risiko: Das Risiko für das Klicken auf den Link wird aufgrund der bekannten Vertrauenswürdigkeit der Domain (fett hervorgehoben Bereich der URL) als gering eingestuft.

2. **Grau** - Das Risiko des Klickens auf diesen Link wird als **unbekanntes Risiko** eingestuft. Hier müssen Sie selbst die Domain überprüfen, um herauszufinden ob der Link Sie zu einer Webseite führt, die einen Phishing-Angriff durchführt oder nicht. Damit Sie nicht vorschnell auf den Link klicken, ist das Klicken für **drei Sekunden** deaktiviert.

Im Folgenden zeigen wir Ihnen jeweils ein **Phishing** und ein **legitimes** Beispiel.

Beispiel 1: Stellen Sie sich vor, dass Sie eine E-Mail öffnen. Die E-Mail sieht vom Design und Absender aus, als würden Sie beim Klicken auf den Link auf einer ARD Webseite zum Thema Corona zu landen.

In diesem Beispiel ist "Hier" der **Phishing** Link, denn Sie landen hier nicht bei "ard.de".

Hier finden Sie me Information

Hinterlegte URL (auch Webadresse genannt):  
<https://2020coronaviruspandemic.com/>

**Unbekanntes Risiko:** Das Risiko für das Klicken auf den Link kann nicht bestimmt werden. Sie müssen hier das Risiko selbst einstufen. Hierzu prüfen Sie die Domain (**fett hervorgehobener Bereich**).

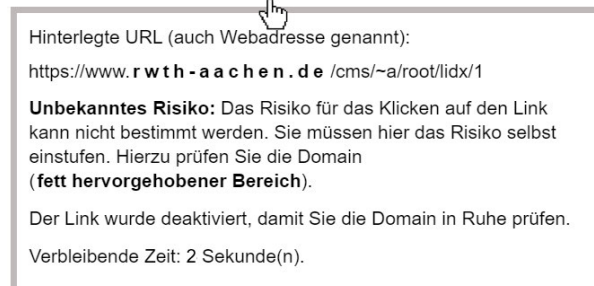
Der Link wurde deaktiviert, damit Sie die Domain in Ruhe prüfen.

Verbleibende Zeit: 2 Sekunde(n).

Beispiel 2: Stellen Sie sich vor, dass Sie eine E-Mail öffnen. Die E-Mail sieht vom Design und Absender aus, als würden Sie beim Klicken auf den Link auf einer RWTH-Aachen Webseite landen.

In diesem Beispiel ist <https://www.rwth-aachen.de/> der **legitime** Link, denn die Domain gehört zur RWTH Aachen.

<https://www.rwth-aachen.de/cms/~a/root/lidx/1>



Hinterlegte URL (auch Webadresse genannt):  
[https://www.rwth-aachen.de /cms/~a/root/lidx/1](https://www.rwth-aachen.de/cms/~a/root/lidx/1)

**Unbekanntes Risiko:** Das Risiko für das Klicken auf den Link kann nicht bestimmt werden. Sie müssen hier das Risiko selbst einstufen. Hierzu prüfen Sie die Domain (**fett hervorgehobener Bereich**).

Der Link wurde deaktiviert, damit Sie die Domain in Ruhe prüfen.  
Verbleibende Zeit: 2 Sekunde(n).

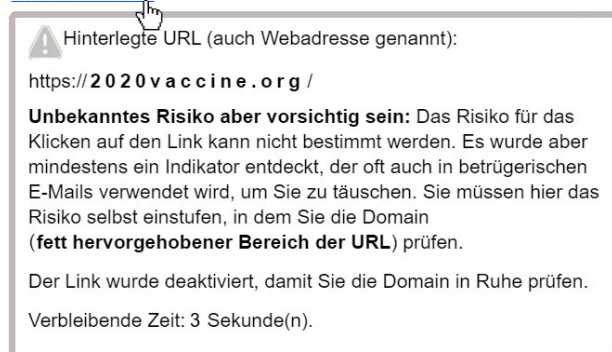
3. **Grau mit Warnsymbol** - Das Risiko des Klickens auf diesen Link wird als unbekanntes Risiko eingestuft. Das Warnsymbol wird angezeigt, weil mindestens ein Indikator gefunden wurde, der auch bei Phishing-Angriffen verwendet wird. Das bedeutet aber nicht, dass es sich hierbei zwangsläufig um eine Phishing URL handelt. Auch in legitimen E-Mails können solche Indikatoren vorkommen. Auch hier müssen Sie selbst überprüfen, ob der Link Sie zu einer Webseite führt, die einen Phishing-Angriff durchführt oder nicht. Damit Sie nicht vorschnell auf den Link klicken, ist das Klicken auch hier für **drei Sekunden** deaktiviert.


Im Folgenden zeigen wir Ihnen jeweils ein **Phishing** und ein **legitimes** Beispiel mit einem Warnsymbol aufgrund eines gefundenen Indikators. Der Indikator ist jeweils, dass die Domain des Links nicht mit dem Link-Text übereinstimmt.

Beispiel 1: Stellen Sie sich vor, dass Sie eine E-Mail öffnen. Die E-Mail sieht aus als käme sie von der Stadt Karlsruhe und würde Links zu Webseiten der Stadt Karlsruhe beinhalten.

In diesem Beispiel ist [www.karlsruhe.de](http://www.karlsruhe.de) der **Phishing**-Link, denn anhand des Dialogs sehen Sie, dass die Webseite nicht zur Domain karlsruhe.de führt. Das Warndreieck erscheint, weil die Domain des Link-Texts nicht zur hinterlegten Domain passt.

[www.karlsruhe.de](http://www.karlsruhe.de)



 Hinterlegte URL (auch Webadresse genannt):  
[https://2020vaccine.org /](https://2020vaccine.org/)

**Unbekanntes Risiko aber vorsichtig sein:** Das Risiko für das Klicken auf den Link kann nicht bestimmt werden. Es wurde aber mindestens ein Indikator entdeckt, der oft auch in betrügerischen E-Mails verwendet wird, um Sie zu täuschen. Sie müssen hier das Risiko selbst einstufen, in dem Sie die Domain (**fett hervorgehobener Bereich der URL**) prüfen.

Der Link wurde deaktiviert, damit Sie die Domain in Ruhe prüfen.  
Verbleibende Zeit: 3 Sekunde(n).

Beispiel 2: Stellen Sie sich vor, dass Sie eine E-Mail öffnen. Die E-Mail sieht vom Design und Absender aus, als würden Sie beim Klicken auf den Link auf einer RWTH-Aachen Webseite landen.

In diesem Beispiel ist [www.rwth-aachenn.de](http://www.rwth-aachenn.de) ein **legitimer** Link. Es wird hier ein Warndreieck angezeigt, weil festgestellt wird, dass die Domain des Link-Texts nicht zu der hinterlegten Domain passt: Im Link-Text hat sich ein Tippfehler eingeschlichen. Dort steht Aachen mit zwei "n". Dies kann wie jeder andere Tippfehler in einer E-Mail schon einmal passieren. Da die hinterlegte Domain aber die der RWTH Aachen ist, handelt es sich hier um *keinen* Phishing Angriff.



[www.rwth-aachen.de](http://www.rwth-aachen.de)



Hinterlegte URL (auch Webadresse genannt):

[http://www.rwth-aachen.de /](http://www.rwth-aachen.de/)

**Unbekanntes Risiko aber vorsichtig sein:** Das Risiko für das Klicken auf den Link kann nicht bestimmt werden. Es wurde aber mindestens ein Indikator entdeckt, der oft auch in betrügerischen E-Mails verwendet wird, um Sie zu täuschen. Sie müssen hier das Risiko selbst einstufen, in dem Sie die Domain (**fett hervorgehobener Bereich der URL**) prüfen.

Der Link wurde deaktiviert, damit Sie die Domain in Ruhe prüfen.

Verbleibende Zeit: 3 Sekunde(n).

Weiter

**ACHTUNG!** Sie müssen die 3 Aufmerksamkeitsfragen richtig beantworten, damit Sie weiter an der Studie teilnehmen können.

**Wie viele Dialoge werden bei der Darstellung unterschieden?**

- 1
- 2
- 3
- 4
- 5

**Bei welchem Fall/bei welchen Fällen müssen Sie selbst die Domain überprüfen?**

Hier ist eine Mehrfachauswahl möglich

- grün
- rot
- grau
- grau mit Warnsymbol
- blau

**Angenommen Sie sehen den Fall "Grau mit Warnsymbol", was ist die richtige Einschätzung ihrerseits?**

- Die URL muss ein Phish sein
- Die URL kann sowohl ein Phish, als auch legitim sein
- Die URL muss legitim sein

Weiter

---

19% ausgefüllt

Sehr gut! Sie haben alle Fragen richtig beantwortet!

**Haben Sie bekannte Farbschwächen?**

- Ja:
- Nein

**Hatten Sie Probleme, die Rahmen der verschiedenen Fälle aufgrund der Farben zu unterscheiden?**

Falls ja, erläutern Sie bitte kurz die Probleme.

- Ja:
- Teilweise
- Nein

Weiter

Links können hinter einem *Button*, *Text* oder *Bild/Logo* integriert werden. Sie werden einen Link entdecken, wenn sich der Mauszeiger in eine Hand umwandelt.

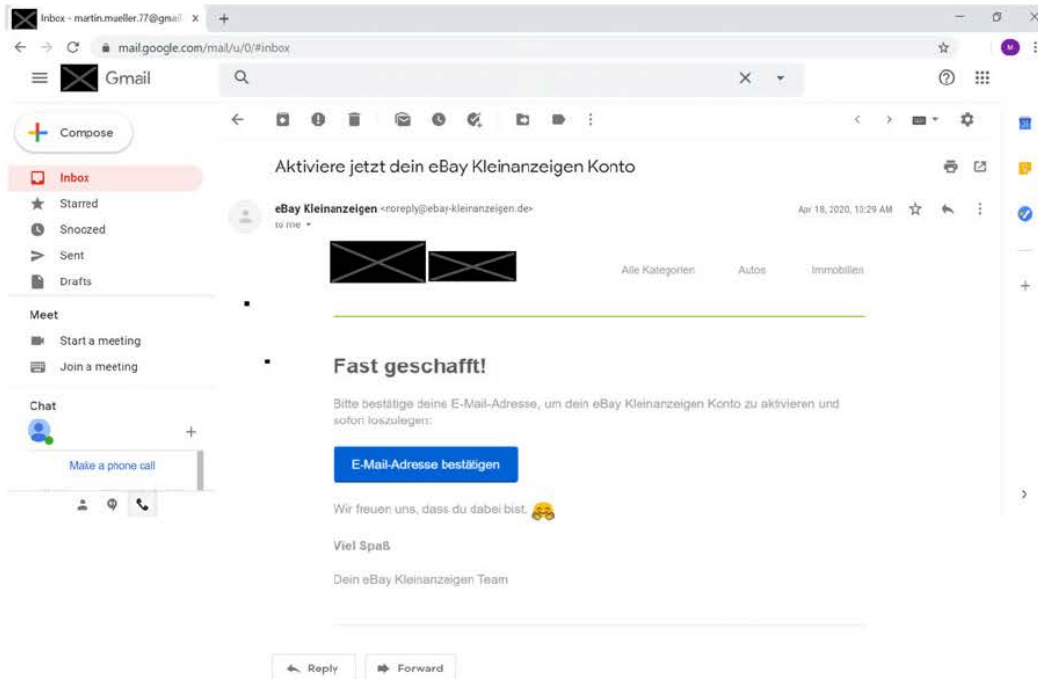


*Hinweis:* In der vorliegenden Studie sind die Links zu Demozwecken deaktiviert, sodass eine Weiterleitung ausgeschlossen ist.

Sie sehen unten ein Beispiel für eine E-Mail im Postfach von Martin Müller in seinem Gmail Account. Es handelt sich dabei um eine legitime E-Mail.

Bitte prüfen Sie diese E-Mail auf die Anzahl der vorhandenen Links und geben Sie unten ihr Ergebnis ein.

Betätigen Sie dann den **Weiter** Button, der sich unten rechts befindet.



Wie viele Links finden Sie in der Beispiel E-Mail?

- 0
- 1
- 2
- 3
- 4
- 5

Weiter

Sehr gut! Sie haben die korrekte Anzahl an Links gefunden! Hier können Sie einen genauen Überblick auf alle integrierten Links sehen:

**Aktiviere jetzt dein eBay Kleinanzeigen Konto**

eBay Kleinanzeigen (noreply@ebay-kleinanzeigen.de) Apr 18, 2020, 10:29 AM

1. [Redacted]

2. Alle Kategorien 3. Autos 4. Immobilien

**Fast geschafft!**

Bitte bestätige deine E-Mail-Adresse, um dein eBay Kleinanzeigen Konto zu aktivieren und sofort loszulegen:

5. [E-Mail-Adresse bestätigen](#)

Wir freuen uns, dass du dabei bist!

Viel Spaß!

Dein eBay Kleinanzeigen Team

Hinterlegte URL (auch Webadresse genannt):  
[https://www.ebay-kleinanzeigen.de/m-benutzer-aktivieren.html?uuiid=7f54a510-5ddb-4de6-8792-9c6b7e57c06e&targetE...  
 experience=WEB&utm\\_source=...](https://www.ebay-kleinanzeigen.de/m-benutzer-aktivieren.html?uuiid=7f54a510-5ddb-4de6-8792-9c6b7e57c06e&targetE...)

Geringes Risiko: Das Risiko für das Klicken auf den Link wird aufgrund der bekannten Vertrauenswürdigkeit der Domain (fett hervorgehoben Bereich der URL) als gering eingestuft.

Reply Forward

<https://www.ebay-kleinanzeigen.de/m-benutzer-aktivieren.html?uuiid=7f54a510-5ddb-4de6-8792-9c6b7e57c06e&targetE...>

Weiter

Im Folgenden werden Sie 20 E-Mails sehen. Ihre Aufgabe ist es, jede E-Mail zu untersuchen und festzulegen, ob das eine legitime E-Mail oder eine Phishing E-Mail ist.

Um die Aufgabe zu bearbeiten, gehen Sie bitte von folgendem **Szenario** aus:

Um die Absender, Dienstleister und Programme, zu denen Sie in der Realität keinen Bezug haben, nicht direkt für betrügerisch zu erklären, gehen Sie im Folgenden bitte davon aus, dass:

- Sie Martin Müller sind und die E-Mail-Adresse: martin.mueller.77@gmail.com, haben.
- Sie alle Dienste nutzen, die in diesem Fragebogen verwendet werden (Amazon, Lufthansa, Google, LinkedIn, DHL, Netflix, GMX, PayPal, Microsoft und Apple).

*Hinweis:* In der vorliegenden Studie sind die Links deaktiviert, sodass eine Weiterleitung ausgeschlossen ist.

Wir wünschen Ihnen viel Spaß!

Weiter

Inbox - martin.mueller.77@gmail.com

mail.google.com/mail/u/0/#inbox

Gmail

Compose

Inbox

Starred

Snoozed

Sent

Drafts

More


Make a phone call

Also try our mobile apps for [Android](#) and [iOS](#)

Willkommen bei Music Premium!

YouTube <noreply-purchases@youtube.com>  
to me

Apr 18, 2020, 10:29 AM



Hallo [martin.mueller.77@gmail.com](mailto:martin.mueller.77@gmail.com).

Willkommen bei deiner kostenlosen 3-monatigen Music Premium-Probiermitgliedschaft. Ab dem 30.11.2020 werden tägliche Beiträge monatlich über die angegebene Zahlungsmethode abgebucht.

Willkommen an Bord.  
Das YouTube-Team

[MITGLIEDSCHAFT ANSEHEN](#)

Details zur Bestellung:  
387248954001738215  
31.08.2020

Music Premium – Kostenloser Test	0,00 €
Music Premium – Abo Monatliche Abrechnung ab 30.11.2020	0,99 €
Zahlungsmittel:	Gesamt 0,00 €
PayPal: <a href="mailto:martin.mueller.77@gmail.com">martin.mueller.77@gmail.com</a>	(Inklusive MwSt.: 0,00 €)

Reply Forward

Dies ist eine Frage zur Kontrolle Ihrer Aufmerksamkeit! Diese Nachricht ist betrügerisch. Wählen Sie trotzdem bitte "legitime E-Mail" und "unsicher" aus.

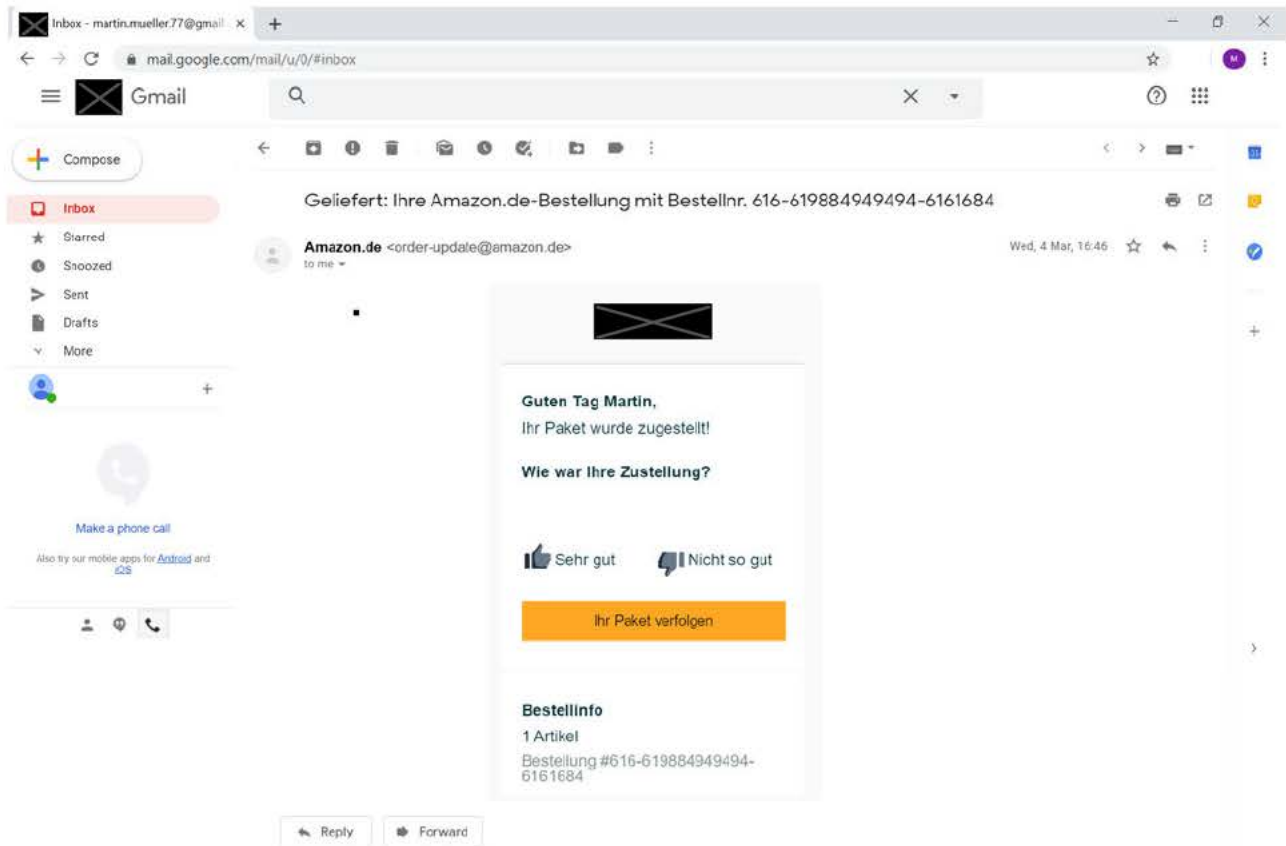
Diese E-Mail ist eine:

phishing E-Mail

legitime E-Mail

Weiter

33% ausgefüllt



Diese E-Mail ist eine:

phishing E-Mail

legitime E-Mail

Weiter



The screenshot shows a Gmail interface with an email from Lufthansa. The email subject is "Lufthansa Flugumbuchung" and it was received on April 18, 2020, at 10:29 AM. The email content is in German and reads:

**Sehr geehrte Kundin, sehr geehrter Kunde,**

**Sie wurden von uns umgebucht, da Ihre Flugreise nicht wie geplant durchgeführt werden kann.**

**Bitte entschuldigen Sie.**

Details zu Ihrer Buchung und mögliche Alternativen können Sie auch online einsehen:  
→ [Meine Buchungen](#)

Freundliche Grüße,  
Ihr Lufthansa Team

**Service**

Sitz der Gesellschaft: Deutsche Lufthansa AG Vanke-Strasse 151-153 50672 Köln	Registeramt: Amtsgericht Köln HRB 2168	→ Star Alliance
Vorsitzender des Aufsichtsrats: Dr. Karl-Ludwig Kloy	Vorstand: Carsten Spohr (Vorsitzender) Thorsten Dirks Christina Foerster Harry Hohmeister Dr. Delfot Kayser Dr. Michael Niggemann	→ Datenschutz
		→ Impressum
		→ Deutsche Lufthansa AG

At the bottom of the email, there are buttons for "Reply" and "Forward".

Diese E-Mail ist eine:

phishing E-Mail

legitime E-Mail

Weiter

The screenshot shows a Gmail interface with a security warning email. The email is titled "Sicherheitswarnung für martin.mueller.77@googlemail.com" and is from Google. The main content of the email is a warning box with the following text:

**Neues Gerät angemeldet**  
martin.mueller.77@gmail.com

Jemand hat sich über ein neues Gerät (Mac) in Ihrem Google-Konto angemeldet. Sie haben diese E-Mail erhalten, weil wir uns vergewissern möchten, dass Sie das waren.

[Aktivität prüfen](#)

Below the warning box, there is a note: "Wir haben Ihnen diese E-Mail gesendet, um Sie über wichtige Änderungen zu Ihrem Google-Konto und den Diensten von Google zu informieren." and a copyright notice: "© 2021 Google Ireland Ltd., Gordon House, Barrow Street, Dublin 4, Ireland".

At the bottom of the email, there are three buttons: "Reply", "Reply all", and "Forward".

Diese E-Mail ist eine:

phishing E-Mail

legitime E-Mail

[Weiter](#)


Martin, ein kostenloser Kurs über strategisches Denken – nur für kurze Zeit

LinkedIn <messages-noreply@linkedin.com> to me

Für 57 % der Führungskräfte sind Soft Skills wichtiger als Hard Skills.\*  
Starten Sie beruflich durch – mit unbegrenztem Zugriff auf Expertenkurse.

[Strategisches Denken und Handeln für Führungskräfte](#)

Dieser Kurs ist kostenlos



Dagmar Gerig  
Leadership Trainer & Coach

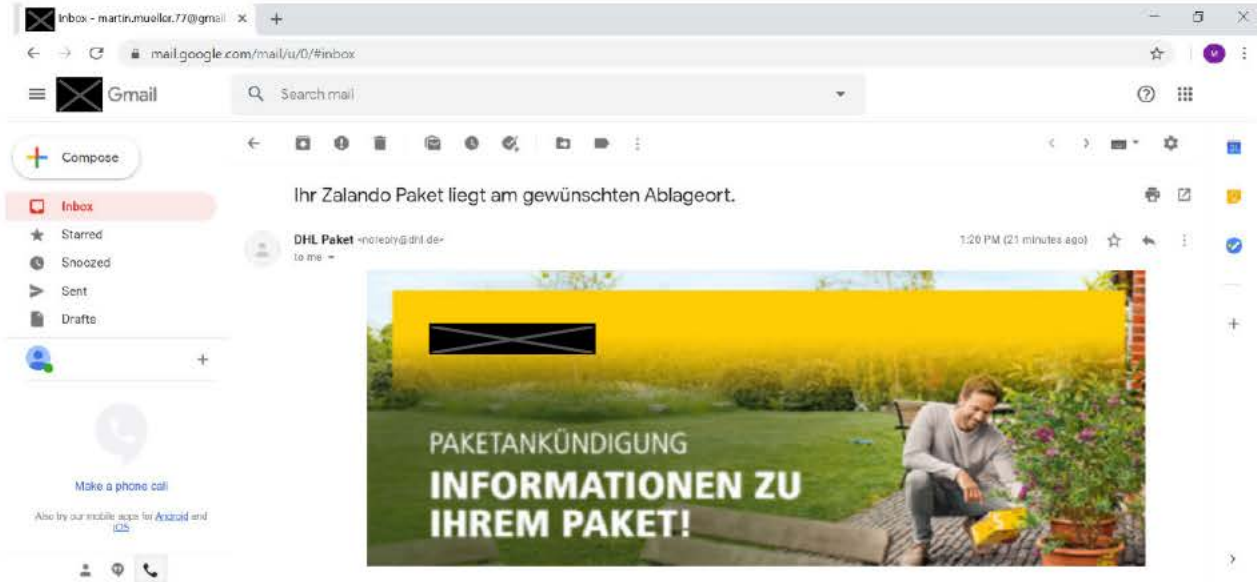
Reply Forward

Diese E-Mail ist eine:

phishing E-Mail

legitime E-Mail

Weiter



Guten Tag,

Ihr Paket mit der Sendungsnummer [00340434281076483641](#) ist angekommen. Wir haben es am vereinbarten Wunschort hinterlegt.

Beste Grüße

*Ihr DHL Team*

Diese E-Mail ist eine:

phishing E-Mail

legitime E-Mail

Diese E-Mail ist eine:

phishing E-Mail

legitime E-Mail

Weiter

The screenshot shows a Gmail interface with the following elements:

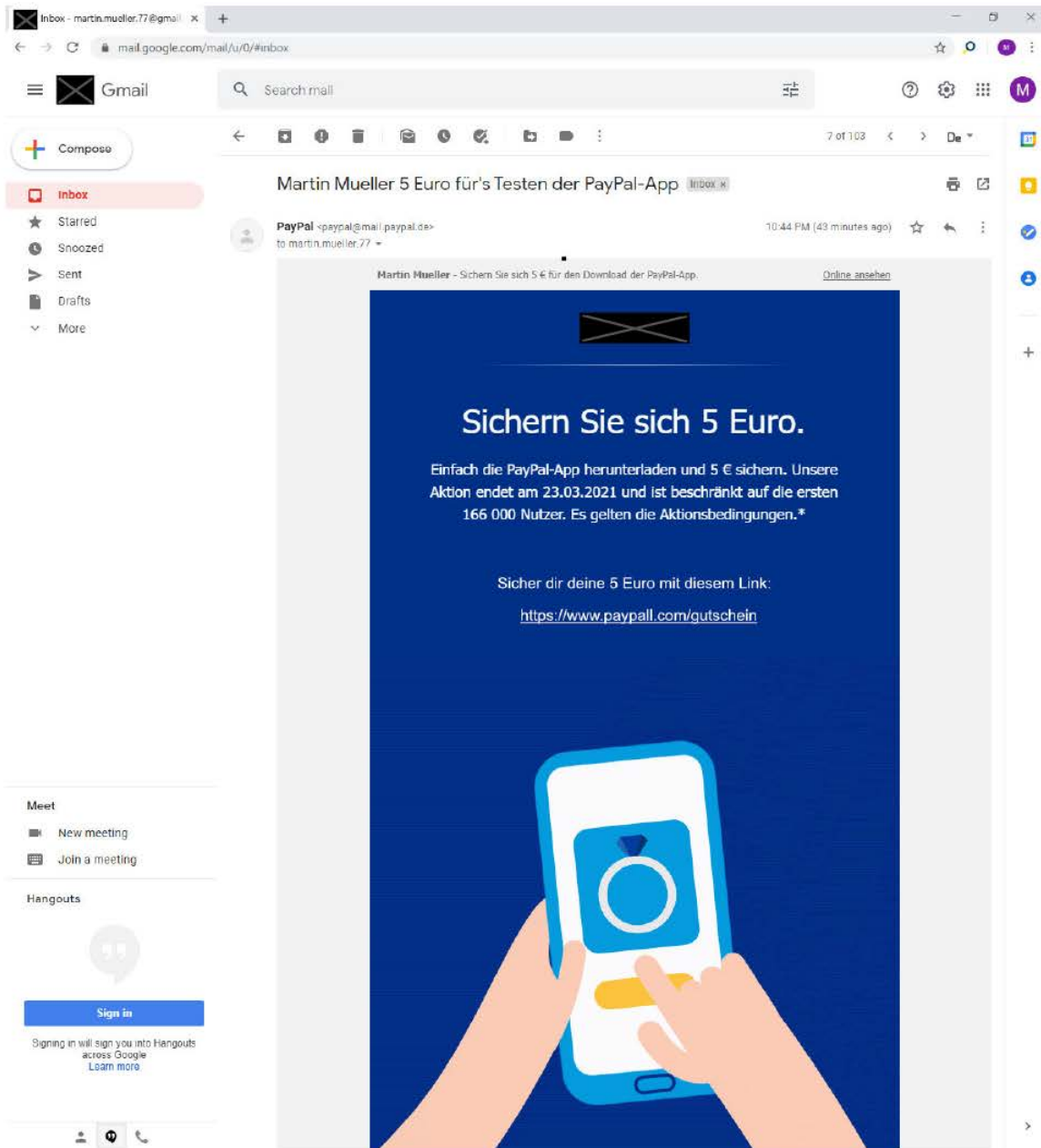
- Header:** "Inbox - martin.mueller.77@gmail.com" and "mail.google.com/mail/u/0/#inbox".
- Left Sidebar:** "Compose", "Inbox", "Starred", "Snoozed", "Sent", "Drafts", "More".
- Bottom Left:** "Meet" section with "New meeting" and "Join a meeting" buttons; "Hangouts" section with a "Sign in" button and a note: "Signing in will sign you into Hangouts across Google. Learn more".
- Main Content:**
  - Subject: "Bestätigung der AGB-Aktualisierung für Ihr GMX Postfach".
  - From: "GMX Kundenmanagement <mailings@produkt.gmx.net>".
  - Time: "10:44 PM (40 minutes ago)".
  - Header: "Kundenmanagement".
  - Section: "Allgemeine Geschäftsbedingungen".
  - Text: "Lieber Herr Martin, vielen Dank, dass Sie mit der Geltung unserer aktualisierten Allgemeinen Geschäftsbedingungen (AGB) einverstanden sind. Damit stehen Ihnen ab sofort neue, kostenfreie Funktionen in Ihrem GMX FreeMail Postfach zur Verfügung.".
  - Text: "Alle Informationen dazu finden Sie unter <https://brief.gmx.net/AGB>. Falls Sie noch einmal einen Blick in die neuen AGB werfen wollen oder diese ausdrucken möchten, finden Sie im Anhang dieser E-Mail das AGB-Dokument inkl. Auftragsverarbeitungsvereinbarung (AVV).".
  - Text: "Wir hoffen, Sie haben Spaß mit den neuen Funktionen und wünschen Ihnen weiterhin viel Freude beim Mailen mit GMX.".
  - Text: "Ihr GMX Kundenmanagement".
- Bottom Right:** "Reply", "Reply all", and "Forward" buttons.

Diese E-Mail ist eine:

phishing E-Mail

legitime E-Mail

Weiter

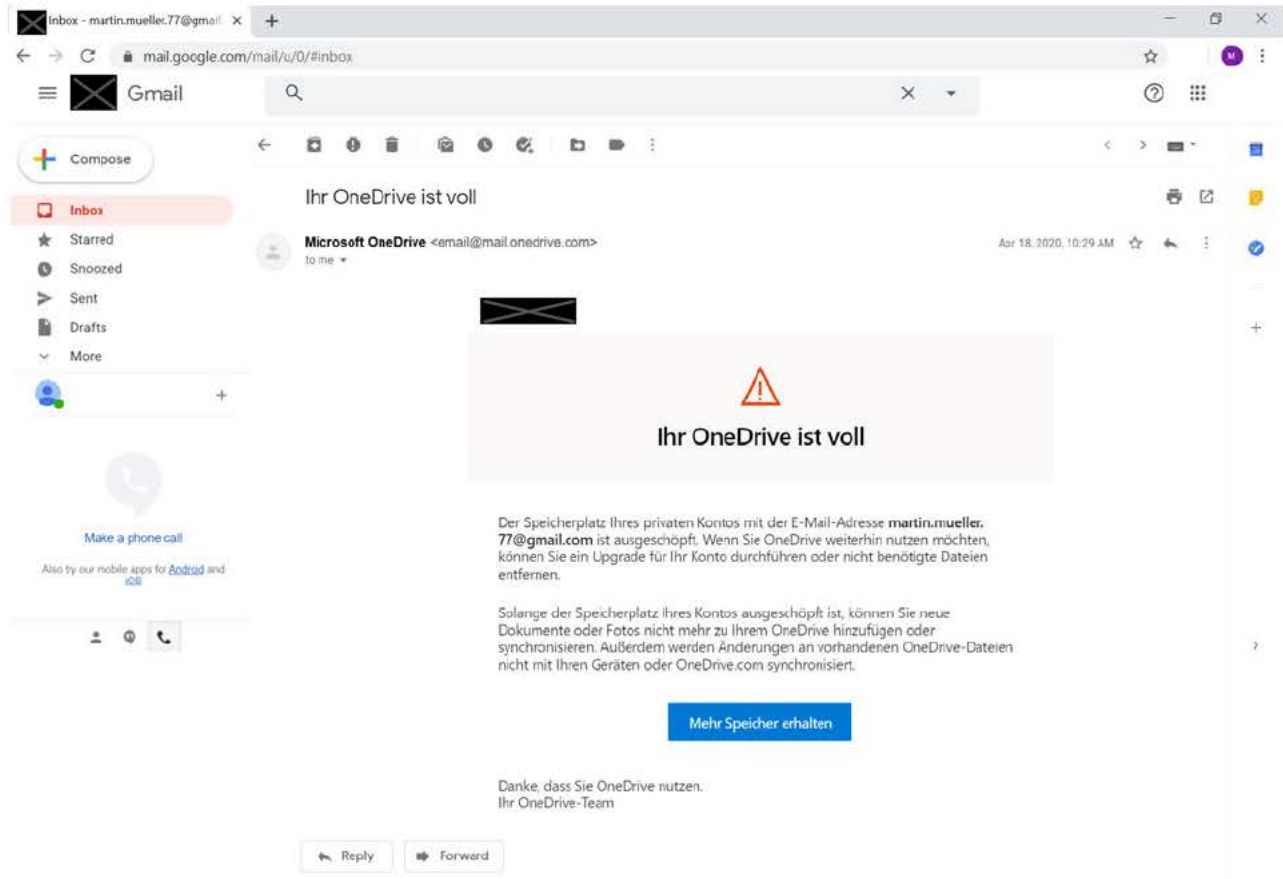


Diese E-Mail ist eine:

phishing E-Mail

legitime E-Mail

Weiter



The screenshot shows a Gmail interface with a phishing email from Microsoft OneDrive. The email subject is "Ihr OneDrive ist voll" (Your OneDrive is full). The sender is "Microsoft OneDrive <email@mail.onedrive.com>". The email body contains a warning icon and the text "Ihr OneDrive ist voll". Below this, it states: "Der Speicherplatz Ihres privaten Kontos mit der E-Mail-Adresse martin.mueller.77@gmail.com ist ausgeschöpft. Wenn Sie OneDrive weiterhin nutzen möchten, können Sie ein Upgrade für Ihr Konto durchführen oder nicht benötigte Dateien entfernen." (Your storage space for your private account with the email address martin.mueller.77@gmail.com is exhausted. If you want to continue using OneDrive, you can upgrade your account or delete unnecessary files.) It also says: "Solange der Speicherplatz Ihres Kontos ausgeschöpft ist, können Sie neue Dokumente oder Fotos nicht mehr zu Ihrem OneDrive hinzufügen oder synchronisieren. Außerdem werden Änderungen an vorhandenen OneDrive-Dateien nicht mit Ihren Geräten oder OneDrive.com synchronisiert." (As long as your account's storage space is exhausted, you cannot add new documents or photos to your OneDrive or synchronize them. Additionally, changes to existing OneDrive files will not be synchronized with your devices or OneDrive.com.) A blue button labeled "Mehr Speicher erhalten" (Get more storage) is visible. At the bottom of the email, it says "Danke, dass Sie OneDrive nutzen. Ihr OneDrive-Team" (Thank you for using OneDrive. Your OneDrive team). The Gmail interface includes a "Compose" button, a sidebar with "Inbox", "Starred", "Snoozed", "Sent", "Drafts", and "More", and a "Make a phone call" button.

Diese E-Mail ist eine:

phishing E-Mail

legitime E-Mail

Weiter



Inbox - martin.mueller.77@gmail.com

mail.google.com/mail/u/0/#inbox

Gmail

Search mail

Compose

Inbox

Starred

Snoozed

Meet

New meeting

Join a meeting

Hangouts

Sign in

Signing in will sign you into Hangouts across Google. [Learn more](#)

**Aktualisiere deine iCloud-Rechnungsdaten, um dein Speicher-Upgrade zu behalten.**

iCloud <icloud\_not\_reply@email.apple.com> to martin.mueller.77

10:44 PM (30 minutes ago)

Hallo Martin Mueller,

wir haben am 06.08.2021 versucht, die Kosten für deinen 50 GB-iCloud-Speicherplan einzuziehen. Es liegt jedoch ein Problem mit deinen Zahlungsdaten vor.

Dein Account wird auf den kostenlosen 5 GB-Speicherplan heruntergestuft, wenn wir dein Abo nicht verlängern können.

Befolge die Anleitungen unten, um deine Rechnungsdaten zu aktualisieren:

1. Gehe zu „Einstellungen“ > „[dein Name]“ > „iTunes & App Store“.
2. Tippe auf deine Apple-ID und anschließend auf „Apple-ID anzeigen“. Du wirst möglicherweise aufgefordert, dich anzumelden.
3. Tippe auf „Zahlungen verwalten“ und folge den Anweisungen. (Wenn du eine ältere iOS-Version verwendest, tippe auf „Zahlungsdaten“.)

Du kannst deine Rechnungsdaten auch von einem [Mac oder PC](#) aus aktualisieren.

Das iCloud-Team

iCloud ist ein von Apple bereitgestellter Dienst. Apple-ID | iCloud-Support | Allgemeine Geschäftsbedingungen | Datenschutz. Copyright © 2021 Apple Distribution International Ltd. Holyhill Industrial Estate, Holyhill, Cork, Ireland. Alle Rechte vorbehalten.

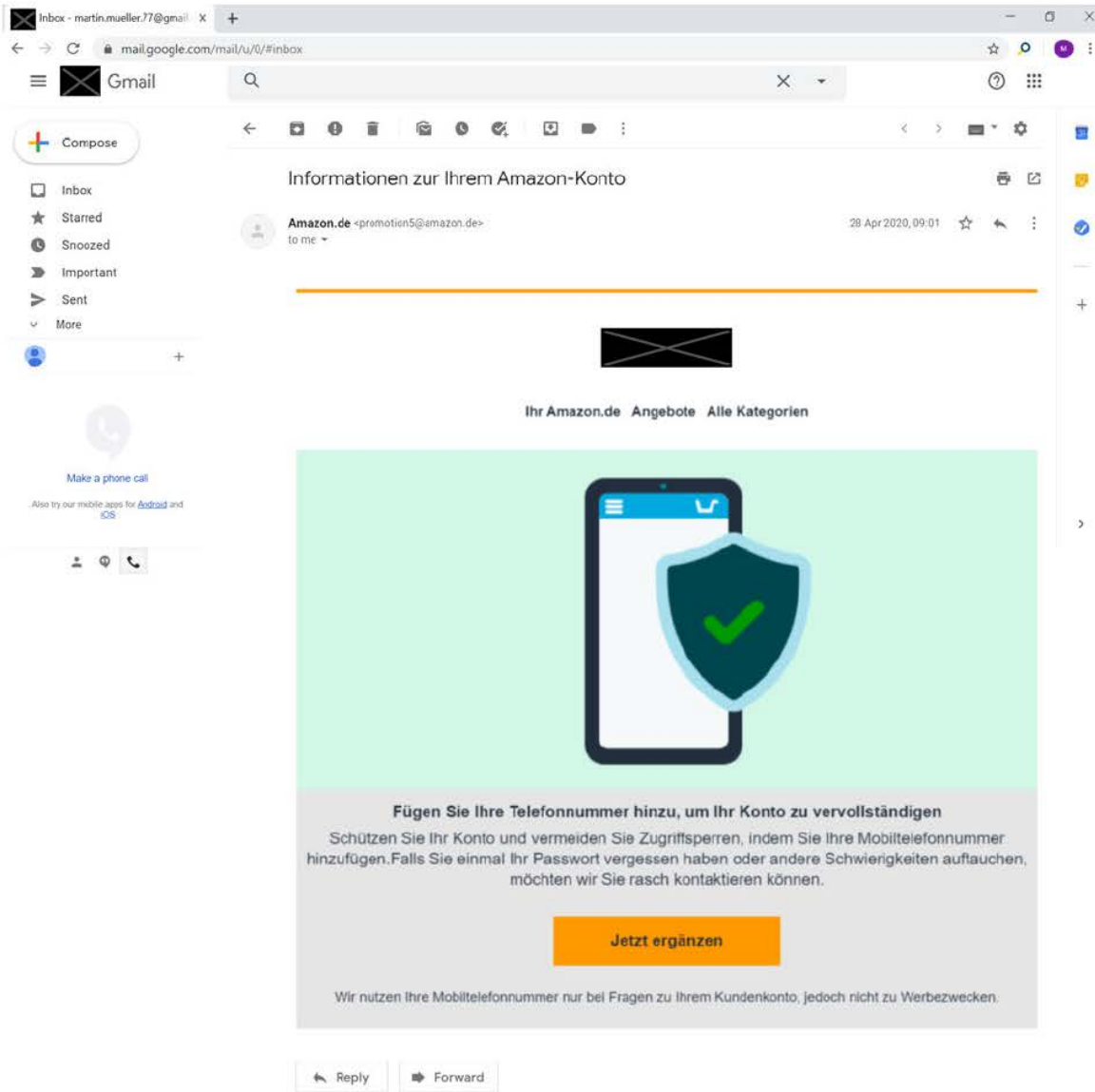
Reply Reply all Forward

Diese E-Mail ist eine:

phishing E-Mail

legitime E-Mail

Weiter



Diese E-Mail ist eine:

phishing E-Mail

legitime E-Mail

Weiter

Inbox - martin.mueller.77@gmail.com

mail.google.com/mail/u/0/#inbox

Gmail

Compose

Inbox

Starred

Snoozed

Sent

Drafts

More

1 of 1296

Subject: Informationen zu Ihrem bevorstehenden Flug

Lufthansa <online@booking.lufthansa.com> to me Wed, 4 Mär, 16:46

### Buchungsänderung

Lufthansa Buchungscode: **457895**

[Buchung anzeigen / bearbeiten](#)

Aufgrund der anhaltenden Coronavirus-Krise muss Lufthansa noch immer vermehrt Flugänderungen vornehmen. Daher haben sich auch bei Ihrer Buchung Änderungen ergeben. Neueste Informationen zum Stand Ihrer Buchung finden Sie hier.

Sie haben uns diesbezüglich bereits kontaktiert? Dann ignorieren Sie bitte diese Nachricht.

**Ihre Umbuchungsmöglichkeiten:**

Lufthansa bietet Ihnen vor dem Hintergrund der aktuellen Situation flexible Umbuchungsmöglichkeiten für alle Tarife.

**Bis zum 31. August 2020** können Sie Ihr Ticket auf ein neues Abflugdatum bis einschließlich **30. April 2021** umbuchen. Ebenfalls können Sie Ihr Reiseziel verändern.

Umbuchungen können Sie direkt über unsere Service Center oder Ihr Reisebüro vornehmen. Sie müssen unser Service Center dabei nicht vor dem originalen Flugdatum kontaktieren – Ihr Ticket behält seine Gültigkeit und kann jederzeit umgebucht werden. Auch nach dem Verstreichen des geplanten Flugdatums sind Umbuchungen möglich.

Zudem bietet Lufthansa bei Ihrer Umbuchung mit Reiseantritt im Jahr 2020 einen Discount von 50 Euro an. Selbst wenn Sie noch nicht wissen, wann Sie Ihren Flug umbuchen möchten, können Sie sich Ihren Discount schon heute sichern.

Mit freundlichen Grüßen  
**Deutsche Lufthansa AG**

Sitz der Gesellschaft: Deutsche Lufthansa Aktiengesellschaft, Köln  
Vorstand: Dr. Karl-Ludwig Alrey

Flughafenkategorie: Amtsgleiche Köln HRH 2168  
Vorstand: Carsten Spohr (Vorstandsvorsitzender / Chairman), Thomas Ditts, Christina Förster, Hans Huber, Dr. Gerd Kayser, Dr. Michael Miggemann

Deutsche Lufthansa AG  
Impressum

Reply Forward

Diese E-Mail ist eine:

phishing E-Mail

legitime E-Mail

Weiter

inbox - martin.mueller.77@gmail.com

mail.google.com/mail/u/0/#inbox

Search mail

Compose

Inbox

Starred

Snoozed

Sent

Drafts

More

Helfen Sie uns, die Sicherheit Ihres Google-Kontos zu erhöhen

Google <no-reply@accounts.google.com> to martin.mueller.77

10:44 PM (41 minutes ago)

Soll martin.mueller.77@gmail.com Ihre E-Mail-Adresse zur Kontowiederherstellung bleiben?

martin.mueller.77@gmail.com

Anhand dieser E-Mail-Adresse kann Google Ihre Identität bestätigen, wenn Sie keinen Zugriff auf Ihr Konto mehr haben oder wir verdächtige Aktivitäten bemerken.

Im Rahmen des Sicherheitschecks können Sie Ihre E-Mail-Adresse zur Kontowiederherstellung (martin.mueller.77@gmail.com) bestätigen und weitere personalisierte Sicherheitsempfehlungen erhalten.

Sicherheitscheck durchführen

Wir haben Ihnen diese E-Mail gesendet, um Sie über wichtige Änderungen zu Ihrem Google-Konto und den Diensten von Google zu informieren.

© 2021 Google Ireland Ltd., Gordon House, Barrow Street, Dublin 4, Ireland

Reply Reply all Forward

Meet

New meeting

Join a meeting

Hangouts

Sign in

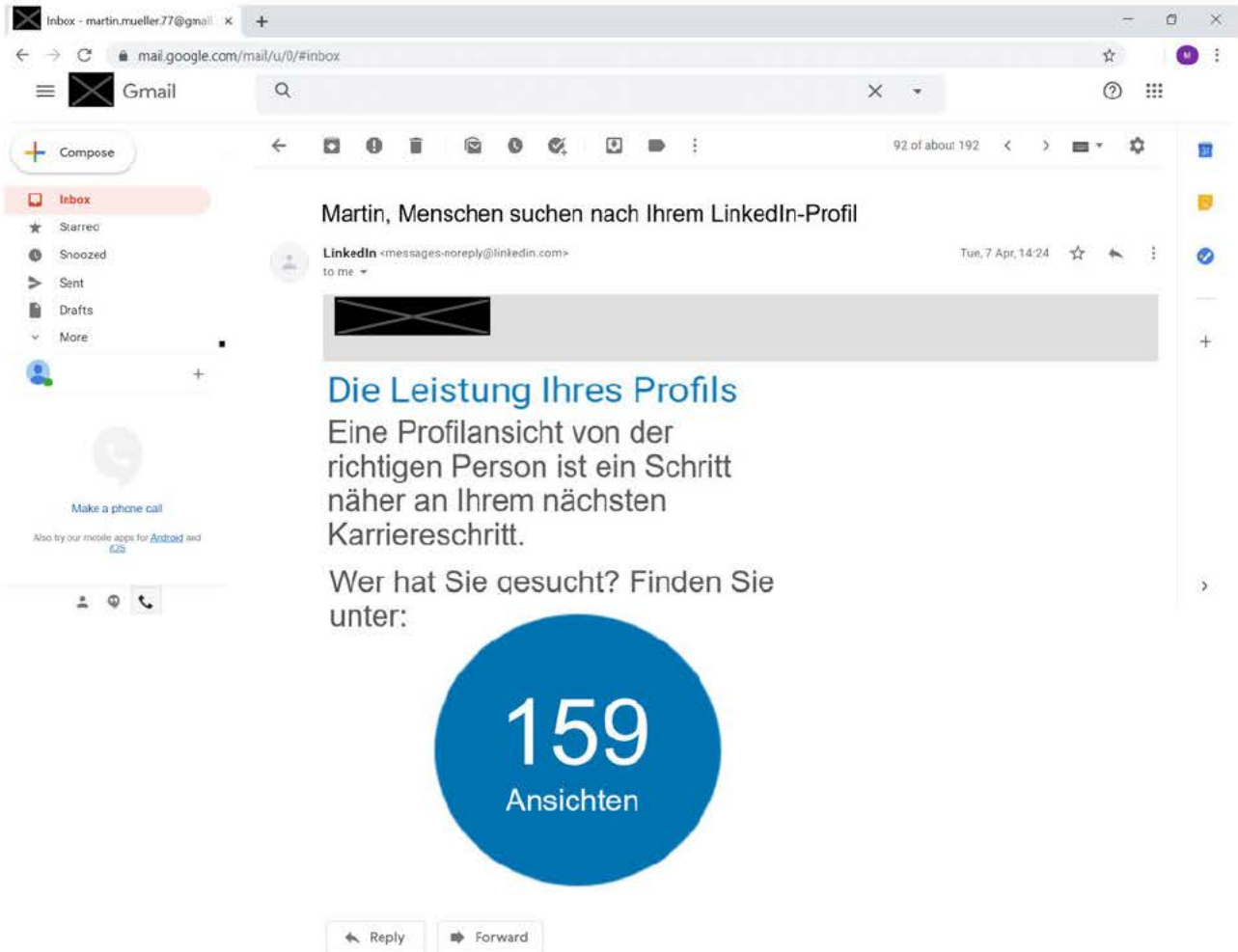
Signing in will sign you into Hangouts across Google. Learn more.

Diese E-Mail ist eine:

○  
phishing E-Mail

○  
legitime E-Mail

Weiter



Diese E-Mail ist eine:

phishing E-Mail

legitime E-Mail

Weiter

Ihr Paket wird heute zugestellt. Jetzt Ablageort buchen ...

**DHL Paket** <noreply@dhl.de> to me Apr 14, 2020, 10:29 AM

**PAKETANKÜNDIGUNG  
IHR PAKET WIRD  
HEUTE ZUGESTELLT!**

Guten Tag,

Ihr Paket mit der Sendungsnummer 00340434281076483642 wurde ins Zustellfahrzeug geladen und wird Ihnen heute im Laufe des Tages zugestellt.

Ihre Gesundheit und die unserer Mitarbeiter haben oberste Priorität. Wir empfehlen Ihnen deshalb die kontaktlose Zustellung an einen Ablageort.

Beste Grüße  
Ihr DHL Team

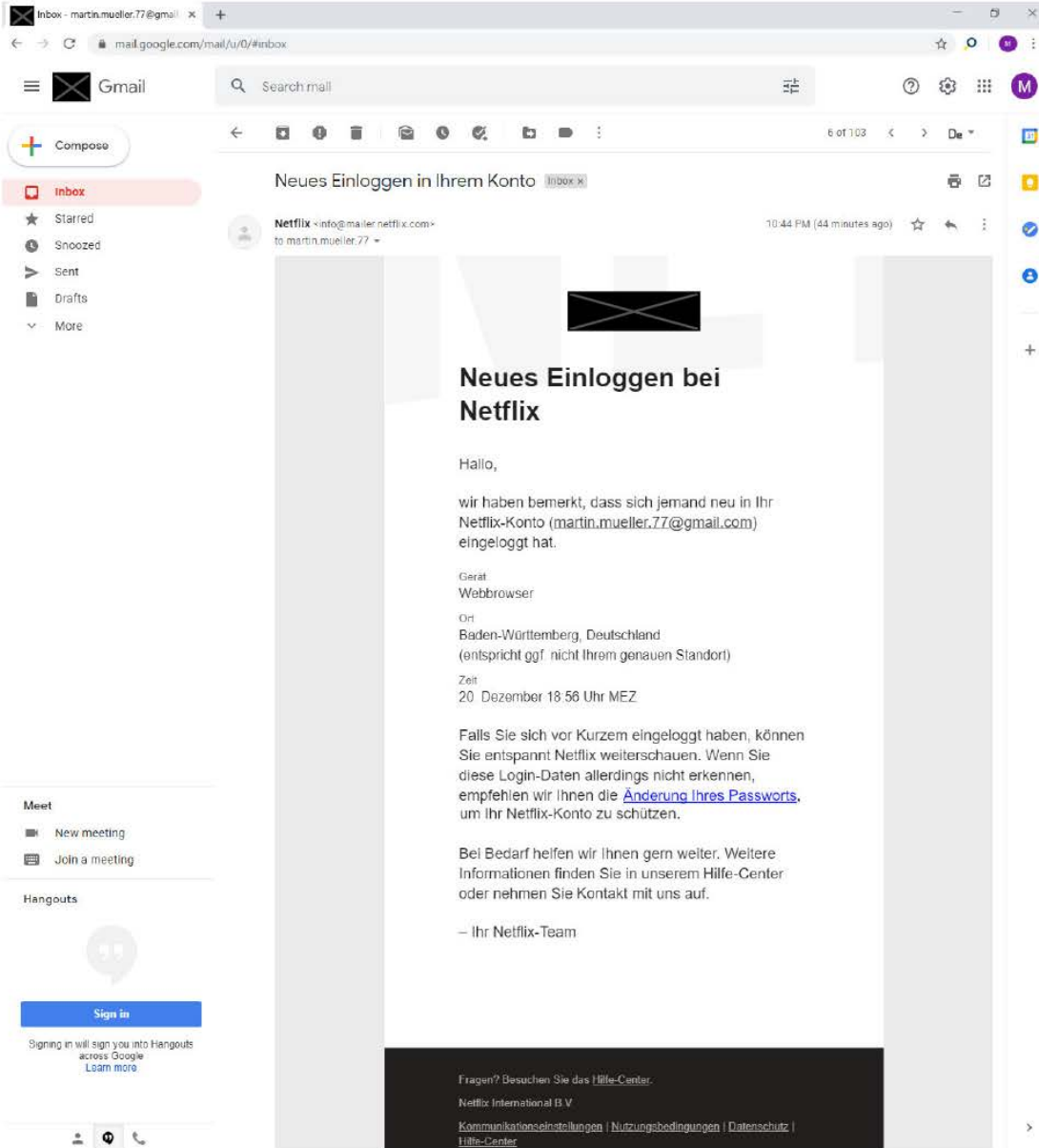
Reply Forward

Diese E-Mail ist eine:

phishing E-Mail

legitime E-Mail

Weiter



Diese E-Mail ist eine:

phishing E-Mail

legitime E-Mail

Weiter

**Speicherplatz für E-Mails fast voll**

**GMX Kundenmanagement** <mailings@system.gmx.net> 10:44 PM (50 minutes ago)

**Kundenmanagement**

### Speicherplatz für E-Mails fast voll

Lieber GMX Nutzer,

der Speicherplatz für Ihre E-Mails ist fast vollständig belegt. Eingehende Nachrichten, die größer sind als der zur Verfügung stehende Speicherplatz, gelangen nicht mehr in Ihren Posteingang. Wir empfehlen Ihnen, nicht mehr benötigte E-Mails aus dem Postfach zu löschen und den Ordner „Gelöscht“ regelmäßig zu leeren.

**Unsere Tipps für Sie:**

- Aktivieren Sie direkt im Browser den kostenlosen **GMX MailCheck** und profitieren Sie von 1,5 GB Speicherplatz für Ihre E-Mails: <https://premium.gmx.de/speichervoll>
- Wechseln Sie zu **GMX Premium** und erhalten Sie dadurch bis zu 10 GB Speicherplatz für Ihre E-Mails.

Wir wünschen Ihnen auch weiterhin viel Freude mit Ihrem GMX Postfach.

Ihr  
**GMX Kundenmanagement**

**Kundenmanagement**

Imprecasum

Hauptplatz Montabaur, Amtsgericht Montabaur, HRG 7606 Geschäftsführer: Thomas Ludwig, Jan Detjen, Sascha Vollmer

Bei dieser E-Mail handelt es sich um eine automatisch versendete Nachricht. Eine Antwort auf diese E-Mail ist nicht möglich, da die Absenderadresse nur zum Nachrichtenversand eingerichtet ist.

Reply Reply all Forward

Diese E-Mail ist eine:

phishing E-Mail

legitime E-Mail

Weiter



The screenshot shows a Gmail interface with an email from PayPal. The email subject is "Anstehende Änderungen der AGB von PayPal". The sender is "PayPal - paypal@mail.paypal.de" and the recipient is "Martin Mueller". The email content is as follows:

Martin Mueller – Sie können die Änderungen auf unserer Website ansehen. [Online ansehen](#)

Hallo Martin Mueller,

wir nehmen mit Wirkung zum 30. Juli 2021 Änderungen an unseren AGB vor, indem wir die PayPal-Nutzungsbedingungen, die Bedingungen für die Nutzung von „Bezahlung nach 14 Tagen“, die Bedingungen für die Nutzung von „Kauf auf Rechnung“ und die Bedingungen für die Nutzung von Money Pools überarbeiten.

Es gibt keinen Handlungsbedarf von Ihrer Seite. Wenn Sie jedoch mehr über die anstehenden Änderungen erfahren möchten, finden Sie Details dazu (ab wann sie gelten und was Sie tun können, wenn Sie die Änderungen ablehnen möchten) auf <https://www.paypal.com/AGB>. Sie können diese Seite auch anzeigen, indem Sie auf PayPal.com in der Fußzeile auf den Link "AGB" und dann auf "Anstehende Aktualisierungen der Richtlinien" klicken.

Wenn Sie Fragen zu den anstehenden Änderungen oder Ihrem PayPal-Konto haben kontaktieren Sie uns.

Vielen Dank, dass Sie PayPal nutzen!

Viele Grüße,  
Ihr PayPal-Team

Diese Nutzungsbedingungen treten am 30. Juli 2021 für alle Kunden in Kraft.

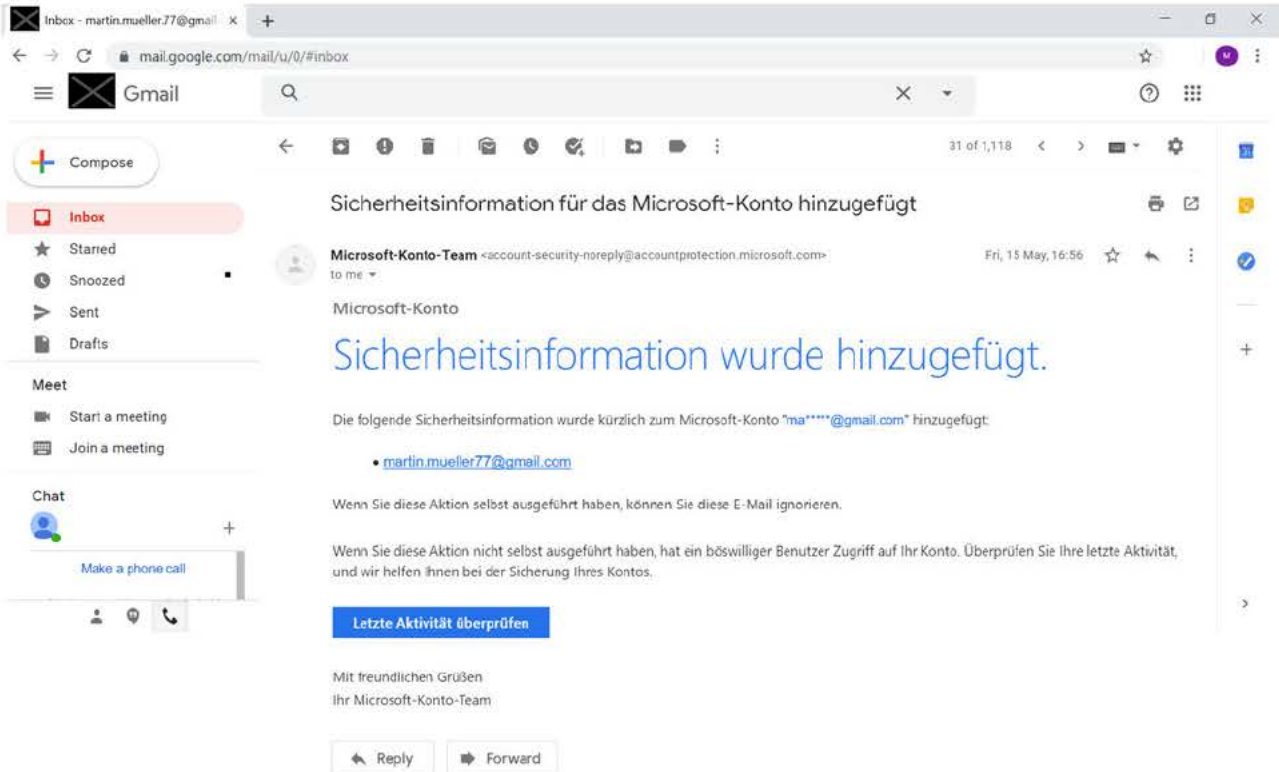
At the bottom of the email, there are buttons for "Reply", "Reply all", and "Forward".

Diese E-Mail ist eine:

phishing E-Mail

legitime E-Mail

Weiter



Diese E-Mail ist eine:

phishing E-Mail

legitime E-Mail

Weiter

Inbox - martin.mueller.77@gmail x +

mail.google.com/mail/u/0/#inbox

Compose

Inbox

Starred

Snoozed

Sent

Drafts

More

Meet

New meeting

Join a meeting

Hangouts

Sign in

Signing in will sign you into Hangouts across Google. [Learn more.](#)

12 of 103

Abo-Bestätigung

Apple <no\_reply@email.apple.com> to martin.mueller.77 - 10:43 PM (30 minutes ago)

Abo-Bestätigung

CLIP STUDIO PAINT

Hello Martin,

Du hast das folgende Angebot angenommen:

App	CLIP STUDIO PAINT
Abo	PRO Dual-Plan (monatlich)
Anbieter	CELSYS, Inc.
Annahmedatum	21.05.2021
Probeabo	8 Monate kostenlos – ab dem 21.05.2021
Abo-Preis	6,49 € pro Monat – ab dem 21.08.2021
Zahlungsmethode	PayPal

Dein Abo verlängert sich automatisch, bis es gekündigt wird.

Um Gebühren zu vermeiden, musst du mindestens einen Tag vor dem jeweiligen Verlängerungsdatum kündigen. [Besuche dein Abo](#), um mehr zu erfahren oder zu kündigen.

Mit freundlichen Grüßen  
Apple

Hilfe bei Fragen zu Abos und Käufen erhältst du auf der [Apple-Support-Website](#).

Copyright © 2021 Apple Distribution International Ltd.

Reply Reply all Forward

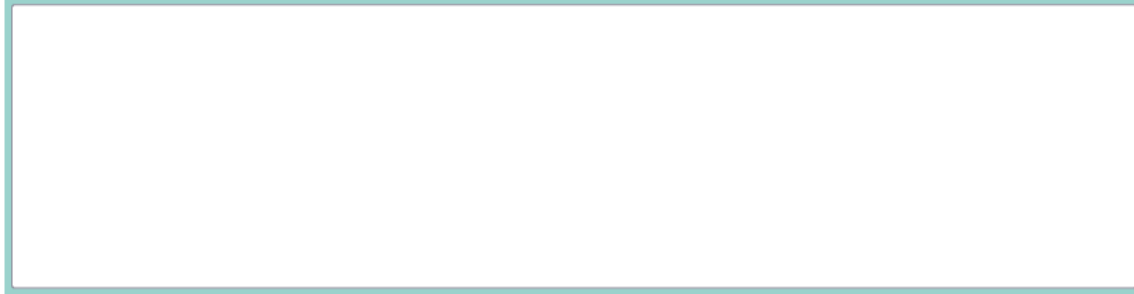
Diese E-Mail ist eine:

phishing E-Mail

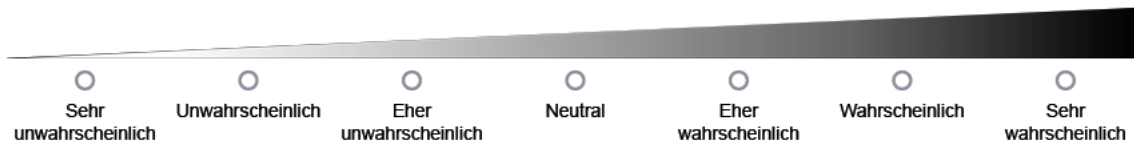
legitime E-Mail

Weiter

Wie sind Sie grundsätzlich beim Beurteilen der Screenshots vorgegangen?



Wie wahrscheinlich ist es, dass Sie dieses Browser-Update einem Freund oder Kollegen empfehlen?



Weiter

Wie würden Sie das Browser-Update insgesamt bewerten?

- Ausgezeichnet
- Sehr gut
- Gut
- Mangelhaft
- Schlecht

Bitte erläutern Sie, wie das Browser-Update Ihre Wahrnehmung des Links verändert haben:

Weiter

Wie hilfreich war das Browser-Update, um auf verdächtige Links hinzuweisen?

- Überhaupt nicht hilfreich
- Ein bisschen hilfreich
- Etwas hilfreich
- Hilfreich
- Sehr hilfreich

Hat das Browser-Update Ihre Wahrnehmung des Links beeinflusst?

- Es mich überhaupt nicht beeinflusst
- Es mich nicht so sehr beeinflusst
- Es mich etwas beeinflusst
- Es mich ein wenig beeinflusst
- Es mich sehr beeinflusst

Weiter

Hat das Browser-Update Sie gestört?

- Überhaupt nicht
- Ein bisschen
- Etwas
- Sehr
- Extrem

Wenn Sie weitere Rückmeldungen zur Verbesserung des Browser-Updates haben, teilen Sie uns dies bitte mit:

Weiter

## Debriefing

Sie haben nun den Studienteil abgeschlossen.

Im Rahmen der Studie wurde Ihnen gesagt, dass es ein Update des Chrome Browsers gab.

In Wirklichkeit gibt es dieses Update nicht.

Aber eine solche Funktionalität gibt es als Add-On bzw. Web-Extension sowohl für Chrome, als auch für Firefox und den E-Mail Client Thunderbird (TORPEDO). <https://secuso.aifb.kit.edu/TORPEDO.php> Bitte füllen Sie noch die demographischen Fragen auf den nächsten beiden Seiten aus.

Weiter



**Welches Geschlecht haben Sie?**

- Männlich
- Weiblich
- Divers
- Keine Angabe

**Wie alt sind Sie?****Welchen Bildungsabschluss haben Sie?**

Bitte wählen Sie den höchsten Bildungsabschluss, den Sie bisher erreicht haben.

- Schule beendet ohne Abschluss
- Noch Schüler
- Volks-, Hauptschulabschluss, Quali
- Mittlere Reife, Realschul- oder gleichwertiger Abschluss
- Abgeschlossene Lehre
- Fachabitur, Fachhochschulreife
- Abitur, Hochschulreife
- Fachhochschul-/Hochschulabschluss
- Anderer Abschluss, und zwar:

**In welcher Branche sind Sie tätig?**

**Haben Sie Erfahrung mit GMail?**

- Ja, ich habe einen GMail Account.
- Ja, ich hatte in der Vergangenheit einen GMail Account.
- Nein, ich hatte noch nie einen GMail Account.

**Sind Sie schon auf eine Phishing Mail hereingefallen?**

Ja

Nein

**Haben Sie sich schon über Phishing informiert?**

- Ja.
- Nein

**Haben Sie schon an einem Phishing Experiment teilgenommen?**

- Ja und zwar an...
- Nein

Weiter

**Möchten Sie zu dieser Befragung oder zum besseren Verständnis Ihrer Antworten noch etwas anmerken?**

Bitte schreiben Sie kurz ein paar Stichworte dazu.

Weiter

---

## **Vielen Dank für Ihre Teilnahme!**

Wir möchten uns ganz herzlich für Ihre Mithilfe bedanken.

Ihr Clickworker Code lautet:

Bei Fragen zur Studie schreiben Sie bitte eine E-Mail an [Benjamin.Berens@kit.edu](mailto:Benjamin.Berens@kit.edu).

Ihre Antworten wurden gespeichert.