Leibniz
Universität
Hannover

Gottfried Wilhelm Leibniz Universität Hannover
Faculty of Electrical Engineering and Computer Science
Institute of IT-Security – Usable Security and Privacy Section

Experiences and challenges with phishing of people with intellectual disabilities

Master's Thesis

for the course of study in Computer Science
by Stina Schäfer (3254180)

1st Examiner:	Prof. Dr. Markus Dürmuth
2nd Examiner:	Prof. Dr. Bettina Lindmeier
Advisor:	M.Sc. Oliver Reithmaier

Issue date:	Nov 27, 2023
Submission date:	May 27, 2024

EIDESSTATTLICHE ERKLÄRUNG

Ich erkläre, dass ich keine Arbeit in gleicher oder ähnlicher Fassung bereits für eine andere Prüfung an der Leibniz Universität Hannover oder einer anderen Hochschule eingereicht habe.

Ich versichere, dass ich diese Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen benutzt habe. Die Stellen, die anderen Quellen dem Wortlaut oder dem Sinn nach entnommen sind, habe ich unter Angabe der Quellen kenntlich gemacht. Dies gilt sinngemäß auch für verwendete Zeichnungen, Skizzen, bildliche Darstellungen und dergleichen.

Ich versichere auch, dass die von mir eingereichte schriftliche Version mit der digitalen Version übereinstimmt. Ich erkläre mich damit einverstanden, dass die digitale Version dieser Arbeit zwecks Plagiatsprüfung verwendet wird.

Hannover, 27. Mai 2024

Stina Schäfer

ABSTRACT

Phishing attacks are a widespread issue and potentially affect all people who use e-mails. This includes people with intellectual disabilities whose perspective is barely considered in cyber security research. The present work examines the experiences and challenges of people with intellectual disabilities with regard to phishing attacks. The qualitative analysis of interviews with 12 participants with intellectual disabilities shows that phishing attacks are a relevant issue for this group. *Missing knowledge* and *reading difficulties* are identified as negatively impacting this group's capability to detect phishing. Furthermore, the influential role of caregivers and relatives in this context is shown. Based on the results of the interviews, suggestions are made for appropriate support for people with intellectual disabilities in dealing with phishing attacks.

KURZFASSUNG

Phishing-Angriffe sind ein weit verbreitetes Problem, welches potenziell alle Menschen betrifft, die E-Mails nutzen. Dazu gehören auch Menschen mit kognitiver Behinderung, deren Perspektive in der Cybersicherheitsforschung kaum berücksichtigt wird. Die vorliegende Arbeit untersucht die Erfahrungen und Herausforderungen von Menschen mit kognitiver Behinderung in Bezug auf Phishing-Angriffe. Die qualitative Analyse von Interviews mit 12 Teilnehmer*innen mit kognitiver Behinderung zeigte, dass Phishing-Angriffe für diese Gruppe ein relevantes Thema sind. *Fehlendes Wissen* und *Leseschwierigkeiten* wurden als Faktoren ausgemacht, welche sich negativ auf die Fähigkeit dieser Gruppe, Phishing zu erkennen, auswirken. Darüber hinaus wurde die einflussreiche Rolle von Betreuenden und Verwandten von Menschen mit kognitiver Behinderung im Zusammenhang mit Phishing-Angriffen aufgezeigt. Basierend auf den Ergebnissen der Interviews werden Vorschläge für eine adequate Unterstützung von Menschen mit kognitiver Behinderung im Umgang mit Phishing-Angriffen gemacht.

CONTENTS

Appendix

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

ATAG	Authoring Tool Accessibility Guidelines
BfV	Bundesamt für Verfassungsschutz
BSI	Bundesamt für Sicherheit in der Informationstechnik
GDPR	General Data Protection Regulation
UAAG	User Agent Accessibility Guidelines
WCAG	Web Content Accessibility Guidelines
WHO	World Health Organization
W3C	World Wide Web Consortium

1 INTRODUCTION

During the last decades, the internet became part of most people's everyday life; shopping, communication, business, dating and banking are just a few examples of the various things that nowadays take place online to a considerable extent. Therefore, access to these services is important for overall social participation in modern society. People with disabilities are frequently excluded from full digital participation because digital devices and software do not consider accessibility to a sufficient level [1–3]. Legislative measures like the 21st Century Communications and Video Accessibility Act [4] from 2010 in the US and the European Accessibility Act [5] from 2019 already take this into account on a legal level and the World Wide Web Consortium (W3C) provides guidelines on how to achieve better accessibility for digital services [6–8]. However, adequate accessibility for all has yet to be achieved [9]. Especially cognitive disabilities are barely considered compared to other forms of disabilities [10]. In order to give everyone the same possibilities for digital participation, there needs to be a rethinking in all areas of information technology. The focus of laws and guidelines lies on webpages and user interfaces and their design. But accessibility is not exclusively an issue for web designers and app developers. With regard to cybersecurity, this means taking the accessibility of security systems more into account. This can be done by providing accessible options for accomplishing security-related tasks like authentication, but also by broadening the view for threats and attack scenarios related to specific characteristics and needs of marginalised groups [11, 12]. One of the most pervasive cyber threats today is social engineering, which is often used to gain initial access to a system [13, 14]. Social engineering attacks are *"focused on the exploitation of a human in order to gain unauthorised access to information"* [15], i. e. the attacker gets a person to do something that provides them access in some way, for example revealing a password or credit card number. Phishing attacks are a form of social engineering attack which *"electronically deceives a user to conform to some action, subsequently, divulging sensitive information"* [16]. E-mails are a common way to contact potential victims for phishing attacks [17]. Among social engineering attacks, phishing represents a very popular type of attack, the Anti-Phishing Working Group reported nearly 1 million phishing attacks world wide for the first quarter of 2024 alone [17]. To offer all members of society the highest possible degree of safety from phishing attacks, it is necessary to include the perspectives of marginalised groups into defense strategies. Research points out that privacy concerns of caregivers of people with intellectual disabilities can lead to limiting the internet access of their clients [18, 19]. Thus, for people with intellectual disabilities, cyber threat protections may promote overall digital participation, as a lower perceived risk may reduce restrictive measures taken by caregivers. However, studies identified various potential cyber risks for people with intellectual disabilities, e. g. having their account hacked, privacy breaches or downloading a virus [1, 19, 20]. Correctly identifying suspicious e-mails is a complex issue which requires focus, knowledge about potential clues and the ability to interpret these clues in context [21, 22]. At the same time difficulties with attention, memory, problem-solving and visual comprehension represent relevant functional categories of intellectual disabilities [23]. This suggests that people with intellectual disabilities could potentially be at risk from e-mail attacks. The aim of this work is to gain insights about the specific experiences and challenges of people with intellectual disabilities with phishing attacks. Therefore, I conducted interviews with people with intellectual disabilities who use e-mails. The insights gained from the responses of the interviewees can then be used to develop more inclusive phishing prevention measures.

2 BACKGROUND

The following background section aims to approach the issue examined in this work from several perspectives; the role of accessibility in security and privacy concerns, digital accessibility for people with intellectual disabilities in computer science research, the state of research on defending social engineering attacks through e-mails and internet use of people with intellectual disabilities as object of research in the fields of special education and psychology.
In addition, a definition of the term *intellectual disability* in the context of this work is given at the beginning, as this term is not used consistently in different contexts.

2.1 DEFINITION OF THE TERM "INTELLECTUAL DISABILITY" FOR THIS WORK

The World Health Organization (WHO) defines intellectual disability as *"a significantly reduced ability to understand new or complex information and to learn and apply new skills (impaired intelligence), with a reduced ability to cope independently (impaired social functioning) which started before adulthood, and has a lasting effect on development."* [24]. In the context of this paper, I refer to the term *intellectual disability* as defined by the WHO. However, it is important to acknowledge that the interpretation of this term depends on context and region and is subject to historical development [25]. Other works with different focus or background may use different terms or definitions, which is why the terms *cognitive disability* and *developmental disability* are used in several instances in this work, namely when referring to research using these terms. *Cognitive disability* is a broader term which includes intellectual disabilities but also a variety of other disabilities affecting cognitive functions, for example dementia, attention deficit disorder (ADD), dyslexia (i. e. difficulties with reading) or dyscalculia (i. e. difficulties with math) [23]. The WHO describes *Developmental disabilities* as *"health conditions that affect the developing nervous system and cause impairments in motor, cognitive, language, behaviour and/or sensory functioning"* [26]. The definitions of *developmental disability* and *intellectual disability* have overlapping parts and the terms are often used together to refer to *intellectual and developmental disabilities* . Nevertheless the term *developmental disability* includes disorders which occur during the developmental stage but do not indicate an intellectual disability [27]. As some of the papers mentioned in this work that use the terms *intellectual disability*, *cognitive disability* or *developmental disability* do not explicitly explain their definitions of these terms, and such terminology is subject to historical development and context, as mentioned above, it can not be ruled out that the authors of these papers actually refer to slightly different definitions. A standard of defining dynamic terms like these in accessibility related research would be desirable to facilitate the comparability of results.

2.2 INCLUSIVE SECURITY AND PRIVACY - A NEW CONCEPT

After cybersecurity research initially focused mainly on technical issues, the last few decades have seen increasing attention towards usability as an essential component of cybersecurity. Accessibility is mentioned occasionally in the context of usability, but remains a marginal issue and is not systematically addressed [11, 12]. In the past years, first steps have been made to develop a framework for a systematic consideration of accessibility as part of security and privacy, bringing up the concept of inclusive security and privacy. In 2017 Wang [12] introduced the concept, stating that inclusive security and privacy is *"the idea of designing security and privacy mechanisms that are inclusive to different human abilities, characteristics, needs, identities, and values"*. They furthermore argue that accessibility should not be seen as just one aspect of usable security and privacy, but as an independent property of security and privacy design, because accessibility goes beyond the design of universally usable systems. However, increased accessibility will benefit all users at the end. They call for an understanding of inclusiveness that includes peoples cultural backgrounds, identities and knowledge as well as their (dis)abilities. Additionally the interaction of these components must be taken into account, e. g. the role of security and privacy concerns in the context of the life situation or possible trade-offs between privacy and other values [12]. In their paper from 2022 Renaud and Coles-Kemp [11] adopt Wang's concept and arguments and argue that accessibility should be seen as an essential part of security and privacy design considerations. They extend these arguments with a less individualised view on accessibility, outlining the societal dimensions of inclusive security and privacy. In digitised modern societies, public services as e. g. healthcare or welfare, are increasingly delivered digitally, making a lack of digital access a serious social risk and providing secure access for all members of society a fundamental demand. They point out that in order to address this issue and achieve greater accessibility, developers and researchers need to consider not only the concrete (dis)abilities of users, but also the barriers that society places in their way, as well as the fact that digital security is linked to social, financial and political circumstances [11].

Although the conceptualization of inclusive security and privacy is relatively recent, there has been some research. Yu et al. [28] investigated

the performance of Gmail phishing warnings when it comes to visually impaired e-mail users. The first step was to conduct semi-structured interviews with visually impaired individuals to find out about their experiences and challenges with phishing detection. Their findings show that often the participants did not recognize the warnings. Building on that, the next step consisted of developing a prototype for a more inclusive warning design. This prototype was then accessed in the main part of the study. Even though their study differs in terms of the group it focuses on, one can derive valuable contributions for this present work from it. First, it shows the necessity and usefulness of specifically analysing user groups with particular needs, when aiming to elaborate inclusive and effective phishing protection strategies. Second, it proves the value of conducting semi-structured interviews for learning about experiences and challenges as a first step which then can serve as a basis for further research [28].
In a literature review, Andrew et al. [29] summarised previous research on accessibility and authentication techniques for people with visual, hearing, cognitive or motor impairments. They state that the group of people with visual impairments receive more attention in research on authentication techniques' accessibility than the other three groups. With regard to the group of users with cognitive impairments, the authors point out the need of collecting more qualitative data about this group to gain insights about their user preferences, requirements and reasons behind difficulties [29]. Hayes et al. [30] conducted a user study with seven cognitively impaired participants to gain insights into participants' challenges and experiences with common authentication procedures. The authors found that the participants had difficulties of the same kind as abled users, e. g. struggling to remember the passphrase or its correct spelling and problems with interpreting occurring error messages. However, the underlying reasons for these difficulties often differ from the ones of abled users. They argue that achieving better accessibility requires designers to keep this in mind to address the various reasons that can cause usability problems for different users when developing authentication technologies [30]. Ma et al. [31] explore the challenges and efficiencies of users with down syndrome compared to neurotypical users in using different knowledge-based authentication methods. Their findings show that users with down syndrome are capable of using all considered methods in a sufficiently efficient way, even though they needed considerably more time for the logging process than neurotypical users. An interesting insight of the study was that mnemonic passwords do not seem to offer advantages over alphanumeric passwords to users with down syndrom, unlike neurotypical users. This underlines the assumption that research results for neurotypical users cannot simply be transferred to users with cognitive disabilities [31].

As inclusive security and privacy is a relatively new concept, its elaboration is still in progress. The works of Wang respectively Renaud and Coles-Kemp, represent a first step and provide the theoretical contours of the concept. Both papers point out that more research is needed in this area and that the concept must be further developed. This work belongs to the field of inclusive security and privacy and aims to contribute to the further development and refinement of the underlying concept by collecting insights into the hitherto little researched complex of intellectual disabled users and e-mail security.

2.3 DIGITAL ACCESSIBILITY FOR PEOPLE WITH INTELLECTUAL DISABILITIES

In the research on digital accessibility for users with intellectual disabilities, web accessibility is taking on a prominent role. There exist several guidelines and policies for web accessibility [6–8], first and foremost the Web Content Accessibility Guidelines (WCAG); an international standard for creating accessible web services, produced by the W3C. The WCAG relies on the following four key principles for accessible web content: perceivable, operable, understandable, and robust, and aim to give recommendations to web designers and developers [6]. Supplementary to this, the W3C provides guidelines for authoring tools (Authoring Tool Accessibility Guidelines (ATAG)) [8] and user agents (User Agent Accessibility Guidelines (UAAG)) [7] which interlock with each other and the WCAG. In 2018 respectively 2023 the versions 2.1 and 2.2 of the WCAG were released, which, inter alia, strive to improve the coverage of the requirements of users with cognitive disabilities [6, 32]. In advance WCAG 2.0 had been criticised for neglecting the perspectives of users with cognitive disabilities [33, 34]. James et al. [33] investigated specialists suggestions for the accessibility improvement of web-apps for people with cognitive disabilities by conducting a literature review. They then mapped their findings against the WCAG 2.0, coming to the conclusion that over half of the specialists advice does not occur in the WCAG 2.0. The suggestions they found covered the categories content and text, layout, functionality, multimedia and navigation. Over all, the authors state that WCAG 2.0 could be improved by providing concrete measures for simplification of structures and process. Furthermore the WCAG2.0 should consider the impact of dynamic content, pop-up windows and similar on users with cognitive disabilities, as such content can hamper accessibility for this group. Where a direct implementation of a recommended feature is not possible, they propose to add help prompts and personalization options [33]. It is important to emphasize that this work was published before WCAG2.1 and WCAG2.2 were released and that the critique refers to WCAG2.0. Nevertheless their identification of potentially problematic features for cognitively impaired users, like e. g. dynamic content, helps to shape the picture of what is needed to increase digital accessibility for this users group. In 2021 Gartland et al. [35] conducted an systematic literature review, aiming to shed light on the current state of measures to enhance web accessibility for people with cognitive impairments. They state that many studies and interventions address the text-based nature of the web and derive the need for non-textual alternatives to increase accessibility. Furthermore they identify the inclusion of people with cognitive disabilities in research and design as an important factor to achieve relevant improvements in web accessibility [35]. In order to benefit from the variety of information and applications on the web, successfully mastering searching tasks is a key element. Several studies investigate the preferences of people with cognitive disabilities in the context of web searching and the problems they face [33, 36–39]. The results show that cognitively disabled people rate searching engines positively and preferred them over searching in a menu structure [36]. As most challenging they identify correctly typing in the search terms and dealing with a great amount of search results [36, 37, 39]. Graphical elements [37, 38], a lucid screen design and breaking down tasks in multiple steps were found to be helpful [33, 36]. Another key element of today's digital society are e-mails. Saggion et al. [40] point out that the ability to use e-mails therefore is essential for full participation in society, especially in the labour market. As part of the *Able to Inlcude* project they developed an accessible e-mail program for people with intellectual or developmental disabilities which focuses on providing support for understanding the content of e-mails. The program offers an automated simplification of text messages which relies on Natural Language Processing technologies. At the moment of publication the evaluation of the program was not completed yet but feedback of people with intellectual or developmental disabilities and their caregivers remained positive so far [40]. With regard to the topic of this thesis, it is noticeable that security aspects were not mentioned at any point in the description of the development or testing process, which thus remains a gap in this approach to e-mail accessibility for people with intellectual disabilities.

Several authors highlight the importance of taking non-technical issues, such as societal aspects or context sensitivity into account, when considering accessibility [11, 18, 41, 42]. An example for an social factor influencing digital accessibility of disabled people are caregivers. To learn about which factors have an impact on the attitude towards smartphone usage of their clients with cognitive disabilities, Heitplatz et al. [18] interviewed 24 caregivers. They found that the clients' living situation and the degree of control they have there, are particularly influential, with a higher degree of control often leading to more restrictions. The caregivers' feelings of responsibility and their own perceived digital competences also affect their mindset about their clients' smartphone usage. It is of special interest in the context of the research question of this work, that data protection and liability concerns are explicitly mentioned as factors that negatively influence the caregivers' view on their clients' smartphone usage. In some cases, this even lead to institutions completely refusing to provide internet access for the cognitive disabled people living there [18]. Such concerns may also exist when it comes to e-mail activities of people with intellectual disabilities. Reducing the risk of damage from cyberattacks via e-mail could counteract these concerns and thus have a positive impact on the autonomy of people with intellectual disabilities.

The field of digital accessibility for people with intellectual disabilities is not extensively researched yet, literature reviews revealed a lack of studies which actively include cognitively disabled participants. Starting points for improving accessibility for this group, in particular with regard to web services, are the integration of non-textual alternatives, simplification of structures and easy-to-find help prompts. Integrating technologies such as Natural Language Processing into applications to help users interact with e-mails appears promising. To address digital accessibility as a whole, non-technical factors, particularly societal aspects, need to be considered as well.

2.4 PHISHING ATTACKS

Social engineering attacks are regularly among the most frequent cyber attacks in Europe and the US, especially phishing attacks occur widely and cause losses in the millions [13, 14]. Accordingly, a lot of research on phishing attacks has been done, much of which is concerned with finding out what factors make people susceptible to such attacks in order to derive countermeasures. Some studies suggest that the demographic attributes gender, age, and education have no influence on the probability of a user to fall for a phishing attack [43, 44]. Others found indication for women and people with lower education being more susceptible to phishing [45–47]. Several studies found indication for some personality traits having a negative influence on phishing susceptibility, e. g. curiosity [44], risk propensity [44] and low self-control [47]. Openness was related with increased ability to deal with malicious e-mails [47, 48]. For extraversion, both positive [48] and negative [47] influence was suggested by different studies. There is indication for internet literacy skills promoting the ability to identify suspicious e-mails [49] but also for computer expertise and internet usage having no effect on it [45, 46]. Time pressure has been proven to affect peoples' ability to determine phishing e-mails negatively [44, 50] as well as habitual patterns of e-mail usage and large e-mail loads [51]. In addition, social factors like social proof, liking and reciprocity have an influence on the user behavior in the context of social engineering attacks and are therefore often instrumentalised by attackers [52, 53]. Self-efficacy has been identified as a supporting factor on the ability of users to detect attacks through e-mails [54, 55]. Furthermore, several studies found that knowledge about attacks also has a positive influence on the ability to detect malicious e-mails [21, 22, 52, 56] and educational interventions have been proven to be a promising approach to reduce phishing susceptibility [43, 56, 57]. On the other hand, studies indicate that educational measures have only short-term effects [58] and only increase suspicion but not the ability to detect phishing [59]. This can lead to anti-phishing education resulting in increasing the number of correctly identified malicious e-mails on the cost of also more legitimate e-mails being falsely assessed as suspicious [60]. Therefore Harrison et al. [22] argue that the focus of educational interventions should not be to increase the attention of users on phishing e-mails but to develop the users' ability to identify phishing e-mails by focusing on a few effective clues in the e-mails. Furthermore, the type of the education material should be considered, less text and more graphics have been found useful [61]. In terms of methodology for education measures, mindful techniques [57] and gamification [43] provide promising results. Another defence strategy approach against e-mail attacks consists of using technical tools like spam filters and browser technologies to detect suspicious e-mails. Study results show that spam filters fail to detect phishing e-mails in a considerable amount of cases and that more credible messages are especially more likely to reach the recipients inbox [62]. Warnings by browser technologies are easily ignored if people are not familiar with it [60]. Moreover, receiving warnings too regularly can entail that users get used to the warnings and tend to ignore them as a consequence which is called "warning fatigue" [63, 64]. In addition, relying on such technologies can lead to a false feeling of safety and the neglection of suspicious indicators beside warnings [60]. Jensen et al. [57] argue that neither educational interventions nor automated tools alone can protect from falling for phishing attacks and both should be considered when developing defence strategies.

Generally speaking, it can be noted that research does not provide a clear picture of the factors increasing susceptibility for e-mail attacks but there are indications that psychological aspects and external circumstances have an influence on it. Educational interventions can help to encounter phishing susceptibility of users but should be designed thoughtfully to be effective. Technical tools are useful to support users in detecting phishing but can not provide absolute safety.

2.5 INTERNET USAGE OF PEOPLE WITH INTELLECTUAL DISABILITIES IN PSYCHOLOGY AND SPECIAL EDUCATION RESEARCH

Research shows that individuals with intellectual disabilities use the internet for similar activities as people without intellectual disabilities e. g. watching video clips, having contact with friends, searching for information, or playing games [19, 65, 66], but with a lower proportion of the group doing so for most of the activities [67]. Especially when it comes to searching for information or new knowledge on the web, people with intellectual disabilities report to perform this activity significantly less often compared to individuals without intellectual disabilities [67]. Overall, the results show that internet activities for entertainment purposes represent a significant part of the internet activities of people with intellectual disabilities, along with social interaction and communication [19, 65–67]. The latter is a mode of particular interest in special education research, as it holds great potential for social inclusion, but also for further exclusion and harm. On the one hand, research shows online communication and social interaction on the web to be perceived as very positive by people with intellectual disabilities, supporting a sense of belonging to the general community and enabling new relationships to be formed and existing ones to be strengthened [2, 65, 68, 69]. On the other hand study results also suggest that people with intellectual disabilities are at increased risk of experiencing cyberbullying and sexual solicitation in social online environments [66, 70, 71]. Furthermore, people with intellectual disabilities frequently experiences exclusion from full participation in digital society, a phenomenon often labelled as *digital divide* which represents an obstacle for social inclusion, as digital services are an elementary part of modern societies [1–3]. The barriers to full access to digital society for this group are divers, Lussier-Desrochers et al. [1] identify five dimensions that have to be considered to enhance digital accessibility for people with intellectual disabilities: access to digital devices, sensorimotor, cognitive and technical requirements and comprehension of codes and conventions. Several studies consider cybersecurity issues in the context of people with intellectual disabilities and online activities, naming various potential risks for this population, e. g. having ones account hacked, privacy breaches, downloading a virus or fraud [1, 19, 20]. Difficulties in understanding risks and poor social judgment and insight have been identified as factors that can put people with intellectual disabilities at increased risk of being harmed by such attacks in the absence of appropriate support [19, 20, 72]. Regarding the awareness for online risks of people with intellectual disabilities, study results provide a mixed picture [20]. Findings of a study by Clements et al. [73] indicate widespread awareness for different online risks among adults with intellectual disabilities and Alfredsson et al. [67] found that adolescents with intellectual disabilities are more careful revealing personal information online than the reference group of adolescents without intellectual disability. On the other hand, in a study by Chalghoumi et al. [19] participants with intellectual disabilities did not show any privacy concerns sharing personal information online. Regarding the question of how to provide appropriate support for people with intellectual disabilities to stay safe online, Chalghoumi et al. [19] argue that the complex of privacy and people with intellectual and developmental disabilities requires a closer look in ethical ways, as there is a tension between autonomy and protection. It must be considered to what extent protection is reasonable and at which point it cuts down peoples self-determination and takes on discriminatory or excluding features [19]. Caregivers and relatives of people with intellectual disabilities take on an important role in this context, as they tend to regulate the internet use of their clients or relatives in order to protect them [19, 68]. Based on their own findings and previous research, Chadwick et al. [20] suppose an approach which focuses on supporting people with intellectual disabilities in protecting themselves online by educational training programs integrating experiential learning, the principle of self-help and a language familiar for people with intellectual disabilities. Study results from Rhagavendra et al. [68] support the practicality of such approaches based on educational intervention, showing that the social media skills of young people with intellectual disabilities can be significantly increased by appropriate social media training.

Internet use among individuals with intellectual disabilities and in particular the potential benefits and risks associated with it, is a current topic in psychology and special education research. The risk of experiencing online attacks is identified as a relevant issue in this context. To address this subject, study results suggest that self-help focused educational training programs adapted to the needs of people with intellectual disabilities represent a promising approach. The potential conflict between the protection and autonomy of people with intellectual disabilities has to be considered in this complex of issues.

3 METHODOLOGY

3.1 STUDY DESIGN

This section explains the choice of research design. It also describes the interview guide which was used for the interviews and ethical considerations of the study.

3.1.1 *Choice of research design*

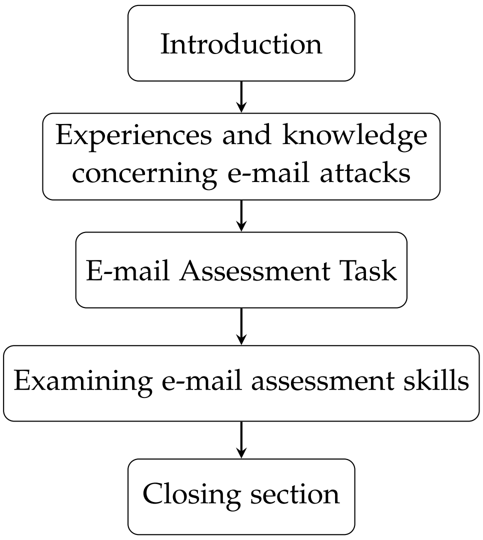
To obtain data suitable to answer the research questions for this work, I conducted semi-structured interviews with people with intellectual disability. Interviews are the method of choice here because the research questions revolve around the experiences, capabilities, and needs of a particular group of people; issues about which much can be learned by talking to individuals from that group. In addition, this approach follows the recommendations of several accessibility researchers who highlight the value of involving people with cognitive disabilities in the research process and the lack of studies doing so [29, 35, 74]. The semi-structured form of the interviews offers a framework for systematic questioning and comparability on the one hand and enough freedom to respond to the participants on the other hand, which makes it suitable for studying people's experiences and perceptions [75]. Yu et al. [28] provide an example of how semi-structured interviews investigating the experiences and challenges of disabled users can serve as a basis for developing tools that promote accessibility for the group being interviewed. The interviews also include an e-mail evaluation task, which is described in detail in section 3.1.2, where the respondents are asked to give their opinion on three e-mails shown. E-mail evaluation tasks are also found in other studies on phishing [50, 76, 77].

3.1.2 *Interview guide*

The interview is structured in several segments, each with its own purpose behind the questions it contains. Figure 3.1 gives an overview of the structure of the interview guide. The interview guide can be found in the appendix A.

INTRODUCTION The interview guide starts with an introduction section, providing information about the study's purpose and the pro-

Figure 3.1: Structure of the interview guide


Introduction
Experiences and knowledge concerning e-mail attacks
E-mail Assessment Task
Examining e-mail assessment skills
Closing section

cedure in easy language and giving the participants the opportunity to ask questions. Afterwards the interview guide schedules some time to go through the information sheet and declaration of consent, which section 3.1.3 discusses in more detail. Then the interview guide continues with some introducing questions about the participants e-mail usage in general, e. g. frequency and purpose of use. Next, the field of e-mail security is addressed with some general, open questions. The purpose of the introduction section is to provide a comfortable entry into the interview and counteracting possible insecurity the interviewees might have by informing them about the procedure and by starting with questions that are generally easy to answer. The questions about e-mail security are formulated very openly at this point of the interview, in order to gain insights into the participants' pre-existing knowledge and attitudes towards the topic.

E-MAIL ATTACKS The next segment starts with a paragraph in which the interviewer provides information about the possibility of false and manipulative e-mail content and explains the principle of phishing in easy language. After giving space for questions and comments on the input, the interview guide continues with questions asking for the participants concrete experiences with e-mail attacks and their handling of them. The questioning distinguishes between: the respondent having experienced an e-mail attack, having received a potentially malicious e-mail, or not having experienced an e-mail attack. The distinction between the three cases allows to ask more precise questions, suitable to the participants experiences. The introductory explanations about e-mail attacks ensure that all participants can imagine something under the term 'e-mail attack' and have at least some knowledge about social engineering attacks. Of course, describing these specific attack possibilities harbours the risk of priming the participants into this direction, but making sure that the participants have an idea of what e-mail attacks are, when they do the rest of the interview, outweighs the risk.

e-mail assessment task Three e-mails were presented to the participants during the interview as printed screenshots of the e-mails opened in the thunderbird e-mail application on a laptop with Windows 10. All three screenshots can be found in appendix B. Two of them are malicious e-mails, one is trustworthy. E-mail 1 is an e-mail pretending to come from a mortally ill person without any inheritors who wants to entrust their heritage (38.500.000 Euro) to the recipient of the e-mail, with the instruction to give it to needy people. To supposedly be able to do so, the sender asks for the recipients full name, address, telephone number, fax number, and profession. E-mail 2 is a trustworthy e-mail that was originally sent by the Meta company in autumn of 2023 to inform their users about changes in their terms of use and privacy policy due to new legal regulations in the European Union. The third e-mail is malicious and pretends to be send by DPD, a package delivery service widely used in Germany. The e-mail contains no plain text, but a picture of a DPD van with some text saying that the delivery of the package has failed and requesting the recipient to click on a button to confirm their address. All three e-mails were originally received by the author and just marginally changed to fit them to the needs of this study. The text in e-mail 1 was slightly shortened by removing some details about the senders life story and references to the COVID-19 pandemic to reduce reading time during the interview. In e-mail 2 the date to when the changes come into force was changed to a date after the interviews to suggest actuality. Also, the salutation was changed to a generic gender-neutral name and the recipient e-mail address in the footer was changed accordingly. By doing so on one hand the identity of the original recipient is hidden and on the other hand the generic name potentially offers points for identification for many different people and is on top easy-to-read. The content of E-Mail 3 was not changed. Both of the malicious e-mails - e-mail 1 and e-mail 3 - were chosen because they contain several clues that are named in the phishing detection advice of the Bundesamt für Sicherheit in der Informationstechnik (BSI) (*engl. federal office for information security*) and the Bundesamt für Verfassungsschutz (BfV) (*engl. federal office for the protection of the constitution*). A list of the clues in the BSI's and BfV's recommendations for phishing detection and their appearance in the malicious example e-mails is provided in table 3.1. In e-mail 1 the sender address is in all probability unknown to the participants and an asking for confidential data is clearly formulated. Urgency is

Table 3.1: Clues provided by the BSI and the BfV in the malicious example e-mails

Clues	email 1	email 3
Unknown/suspicious sender address	x	x
Asks for confidential data	x	x
Urgency	x	(x)
Asks to click on link or attachment		x
Linguistic inaccuracy	x	x

also highlighted both in the e-mail's text and subject and the generic salutation represents a linguistic inaccuracy. The recipient is not asked to click on a link or attachment in e-mail 1. For e-mail 3 applies that the sender address has evidently no relation to the DPD from where the e-mail was allegedly sent. The request for confidential data is made by asking for an address confirmation and the urgency is created indirectly by the fact that a package is waiting to be delivered. In e-mail 3 the call for clicking on a button respectively link is very present and a salutation is completely missing which represents a linguistic inaccuracy. Additionally, three different tracking IDs appear in e-mail 3 which is an apparent indicator for the suspicious nature of the e-mail.

ASSESSMENT SKILLS The next section of the interview aims to gain more insights about the participants' competences in detecting suspicious e-mails. First, the participants are asked to assess their own capabilities in identifying suspicious e-mails. To learn more about their assessment strategies, the participants are then asked to identify clues that could point to potentially malicious e-mails and explain why this is a suspicious indicator in each case. If the participants did not mention the clues *sender address*, *link* and *urgency*, the interviewer informs them in each case that this can be a clue and asks them to explain why they think this can help to identify suspicious e-mails. The clues were chosen because they are all part of the phishing detection advice of the BSI and the BfV [78, 79]. As it would have taken too much time to specifically ask for all references on the list, the three indicators above were chosen because they are more convenient than *linguistic inaccuracy* or *asks for confidential data*, which require a classification of what "inaccuracy" or "confidential" mean in the specific context. Concerning the clue "ask to click on link or attachment", attachments were omitted to simplify the question and reduce redundancy. Finally, the participants were asked what they think would help them to detect malicious e-mails in order to collect information about which type of support people with intellectual disabilities wish for. The beginning of this interview segment serves to get an idea of the participants self-perception and their degree of insecurity or self-confidence when dealing with e-mail attacks. This is especially interesting as previous research showed the positive influence of self-efficacy on developing effective cyber security skills [54, 55]. The naming of some specific clues and asking the participants about their comprehension of them ensures that an impression of the understanding of suspicious indicators of every participant can be obtained, even if they do not name any of their own initiative.

CLOSING SECTION The interview guide concludes with an closing section. This is important to create a moment for reflection [35, 80] and gives the participants the possibility to make additional remarks on the topic, ask questions and give feedback to the interviewer.

3.1.3 *Ethics*

The interviews for this study were conducted in compliance with the EU's General Data Protection Regulation (GDPR) and adheres to the principles for information and communication technology research established in the Menlo report [81]. All interviewees got an information sheet before the interview, informing them about the purpose of the study, their rights under the GDPR and contact possibilities for inspection of the personal data material and revocation. It also provides information about the collection, processing, storage, and deletion of data, as well as the right to withdraw from participation at any time and the voluntariness of participation. A declaration of consent for participation at the study and processing of the data was signed by all participants after reading the information sheet and before the interview. The information sheet and declaration of consent, were oriented on examples from special education research studies provided from the Institute of Special Education at the Gottfried Wilhelm Leibniz Universität Hannover. Both forms were adjusted to the rules for easy language by the Netzwerk Leichte Sprache *(engl. network easy language)* [82] in order to enhance accessibility. Due to the juridical nature of the GDPR and the missing text checking by easy language auditors as recommended by the Netzwerk Leichte Sprache, the information sheet and declaration of consent might not entirely meet the requirements for easy language. To counter this and to ensure informed consent for all interviewees, the participants were given as much time as they needed to go through the information sheet and the declaration of consent. Furthermore, they were offered the possibility to read it together with the interviewer or a caregiver, upon their choice. Additionally, the participants were asked if they preferred the presence of a caregiver from their respective institution during the process of reading and signing the information sheet and declaration of consent. During the interview the interviewer payed attention to potential signs of discomfort and stress from the participants and offered to pause or reminded of the right not to answer, when it seemed appropriate. For their participation, all interviewees received an expense allowance in form of a ten euros voucher for a shopping center in the region.

3.2 DATA COLLECTION

This chapter contains a description of the data collection procedure which includes the recruitment of participants and the conduction of the interviews.

3.2.1 *Recruitment*

To recruit participants for this study, I used purposive sampling, a sampling technique where participants are intentionally selected who most likely match the requirements arising from the research questions [75]. This approach is suitable when studying a population with particular characteristics, such as in this case the population of adults with intellectual disabilities who use e-mails [83]. I contacted several designated institutions were people with disabilities work or live to reach people from this population. Due to the limited time and financial restrictions for this study I contacted only institutions near Hannover. The contact to the interviewees was in all cases established through some sort of caregivers, which led to some limitations regarding the recruited sample. Hence, the perspective of people with intellectual disabilities who live without institutional care and do not work in places designated for people with disabilities does not get considered. Moreover, caregivers may preselect by approaching possible interviewees based on their personal assessment of their clients. In three cases I was able to make contact and conduct interviews with clients, respectively employees from this institutions.

The group of Interviewees for this study consisted of twelve people. Five of them (42 %) identified as female, seven as male (58 %). The age of the participants ranged from 20 to 52 years, with an average age of 31 years and a standard deviation of 11. Overall the participants of this study were rather young, with 50 % of them being under 26 years old. Table 3.2 gives an overview about the participants age distribution. All of the interviewed individuals were employed at the time of the interview and worked in different professional fields, like e. g. joinery, kitchen, agriculture or office work.

Table 3.2: Age of the study participants

Age groups	Participants
< 26	6 (50 %)
26 - 40	3 (25 %)
> 40	3 (25 %)

3.2.2 *Conduction of the interviews*

The interviews were conducted in January 2024. In every case, interviews took place at the institution through which contact to the participants was made, thus at an institution where the interviewees live or work. This was because travelling to the university for the interview would not have been possible or involved a great deal of effort for several participants. Therefore all interviews were conducted at the respective institutions in order to increase comparability. Moreover, being in a familiar environment promotes spontaneity, openness and relaxed behaviour of the interviewees [84] and can diminish stress [35]. Additionally, this allowed for a caregiver known to the participants to be present in all cases when going through the information sheet and the consent form. Negative effects of this arrangement were that the setting was not the same for all interviews as some participants were interviewed at their place of work and some at their home. Also the interviewer could not control the environment and quietness as in a university room could not be ensured. Even though all institutions provided a separate room for the interviews, in some cases there were loud noises outside because of the everyday life at the institution. In two situations the interview was interrupted for a short moment because of someone else entering the room. Before the start of each interview, the participant read and signed the information sheet and the declaration of consent and then filled out a demographic questionnaire, collecting data about the participants' age, gender and profession. In nine out of twelve cases a caregiver from the respective institution was present when the participant read and signed the information sheet and the declaration of consent. In three cases the participants preferred to do this just with the interviewer. One participant asked for a person to support them during the interview, thus according to their request a caregiver was present in this case. The caregiver did not intervene at any point, but nevertheless it must be taken into account that their presence may have influenced the participants answers. In all other cases the interviews were conducted without the presence of a caregiver. Following the approach of semi-structured interviews, the questions generally adhered to the interview guide but follow up questions or explanations were supplemented when it was reasonable. At the same time the interviewer took account of possible symptoms of stress or discomfort from the participants and adapted the style of questioning to it, i. e. dispensed with follow up questions and signaled the participant that they can take as much time as they needed to answer. Some participants reported difficulties reading and therefore requested support for reading the e-mails in the e-mail evaluation task. For participants T9 and T12, the interviewer read the e-mails aloud and participant T8 used an app which read the e-mails aloud after scanning them. The fact that some participants read the e-mails on their own and some did not certainly reduces the comparability between the participants. However, as reading difficulties occur regularly among people with intellectual disabilities and this study considers the population of people with intellectual disabilities as a whole, this actually adds to the validity of the study's findings. After the interview the participants had the possibility to add anything they did not want to say when recording was on and to discuss questions that may have come up during the interview. If the participants wished to be, they were also educated about the nature of the e-mails in the evaluation task. After this the participants received the expense allowance vouchers.

3.3 DATA ANALYSIS

This chapter describes the process of analysing the collected data. The interviews were recorded and transcribed. Then, the transcripts of the interviews were analysed using the content structuring qualitative content analysis method according to Kuckartz and Rädiker [85]. This method consists of several steps which are displayed in figure 3.2.

3.3.1 *Analysis of the interview data*

For the first step of the content structuring qualitative content analysis I read through all interviews, noted meaningful passages and topics and wrote short case summaries of all interviews. The latter can be found in the appendix C. Afterwards, I inductively developed main categories based on the material resulting from the first step. The main categories formed in this process are: *experiences, assessment strategies, handling strategies, individual factors, challenges* and *support suggestions*. In the third step, I coded all transcripts with these main categories. When I came across passages of which the meaning was not entirely clear to me, I added *unclear* as a help category to mark such passages. In the next step I inductively formed subcategories by means of the data for each main category and, if useful, subcategories of the subcategories to capture more detailed data. All codes with associated descriptions can be found in the codebook which is displayed in the appendix D.1. Then the transcripts were coded again with the

Figure 3.2: Steps of the content structuring qualitative content analysis method

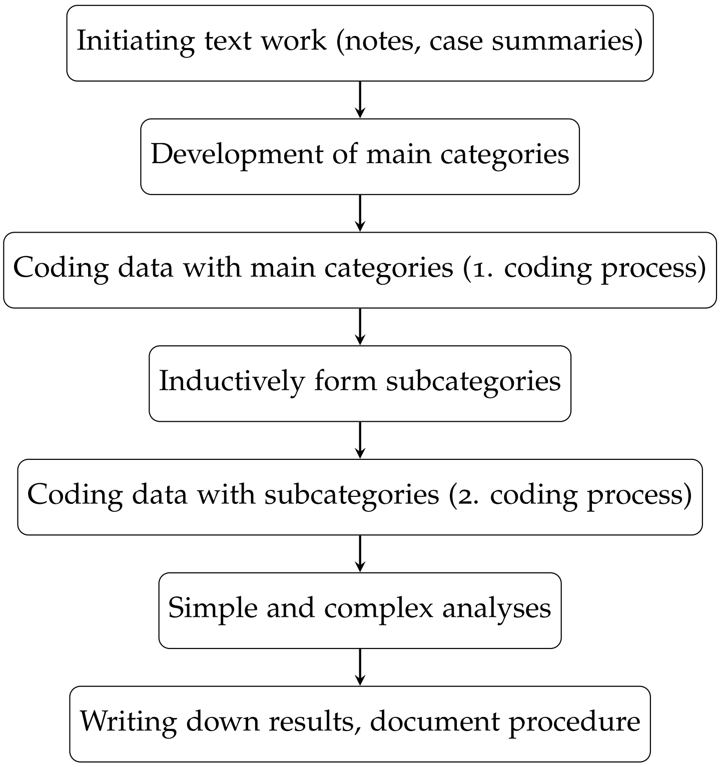

Initiating text work (notes, case summaries)
Development of main categories
Coding data with main categories (1. coding process)
Inductively form subcategories
Coding data with subcategories (2. coding process)
Simple and complex analyses
Writing down results, document procedure

Figure based on the graphic by Kuckartz and Rädiker [85]

subcategories in a second coding iteration. During this process some of the subcategories were again modified when appropriate based on the data. In this cases I went through all passages coded with the next higher-level category to apply the new or modified subcategories. After the coding was finished, I analysed the coded data. For each main category and some broader subcategories, the arising topics were collected. The frequency of subcategories was considered to identify main topics and patterns. Furthermore, I did comparisons between subcategories of a main category and looked for correlations of categories, both within and across main categories. Afterwards I wrote down the results of the analysis, using graphics and tables additionally to the text. During the writing process I sometimes came back to the analysis step to further investigate a point that arose while ordering the results and putting them into context.

3.3.2 *Analysis of the e-mail assessment task*

To evaluate the results from the e-mail assessment task, I applied another coding strategy than the content structuring qualitative content analysis because the purpose of the e-mail assessment task was not to identify emerging topics or patterns in the participants answers, but to get an overview about the participants success in assessing the example e-mails. Therefore I created a separate set of codes specifically adjusted to answer the following questions:

- Which participant gave which assessment for each of the e-mails?
- How was the quality of the justifications the participants gave for their assessment for each of the e-mails?
- What responding/clicking behavior was reported by which participant for each e-mail?
- How much time took each participant to read each e-mail?

Therefore a code for each e-mail was necessary, along with codes for the e-mails assessment which are *attack*, *trustworthy* and *uncertain* and for the quality of this assessment, *reasonable*, *partially reasonable* and *not reasonable*. These codes were all summarized under the main category *e-mail assessment*. Furthermore, I added codes for the participants answer on whether they would respond/click or not, *yes*, *no* and *uncertain* which belong to the main category *responding/clicking behavior*. To be able to categorize the reading time for the e-mails, I computed the distribution of the reading times for each e-mail and the respective lower quantile and upper quantile. The reading times in the upper quantile were assigned to the code *long*, the reading times in the lower quantile were assigned to the code *short* and all in between was assigned to the code *medium*. These codes belong to the main category *reading time*. All codes for the e-mail assessment tasks analysis can be found in the codebook in the appendix D.2, along with their respective description. After generating this set of codes, the transcripts were coded with it. For the analysis I used code overlaps to assign the participants responses to the different e-mails and analysed the distribution of the subcategories for each main category to get a picture of the respective topic and to answer the questions mentioned above.

4 RESULTS

This chapter presents the results of the analysis of the interviews and the e-mail assessment task. The latter is considered first, as its results give an overall impression of the participants' capabilities to detect malicious e-mails. This allows the results of the e-mail assessment task to be used as an indicator of the participants' susceptibility to phishing when discussing subsequent results. The sections follow the structure of the main categories in the codebook, which are: e-mail assessment task, experience with online attacks, assessment strategies, incident handling, individual factors, challenges and support suggestions. Challenges and support suggestions are discussed together in one section. All cited quotes were translated from German into English. "I:" marks passages when the interviewer is speaking, "T·:" is for statements of the participants.

4.1 E-MAIL ASSESSMENT TASK

The e-mail assessment task was included into the interviews to gain an impression of the participants' capabilities in telling trustworthy and malicious e-mails apart by assessing the three example mails which were described in detail in section 3.1.2. Additionally, the participants were asked about the reasons for their choice to investigate their capabilities on a deeper level. 25% of the participants assessed all three e-mails accurately and seven out of twelve participants correctly determined at least two out of three. Four participants correctly assessed one e-mail and one participant none. However, the majority of participants with only one properly classified e-mail remained uncertain about at least one e-mail and none of the participants assessed all three emails incorrectly. An overview about the assessment success in the e-mail evaluation task for each participant is given in table 4.2. Looking at the reasons for the participants' decisions concerning the trustworthiness of the example e-mails, more than a third of the answers given are not reasonable in terms of defending attacks. Table 4.1 gives an overview about the distribution of reasonable and not reasonable arguments by the participants for each e-mail. The participants' results are sorted by the number of reasonable and partially reasonable justification for assessment.

When comparing the reasonableness of justification with the results of the participants in the e-mail evaluation task, it becomes clear that in six cases the correct assessment results are based on an inappropriate justification, which are marked in table 4.2 with red frames. This

Table 4.1: Reasonableness of the participants' assessment in the e-mail assessment task, sorted by the number of reasonable and partially reasonable justification for assessment

E-mail	T1	T10	T2	T3	T5	T6	T8	T12	T7	T4	T9	T11
1	✓	✓	✓	✓	✓	(✓)	✓	(✓)	×	×	×	×
2	✓	✓	✓	✓	✓	×	×	×	✓	×	(✓)	×
3	✓	✓	(✓)	×	×	✓	(✓)	✓	×	(✓)	×	×

✓reasonable, (✓) partially reasonable, × not reasonable

insight is particularly significant with respect to the validity of results from e-mail evaluation tasks. The reasons for the participants' choices should be considered additionally to assessment success in terms of correct or incorrect classification in order to get meaningful results.

It is noteworthy that the two participants who correctly identified e-mail 3 as malicious with reasonable justification were the same two participants that assessed all of the e-mails correctly and reasonable. This suggests that e-mail 3 was most difficult to judge. The all-over assessment results broken down by e-mails, support this suggestion.

Table 4.2: Assessment results in the e-mail assessment task

Participant	E-mail 1	E-mail 2	E-mail 3
T1	correct	correct	correct
T2	uncertain	correct	uncertain
T3	correct	correct	false
T4	$\boxed{\text{correct}}$	$\boxed{\text{correct}}$	false
T5	correct	correct	false
T6	uncertain	false	uncertain
T7	$\boxed{\text{correct}}$	correct	uncertain
T8	correct	uncertain	uncertain
T9	$\boxed{\text{correct}}$	correct	$\boxed{\text{correct}}$
T10	correct	correct	correct
T11	$\boxed{\text{correct}}$	false	false
T12	correct	false	uncertain

Green: correct assessment; yellow: uncertain about assessment; red: false assessment; red frame: correct assessment based on not reasonable justification

E-mail 1 is not falsely assessed as trustworthy by any of the participants, with six of them also giving reasonable arguments for their choice, but e-mail 3 is falsely designated trustworthy by four out of twelve and moreover one of the three correct assessments is based on not reasonable justification. Additionally, participants were uncertain about e-mail 3 in five cases, compared to two and one cases for e-mail 1 and e-mail 2, respectively. The valid example e-mail - e-mail 2 - was identified falsely as malicious in three cases and one person was uncertain about it, showing that telling apart malicious and trustworthy e-mails poses a challenge in both directions.

The reported clicking willingness overall fits the participants' e-mail assessment; none of the participants said they would respond to or click on a link in an e-mail which they designated as attack. In one case a participant was uncertain about responding or not, even though they assessed the e-mail as an attack. However, this was about answering the sender of e-mail 1 with some wishes for recovery but without sending the data requested from the sender. In case of uncertainty about the trustworthiness of an e-mail, some participants would respond/click anyway and some not.

Table 4.3: Participants' clicking/responding behavior

Participant	E-mail 1	E-mail 2	E-mail 3
T1	no	**yes**	no
T2	*maybe*	**yes**	**yes**
T3	no	**yes**	**yes**
T4	no	no	**yes**
T5	no	**yes**	**yes**
T6	**yes**	no	**yes**
T7	no	*maybe*	*maybe*
T8	no	no	no
T9	*maybe*	no	no
T10	no	no	no
T11	no	no	no
T12	no	no	no

The time the participants took for reading the e-mails varied strongly. For e-mail 1, participants spent between 16 and 104 seconds reading, for e-mail 2 between 18 and 146 seconds and for e-mail 3 between 5 and 52 seconds. The shorter reading time for e-mail 3 is probably due to the significantly lower amount of text in it. The reading time was only measured for those participants who read the e-mails independently. A categorizing of the reading time in *short*, *medium* and *long* was achieved by computing the distribution for each e-mail an defining the lower quantile as *short*, the upper quantile as *long* and all in between as *medium*. The distribution of the participants reading times resulting from this is shown in table 4.4 and the distribution of the reading time for each e-mail in figure 4.1. It is apparent that the two participants with the shortest overall reading times are the same ones who had the poorest results concerning the reasonableness of their assessment choices. On the other hand, one participant with very good results showed rather short reading times as well and the participants with long reading times had medium results. This suggests that taking too short time reading the e-mails could negatively influence the e-mail assessment; however, after reaching a certain amount of time, longer reading times have no further influence. Also, reading time depends on the individual reading abilities of a person which renders results of different participants difficult to compare.

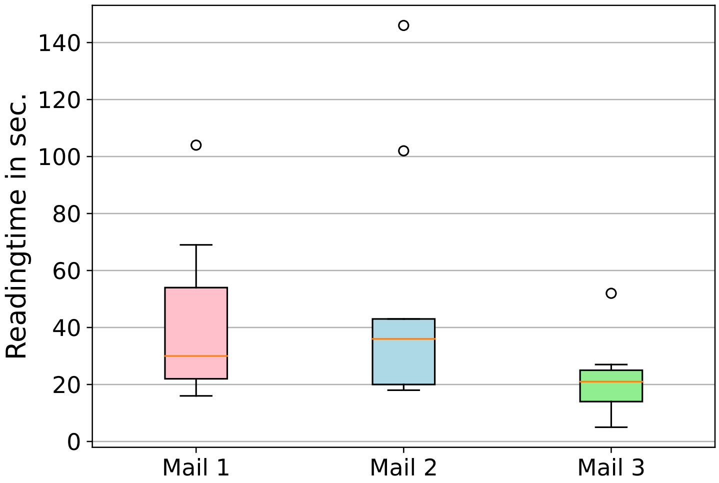
Table 4.4: Participants' reading times for the example e-mails

Participant	E-mail 1	E-mail 2	E-mail 3
T1	medium	medium	medium
T2	medium	medium	medium
T3	long	long	long
T4	short	medium	short
T5	medium	long	long
T6	medium	medium	medium
T7	medium	medium	long
T8	-	-	-
T9	-	-	-
T10	long	short	short
T11	short	short	medium
T12	-	-	-

Reading times of participants who did not read the e-mails independently (T8, T9, T12) were not considered

At some points participants made choices in the e-mail assessment task that contradicted other statements during the interview. Participant T3 designated e-mail 3 as trustworthy even though they previously reported having once received an malicious e-mail pretending to come from a delivery company. Apparently this experience did not make them explicitly suspicious about such e-mails. Participant T11 assessed e-mail 3 as trustworthy despite they understood it in a way that the

Figure 4.1: Distribution of reading times for each e-mail



Colored boxes mark the area between the first and the third quantile (medium reading time); red lines mark the median

sender wants them to give money.

The results of the e-mail assessment task show that the capabilities of people with intellectual disabilities in telling trustworthy and malicious e-mails apart vary - both between the individual participants and with regard to the type of e-mails. The participants' reported response/click behavior is consistent in that they indicate that they would not respond or click when they assess an e-mail as an attack. Not reasonable justifications for the participants' assessment of e-mails are a present issue and should always be considered when interpreting the results of e-mail assessment tasks.

4.2 Experiences with online attacks

One aim of this study is to learn about experiences with phishing attacks of people with intellectual disabilities. The questions about this topic in the interview guide address participants' concrete experiences with online attacks and also the consequences of experienced attacks. Furthermore, the participants were asked about experiences with e-mails similar to those in the e-mail assessment task. Three out of twelve participants reported having received an e-mail similar to e-mail 1 before and five received an e-mail similar to e-mail 3. This indicates that the participants have overall moderate experiences with attack e-mails similar to those. Regarding suspicious e-mails in general, ten out of twelve participants reported having received an e-mail that seemed suspicious to them. Seven of them further stated that they experienced other forms of social engineering attacks in the past. Incidents on social media platforms where reported three times and two times attacks through SMS, phone calls and instant messengers, respectively. The two participants who mentioned no experience with suspicious e-mails did not report to have experiences with any other forms of online attacks either. These results show that social engineering attacks through e-mails affect people with intellectual disabilities, as 83% of the participants reported having received suspicious e-mails before. The fact that more than half of the participants talked about other social engineering attacks during the interview, even though the questions revolved around attacks trough e-mails, suggests that social engineering in general represents a widespread issue for this population. Additionally, two participants mentioned having been victims of successful cyberattacks; one participant had their facebook account hacked and another participant experienced a malware attack which lead to the loss of several accounts. In both cases it was not clear whether social engineering was part of the attack vector or not, but it underscores the importance of cybersecurity measures for people with intellectual disabilities.

Asked about the consequences of attacks through e-mails, seven participants stated not having experienced any consequences, even though six of them also mentioned that the attack experience made them more careful when using e-mails. For example when participant T6 was asked if the attack experience influenced their handling of e-mails, they said:

> *T6: "Well, a bit. But I have / I also take experiences with me."*
> *I: "When you are saying "a bit", what kind of impact did it have?"*
> *T6: "So nothing bad now, but... I was a bit careful not to fall for it so quickly."*

In two cases, participants reported consequences of experienced attacks, both of which were emotional in nature. In one case the participant explained that these e-mails often make them feel sad and participant T12 described that they fell into depression after an e-mail attack:

> *I: "Did the attack have any consequences for you? Did anything happen afterwards?"*
> *T12: "Yes. I fell into a very bad illness, I got depressed. Because I react really badly to attacks, whether it's attacks on the internet or attacks in general."*

Two participants stated to have not experienced e-mail attacks and thus could not provide any information about experienced consequences. As well as another participant who said they could not remember whether they have had experienced an attack through an e-mail or not. The data contains no indication for a relation between the participants' amount of experiences with online attacks and their results in the e-mail assessment task.

Overall, it can be stated that none of the participants in this study reported having experienced a successful attack through an e-mail and thus no one disclosed any consequences in form of financial loss, identity theft or similar. But even attempted attacks lead to negative effects for two of the participants in form of negative feelings up to depressions.

4.3 assessment strategies

In this section, assessment strategies to identify malicious e-mails of the participants are considered, as those can give information about potential difficulties for people with intellectual disabilities in the context of defending against e-mail attacks. Information about the participants assessment strategies were gained by asking the participants concretely for things they would do to identify malicious e-mails and also by analysing the participants' statements during the e-mail assessment task or details they mentioned at other points during the interview. It has to be noted that in some cases strategies occurring in the interviews were named in relation to other forms of digital messages than e-mails, for example messages on social media. However, as the assessment strategies mentioned can be applied on various sorts of online messages, these cases are still considered and the results in this section refer to assessment strategies for online messages in general which includes e-mails in particular.

Looking at the assessment strategies mentioned by the participants in this study, two approaches stood out: looking for clues in the message indicating either trustworthiness or suspiciousness, and speaking with others. The former was a strategy applied by all participants, as all twelve named at least one clue, table 4.5 gives an overview about the number of suspicious and trust clues named by each participant. A list of all suspicious clues respective trust clues named by the participants along with the number of interviews it occurred in and the total number of mentions in all interviews can be found in table 4.6 and table 4.7. Invalid clues are highlighted in grey in the tables.

In some cases there is a negative and a positive variant of the same indicator which leads to complementary clues on the two lists, for example *lingustic inaccuracy* as suspicious clue and *linguistic accuracy* as trust clue. The sender appears to be an indicator most frequently, as *suspicious sender* respectively *trusted sender* are both on top of the lists for suspicious and trust clues. Sender occurs as suspicious clue in eight interviews and as trust clue in six. For most of the participants mentioning *suspicious sender* as a clue, a message was designated sus-

Table 4.5: Number of clues named by each participant

Participant	Suspicious clues		Trust clues	
	Valid	Invalid	Valid	Invalid
T1	4	0	1	0
T2	4	0	3	0
T3	2	1	2	1
T4	5	1	2	1
T5	2	0	1	0
T6	4	2	2	0
T7	2	0	1	0
T8	4	1	1	0
T9	1	0	1	0
T10	6	0	2	0
T11	1	0	0	0
T12	3	1	1	0

picious when they did not know the sender. For example, after being asked when they would assess an e-mail as suspicious, participant T8 explained:

> *T8: "Yes, if I know it's such an attack. When I don't know the person."*
> *I: "Okay."*
> *T8: "The name, I'm, okay, Wilfried, yes, any last name, it doesn't matter. And then I realize, "okay, that's an attack". When I don't know the person."*

Only three participants considered the actual sender address when talking about the sender of an e-mail. They explained to be suspicious when the sender address looks strange or does not fit to the alleged sender, as it was the case for e-mail 3 in the e-mail evaluation task. Participant T1 remarked on e-mail 3:

> *T1: "No, definitely not serious."*
> *I: "Okay. Why do you think that?"*
> *T1: "The error in 'Tracking' alone. Then the e-mail, which doesn't seem to match DPD."*

To not look at the e-mail address itself is particularly problematic in the context of malicious e-mails pretending to come from a well-known company as it is the case for e-mail 3. Such e-mails can easily be falsely classified as trustworthy when the concrete address remains unchecked because the sender, i. e. the company, is considered as

Table 4.6: Suspicious clues named by the participants with the respective number of occurrence

Suspicious Clues	No. of interviews clue occurred in	Total no. of occurrence
Suspicious sender	8	20
Implausibility	8	17
Demands confidential data	6	9
Linguistic inaccuracy	5	7
Date or time	4	4
Urgency or threat	3	3
Asks for money	3	3
Pictures	2	2
Similarity to known attacks	2	2
Links	1	1
Is about data protection policy	1	1

Invalid clues are highlighted in grey

known by the recipient. The answers of some participants revealed this misleading conclusion with regard to e-mail 3:

> *I: "So for the assessment, do you think this e-mail is an attack or that it's trustworthy?"*
> *T4: "That it's trustworthy."*
> *I: "Okay. And why do you think that?"*
> *T4: "Because I used to like ordering things there. And they also sent the e-mail to my father."*

Complementary to the reasons why a sender was designated suspicious, a sender was characterized as trustworthy when it was known or appeared suitable to the content.

Implausibility was another frequently mentioned indication which occurred in eight interviews as a suspicious clue. Mistrust because of implausibilities within the e-mails occurred often during the e-mail evaluation task with regard to e-mail 1; half of the participants declared to be skeptical because of the high amount of money which appeared improbable to them. Furthermore, participants reported to be suspicious when the context of a message does not fit, for example when receiving a message from a delivery service without having ordered something or e-mails from providers where they do not own an account. Accordingly, participants rather considered a message as trustworthy if it *fits in the situation* which was named by

Table 4.7: Trust clues named by the participants with the respective number of occurrence

Trust Clues	No. of interviews clue occurred in	Total no. of occurrence
Trusted sender	6	7
Unsuspicious concern	4	5
Fits in the situation	4	4
Linguistic accuracy	2	3
Pictures	1	1
Friendly wording	1	1

Invalid clues are highlighted in grey

four participants as trust clue. An *unsuspicious concern* was mentioned by four participants as a positive indicator for the trustworthiness of messages. A concern was considered unsuspicious either when the participants perceived it as a usual thing, for example privacy policy information, or when suspicious indicators were missing. Participant T2 for example stated with regard to e-mail 2:

> *I: "And what are your thoughts about this e-mail?"*
> *T2: "That this is um... not an attack."*
> *I: "And why do you think that?"*
> *T2: "It doesn't say here that you should get in touch, that you should report back. And it doesn't say um ... no amount or anything. Or... So I would say that it's not an attack."*

Half of the participants mentioned *demands confidential data* as a suspicious clue. Participants classified a person's name, address, telephone number, and bank account number as confidential. In terms of *linguistic inaccuracy* which was mentioned in five interviews as suspicious clue and *linguistic accuracy*, named in two interviews as trust clue, participants reported that they would look for spelling or grammatical errors and if the writing style seemed "professional". The unusual salutation as suspicious clue in e-mail 1 and the personal salutation in e-mail 2 as trust clue were both mentioned only once by the same participant. Three participants explained becoming suspicious when a message conveys *urgency or threat*. Three designated it suspicious when the sender of a message *asks for money*. *Similarity to known attacks* and *pictures* in an e-mail were described as suspicious clues by two participants each and one participant said they would be cautious if a message contains a *link*.

There were two unfounded clues named by the participants in terms of both suspicious and trust clues. Four participants mentioned they would be cautious if a message contains a *date or time*. For example, participant T12 answered to the question about the trustworthiness of e-mail 2:

> *T12: "Not trustworthy. Because there are things in there where I think... a date was simply written in, that can just / To enter a date, you think to yourself: yeah, no. Because, um... because with most of the things that have a date in them, you think to yourself: is that really true?"*
> *I: "Why?"*
> *T12: "Because the dates can be faked. That means they give some date that is not correct."*

One participant considered e-mail 2 to be an attack because it *is about data protection policy* and they thought that meant that their data could be given away by the company if they reacted to the e-mail. The presence of *pictures* and a *friendly wording* in the example e-mails were both designated as trust clues by one participant each.

As mentioned before, another strategy frequently used by the participants to distinguish malicious and trustworthy messages, is to speak with others. This assessment strategy was reported by nine out of twelve participants, and the role of the people they asked for support was named by participants as family, friends, caregivers, and colleagues. Family members were named most often, specifically from six participants, caregivers and friends were mentioned by five participants and two participants declared they would talk to colleagues. Five participants brought up more than one type of person they would ask for support when it comes to the assessment of online messages. An overview about the emergence of the different categories of people asked for support is given in table 4.8. It has to be mentioned in this context, that in the case of seeking support from others, the participants spoke about support for message assessment and for handling messages at the same time at many points in the interviews. Therefore, findings for assessment strategies may appear to recur in section 4.4.

Table 4.8: Persons the participants would ask for support for assessing e-mails with the respective number of occurrence

Role of the person	No. of participants naming this as support contact
Family member	6
Caregiver	5
Friend	5
Colleague	2

However, there were also cases where statements only referred to either assessment or handling strategy and the respective classification in the context in both cases is valuable as a separate result, which is why this strategy is discussed in both sections. Seeking support from others in the context of online message evaluation was brought up by participants as a strategy for dealing with a situation in which they receive a dubious message:

> *I: "And have you ever received an e-mail where you weren't sure whether it was an attack or not?"*
> *T8: "Yes, I got one before and I just asked my friend."*
> *I: "Okay."*
> *T8: "[Name] that's my friend. And I always work with him. And he knows his stuff really well and then I ask him. Then I always show him beforehand."*

As in the quote above, seeking support from others often involves showing the message to another person, which requires a high level of trust and poses a privacy issue. However, none of the participants expressed any concerns in this regard. Speaking with others in the field of assessing the trustworthiness of messages also contains sharing experiences and knowledge about experiences in this field and the field of cybersecurity in general. For example, when participant T6 was asked about subjects, about which they speaks with their friend, they answered:

> *T6: "He also explains to me how and stuff like that. And sometimes gives me tips."*
> *I: "Okay."*
> *T6: "So the combination is / So we talk to each other about how to solve it better and so on."*

Besides looking for clues in the messages and speaking with others, a few more assessment strategies were named by the participants. One participant explained that in order to assess the trustworthiness of a message, they would do some research on the internet. Another participant stated to examine links in e-mails to may see *"what else is in there"* and again another participant reported to call the alleged sender of the message to verify its trustworthiness.
A potentially dangerous assessment strategy was brought up by two participants who said they would respond to the sender of an e-mail to find out if the e-mail was an attack or not. For example, when being asked about their assessment regarding the trustworthiness of e-mail 1, which they was uncertain about, participant T6 stated:

> *T6: "Then, of course, I write to the person themselves to find out whether it's really genuine or whether they're deceiving me or something."*

At some points it was not clear what participants meant when they spoke about assessment strategies for online messages. For example, participant T11 described something that sounded much like warnings from an anti-virus software but denied using one. There is no indication for a correlation between the number of clues mentioned by a participant and the participants' results in the e-mail assessment task regarding the correct or incorrect identification of attack e-mails, but in terms of the reasonableness of the arguments for their choice. Good results regarding the reasonableness of the justifications correspond with a relatively high number of mentioned valid clues and less invalid clues: Those participants who gave only reasonable or partially reasonable justifications named more valid clues and no invalid clues. Conversely, the participant giving only unreasonable arguments for their choice in the e-mail assessment task named only one clue, which is the lowest value of all participants.

To summarise, it can be said that *looking for clues*, either suspicious or trust clues, and *speaking with others* were the assessment strategies named most frequently. The clues described by the participants were mainly reasonable, with a few exceptions for both suspicious and trust clues. Participants achieving good results in the e-mail assessment task in terms of quality of their choices' justification tended to name more valid and less invalid clues than participants with lower results. People who were mentioned by participants as supporting them with e-mail assessment were family members, caregivers, friends and colleagues. None of the participants reported any privacy concerns when speaking about seeking support from others, even though this often involves showing the message to another person.

4.4 handling of incidents

This section considers the participants' strategies to handle suspicious e-mails in order to investigate the role of such strategies in the context of challenges faced by people with intellectual disabilities when it comes to attacks through e-mails. Some questions in the interview guide asked specifically for the participants' behavior when receiving a suspicious e-mail and sometimes participants mentioned details about their handling strategies in the context of questions about other topics. During the interviews the participants named different strategies to handle incidents with suspicious e-mails, which are all listed in table 4.9 along with the respective number of interviews mentioning it and the total number of occurrences in all interviews.

The strategy that occurred most frequently was getting support which was brought up by eleven out of twelve participants. As mentioned in the previous section, at some points the participants' statements concerning seeking support from others refer to both e-mail assess-

Table 4.9: Handling strategies named by the participants with the respective number of occurrence

Handling strategies	No. interviews strategy occurred	Total no. occurrences
Get support	11	33
Delete message	8	16
Ignore message	5	11
Being careful	3	5
Juridical steps	2	6
Block sender	2	4

ment and handling of suspicious e-mails. Similar to the results for the e-mail assessment, participants reported to ask family members, friends, caregivers or colleagues for support to handle suspicious e-mails. Family members and caregivers were named by six participants each, friends by three participants and colleagues by one, as it is shown in table 4.10. These results are similar to the ones for seeking support for e-mail assessment with caregivers being asked for support slightly more often and friends or colleagues slightly less often when it comes to handling of suspicious e-mails. In the context of seeking support for handling suspicious e-mails, the participants reported showing their e-mails to the person they ask for help very often which poses a privacy issue and requires a high level of trust. Yet, none of the participants expressed any concerns in this regard. The function this strategy has for the participants varies; for some it means getting a second opinion to make a good decision, like for participant T1 who answered the question about what they talk about with the people they ask for support as follows:

Table 4.10: Persons the participants would ask for support for handling suspicious e-mails with the respective number of occurrence

Role of the person	No. of participants naming this as support contact
Family member	6
Caregiver	6
Friend	3
Colleague	1

> *T1: "That I say, watch out, this and that e-mail seems suspicious to me, do you know anything about it, right? Or that the dialog in the messenger seemed strange to me. I'm talking about the salutation now. And that you simply listen to their opinion."*

Others expressed that they feel very insecure dealing with such incidents on their own and would like someone to guide them on what to do. For example, participant T11 said:

> *I: "And have you ever received an e-mail with which you weren't sure whether it was an attack or not?"*
> *T11: "Yes, then I immediately showed it to an employee, to someone."*
> [...]
> *I: "Okay. And then what do you talk about with these people? When you get an e-mail like that?"*
> *T11: "What is it, what should I do with it? I always ask that. Before I do something wrong, I first ask what I should do with it, whether I should leave it or delete it."*

One participant named no other handling strategy besides getting support by others and if one sees reporting to the police as some sort of seeking support as well, then there are even two participants to whom this applies. This further underlines the important role of this strategy among the participants. Eight participants described that they would delete messages which appear suspicious to them and five participants stated to ignore such messages. Being careful was named by three participants as a way of dealing with suspicious messages. As concrete precautionary measures "not clicking on links" was named but not specified otherwise. Two participants stated they would report to the police when they get a malicious e-mail. Blocking the sender of a suspicious message was mentioned by two participants, in one case with regard to contacts on social media and in the other case related to phone numbers. The data gives no indication for a correlation between the handling strategies a participant named and their success in the e-mail assessment task, neither regarding the concrete assessment nor the reasonableness of the assessments justifications. The same applies to assessment strategies.

All in all the results illustrate that the participants have some strategies to cope with suspicious e-mails among which *get support* takes on the most prominent role. This strategy often involves showing messages to another person, which was not designated as an issue by any of the participants.

4.5 THE INFLUENCE OF INDIVIDUAL FACTORS

This section considers individual factors observed in the interviews and their potential influence in the context of people with intellectual disabilities and attacks trough e-mails. Some questions in the interview guide asked explicitly for such factors, e. g. for the participants general e-mail usage, their self-assessment concerning recognizing attacks and their understanding of some specific clues. Other individual factors were extracted from statements of the participants that referred to questions about other topics but nevertheless reveal information about personal characteristics.

Regarding the participants' e-mail usage, the range of usage frequency varied strongly: one participant reported using e-mails a few times a year, five participants a few times a month, four participants several times a week, and two participants stated to use e-mails daily. An overview about the participants' e-mail usage frequency is given in table 4.11. Regarding the purposes for e-mail usage among the participants, private communication and using online services or shops were most frequently mentioned, each by eight participants. Five participants reported they use e-mails for professional communication, and two participants said they use e-mails to communicate with public authorities. Table 4.12 displays the frequency of the participants' purposes for e-mail usage. There is no indication for a relation between the e-mail usage of the participants and the experiences with online attacks or the assessment or handling strategies they named. The

Table 4.11: Frequency of e-mail usage of the participants

Frequency of e-mail usage	No. of participants
Daily	2
Several times per week	4
Several times per month	5
A few times per year	1

Table 4.12: Purposes for e-mail usage of the participants

Purpose of e-mail usage	No. of participants
Private communication	8
Online services and shops	8
Professional communication	5
Communication with public authorities	2

same applies to the results of the e-mail assessment task.

At one point in the interview, the participants were asked to evaluate how easy or hard it is for them to recognize attacks through e-mails. Two participants said that it is easy for them, four stated that it is moderately difficult, three find it hard and three participants said that they do not know or did not answer the question. The ones stating that they perceive assessing e-mails as moderately difficult explained that it is sometimes hard and sometimes easy depending on the concrete e-mail or, in one case, whether they can use their app for reading support. There is no indication for a connection between the participants self-assessment and their experiences with online attacks or their handling strategies for suspicious messages. In terms of the clues given by the participants, invalid clues were given only by those participants who said they found it sometimes hard and sometimes easy to detect attacks and by one other participant who did not provide a self-assessment. Furthermore, participants who stated it was easy for them to identify e-mail attacks named more valid suspicious clues on average than the others. Considering the results in the e-mail assessment task in relation to the participants' self-assessment, no difference can be determined in terms of participants who stated they find it hard to detect attack e-mails and those who said they find it moderately hard. However, it is apparent that the two participants who said that it is easy for them to identify malicious e-mails are the same two participants who assessed all three e-mails correctly and gave reasonable justifications for their choice. Additionally, the three participants who said they can not say if they find it easy or hard to detect malicious e-mails had the lowest values in terms of reasonableness in the e-mail assessment task. These findings suggest that people with intellectual disabilities are capable to realistically assess their capabilities in detecting malicious e-mails in case they already have some skills in this field. In particular the data provides no indication for overconfidence among the participants.

To gain insight into their understanding of clues, participants were asked why they think it is useful to look at the sender address of an e-mail and to check whether an e-mail contains urgency or links to assess its trustworthiness. Their answers were categorized into "correct explanation", for answers that are correct and extensive to an amount that a solid understanding of the clue can be assumed, "incomplete explanation", if the answer is not false but lacks important features and therefore creates the impression that the clue purpose was not fully understood, "false explanation", if the answer reveals a misunderstanding of the clue function and "no explanation" for missing answers or when participants stated that they do not know. The distribution of these categories among the participants, sorted by degree of understanding, measured by the number of "correct explanation", "incomplete explanation", "no explanation" and "false explanation" is shown in table 4.13. These results suggest no big differences in the degree of understanding of the different clues: all clues were at least partly understood by roughly half of the participants and adequately understood by about a quarter of the participants. When considering minor differences, one can observe that the clue *links* has slightly worse results as the other two, as here appears the only "false explanation" answer and slightly more "no explanation" answers. This could be an indicator that the clue *links* might be more difficult to understand or that it is not well known among the participants. Considering the naming of *links* in the context of e-mail assessment by the participants, one can determine that only one participant mentioned it as a clue and also the same participant said that they would further examine links to assess their reliability. This suggests that *links* are not commonly known by the participants as a possible clue to assess the trustworthiness of e-mails and their understanding of this clue therefore may be less present.

Table 4.13: Participants' understanding of specific clues, sorted by the degree of understanding, i. e. the number of correct, incomplete, missing and false explanations given

	T1	T10	T3	T6	T12	T11	T2	T5	T8	T4	T7	T9
Sender	✓	✓	(✓)	✓	(✓)	(✓)	×	×	(✓)	×	×	×
Links	✓	✓	✓	!	(✓)	(✓)	×	×	×	×	×	×
Urgency	✓	✓	✓	✓	(✓)	×	(✓)	(✓)	×	×	×	×

✓correct explanation, (✓) incomplete explanation,
! false explanation, × no explanation

Regarding the results of the individual participants, the understanding of the clues varies strongly: two participants gave a correct explanation for all three clues, three participants gave no explanation in all cases and the other seven participants cover the whole range in between. Note that the case of a false explanation occurred only once which implies that wrong interpretations of the purpose of clues do not seem to be common among the participants. When associating the degree of understanding with the number of "correct explanation", "incomplete explanation", and "no explanation", a higher degree of understanding shows no correlation with the number of clues named and also not with reported experiences or handling strategies. Regarding the e-mail evaluation task, no correlation is indicated concerning just the assessment success but in terms of the reasonableness of the justification for the assessment. The two participants who gave a correct explanation for all three clues were the same who gave reasonable justification for all three e-mails in the e-mail assessment task. Moreover, the three participants who gave no explanation for all three clues also achieved relatively low values concerning reasonableness in the e-mail assessment task. An exception within this context is participant T11 who gave no reasonable justification for their choices in the e-mail assessment task but achieved average results in terms of explaining the three clues asked for. These findings are not surprising, as it is sensible that a better understanding of clues would increase the capability of assessing e-mails with a reasonable justification.

Next, the individual factors that were not specifically asked about, but came up during the interviews are considered. Four participants expressed awareness for the importance of a responsible and careful handling of personal data during the interview. This was mostly related to being careful where to provide one's e-mail address, probably due to the topic of the interview, but the importance of privacy policies and the risk of personal data being spread in the internet in general were also addressed. At some points, however, participants reported to not behave in a privacy-responsible way, even though they knew better. For example, participant T6 stated on their clicking behavior in the e-mail task:

> *T6: "Because otherwise the data from me could be passed / But sometimes I fall for it anyway."*
> *I: "Mhm (agreeing)."*
> *T6: "Yes, sometimes it arouses curiosity, of course. But you should still leave it alone."*

There is no indication for a correlation between expressing an aware attitude towards privacy issues and the experiences with attacks, the assessment and handling strategies mentioned by the participants or the results in the e-mail assessment task.

When being asked for e-mail attacks they know, a third of the participants denied knowing any. One of them described social engineering attacks at another point of the interview but the other three indeed did not show any previous knowledge about attacks during the interview. Eight participants revealed some previous knowledge about online attacks in their answers. In six cases, this referred to social engineering, in two cases to malware and in one case to attackers exploiting the carelessness of users left logged on to unattended computers. The prevalence of social engineering here might be due to the previously explained topic, nevertheless the participants showed awareness for the risk of scams and fakes in online communication. However, explanations of social engineering attacks mostly remained rather imprecise. The term "phishing" was used only by one participant which suggests that the majority of the participants might not be familiar with this term. For example, when being asked about their thoughts about e-mail security, T12 answered:

> *T12: "Um... there are e-mail sites where you sometimes don't know if they're that good."*

> *I: "Mhm (agreeing). What does not good mean, for example?"*
> *T12: "Um... difficult. Where people just write something in and you just / How should I explain that? That's difficult to explain. One just, um... have to think about it.*
> *I: Yes, we have time.*
> *T12: Just telling people false things that don't exist in reality. And there are people who believe that. And, yes, that's just... "*

An exception was the so called "grandparent scam" which was mentioned by two participants who both seemed to be familiar with the term and the attack it describes. This increased degree of familiarity could be due to the high presence of this attack in media reporting or because of the descriptive nature of the term and the fact that is has a German equivalent, other than "scam" or "phishing" which are commonly used as English terms in German language. In relation to social engineering attacks, two participants mentioned social media and one dating apps as environments where such attacks could probably occur, one participant also described the widespread existence of fake accounts in this context. Two of the participants provided information about where they had been informed about online attacks citing "school", "smartphone course" and "the news" as sources of information. The data indicates no correlation between the knowledge about online attacks and the participants' experiences with it or the handling strategies they reported. Regarding the clues to assess the trustworthiness of e-mails named by the participants in relation with their knowledge about online attacks, one can observe that the four participants who revealed no previous knowledge about online attacks have the lowest results in terms of reasonableness of their choices' justification in the e-mail assessment task. Also the three participants who said they do not know any attacks and indeed revealed no such knowledge at other points of the interview, were the same three participants who stated that they can not say if detecting attacks through e-mails is easy or hard for them. This suggests that some knowledge of attacks is required to give a self-assessment of one's ability to identify malicious e-mails. Two participants revealed partially missing knowledge about attacks respectively assessment strategies: one said they know that one can differentiate malicious and trustworthy links but they can not remember how and another participant asked if it happens sometimes that people pretend to be someone else in online messages. Two participants described missing knowledge to reduce the amount of unwanted e-mails they get and about the reasons why they get this e-mails. These lacks of knowledge were brought up in the interviews by the participants themselves when they reported about an issue or a question which concerns them, showing that there is a demand for education among the participants and that they have some interest in the topic.

Four participants expressed insecurity regarding e-mails or technology in general. There is no correlation between the expression of insecurity, the experiences with online attacks nor the assessment or handling strategies described by the participants. The same applies to the results in the e-mail assessment task. With regard to the four participants who mentioned fear of being attacked, it is noteworthy that they make up four out of the five participants who stated not having any experiences with other attacks than suspicious e-mails. Thus, a lower amount of attack experiences appears to go along with an increased fear of being attacked. This might be caused either by the circumstance that people with more fear apply more security mechanisms or that experiencing attacks without great negative impact reduces the fear of attacks. There was no recognizable relation between participants stating to be scared of being attacked and the assessment or handling strategies they named or their results in the e-mail assessment task.

It can be said that the results indicate a correlation between some individual factors and the capability to correctly assess malicious e-mails; few *knowledge about attacks* and poor *understanding of clues* are associated with lower results in the e-mail assessment task. Furthermore the data shows that the self-assessment of the participants with regard to their skills in assessing e-mails is fairly accurate and particularly discloses no tendency towards self-overestimation.

4.6 challenges

One goal of this study is the investigation of the challenges that people with intellectual disabilities face in the context of e-mail attacks. Interview passages can reveal challenges of the participants in different ways: the participants themselves declare that they have some difficulties, or the participants' statements contain information about the participants' knowledge, behaviour, assumptions and similar, which can be categorised as potentially causing difficulties. Difficulties mentioned by the participants themselves arose around different topics. As mentioned in section 4.5, three participants reported to find it generally hard to tell trustworthy and malicious e-mails apart. Also, three participants expressed difficulties explaining what they mean when being asked about their thoughts on e-mail security, suspicious clues, or the example e-mails. This could indicate a lack of appropriate vocabulary in the field of e-mail security as well as a rather limited familiarity with the topic. It is apparent that the three participants reporting difficulties with communicating their thoughts on e-mail security reported little experiences with online attacks; two of them reported not having any experience and one reported only to have received suspicious e-mails but mentioned no further experiences with online attacks. This could indicate that experiencing online attacks has a learning effect in terms of learning the relevant vocabulary, but it could also suggest that participants did not report their experiences because they were unable to express themselves in this context. One participant commented on several interview questions that they consider them quiet difficult, which implies that the comprehensibility of the questions was not sufficient for all participants.

An issue that occurred in seven out of twelve interviews were difficulties with reading or understanding text. Five participants reported general reading difficulties, in two cases these difficulties were so severe that the interviewer read aloud the e-mails in the e-mail assessment task and one participant used an app on their smartphone which read aloud the example e-mails. Three participants made statements which implied a misunderstanding of the content of the example e-mails. For e-mail 1 and e-mail 3, one participant each apparently understood it in such way that the sender wants to have some money of the recipient which was not part of the e-mail's content. Further, e-mail 1 was perceived as a severe threat in two cases which was probably related to the potentially frightening topics of illness and death in the e-mail. For example participant T7 said about e-mail 1:

> *I: "What are your thoughts on this e-mail?"*
> *T7: "Um... the thoughts... Yes... So when I get e-mails like that here now, I somehow feel very, very anxious. Because I can't really do anything with e-mails like this because there are always so many topics that I read through. And, er... but above all, um... that always scares me with the certain death sentence. So if someone condemns me to death, for me it means that he or she will kill me."*

These results show that general problems with understanding text are a relevant part of the context of people with intellectual disabilities and phishing attacks. Participants reporting problems with reading or understanding text achieved rather low results in the e-mail assessment task when taking quality of justification into account and showed relatively little understanding of clues and low knowledge about attacks. These results indicate that poor skills in reading and understanding text have a negative influence on the capability to detect malicious e-mails and thus increase the risk to fall for attacks through e-mails. There is no indication for a correlation between problems with reading or understanding text and the experiences with online attacks or the assessment and handling strategies reported by the participants in the data. In four cases participants asked for an explanation of a word in the e-mail which they did not know, two times each for "Tracking" and "Metaprodukte". This suggests that English words or proper names without further explanation in e-mails can pose an obstruction for understanding for people with intellectual disabilities.

Half of the participants reported a in some way problematic behavior. Concerning the interpretation of clues, there were two cases when a sender was designated as known and thus trusted only because the participants knew the name of the company that was written in the e-mail, namely facebook and DPD. The concrete sender e-mail address was not further mentioned and the whole e-mail was assessed as trustworthy because of this conclusion which poses a risk of falling for malicious e-mails pretending to come from well-known companies. Furthermore, three participants based their assessment for e-mail 3 only on the question whether they were actually waiting for a delivery or not, without looking at other factors. This behavior could lead to falling for attacks that incidentally come at a moment when their concern seems plausible. Two participants said they would write back to the sender of a potentially malicious e-mail to find out about the e-mail's trustworthiness and one participant said they would answer the sender of e-mail 1 with wishes for recovery. This behavior could lead to falling for scams as a malicious sender would of course lie about their own trustworthiness and could apply further manipulation strategies once a contact has been established. The data provides no indication for a relation between problematic behavior and experiences with online attacks or the assessment or handling strategies mentioned by the participants. Considering the results of the e-mail assessment task it is apparent that problematic behavior was not reported by the participants with very good results but was observed among participants with moderate to low results. Also the reporting of problematic behavior can be associated with lower results regarding the understanding of clues. The results show that problematic behavior in the context of e-mail security is a relevant issue among the participants.

To encounter the challenges of people with intellectual disabilities in the context of attacks through e-mails, adequate support opportunities are needed. To learn about these, one question in the interview guide concretely asked for the participants suggestions for support measures and additionally to this some participants gave implicit suggestions during the interview. Seven participants described their ideas for support measures they would appreciate. Having a person available to help them was mentioned most often, namely four times. As *get support* was a very present strategy for both assessing and handling e-mails, it is no surprise that this was named as support suggestion as well and indicates that the participants are comfortable with this practice. However, from a privacy focused point of view, this strategy is objectionable as it usually contains showing ones e-mails to another person. Two participants wished for more educational interventions to support people with intellectual disabilities dealing with e-mail attacks. One of the participants suggested to inform more about attacks in newspapers and on television. The other participant said the topic should be taught in schools and particularly before a person starts using e-mails it should be ensured that they were educated about possible risks. Supporting software which gives some sort of notification in case of receiving possibly malicious e-mails was suggested by two participants. One participant further commented that this software should only consider e-mails that already passed a spam filter to reduce potential annoyance through frequent warnings.

Overall, it has been shown that there are some challenges people with intellectual disabilities face when it comes to phishing attacks. Problems with reading or understanding text and difficulties to express thoughts about this topic were observed in several instances. Moreover, half of the participants described somewhat problematic behavior regarding attacks through e-mails. The participants suggested educational measures, supporting software and the availability of a contact person as possible supporting measures.

5 DISCUSSION

The following chapter discusses the results of the previous chapter in the context of the research objective of this study, which is the experiences and challenges of people with intellectual disabilities with phishing. The results will be related to the findings of other studies. Suggestions for anti-phishing measures for people with intellectual disabilities arising from these findings are also discussed.

5.1 EXPERIENCES OF PEOPLE WITH INTELLECTUAL DISABILITIES WITH PHISHING ATTACKS

Previous research showed that people with intellectual disabilities use the internet for the same activities as other users [19, 65, 66]. The findings of this work are similar with regard to e-mail activities: the participants of this study used e-mails for private and professional communication, for using online services and communication with public authorities which are common e-mail usage scenarios. As phishing attacks are a widespread phenomenon [13, 14] and all participants in this study were e-mail users, it is not surprising that 83% of the participants in this study reported having experiences with suspicious e-mails. Other studies found people with intellectual disabilities at a potentially increased risk for privacy breaches, downloading a virus, fraud or having ones account hacked [1, 19, 20]. The results of this study support this suggestion as two of the participants in this study reported having been victim of one of these attacks; one participant had their account hacked and the other one downloaded some malware. However, the sample size of this study does not allow any quantitative conclusions to be drawn. In both cases the participants did not know whether the successful attack was related to e-mails. Indeed, none of the participants reported having experienced a successful e-mail attack, but again, due to the small sample size, this does not imply that the risk of falling for such attacks is low for people with intellectual disabilities. The results show that social engineering attacks in general are a relevant issue for this population and that e-mails are not the only communication channel which should be considered in this context; attacks through phone calls, SMS, instant messengers, and on social media were reported by several participants. Research showed that cyber risks perceived by caregivers of people with intellectual disabilities can lead them to limiting the internet access of their clients [18, 19, 68] which hinders people with intellectual disabilities to fully participate in modern society [1, 11, 40, 86]. Therefore, to support societal inclusion of people with intellectual disabilities, further research on how social engineering attacks affect people with intellectual disabilities and how effective defence strategies could look like for this population, is needed.

5.2 CHALLENGES IN THE CONTEXT OF PEOPLE WITH INTELLECTUAL DISABILITIES AND PHISHING ATTACKS

The results of this study show that the capabilities of people with intellectual disabilities to tell apart malicious and trustworthy e-mails vary strongly and are influenced by multiple factors. Two participants demonstrated good skills in dealing with malicious e-mails, proving that having an intellectual disability does not necessarily mean being at particularly high risk to fall for e-mail attacks. Nonetheless the data collected during this study revealed some challenges in the context of people with intellectual disabilities and attacks trough e-mails.
The results of this study are in accordance with contradicting studies which found people with intellectual disabilities either to be aware of different online risks [67, 73] or showing no awareness for privacy issues [19]. On one hand all participants showed risk aware behavior in terms of not clicking or responding when they identified an e-mail as malicious. Furthermore, some participants expressed an aware attitude towards privacy and security issues. On the other hand some participants showed problematic behavior, e. g. responding to the sender of e-mail 1 to ask about their trustworthiness or naming *friendly wording* as a trust clue. This supports the findings of previous research naming difficulties in understanding risks and poor social judgment and insight as factors that can put people with intellectual disabilities at increased risk of being harmed by online attacks [19, 20, 72].
The results of this study suggest that *knowledge about attacks* is an influencing factor for the capabilities of people with intellectual disabilities to identify phishing attacks: more knowledge about attacks was found to be helpful, missing knowledge in this field was identified as a negative factor. Moreover, the results show that this also counts for knowledge about defence strategies, as more knowledge about clues supports the ability to correctly assess e-mails. Knowledge about clues includes the number of known clues as well as the quality of their understanding. These findings are consistent with previous studies which found knowledge about attacks and defence strategies to have a positive influence on the ability to detect social engineering attacks through e-mails [21, 22, 52, 56]. Considering that a third of the participants in this study showed no previous knowledge about attacks and five out of twelve mentioned only two clues or less, it becomes clear that *missing knowledge* about attacks and assessment strategies poses a relevant issue in the context of people with intellectual disabilities and

phishing attacks. The assessment strategies named by the participants to assess e-mails mostly focus on the content of an e-mail, e. g. "is it plausible?", "are there linguistic inaccuracies?", "does it demand for personal data or money?". Other clues, like potentially spoofed e-mail addresses or manipulated links were neglected, although they are more reliable. These results match with the findings of other studies which found focusing on textual content rather than other clues to be an issue with assessment strategies for e-mails [76] and that suspicious sender addresses are more often overlooked than linguistic inaccuracies [56].

Several studies found reading difficulties to be a common accessibility issue among people with intellectual disabilities in online contexts [2, 35, 37–40]. The results of this work show this also holds true for e-mail security, as reading difficulties were related to relatively low e-mail assessment capabilities. It is evident that problems with reading and understanding text impede an adequate interpretation of the content of e-mails and thus of their trustworthiness. However, the data does suggest an additional way in which reading difficulties appear to have a negative impact on the ability to identify malicious e-mails: Problems with reading or understanding text are associated with relatively low knowledge of attacks, which in turn is associated with lower assessment skills. This deficit in knowledge might be due to a lack of non-textual or easy-to-read information about online attacks. Heitplatz et al. [87] found that caregivers in Germany criticise a lack of educational programs for digital competence which are suitable for people with intellectual disabilities and do not exclude those who can not read.

Seeking support from others, namely from caregivers, family members, friends, and colleagues, was a prominent strategy named by the participants for both, assessing and handling e-mails. This is in accordance with the findings of Chalgoumi et al. [19] who found that caregivers and relatives of people with intellectual and developmental disabilities often help their clients and relatives with IT issues and have great influence on their attitudes and behaviors related to security and privacy. None of the participants of this study raised any privacy issues in terms of showing their e-mails to others in order to get support. Nevertheless this practise cuts down the privacy of people with intellectual disabilities and creates dependency on other people, especially if other, independent strategies are not taught. With regard to the risk of privacy breaches Chalgoumi et al. [19] argue: *"when using IT, persons with IDD* [intellectual or developmental disabilities] *often bear the brunt of a trade-off between autonomy and privacy"*. In context of attacks through e-mails, safety is added as a third factor that has to be considered besides privacy and autonomy: In the absence of other effective support the reduced privacy and autonomy through sharing ones e-mails with another person to get support might represent the best solution in order to achieve a sufficient level of safety. Another question arising in the context of people with intellectual disability seeking support with e-mails from others, is whether caregivers and relatives have sufficient skills to offer adequate support in all cases. A study by Heitplatz et al. [87] shows that caregivers in Germany report that not all employees have sufficient knowledge and media skills to provide adequate IT support for their clients. This is a serious concern given the important role of caregivers in the context of people with intellectual disabilities and phishing attacks, as revealed by the results of this study. The ability to independently use IT constitutes a great achievement for people with intellectual disabilities [19] and promotes their autonomy and social inclusion [11, 40, 86]. Therefore assessment and handling strategies in the context of e-mail attacks besides *get support from others* should be promoted.

5.3 FINDINGS TOWARDS AN APPROACH TO SUPPORT PEOPLE WITH INTELLECTUAL DISABILITIES IN DEALING WITH PHISHING ATTACKS

The results of this study support the argumentation of Chadwick et al. [20] who propose educational training programs as a promising way to support people with intellectual disabilities in dealing with online risks. Educational interventions in general have been proven to be helpful to counter difficulties of users in assessing suspicious e-mails [43, 56, 76]. However, providing information about attacks can evoke exaggerated mistrust leading to an increased number of legitimate e-mails being categorised as attacks [59, 60] and the effect of such educational interventions diminishes over time [58]. Nevertheless, the results of this study suggest that knowledge about attacks and understanding of clues to assess e-mails have a positive influence on the ability of people with intellectual disabilities to detect malicious e-mails. Furthermore, some of the participants in this study stated having no knowledge about attacks at all. Thus, educational interventions appear useful at this point. With regard to the question of how to design appropriate educational interventions for people with intellectual disabilities, the findings of this study give several indications. The results of this work support the findings of Downs et al. [76] who found that understanding the clues, not merely identifying them is important to effectively increase the ability of people to detect phishing. They conclude that *"Education therefore needs to begin at a very basic level and to explain the intuition behind recommended strategies in a non-technical way"* [76]. This equally holds true for people with intellectual disabilities, as shown by this work. In addition, educational measures about e-mail attacks for people with intellectual disabilities should avoid English terms and be written in easy-to-read language to increase accessibility. Furthermore, text-alternatives should be provided. This is in line with the recommendations of other studies regarding web accessibility [33, 35, 40]. Jensen et al. [57] argue that approaches containing both, educational interventions and the use of supporting technical tools, are most effective. As the focus of this study is on the experiences and behaviours of the participants, the question of the use of anti-phishing tools by people with intellectual disabilities cannot be answered at this point. However, technical tools to support people in reading and understanding e-mails appear as a promising approach to decrease the negative impact of reading difficulties on the ability to detect malicious e-mails. Saggion et al. [40] gave an example of how such tools could be realised using user centered design and Natural Language Processing technologies. Further research should consider how to best integrate phishing warnings into such tools.

The results of this work are in line with other studies showing that caregivers and relatives of people with intellectual disabilities take on an important role in defending online attacks [18, 19]. Approaches to support people with intellectual disabilities in dealing with phishing should take this into account. Heitplatz et al. [87] propose a tandem model to educate caregivers and their clients at the same time and to promote learning from each other about possible issues. Involving the caregivers or relatives in the learning process could also be beneficial in reducing overprotection, as it may help them to be more realistic about their clients' or relatives' capabilities.

5.4 methodological findings

Gartland et al. [35] point out the benefits of accessibility studies which involve participants with disabilities and the lack of such studies. This work shows that conducting interview studies with people with intellectual disabilities are a suitable method to find out about their experiences and challenges with cyber attacks. However, there were interview passages when the content of participants' statements was unclear or incomprehensible to the interviewer. Further questioning proved to be difficult in some cases and seemed to be very stressful for some participants. This emphasises the usefulness of test runs before the interviews with intellectually disabled people and preparing suitable follow-up questions. Moreover, letting easy-to-read experts check the interview guide can increase comprehensibility of the questions. These preparatory steps were not taken in this case and could have reduced the number of unclear statements.

Pitfalls when using e-mail assessment tasks to measure phishing susceptibility were already pointed out by several studies [59, 62, 64]. They address the importance to also consider false positives, i. e. legitimate e-mails designated as attacks, in order to assess the ability to identify attacks instead of measuring general mistrust [59]. Furthermore, it is useful to investigate participants' reasons for their assessment as a correct decision may base on a false assumption [62]. The results of this study support this finding as the analysis of the participants assessment reasons showed incorrect justification behind correct choices in a considerable amount of cases. Studies including an e-mail assessment task should take the participants' reasons for their assessment into account in order to get more reliable estimations of the participants' phishing susceptibility.

5.5 LIMITATIONS

One limitation of this study lies in the recruitment method which established contact to participants through institutions where people with intellectual disabilities work or live. Therefore perspectives of people who live and work outside of such institutions were not captured. Furthermore, caregivers may have preselected the participants based on their assessment of their clients. Most participants in this study were relatively young and only people living in the region around Hannover were considered. The situation of older people or people living in other regions might be different.

The e-mail assessment task provided only printed versions of e-mails and therefore did not capture participants' actual behavior but rather what they imagine how they would react. Their behavior in real-world scenarios may differ from that. Lack of real-world applicability is a common problem in phishing studies [64]. In addition, the clues mentioned by participants may have been influenced by the nature of the example e-mails in the e-mail assessment task. Different example e-mails might have led to an increased naming of different clues. Therefore, studies with more and different e-mails in a more realistic scenario would be useful.

6 CONCLUSION

6.1 SUMMARY

In this study the experiences and challenges of people with intellectual disabilities with phishing were examined. Therefore interviews with twelve participants with intellectual disabilities were conducted which involved an e-mail assessment task with three example e-mails. The interviews were analysed using content structuring qualitative content analysis. The data showed that social engineering attacks are a relevant issue for people with intellectual disabilities and that experiences with phishing attacks are common in this population. The results further display that the capability to detect malicious e-mails varies strongly between individuals. Also the awareness for risks and privacy issues differed among the participants: some expressed awareness for possible risks while others showed problematic behavior with regard to e-mail attacks. The assessment strategies of the participants mainly focused on the content of an e-mail instead of technical, more reliable clues. The study identified *Missing knowledge* about attacks and assessment strategies as having a negative impact on the capability of people with intellectual disabilities to detect phishing. Furthermore, *difficulties with reading and understanding text* were found to be impeding in this context. *Get support* from others was determined as a prominent strategy of people with intellectual disabilities to assess and handle suspicious e-mails. Concerns because of the immanent privacy issues of this strategy were not brought up by any of the participants. The results of this study indicate that educational interventions using easy-to-read language and text-alternatives are a promising approach to support people with intellectual disabilities in detecting malicious e-mails. The role of caregivers and relatives of people with intellectual disabilities should also be considered in such interventions. The study shows that interviews with people with intellectual disabilities are a suitable method to gain qualitative data about the experiences and issues with cybersecurity of this population.

6.2 FUTURE WORK

The results of this work give an overview about the complex of people with intellectual disabilities and phishing attacks. Future research should be done to investigate the emerged topics on a deeper level. With regard to knowledge about attacks and assessment strategies it would be interesting to further examine what impedes and supports people with intellectual disabilities in gaining knowledge about this topic and how well the current available materials meet their needs. Furthermore, the role that reading difficulties take on in this context should be investigated, as well as the possibilities to counter these with supporting technical tools. As the participants mentioned experiences with social engineering attacks trough other ways than e-mails, e. g. SMS and phone calls, future research should examine defence strategies for those forms of attacks with regard to people with intellectual disabilities. Further research should also consider the role of caregivers and relatives of people with intellectual disabilities in the strained context of online safety and autonomy of their clients respectively relatives. Finally, research should develop and test anti-phishing measures suitable for people with intellectual disabilities which can include educational interventions and technical tools.

APPENDIX

A INTERVIEW GUIDE

Interview guide

Experiences and challenges with phishing of people with intellectual disabilities
(Erfahrungen und Herausforderungen mit Phishing von Menschen mit kognitiver Behinderung)

Forschungsfragen:

RQ1 What experiences do people with intellectual disabilities have with attacks by email?
(Was für Erfahrungen haben Menschen mit kognitiver Behinderung mit Angriffen per E-Mail?)

RQ2 What challenges do people with intellectual disabilities face when it comes to email attacks?
(Welche Herausforderungen bestehen für Menschen mit kognitiver Behinderung bezüglich Angriffen per E-Mail?)

RQ3 What are possible starting points for supporting people with intellectual disabilities in recognizing email attacks?
(Was sind mögliche Ansatzpunkte, um Menschen mit kognitiver Behinderung bei der Erkennung von Angriffen per E-Mail zu unterstützen?)

Section	Question	RQ	Time
Begrüßung	Liebe Interviewpartner oder Interviewpartnerin, ich bin Stina Schäfer und bin Studentin an der Leibniz Universität Hannover. Meine Abschlussarbeit schreibe ich im Bereich IT-Sicherheit. Ich beschäftige ich mich mit Erfahrungen von Menschen mit kognitiver Behinderung, die E-Mails nutzen. Dabei interessieren mich vor allem Dinge, die die Sicherheit betreffen.		15 Min

Ich interessiere mich für Ihre Erfahrungen mit E-Mails und Ihre Gedanken dazu. Besonders interessant sind für mich alle Dinge, die mit Sicherheit und Angriffen durch E-Mails zu tun haben. In dem Interview können Sie von Ihren Erfahrungen erzählen. Dafür werde ich Ihnen Fragen zu dem Thema stellen. Außerdem werde ich Ihnen E-Mails zeigen und Sie können mir sagen, was Sie darüber denken. Sie können selbst entscheiden, was Sie beantworten und erzählen möchten.
Nachdem Sie dieses Schreiben durchgelesen haben, können Sie entscheiden, ob Sie ein Interview mit mir machen möchten. Wenn Sie einverstanden sind, können Sie dieses Schreiben unterschreiben und danach können wir mit dem Interview anfangen. Wenn Sie möchten, wird Frau/Herr XY (sopäd. Fachkraft) das Schreiben mit Ihnen zusammen lesen und Fragen beantworten.
Das Interview wird etwa 30-40 Minuten dauern. Um das Interview später auswerten zu können, möchte ich das Gespräch gerne mit einem Aufnahmegerät aufzeichnen. Die Aufnahme wird zur Auswertung transkribiert und anonymisiert. Das bedeutet, ich schreibe auf, was in der Aufnahme gesagt wurde. Dabei schreibe ich die Sachen so auf, dass niemand dadurch wissen kann, dass Sie die Person sind, um die es geht. Danach wird die Aufnahme gelöscht.
Ich freue mich, wenn Sie sich zu einem Interview bereit erklären. Melden Sie sich gerne, wenn Sie Fragen haben!

Einverständniserklärung unterschreiben, alle Fragen klären

Ich werde nun die Tonaufnahme starten. Sind Sie damit einverstanden?

	Ich starte jetzt die Aufzeichnung! *Aufzeichnung starten* “Ich habe die Aufnahme gestartet, bitte sagen Sie nochmal, dass Sie mit der Aufzeichnung einverstanden sind.”		
Einführung	Wir fangen mit ein paar allgemeinen Fragen zu E-Mails an. • Nutzen Sie E-Mails? [F1] • Wie oft nutzen Sie E-Mails? [F2] • Für welche Dinge benutzen Sie E-Mails? [F3] **Falls** sie nicht genannt wurden, nach den Kategorien „berufliche Kommunikation“, „private Kommunikation“, „Online Dienste“ fragen. • E-Mails sind sehr verbreitet und werden von vielen genutzt. Mich interessiert dabei vor allem alles, was mit Sicherheit zu tun hat. Was für Gedanken haben Sie zur Sicherheit von E-Mails? [F4] • Kennen Sie irgendwelche Angriffe durch E-Mails? [F5]	RQ1	5 Min
Infos zu Angriffen	Ich werde Ihnen jetzt ein bisschen was über Angriffe per E-Mail erzählen. Wenn Sie Fragen dazu haben, melden Sie sich gern zwischendurch. E-Mails können für kriminelle Zwecke genutzt werden. Zum Beispiel können Angreifer falsche Dinge in E-Mails schreiben, um die Person, die die E-Mail liest, dazu zu bringen Ihnen Geld zu überweisen. Eine häufige Art von Angriff sind sogenannte Phishing Angriffe. Dabei fälschen die Angreifer eine Internetseite von einem bekannten online Dienst, z.B. facebook.		3 Min

	Das heißt, sie erstellen eine Seite, die genauso aussieht wie die echte Seite. In Wahrheit wird die Seite aber von den Angreifern kontrolliert. Dann schicken Sie Leuten E-Mails mit einem Link zu der gefälschten Seite und sagen ihnen, dass es ein Problem mit ihrem Account gibt. Um das Problem zu lösen, sagen die Angreifer, soll die Person auf den Link klicken und ihr Passwort eingeben. Aber der Link führt zu der gefälschten Seite. Diese Seite wurde so gemacht, dass sie speichert, wenn dort jemand etwas eingibt. Wenn die Person, die die E-Mail bekommen hat, dort ihr Passwort eingibt, speichert die Seite also das Passwort. So bekommen die Angreifer die Passwörter von anderen Leuten. Das sind nur zwei Beispiele für Angriffe per E-Mail, es gibt aber noch mehr. Die Angreifer sind kreativ. Haben Sie Fragen oder Anmerkungen dazu?		
Fragen zu Erfahrungen	Haben Sie schon einmal einen Angriff durch eine E-Mail erlebt? Zum Beispiel so einen Angriff, wie die, die ich eben beschrieben habe, oder etwas ähnliches? [F6] **Falls ja:** • Wie haben Sie auf die E-Mail reagiert? [F6.1] • Woran haben Sie erkannt, dass die E-Mail ein Angriff war? [F6.2] • Wann haben Sie erkannt, dass die E-Mail ein Angriff war? [F6.3] • Hatte der Angriff Folgen für Sie? [F6.4] Falls ja: Was für Folgen hatte der Angriff für Sie? [F6.5] • Hat der Angriff ihren Umgang mit E-Mails beeinflusst? [F6.6] Folgefragen, falls andere Person als Rückversicherung genannt wird bei Antworten auf die vorherige Fragen:	RQ1 RQ2	5 Min

- Mit wem halten Sie Rücksprache? [F6.7]
- Über was sprechen Sie dann mit dieser Person? [F6.8]

Falls F6 mit „nein" beantwortet wurde:
Haben Sie schon einmal eine E-Mail bekommen, bei der Sie unsicher waren, ob sie ein Angriff ist oder nicht? [F7]
Falls ja:

- Wie haben Sie auf die E-Mail reagiert? [F7.1]
- Woran haben Sie erkannt, dass die E-Mail vielleicht ein Angriff war? [F7.2]
- Wann haben Sie erkannt, dass die E-Mail vielleicht ein Angriff war? [F7.3]
- Hatte die E-Mail Folgen für Sie? [F7.4]
- **Falls ja:** Was für Folgen hatte die E-Mail für Sie? [F7.5]
- Hat diese Erfahrung ihren Umgang mit E-Mails beeinflusst? [F7.6]

Folgefragen, falls andere Person als Rückversicherung genannt wird bei Antworten auf die vorherige Fragen:

- Mit wem halten Sie Rücksprache? [F7.7]
- Über was sprechen Sie dann mit dieser Person? [F7.8]

Falls F6 und F7 mit „nein" beantwortet wurden:
Denken Sie es könnte passieren, dass Sie eine E-Mail bekommen, die ein Angriff ist? [F8]

	Falls ja: • Wie würden Sie auf die Mail reagieren? [F8.1] • Was würden Sie tun, um herauszufinden, ob die E-Mail ein Angriff ist? [F8.2] Folgefragen, falls andere Person als Rückversicherung genannt wird bei Antworten auf die vorherige Fragen: • Mit wem genau halten Sie Rücksprache? [F8.3] • Über was sprechen Sie dann mit dieser Person? [F8.4] **Falls nein:** Warum denken Sie, dass Sie keine E-Mails bekommen, die ein Angriff sind? [F8.5]		
E-mails vorlegen	Als nächstes werde ich Ihnen nacheinander drei E-Mails zeigen. Sie können sich die E-Mail in Ruhe angucken. Zu jeder E-Mail werde ich Ihnen ein paar Fragen stellen. *E-Mail 1 vorlegen.* • Haben Sie eine ähnliche E-Mail schon mal bekommen? [Fe1.1] • Was sind ihre Gedanken zu dieser E-Mail? [Fe1.2] • Falls keine Einschätzung zu Angriff/kein Angriff kam: Denken Sie, dass diese E-Mail ein Angriff sein könnte oder ist sie vertrauenswürdig? [Fe1.2.1] • Warum denken Sie dass diese Mail vertrauenswürdig/ein Angriff ist? [FE1.3] • Würden Sie auf diese E-Mail antworten? [FE1.4] • **Falls nein**: Warum nicht? [FE1.4.1] • **Falls ja**: Wie würden Sie auf diese E-Mail antworten? [FE1.4.2]	RQ1 RQ2	20 Min

E-Mail 2 vorlegen

- Haben Sie eine ähnliche E-Mail schon mal bekommen? [Fe2.1]
- Was sind ihre Gedanken zu dieser E-Mail? [Fe2.2]
- Falls keine Einschätzung zu Angriff/kein Angriff kam: Denken Sie, dass diese E-Mail ein Angriff sein könnte oder ist sie vertrauenswürdig? [Fe2.2.1]
- Warum denken Sie dass diese Mail vertrauenswürdig/ein Angriff ist? [FE2.3]
- Würden Sie auf den Link klicken? [Fe2.5]
- **Falls nein**: Warum nicht? [Fe2.5.1]

E-Mail 3 vorlegen

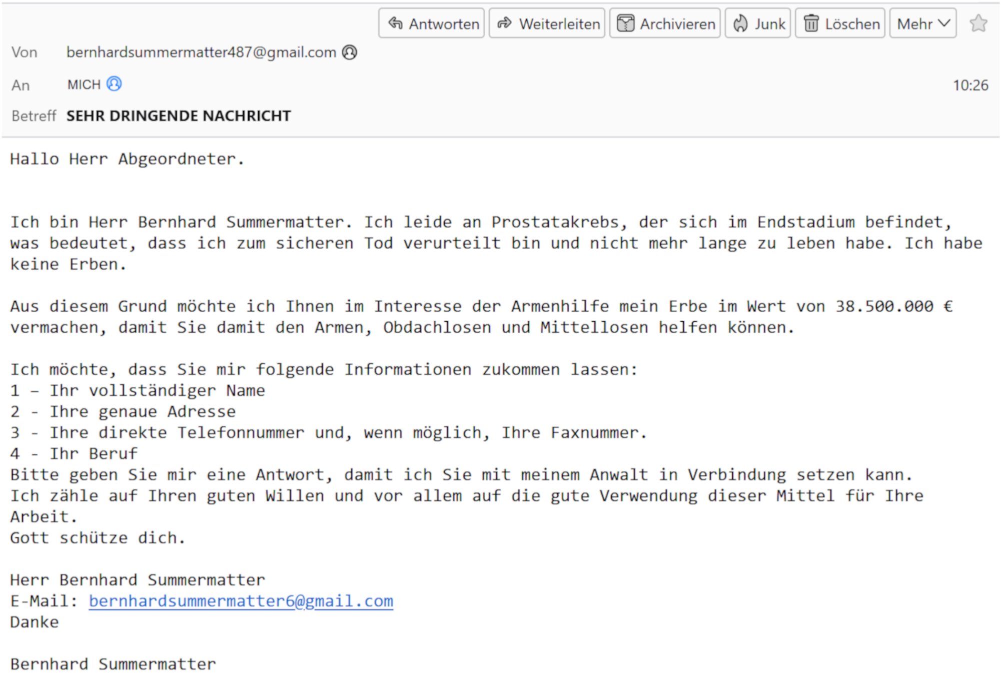
- Haben Sie eine ähnliche E-Mail schon mal bekommen? [Fe3.1]
- Was sind ihre Gedanken zu dieser E-Mail? [Fe3.2]
- Falls keine Einschätzung zu Angriff/kein Angriff kam: Denken Sie, dass diese E-Mail ein Angriff sein könnte oder ist sie vertrauenswürdig? [Fe3.2.1]
- Warum denken Sie dass diese Mail vertrauenswürdig/ein Angriff ist? [FE3.3]
- Würden Sie auf den Link klicken? [Fe3.5]
- **Falls nein**: Warum nicht? [Fe3.5.1]

Fragen zu Schwierigkeiten	Nun habe ich noch ein paar Fragen zur Abwehr solcher Angriffe. Wie schwer oder leicht finden Sie es, Angriffe per Mail zu erkennen? [F9] Um einzuschätzen, ob eine Mail ein Angriff sein könnte, kann man auf bestimmte Dinge achten. Dann kann man sagen „Wenn eine E-Mail so geschrieben ist, dann ist sie vielleicht ein Angriff." [Hier Beispiel der interviewten Person aufgreifen, falls sie vorher bereits ein Merkmal genannt hat.] Was für Dinge fallen Ihnen ein, auf die man achten könnte, um einen Angriff zu erkennen? [F10] *Wenn ein Begriff genannt wird, immer nachfragen, warum dies ein Hinweis auf einen Angriff sein könnte.* **Falls Absender/URL/(Zeit-)Druck nicht genannt wurden:** Eine Möglichkeit wäre, sich die Mail-Adresse von der die E-Mail verschickt wurde, genau anzuschauen. Was denken Sie, warum könnte das nützlich sein? [F11] Wenn die E-Mail einen Link enthält, sollte man sich den Link genau anschauen. Was denken Sie, warum könnte das nützlich sein?[F12] Wenn in der E-Mail Druck aufgebaut wird, z.B. wenn gesagt wird: „Sie müssen schnell hier ihre Daten eingeben, sonst wird ihr Konto gesperrt.", ist das ein Hinweis, dass die Mail ein Angriff sein könnte.Was denken Sie, warum ist das verdächtig? [F13] Was würde Ihnen helfen, Angriffe per E-Mail zu erkennen? [F14]	RQ2 RQ3	7 Min

Abschluss	Nun sind wir gleich am Ende des Interviews angekommen. Gibt es etwas, wonach ich nicht gefragt habe, was für Sie aber wichtig ist? Wenn Sie noch etwas zu dem Thema sagen möchten, können Sie das jetzt gerne machen. Haben Sie noch irgendwelche Fragen? Zum Schluss würde ich gerne wissen, wie Sie das Interview fanden. Sagen Sie gerne wenn es Ihnen gut gefallen hat, aber auch wenn Sie Kritik haben. Vielen Dank für die Teilnahme an dem Interview!	5 Min

B THE EXAMPLE E-MAILS

B.1 E-MAIL 1



Von bernhardsummermatter487@gmail.com

An MICH

10:26

Betreff **SEHR DRINGENDE NACHRICHT**

Hallo Herr Abgeordneter.

Ich bin Herr Bernhard Summermatter. Ich leide an Prostatakrebs, der sich im Endstadium befindet, was bedeutet, dass ich zum sicheren Tod verurteilt bin und nicht mehr lange zu leben habe. Ich habe keine Erben.

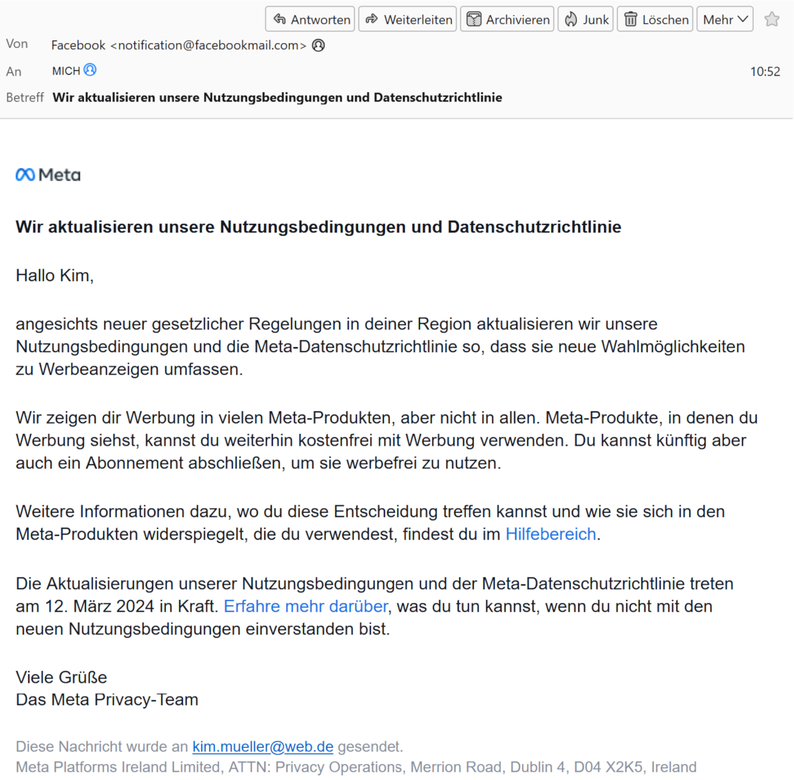
Aus diesem Grund möchte ich Ihnen im Interesse der Armenhilfe mein Erbe im Wert von 38.500.000 € vermachen, damit Sie damit den Armen, Obdachlosen und Mittellosen helfen können.

Ich möchte, dass Sie mir folgende Informationen zukommen lassen:
1 – Ihr vollständiger Name
2 - Ihre genaue Adresse
3 - Ihre direkte Telefonnummer und, wenn möglich, Ihre Faxnummer.
4 - Ihr Beruf
Bitte geben Sie mir eine Antwort, damit ich Sie mit meinem Anwalt in Verbindung setzen kann.
Ich zähle auf Ihren guten Willen und vor allem auf die gute Verwendung dieser Mittel für Ihre Arbeit.
Gott schütze dich.

Herr Bernhard Summermatter
E-Mail: bernhardsummermatter6@gmail.com
Danke

Bernhard Summermatter

B.2 E-MAIL 2



Von Facebook <notification@facebookmail.com>

An MICH

10:52

Betreff **Wir aktualisieren unsere Nutzungsbedingungen und Datenschutzrichtlinie**

Meta

Wir aktualisieren unsere Nutzungsbedingungen und Datenschutzrichtlinie

Hallo Kim,

angesichts neuer gesetzlicher Regelungen in deiner Region aktualisieren wir unsere Nutzungsbedingungen und die Meta-Datenschutzrichtlinie so, dass sie neue Wahlmöglichkeiten zu Werbeanzeigen umfassen.

Wir zeigen dir Werbung in vielen Meta-Produkten, aber nicht in allen. Meta-Produkte, in denen du Werbung siehst, kannst du weiterhin kostenfrei mit Werbung verwenden. Du kannst künftig aber auch ein Abonnement abschließen, um sie werbefrei zu nutzen.

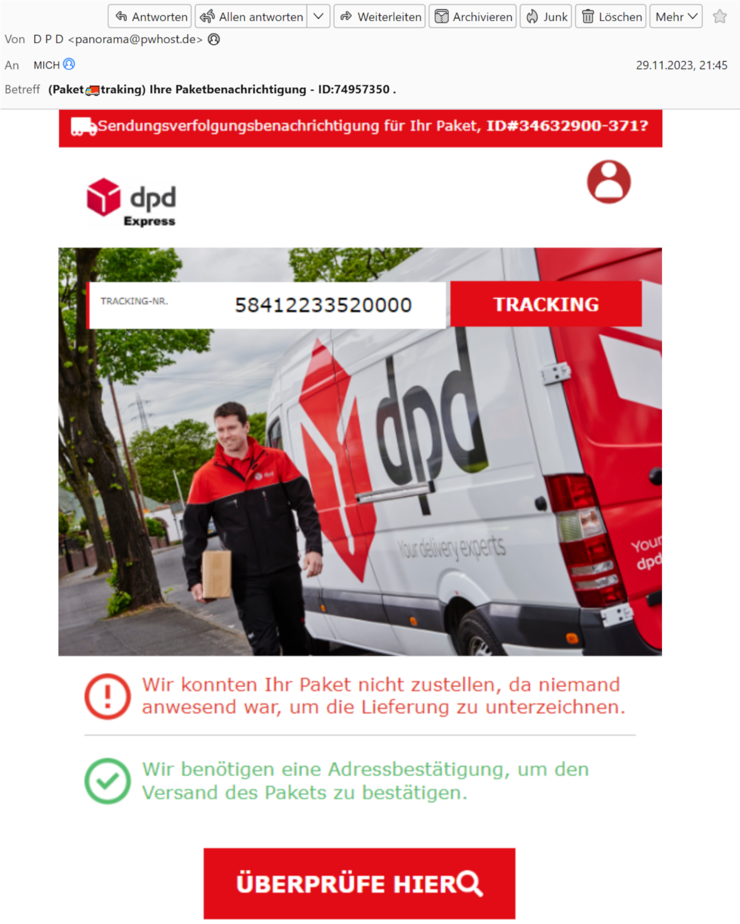
Weitere Informationen dazu, wo du diese Entscheidung treffen kannst und wie sie sich in den Meta-Produkten widerspiegelt, die du verwendest, findest du im Hilfebereich.

Die Aktualisierungen unserer Nutzungsbedingungen und der Meta-Datenschutzrichtlinie treten am 12. März 2024 in Kraft. Erfahre mehr darüber, was du tun kannst, wenn du nicht mit den neuen Nutzungsbedingungen einverstanden bist.

Viele Grüße
Das Meta Privacy-Team

Diese Nachricht wurde an kim.mueller@web.de gesendet.
Meta Platforms Ireland Limited, ATTN: Privacy Operations, Merrion Road, Dublin 4, D04 X2K5, Ireland

B.3 E-MAIL 3



Von D P D <panorama@pwhost.de>

An MICH 29.11.2023, 21:45

Betreff **(Paket🚚traking) Ihre Paketbenachrichtigung - ID:74957350 .**

🚚Sendungsverfolgungsbenachrichtigung für Ihr Paket, **ID#34632900-371?**

TRACKING-NR. 58412233520000

Wir konnten Ihr Paket nicht zustellen, da niemand anwesend war, um die Lieferung zu unterzeichnen.

Wir benötigen eine Adressbestätigung, um den Versand des Pakets zu bestätigen.

ÜBERPRÜFE HIER

C

CASE SUMMARIES OF THE PARTICIPANTS

Participant	Summary
T1	T1 is a frequent e-mail user and seems to be quiet competent in recognizing and handling e-mail attacks. They is active in social networks and is aware of the risks with social engineering there. They mentioned several correct clues to keep suspicious and trustworthy e-mails apart. Nevertheless they reported an incident were they recognized a scam only after being made aware from others and is not always able to explain the use of certain clues or security advice. They mentions that they sometimes asks others for help but seems to rely on their own assessment in general. They suggest that more public information about social engineering might increase their ability to fend off such attacks.
T2	T2 uses e-mails frequently even though they expresses great insecurity and concerns with regard to possible online attacks and is therefore very cautious. They assesses their technical skills as low and says that they finds it hard to detect malicious e-mails. Accordingly, they often shows insecurity related to their own answers, even though their answers show that they is able to recognize some valid suspicion clues. Overall they seems to have some difficulties to reliably determine malicious e-mails, which might be partly due to their low self-confidence in that context, but basic capabilities in that area are also present.
T3	T3 uses e-mails very rarely. They is aware of the possibility of social engineering attacks via digital communication technologies and reported incidents they experienced themselves as well as those they had heard about. They assesses their ability to identify malicious e-mails as dependant from the e-mails content which matches with their results in the e-mail task and with the variability of correctly and false interpreted clues in their answers.

Participant	Summary
T4	T4 reports that they uses e-mail frequently but nevertheless seems to be rather insecure dealing with e-mails. They mentions problems to remember something several times as well as difficulties with reading. When it comes to assessing the trustworthiness of e-mails they brings up a few correct suspicion clues but names some invalid trust indicators as well. They also seems to rely on caregivers to handle e-mails.
T5	T5 uses e-mails frequently but reports to never having experienced an e-mail attack. On the one hand they reports to be careful who they gives their e-mail address to but on the other hand they does not seem to look critically on various shops demanding their customers e-mail addresses. They seems to rely on their feeling when it comes to malicious e-mails and mentions few concrete clues to identify them. For dealing with possible attacks they designates caregivers as important support.
T6	T6 uses e-mails frequently and their answers show that they is aware of privacy issues and the possibility of scamming attacks in the online world. Also they mentions several valid clues to identify suspicious e-mails. Nevertheless they seems to have difficulties to apply their knowledge about the topic in an efficient way, as their answers in the e-mail evaluation task suggest. This matches with their self assessment on recognizing e-mail attacks which they reports as depending on the concrete instance. When dealing with suspicious emails, they relies on the help of people they trusts.
T7	T7 uses e-mails frequently and reports having some experiences with e-mail respectively online attacks, which seem to have a great emotional impact on them. Their assessment strategy for e-mails mainly relies on careful reading, they mentioned only few concrete clues. For dealing with suspicious e-mails they states to need support of others, but explicitly not from family members and only from young people. Their answers in the e-mail evaluation task and their self-assessment also suggest that correctly identifying suspicous e-mails is challenging for them. They names help by others as valuable support strategy for them.

Participant	Summary
T8	T8 uses e-mails regularly and shows awareness for the possibility of security and privacy issues in the online world. They also reports to have experienced cyber attacks. Because they has difficulties with reading they uses an app on their smartphone which reads aloud texts. In the assessment of the trustworthiness of e-mails they shows a lot of mistrust. The clues they names are rather imprecise and their answers suggest that they rather relies on the assessment of a friend who has technical knowledge than on their own. In dealing with suspicious e-mails they names this friend as an important support as well.
T9	T9 uses e-mails rarely and reports to have any experiences with e-mail attacks. For reading they needs support from others. They seems to be overstrained with some of the questions. Even though their assessments of the example e-mails were correct, their answers revealed that the reasons behind their conclusion were not always reliable to identify malicious e-mails. In dealing with suspicious e-mails they relies on the help of others.
T10	T10 uses e-mails rather seldom but seems very confident in dealing with technology in general. They reports several incidents of online attacks, one of which had serious consequences for them but was not necessarily related to e-mails. They seems capable to detect malicious e-mails as they names multiple valid clues for identifying malicious e-mails and is able to explain why they are useful. This is consistent with their results in the e-mail evaluation task and their self-assessment. Also they says they does not need help to deal with incidents. For support they suggests a program that marks eventually insecure e-mails that pass the spam-filter.
T11	T11 uses e-mails rather seldom and seems to be quiet insecure dealing with e-mails. They mentions very few clues to detect malicious e-mails and the results of the e-mail evaluation task also suggest that this is difficult for them. For both, assessment and handling of suspicious e-mails, they relies on the help of others.

Participant	Summary
T12	T12 uses e-mails rather seldom and not for a long time yet. They says that they often needs support from others in dealing with e-mails and that they has difficulties with reading. They reports to have experiences with e-mail attacks, one of which had serious consequences for her. They shows awareness for the possibility of online attacks and mentions several valid clues to identify malicious e-mails, even though their explanations behind these clues are not always entirely correct. When it comes to applying these clues, however, they seems to be insecure and seeks help from others. They emphasises the importance of education about online attacks, especially for people with disabilities and makes clear that the current status quo is not enough in their opinion.

D CODEBOOK

The following chapter displays the codebook which was used to analyse the interviews and the e-mail assessment task. Below each code a description of the code is given in the left part of the table and an example quote on the right side. Subcodes are indented under their respective upper code.

D.1 CODEBOOK FOR THE ANALYSIS OF THE INTERVIEWS

Experiences with online attacks	
Includes experiences the participants made in the context of social engineering attacks. Can also be the absence of experiences.	I: "And have you ever received an e-mail that you weren't sure whether it was an attack or not? " T8: "Yes, I've received one before and I just asked my friend."
Experiences with suspicious e-mails	
Participants report experiences with e-mail attacks where themselves have been targeted.	I: "And have you ever received an e-mail that you weren't sure whether it was an attack or not? " T8: "Yes, I've received one before and I just asked my friend."
No experiences with suspicious e-mails	
Participant states to not have no experiences with e-mail attacks with themselves as target.	I: "Have you ever experienced an attack by e-mail?" T9: Nope. I: And have you ever received an e-mail where you weren't sure whether it was an attack or not? T9: Not like that either.
Experiences with e-mails similar to example mails	
Participant says to have received or not received an e-mail similar to an example e-mail of the assessment task.	I: "Have you ever received a similar email?" T1: "Yes, I have."

Received similar	
Participant states having received a similar e-mail.	I: "Have you ever received a similar email?" T1: "Yes, I have."
Not received similar	
Participant states not having received a similar e-mail.	I: "Have you ever received a similar e-mail?" T9: "Fortunately never."
Not know if received similar	
Participant says they does not know if they received a similar e-mail.	I: "Have you ever received a similar e-mail?" T4: "I just don't know."
Experiences with other (not e-mail) social engineering attacks	
Experiences the participants report where themselves had been attacked with some form of social engineering attack that was not e-mail. Could be for example on social media, at the phone, via messenger.	T4: "Does that also work when you get calls? Uh, outside? I've had people call me before who also wanted my data."
Instant messenger	
Participants report to have experienced a social engineering attack via a messenger application.	T8: "I have already received some others, via WhatsApp too."
SMS	
Participants report to have experienced a social engineering attack via SMS.	T8: "Something like that/ not yet an e-mail, but I have already received a SMS. Send me that much money. "
Phone call	
Participants report to have experienced a social engineering attack via phone call.	T4: "Does that also work when you get calls? Uh, outside? I've had people call me before who also wanted my data."

Social media	
Participants report to have experienced a social engineering attack via social media.	I: "Have you ever experienced an attack by e-mail?" T8: "Not yet, actually. So only on Facebook yet."
Experiences with attacks besides social engineering	
Participant reports to have experienced an attack that was no social engineering attack.	T10: "I also survived an attack, which also has to do with a virus, but not directly via e-mail, but my e-mail was also used for this. "
Consequences of attacks	
Participants tell about consequences for them that followed from social engineering attack(s). Can also be the absence of consequences. Includes influence on further use of e-mails or online behavior.	I: "Has the attack influenced the way you deal with emails?" T12: "That I just pay more attention to who I write to and ask again if such attacks happen. What I should do or whether the person can help me."
Yes	
Participant reports consequences that followed an attack. Can be financial, social, emotional, etc.	I: "Did the attack have any consequences for you? Did anything happen afterwards?" T12: "Yes. I fell into a very bad illness, I got depressed."
No	
Participant reports that the attack(s) had no consequences for them.	I: "Did the attack have any consequences for you? " T1: "No."
Influenced e-mail usage	
Participant describes that the experience with attacks influenced their e-mail usage.	I: "Has the attack influenced the way you deal with emails?" T12: "That I just pay more attention to who I write to and ask again if such attacks happen. What I should do or whether the person can help me."

Assessment strategies	
Includes everything the participants do to assess the trustworthiness of e-mails.	T6: "Or you know how they write or there are a few mistakes in the text. The attackers sometimes write, um / sometimes wrong messages or something. Words are missing in there and so on."
Suspicious clues	
Participants mention clues that they designate as useful to identify malicious e-mails. Can be e.g. suspicious sender address, urgency, links, etc.	T1: "Well, I'm always / so personally I'm always careful when it comes to account data. (. . .) And private data."
Suspicious sender	
Participant names sender address as indicator for suspiciousness. Can be an unknown sender, address does not fit to content, spoofed, etc.	T2: "If I don't know the addresses, then... (...) if there are so many letters and that, then... I don't open it."
Implausibility	
Participant assesses parts of the e-mails content as implausible and thus the e-mail as potentially suspicious.	T10: "For example, as I had it again today, which I also deleted straight away, I realized that there was some kind of subscription playing around. But then I also realized that I don't have anything like that."
Linguistic inaccuracy	
Participant describes the style of writing or formulations as suspicious. Can be grammar errors, generic addressing, etc.	T6: "Or you know how they write or there are a few mistakes in the text. The attackers sometimes write, um / sometimes wrong messages or something. Words are missing in there and so on."

Demands confidential data	
Participants name the asking for confidential data as suspicious. Confidential data can be e.g. address, name, bank account number etc.	T3: For example, I would ask for the points that are here, full name and exact address. That would be my exact home address, for example. And the telephone number would be my landline number in this case. I would on this e-mail for example / this doesn't seem quite serious to me."
Date or time	
Participants designate dates or time specifications in messages as suspicious.	T3: "Some people or, often, give a time, then I would be careful and say: No. I would say that seems strange to me."
Urgency/threat	
Participant designates urgency/threat in messages as suspicious.	T10: "My thoughts on this e-mail are that the data is pretty much forced to be given directly." I: "And what do you think about that?" T10: "Yes, I get an uncomfortable feeling about that."
Asking for money	
Participant designates asking for money in messages as suspicious.	T4: "How they write it down. That's how much money we want, if not he threatens something. I think that's bad."
Pictures	
Participants say pictures in messages are an indicator for suspiciousness.	T10: "Yes, whether there are any buttons here, for example... or images like the DPD thing."
Similarity to known attacks	
Participants use their knowledge about attacks to assess messages they get by comparing them to attacks they know.	T2: "That's difficult. Because I think there was an e-mail like that in the news. That you shouldn't reply to it."

Link	
Participant names in e-mail contained links or attachments one is asked to click on as suspicious.	T10: "Yes, whether there are any buttons here, for example... or images like the DPD thing."
Mentions data protection policy	
Participants designates an e-mail as suspicious because it is about data protection policy.	T6: "Because I would be sure that my data and so on would be given out." I: "Mhm (agreeing)." T6: "Because it says data protection lines and they would then have my data."
Trust clues	
Participants mention clues that they designate as useful to identify trustworthy e-mails. Can be e. g. trusted sender address, professional style of writing etc.	T4: "How they write it down. That's how much money we want, if not he threatens something. I think that's bad."
Trusted sender	
Participants state that a trusted sender is a clue for trustworthiness of the e-mail.	T2: "If I know them, yes. So if I knew the (...) If I knew the sender, I think I would click."
Unsuspicious concern	
Participants name unsuspicious content of messages as indicator for its trustworthiness.	T5: "Because it says nothing about attacking. So it doesn't say anything about attacking or what could happen or anything else. It just says, because of data protection and advertising."
Fits in situation	
Participants describe to trust messages when the content suits to the situation, e. g. message from delivery service when they ordered something.	T2: "I would first have to check whether I would receive a parcel at all, whether I had ordered anything. If I had ordered something, then it would be trustworthy for me."

Linguistic accuracy	
Participants designate an professional style of writing, the absence of spelling errors, a personal salutation etc. as clue for trustworthiness of a message.	T3: "So you can tell that it’s. . . what do you call it, that it’s written more professionally. That there’s no fraud or deception behind it."
Picture	
Participant explains to interpret pictures in an e-mail as an indicator for its trustworthiness.	T3: "Because there’s also a photo with the original delivery bus. (. . .) Because this photo is also included."
Friendly wording	
Participant explains to interpret friendly wording in an e-mail as a clue for its trustworthiness.	I: "What do you mean it’s good down there?" T4: "Because it’s so nice." I: "Mhm (agreeing). T4: "I would also write that to my family from time to time."
Speak with others	
Participants use their knowledge about attacks to assess messages they get by comparing them to attacks they know.	T2: "That’s difficult. Because I think there was an e-mail like that in the news. That you shouldn’t reply to it."
Family member	
Participants state to speak with family members for assessing the trustworthiness of messages.	I: "Mhm (agreeing). And how would you do that, find out?" T12: "Either ask friends who are also familiar with this kind of thing. . . Ask family members. . . ask people at work who know about it."
Caregiver	
Participants state to speak with caregivers for assessing the trustworthiness of messages.	I: "Okay. And then what would you talk to the employees about?" T4: "That I get e-mails and that I don’t know which e-mails I should answer or not."

Friend	
Participants state to speak with friends for assessing the trustworthyness of messages.	T1: "And I've also asked around among friends with similar experiences."
Colleague	
Participants state to speak with colleagues for assessing the trustworthyness of messages.	T12: "First of all. . . to find out whether it's all really true. Because. . . it could be that it's not true at all." I: "Mhm (agreeing). And how would you do that, find out?" T12: "Either ask friends who are also familiar with this kind of thing. . . Ask family members. . . ask people at work who know about it."
Examine links	
Participants explain to examine links to check on a messages' legitimacy.	T10: "If then I would, as I might still do, simply not press it properly and then go to "examine". An extra window will then appear with all the source code, right? You can usually look there to see what else is in there."
Online research	
Participants state to do online research for assessing the trustworthyness of messages.	T6: "Then you know where, who wrote it or where it came from. Or check whether it's really from the company or the person." I: "Mhm (agreeing). How would you check that?" T6: "(. . .) That's difficult. Maybe look on the internet or something like that."
Call alleged sender	
Participant says they would call the alleged sender to approve the trustworthiness of the message.	T2: "Because if I have something, I call the savings bank or the bank straight away anyway to see if it's really true, or I go there in person."

Write back to sender	
Participants explain they would write back to the sender of a message to assess its trustworthiness.	I: "And what would you do to find out if the email is an attack?" T5: "Well then I would just, um, to the perpetrators, write back who it was."
Handling incidents	
Inlcudes everything the participants do to handle suspicious e-mails or other forms of social engineering incidents (e. g. phone calls ect.).	I: "Then, have you ever received an email where you weren't sure whether it was an attack or not?" T6: "Well, I didn't respond to it. I deleted it immediately."
Delete message	
Participant explains to delete messages they identify as suspicious.	I: "Then, have you ever received an email where you weren't sure whether it was an attack or not?" T6: "Well, I didn't respond to it. I deleted it immediately."
Ignore message	
Participant explains to ignore messages they identify as suspicious.	T2: "Well, I read it, but I didn't answer it."
Block sender	
Participant names blocking of the sender as strategy to handle incidents with suspicious contacts.	I: "Okay. And how did you react to this message?" T1: "I first played along with the game and then blocked the person."
Juridical steps	
Participants explain they had or would take legal action as a consequence of a suspicious message.	T4: "Mhm (thoughtfully). That I tell the employees that I will go to the police and show them, the police, this e-mail."
Being careful	
Participant names 'being careful' or similar as strategie to cope with suspicious e-mails.	T11: "Yes, I handle it carefully, carefully. First ask what it is. Yes, what is it?"

Get support	
Participant reports to get help from other people when having to handle an incident with a suspicious message.	I: "And what would you do to find out if the email is an attack?" T5: "Well then I would just, um, to the perpetrators, write back who it was."
Caregiver	
Participants say they get support in handling suspicious messages from caregivers.	I: "And if you were to receive an e-mail like that, i. e. an attack, how would you react to it? T4: "First of all, I would let the staff know that I'm getting calls or e-mails."
Friend	
Participants say they get support from friends to handle suspicious messages.	I: "And have you ever received an e-mail that you weren't sure whether it was an attack or not?" T8: "Yes, I've received one before and I just asked my friend."
Family member	
Participants say they get support in handling suspicious messages from family members.	T7: "From what I've read, that sounds more like a threat to me. I would either show them to my parents when I'm with my parents, or to the caregivers here, and then talk about it."
Colleagues	
Participants say they get support in handling suspicious messages from colleagues.	I: "Shown straight away. And who do you show an e-mail like this to when you say you /" T11: "My colleagues or sometimes my boss in [workplace]. Also sometimes show [name]."
Individual factors	
Includes everything in the context of social engineering attacks that is related to the participants individual knowledge, habits, attitudes or personality.	T7: "E-mail security, um... I don't like it at all when it comes to e-mails, when it comes out so publicly. So in the world at large."

E-mail usage	
Statements about the participants e-mail usage. How often do they use e-mails and for which tasks.	I: "And how often do you use e-mail?" T4: "Well, once or twice a week."
Few times per year	
Participant states using e-mail only a few times per year.	I: "Would you say that happens several times a month or a few times a year?" T3: "A few times a year I would tend to say. . . "
Few times per month	
Participant states using e-mail a few times per month.	T10: "Sometimes it's like this, sometimes like this. I: "Yes, and so on average maybe several times a week or only every few weeks...?" 10: "Yes, maybe every few weeks."
Several times per week	
Participant reports using e-mails several times per week.	I: "And how often do you use e-mail?" T4: "Well, once or twice a week."
Daily	
Participant reports using e-mails daily.	I: "And how often do you use e-mail?" T1: "Daily."
Online services or shops	
Participant says using e-mails to use online services or shops.	I: "And what kind of things do you use e-mails for?" T5: "Yes, for example, when I register for something, I have to enter my e-mail address."
Private communication	
Participant says using e-mails for private communication.	I: "And what kind of things do you use e-mail for?" T1: "Private e-mail correspondence."

Professional communication	
Participant says using e-mails for professional communication.	T2: "At work, I also answer and write e-mails when I'm sitting in the front office."
Communication with public authorities	
Participant says using e-mails for communication with public authorities.	I: "Okay. And what kind of things do you use e-mail for?" T1: "Private e-mail correspondence. Then with the public authorities, for example."
Unclear	
Text passages regarding the e-mail use of participants where it is unclear what the participants mean or they say they do not know.	T4: "When I write what I need or what I don't need. I also get data that is so external and then I delete it again and sometimes it comes back, sometimes not, sometimes again." I: "Okay. And is that when you write emails privately with someone, i. e. private contact or professional contact?" T4: "I don't even know anymore."
Understanding of clues	
This code refers to the answers of the participants on the questions for the specific clues 'sender address', 'link' and 'urgency' which are asked in the last part of the interview.	I: "One possibility would be to take a close look at the e-mail address from which the e-mail was sent." T3: "That's right." I: "Why do you think that might be useful?" T3: "It would make it easier to trace."

Sender address	
Answers of the participants on the question for their understanding of the specific clue ′sender address′ asked in the last part of the interview.	I: "Another possibility would be to take a closer look at the e-mail address from which the e-mail was sent. Why do you think that could be useful?" T8: "Useful?" I: "To recognize an attack." T8: "Yes, then everyone has a different e-mail address."
Correct	
Participant gives a correct explanation for the clues ′sender address′.	T10: "Because the sender addresses were actually always made by the attackers themselves. For example, websites that may not even exist. Or the domain in general, I can see that quite easily." I: "Mhm (agreeing). How do you see that then?" T10: "Here, for example, if it says CZ or something like that on the back. Or CN or whatever."
Incomplete	
Participant gives an incomplete explanation for the clue ′sender address′.	I: "So, one possibility would be to take a close look at the e-mail address from which the e-mail was sent. Why do you think that could be useful? To recognize an attack." T12: "Mhm (thoughtfully) (...) Firstly, from which country... because sometimes the attacks also come from other countries. Not always, but often enough. Um... Yes."

No explanation	
Participant gives no explanation for the clue ’sender address’.	I: "One thing you can do is to take a close look at the e-mail address from which the e-mail was sent. Can you imagine why that might be useful?" T9: "Mhm (thoughtfully) (...) I don’t know anything about that."
Links	
Answers of the participants on the question for their understanding of the specific clue ’link’ asked in the last part of the interview.	I: "Another thing you can do is to look closely at links in e-mails. Why do you think that could be useful? (...) Okay, you’re shaking your head?" T2: "I don’t know..."
Correct	
Participant gives a correct explanation for the clues ’link’.	I: "And if emails contain a link, you should always take a close look at it. Why do you think that could be useful?" T1: "(...) Because the link can be dubious, so to speak?" I: "Mhm (agreeing)." I: "Yes." I: "And what does dubious mean to you?" T1: "For me it means that it doesn’t come from the company, so to speak, but was set up for the purpose of abuse."
Incomplete	
Participant gives an incomplete explanation for the clues ’link’.	I: "Why do you think that could be useful?" T11: "You never know what’s behind it, or anything. Whether there’s an attack behind it or something else." I: "What could be behind it, for example / So what do you mean by hidden or concealed?" T11: "(...) I don’t know at the moment."

No explanation	
Participant gives no explanation for the clue ’link’.	I: "And if the e-mail contains a link, you should also take a close look at the link. Why do you think that could be useful?" T8: "The link? Well... I’m not getting any further."
False explanation	
Participant gives a false explanation for the clue ’link’.	I: "Another thing you can do is, if an e-mail contains a link, you can take a close look at the link. Why do you think that could be useful?" T6: "Yes, it’s a bit useful for people who have a disability, of course. Then they know immediately where they can look. Because it’s often clarified via the internet with people who don’t have any experience with it yet."
Urgency	
Answers of the participants on the question for their understanding of the specific clue ’urgency’ asked in the last part of the interview.	T1: "Because as you just said, the pressure build-up / normally, normally you argue for account freezes. Because you’re not, you’re no longer solvent or something, right? Or get counselors, but not just like that without argument."
Correct	
Participant gives a correct explanation for the clues ’urgency’.	I: "And why do you think that’s suspicious?" T1: "Because as you just said, the pressure build-up / normally, normally you argue for account freezes. Because you’re not, you’re no longer solvent or something, right? Or get counselors, but not just like that without argument."

Incomplete	
Participant gives an incomplete explanation for the clue ’urgency’.	T5: "That um / For example, that’s just a threat. If someone says, quick, quick, quick, and the person can’t do it quickly, that’s a warning, a threat." I: "Mhm (agreeing). And why exactly is that perhaps an indication of an attack?" T5: "Because the perpetrator really wants to have this e-mail address."
No explanation	
Participant gives no explanation for the clue ’urgency’.	I: "Why do you think that’s suspicious?" T9: "(...) Um, he could always write worse...or something. And you’re not exactly sure whether you can let that happen." I: "Yeah, what exactly do you mean?" T9: "Yes, that’s always so difficult to answer."
Insecurity with e-mails/technique	
Participant expresses insecurity with e-mails and/or technique in general.	T2: "Um...I’m not familiar with the technology anyway. And that’s why I always get help from someone else who can help me somehow. And that / as I said, I don’t know much about technology. I’m always afraid that I’m doing something wrong anyway."
Fear of attacks	
Participant expresses fear of being attacked online.	T2: "With emails, I’m always...I’m always afraid that I’ll somehow get a virus on my cell phone. Or that it will be hacked."

Attitude towards security/privacy	
Participant says something revealing information about their attitude towards privacy/security.	T7: "E-mail security, um...I don't like it at all when it comes to e-mails, when it comes out so publicly. So in the world at large."
Knowledge about attacks	
Participant reports knowledge about online attacks. Can base on own experiences or other, like e. g. speaking with friends, read about it or similar. Can be missing knowledge.	I: "Why do you think that's suspicious?" T9: "(...) Um, he could always write worse...or something. And you're not exactly sure whether you can let that happen." I: "Yeah, what exactly do you mean?" T9: "Yes, that's always so difficult to answer."
Missing knowledge	
Participants express a lack of knowledge about cyber security.	I: "What are your thoughts on the security of e-mails?" T4: "I don't know anything about that."
Attacks	
Participant reports missing knowledge with regard to cyber attacks.	I: "Do you know of any attacks by e-mail? (...) Have you ever heard of anything?" T9: "Nope."
Things on computer	
Participant reports having a problem with something they do not want happening on their device, for example spam.	T7: "And I also don't know how to get rid of the, uh, this e-mails that I always get, how I can best get rid of it."

Other	
Participant reports missing knowledge about something security related but not attacks or things happening on their computer.	T3: "I think we once did a test like this / Somewhere I once did a test like this. There are differences. Because you can / I think you can tell whether it's a real link, i. e. a reputable one, so no fake or no..." (...) I: "Mhm (agreeing)." T3: "But I don't really know how to tell the difference like that anymore."
Social engineering	
Participant shows knowledge about social engineering attacks.	T1: "Not through an e-mail, but I just remembered Facebook. If you've commented on something or something like that, there are posts there. That trustworthy people, both men and women, then write, "How are you?" and then more and more trust is gained, right up to account details, which are then requested."
Grandchildren trick	
Participant shows knowledge about the 'grandchildren trick'.	T6: "That you can use the internet / Because I've also heard about this, what's the name of this one? Where you write to the grandma and suddenly it's not the grandchild."
Malware	
Participant shows knowledge about malware attacks.	I: "Do you know of any attacks through emails?" T8: "Virus."

Account hacking	
Participant shows knowledge about account hacking.	T5: "For example. . . For example, if someone logs into my, my computer's e-mail and someone logs in, (incomprehensible word) or whatever it's called. Exactly, it can also happen that someone logs in to my account, for example, and it doesn't work. So strangers who want to try to access the e-mail."
Fake accounts	
Participant shows knowledge about fake accounts.	T6: "And I mean, there are no real people on dating apps, more like robots, like AIs."
Social media	
Participants talk about the possibility of being attacked on social media platforms.	T3: "I can say that I have never registered for / on Facebook. That means I can't have received a false message from someone like that via Facebook."
Dating apps	
Participants talk about the possibility of being attacked on dating apps.	T6: "Oh yes, especially dating apps. Getting to know people that way. That's especially / So for young people and adults. That's bad, because they're usually photos that have simply been stolen."
Source	
Participants talk about where they got their knowledge about cyber securits from.	T2: "And the, someone / I think I did a smartphone course and I just looked to see what it was."
Self-assessment	
Participant expresses assessment of their own capabilities to detect phishing attacks.	I: "How difficult or easy do you find it to recognize attacks by e-mail?" T6: (. . .) "Yeah, like that, average. Normal, in the middle."

Easy	
Participants say that it is easy for them to detect phishing.	I: "How difficult or easy do you find it to recognize attacks by email?" T10: "Well, I personally find it easy because you can usually tell from the email, from the address."
Medium	
Participants say that it is medium difficult for them to detect phishing.	I: "How difficult or easy do you find it to recognize attacks by e-mail?" T6: (. . .) "Yeah, like that, average. Normal, in the middle."
Hard	
Participants say that it is hard for them to detect phishing.	I: "How difficult or easy do you find it to recognize attacks by e-mail?" T2: "Difficult."
Not know	
Participants say that they can not tell if it is hard or easy for them to detect phishing.	I: "How difficult or easy do you find it to recognize attacks by e-mail?"(. . .) T11: "Mhm (thoughtfully) (. . .) I don't know right now."
Other	
Text passages about individual factors that do not fit into one of the other categories.	T6: "But sometimes I still fall for it." I: "Mhm (agreeing)." T6: "Yes, sometimes it arouses curiosity, of course."
Challenge	
Includes everything were the participants name as being difficult for them or what can be categorised as problematic in the context of e-mail security.	T5: "Um. . . My e-mail thoughts are just that (. . .) um, I don't know myself right now. But. . . that (. . .) It's difficult to explain right now."

Problems with reading/understanding text	
Participant shows problems to fully understand a text or reports difficulties with reading.	T4: "Because. . . it says something / because I don't understand it. And I always need help. I have such a / also a bit reading difficulties."
General reading difficulties	
Participant reports to have difficulties with reading.	T4: "Because. . . it says something / because I don't understand it. And I always need help. I have such a / also a bit of a reading disability."
False interpretation of text	
Participants' statement implies that they interpreted the text differently from what was actually written to an amount that shows a severe misunderstanding of the text.	I: "And what are your thoughts on this e-mail?" [e-mail 3, which asked for an address, not mentioned any money] T11: "(. . .) That I should give money." (. . .) I: "Why?" T11: "Because they want money."
Unknown word	
Participant says that they do not know a word or asks for the meaning of a word.	T12: "What is 'metaproducts'? I've never heard of it before."
English	
Participant asks for the meaning of an English word or says that they does not know the meaning of an English word.	T3: "Oh wait, tracking, what does that mean here?"
Expressed difficulty	
Participants express some sort of difficulty during the interview.	I: "How difficult or easy do you find it to recognize attacks by e-mail?" T2: "Difficult."

Problem explaining what they mean	
Participant expressed difficulties to explain what they mean.	T5: "Um. . . My e-mail thoughts are just that (. . .) um, I don't know myself right now. But. . . that (. . .) It's difficult to explain right now."
Self-assessment	
Participant explains that they find it hard to identify malicious e-mails.	I: "How difficult or easy do you find it to recognize attacks by e-mail?" T2: "Difficult."
Difficult question	
Participant says that they find a question difficult to answer or to understand.	T9: "Mhm (thoughtfully), have to think for a moment. (. . .) That's kind of a difficult question."
Other	
Participants expressed difficulties that can not be categorised into the other codes.	T12: "That's because I'm not yet very good at a lot of things with e-mail. And that's why someone else always does it for me."
Problematic behavior	
Participants report behavior which is problematic in the context of cybersecurity.	T3: "Oh wait, tracking, what does that mean here?"
Definition of trusted sender	
Participants' statement implies a somehow problematic definition of 'trusted sender'. e. g. when considering DPD as trustworthy because they know DPD but without looking at the concrete e-mail address.	T4: "That they are trustworthy." I: "Okay. And why do you think that?" T4: "Because I used to like ordering things there. And they also sent my father's e-mail over."

Plausibility as only clue	
Participant would assess an e-mail as trustworthy only because its' content appears plausible without looking at other clues.	I: "But do you think that this e-mail could be an attack or that it is trustworthy?" T2: "(...) I would first have to check whether I had received a parcel at all, whether I had ordered anything. If I had ordered something now, then it would be trustworthy for me."
Write back to sender	
Participant explains that they would write back to the sender of an suspicious e-mail to find out about its' trustworthiness.	[about e-mail 1] T6: "Then, of course, I write to the person themselves to find out whether it's really genuine or whether they're deceiving me or something. So first write in a reasonable tone. Not like that..."
Support suggestion	
Includes everything the participants say that would help them to deal with e-mail attacks.	I: "What would help you to recognize attacks by e-mail?" T11: "If you went to someone immediately and showed them that first."
Support person	
Participant says that it would help them to have a supporting person.	I: "What would help you to recognize attacks by e-mail?" T11: "If you went to someone immediately and showed them that first."
Supporting software	
Participant says that it would help them to have a software supporting them in detecting phishing.	T2: "What would help me? (...) Yes, somehow, that they warn me with a red button or with a red...something red where it stops or doesn't open. I don't know. Some kind of hint maybe."

Education	
Participant says that education would be helpful for them to detect phishing.	I: "What would help you to recognize email attacks?" T12: "That people get better informed about e-mail attacks."
Contradiction	
Code to mark contradictions in the interviews.	I: "Yes, do you know of any attacks by e-mail?" T12: "No." [but previously described an attack]
Unclear	
Text passages where it is unclear what the participants mean.	I: "And what would you do to find out if the e-mail is an attack?" T4: "Go to the site where you get the e-mails and then see if there are any people hacking my e-mails."

D.2 CODEBOOK FOR THE ANALYSIS OF THE E-MAIL ASSESSMENT TASK

E-mail 1	
Everything that the participant says about e-mail 1 in the e-mail assessment task.	(...) [T1 reads e-mail 1] 00:07:43-00:08:13 T1: "Jo." I: "Okay. All right, no questions?" T1: "Yes, yes." I: "Very good. Then the first question. Have you ever received a similar e-mail before?" T1: "Yes, I have." ...
E-mail 2	
Everything that the participant says about e-mail 2 in the e-mail assessment task.	(...) [T2 reads e-mail 2] 00:13:26-00:14:02 T2: "Mhm (agreeing)." I: "Are you through?" T2: "Yes." I: "Okay. Have you ever received a similar e-mail before?" T2: "No." ...
E-mail 3	
Everything that the participant says about e-mail 3 in the e-mail assessment task.	(...) [T4 reads e-mail 3] 00:16:27-00:16:32 T4: "That's from DPD." I: "Mhm (agreeing)." T4: "I think they want the parcel to arrive or not be damaged. I think that here at DPD, it's good." ...

ET - assessment	
The participants' assessment of the example e-mails in the e-mail task (ET).	T10: "I do believe that this is an attack."
Attack	
Participant thinks an e-mail in the assessment task is an attack.	T10: "I do believe that this is an attack."
Trustworthy	
Participant thinks an e-mail in the assessment task is trustworthy.	T1: "It is definitely serious."
Uncertain	
Participant is not sure if an e-mail in the assessment task is trustworthy or not.	T6: "So a bit / (incomprehensible 00:20:15-00:20:19) So trustworthy, so a bit. Half in that way."
ET - reasonableness of choice	
Text passages that contain justifications of the participants' assessment of the example e-mails in the assessment task.	T3: "Because there's also a photo with the original delivery bus."
Reasonable	
Participant gives reasonable justification for assessment of an e-mail in the assessment task.	[about e-mail 2] T1: "Because I think that, depending on her gender, Kim is a user or a user who is simply a client, I'll say, or a client in Meta."
Partially reasonable	
Participant gives a partially reasonable justification for assessment of an e-mail in the assessment task.	T12: "I wouldn't accept the money. Because it's a stranger you don't know. You don't know whether there are any debts or anything else in the inheritance."
Not reasonable	
Participant gives a justification for assessment that is not reasonable.	T3: "Because there's also a photo with the original delivery bus."

ET - clicking/responding behavior	
Participant says wheher they would click/respond or not to the e-mail in the assessment task.	I: "And the e-mail asks you to reply. Would you answer it?" T1: "No, definitely not."
Yes	
Participant says they would click/answer.	T5: "Well, I would click on it, yes."
No	
Participant says they would not click/answer.	I: "And the e-mail asks you to reply. Would you answer it?" T1: "No, definitely not."
Uncertain	
Participant says they is uncertain if they would click/answer.	I: "Right, while we're on the subject of the button, would you click on it?" T7:" Phew. . . I'm rather unsure about that now."
ET - reading time	
Time the participant spend to read the e-mails in the assessment task. Can be either short, medium or long. Categories are different for every e-mail, depending on the respective reading times for each e-mail. Upper quantile: long; lower quantile: short; all in between: medium.	(...) [T6 reads e-mail 3] 00:18:51-00:19:12
Short	
E-Mail 1: reading time between 0 and 22 sec E-Mail 2: readingtime between 0 and 20 sec E-Mail 2: readingtime between 0 and 14 sec	

Medium
E-Mail 1: readingtime between 23 and 54 sec
E-Mail 2: readingtime between 21 and 43 sec
E-Mail 3: readingtime between 15 and 25 sec
Long
E-Mail 1: readingtime more than 54 sec
E-Mail 2: readingtime more than 43 sec
E-Mail 3: readingtime more than 25 sec

BIBLIOGRAPHY

[1] D. Lussier-Desrochers, C. L. Normand, A. Romero-Torres, Y. Lachapelle, V. Godin-Tremblay, M.-È. Dupont, J. Roux, L. Pépin-Beauchesne, and P. Bilodeau, "Bridging the digital divide for people with intellectual disability", *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, vol. 11, no. 1, May 2017. DOI: 10.5817/CP2017-1-1.

[2] C.-N. Shpigelman and C. J. Gill, "How do adults with intellectual disabilities use facebook?", *Disability & Society*, vol. 29, no. 10, pp. 1601–1616, 2014. DOI: 10.1080/09687599.2014.966186.

[3] S. J. Macdonald and J. Clayton, "Back to the future, disability and the digital divide", *Disability & Society*, vol. 28, no. 5, pp. 702–718, 2013. DOI: 10.1080/09687599.2012.732538.

[4] The 111th United States Congress, *Twenty-first century communications and video accessibility act of 2010'*, [Online]. Available: https://www.govinfo.gov/content/pkg/PLAW-111publ260/pdf/PLAW-111publ260.pdf (last accessed on May 20, 2024)., 2010.

[5] European Parliament and the council of the european union, *Directive (eu) 2019/882 of the european parliament and of the council of 17 april 2019 on the accessibility requirements for products and services*, [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0882 (last accessed on May 20, 2024), 2019.

[6] World Wide Web Consortium, *Web content accessibility guidelines (WCAG) 2.2*, https://www.w3.org/TR/WCAG22/ (last accessed on May 2, 2024), 2023.

[7] World Wide Web Consortium, *User agent accessibility guidelines (UAAG) 2.0*, https://www.w3.org/TR/UAAG20/ (last accessed on May 2, 2024), 2015.

[8] World Wide Web Consortium, *Authoring tool accessibility guidelines (ATAG) 2.0*, https://www.w3.org/TR/ATAG20/ (last accessed on May 2, 2024), 2015.

[9] European Commission and Directorate-General for Employment, Social Affairs and Inclusion and S. Grammenos, *The digital transition and persons with disabilities – Statistics on use of electronic durables, digital skills, work and participation*. Publications Office of the European Union, 2021. DOI: doi/10.2767/646246.

[10] M. Kulkarni, "Digital accessibility: Challenges and opportunities", *IIMB Management Review*, vol. 31, no. 1, pp. 91–98, 2019. DOI: https://doi.org/10.1016/j.iimb.2018.05.009.

[11] K. Renaud and L. Coles-Kemp, “Accessible and inclusive cyber security: A nuanced and complex challenge”, *SN Computer Science*, vol. 3, no. 5, p. 346, Jun. 2022. DOI: 10.1007/s42979-022-01239-1.

[12] Y. Wang, “The third wave? inclusive privacy and security”, in *Proceedings of the 2017 New Security Paradigms Workshop*, ser. NSPW ’17, Santa Cruz, CA, USA: Association for Computing Machinery, 2017, pp. 122–130. DOI: 10.1145/3171533.3171538.

[13] European Union Agency for Cybersecurity, “ENISA threat landscape 2023: July 2022 to June 2023”, 2023, [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023; (last accessed on Mar. 20, 2024).

[14] Federal Bureau of Investigation, “Internet crime report 2023”, 2023, [Online]. Available: https://www.ic3.gov/media/PDF/AnnualReport/2023_IC3Report.pdf; (last accessed on May 5, 2024).

[15] F. Mouton, L. Leenen, M. M. Malan, and H. S. Venter, “Towards an ontological model defining the social engineering domain”, in *ICT and Society*, K. Kimppa, D. Whitehouse, T. Kuusela, and J. Phahlamohlaka, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 266–279.

[16] K. Jansson and R. von Solms, “Phishing for phishing awareness”, *Behaviour & Information Technology*, vol. 32, no. 6, pp. 584–593, 2013. DOI: 10.1080/0144929X.2011.632650.

[17] Anti-Phishing Working Group, “Phishing activity trends report, 1st quarter 2024”, 2024, [Online]. Available: https://docs.apwg.org/reports/apwg_trends_report_q1_2024.pdf?_gl=1*kx572t*_ga*MTA2NjQxNDYyOS4xNzE2MTEwOTY4*_ga_55RF0RHXSR*MTcxNjExMDk2OC4xLjEuMTcxNjExMDk4NC4wLjAuMA.

[18] V. N. Heitplatz, C. Bühler, and M. R. Hastall, “Caregivers’ influence on smartphone usage of people with cognitive disabilities: An explorative case study in Germany”, in *Universal Access in Human-Computer Interaction. Multimodality and Assistive Environments*, M. Antona and C. Stephanidis, Eds., Cham, Switzerland: Springer International Publishing, 2019, pp. 98–115.

[19] H. Chalghoumi, V. Cobigo, C. Dignard, A. Gauthier-Beaupré, J. W. Jutai, Y. Lachapelle, J. Lake, R. Mcheimech, and M. Perrin, “Information privacy for technology users with intellectual and developmental disabilities: Why does it matter?”, *Ethics & Behavior*, vol. 29, no. 3, pp. 201–217, Apr. 2019. DOI: 10.1080/10508422.2017.1393340.

[20] D. D. Chadwick, ""You want to know that you're safe": Experiences of risk, restriction and resilience online among people with an intellectual disability", *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, vol. 16, no. 3, Jul. 2022. DOI: 10.5817/CP2022-3-8.

[21] J. S. Downs, M. Holbrook, and L. F. Cranor, "Behavioral response to phishing risk", in *Proceedings of the Anti-Phishing Working Groups 2nd Annual ECrime Researchers Summit*, ser. eCrime '07, Pittsburgh, Pennsylvania, USA: Association for Computing Machinery, 2007, pp. 37–44. DOI: 10.1145/1299015.1299019.

[22] B. Harrison, E. Svetieva, and A. Vishwanath, "Individual processing of phishing emails: How attention and elaboration protect against phishing", *Online Information Review*, vol. 40, no. 2, pp. 265–281, Apr. 2016. DOI: 10.1108/OIR-04-2015-0106.

[23] WebAIM, *Cognitive disabilities*, https://webaim.org/articles/cognitive/ (last accessed on Apr. 15, 2024), 2020.

[24] World Health Organization, "WHO guideline: Recommendations on digital interventions for health system strengthening", 2019, [Online]. Available: https://iris.who.int/bitstream/handle/10665/108010/e94506.pdf (last accessed on Mar. 20, 2024).

[25] V. Cluley, "From "learning disability to intellectual disability" - perceptions of the increasing use of the term "intellectual disability" in learning disability policy, research and practice", *British Journal of Learning Disabilities*, vol. 46, no. 1, pp. 24–32, 2018. DOI: https://doi.org/10.1111/bld.12209.

[26] World Health Organization and the United Nations Children's Fund (UNICEF), "Global report on children with developmental disabilities: From the margins to the mainstream.", 2023, [Online]. Available: https://www.unicef.org/media/145016/file/Global-report-on-children-with-developmental-disabilities-2023.pdf (last accessed on May 20, 2024).

[27] R. L. Schalock, R. Luckasson, and M. J. Tassé, "The contemporary view of intellectual and developmental disabilities: Implications for psychologists", *Psicothema*, vol. 31, no. 3, pp. 223–228, Aug. 2019. DOI: 10.7334/psicothema2019.119.

[28] Y. Yu, S. Ashok, S. Kaushik, Y. Wang, and G. Wang, "Design and evaluation of inclusive email security indicators for people with visual impairments", in *2023 IEEE Symposium on Security and Privacy (SP)*, 2023, pp. 2885–2902. DOI: 10.1109/SP46215.2023.10179407.

[29] S. Andrew, S. Watson, T. Oh, and G. W. Tigwell, "A review of literature on accessibility and authentication techniques", in *Proceedings of the 22nd International ACM SIGACCESS Conference on Computers and Accessibility*, ser. ASSETS '20, , Virtual Event, Greece, Association for Computing Machinery, 2020. DOI: 10.1145/3373625.3418005.

[30] J. Hayes, X. Li, and Y. Wang, ""I always have to think about it first": Authentication experiences of people with cognitive impairments", in *Proceedings of the 19th International ACM SIGACCESS Conference on Computers and Accessibility*, ser. ASSETS '17, Baltimore, Maryland, USA: Association for Computing Machinery, 2017, pp. 357–358. DOI: 10.1145/3132525.3134788.

[31] Y. Ma, J. Feng, L. Kumin, and J. Lazar, "Investigating user behavior for authentication methods: A comparison between individuals with down syndrome and neurotypical users", *ACM Trans. Access. Comput.*, vol. 4, no. 4, Jul. 2013. DOI: 10.1145/2493171.2493173.

[32] World Wide Web Consortium, *Web content accessibility guidelines (WCAG) 2.1*, https://www.w3.org/TR/WCAG21/ (last accessed on May 2, 2024), 2023.

[33] A. James, E. Draffan, and M. Wald, "Designing web-apps for all: How do we include those with cognitive disabilities?", in *Harnessing the Power of Technology to Improve Lives*, vol. 242, IOS Press, 2017, pp. 665–668. DOI: http://dx.doi.org/10.3233/978-1-61499-798-6-665.

[34] J. Clark, *To hell with WCAG 2*, https://alistapart.com/article/tohellwithwcag2/ (last accessed on Jan. 2, 2024), 2006.

[35] S. Gartland, P. Flynn, M. A. Carneiro, G. Holloway, J. d. S. Fialho, J. Cullen, E. Hamilton, A. Harris, and C. Cullen, "The state of web accessibility for people with cognitive disabilities: A rapid evidence assessment", *Behavioral Sciences*, vol. 12, no. 2, 2022. DOI: 10.3390/bs12020026.

[36] R. Hu and J. H. Feng, "Investigating information search by people with cognitive disabilities", *ACM Trans. Access. Comput.*, vol. 7, no. 1, Jun. 2015. DOI: 10.1145/2729981.

[37] B. Harrysson, A. Svensk, and G. I. Johansson, "How people with developmental disabilities navigate the internet", *British Journal of Special Education*, vol. 31, no. 3, pp. 138–142, 2004. DOI: https://doi.org/10.1111/j.0952-3383.2004.00344.x.

[38] R. Johnson and J. R. Hegarty, "Websites as educational motivators for adults with learning disability", *British Journal of Educational Technology*, vol. 34, no. 4, pp. 479–486, 2003. DOI: https://doi.org/10.1111/1467-8535.00344.

[39] T. Rocha, M. Bessa, L. Magalhães, and L. Cabral, "Performing universal tasks on the web: Interaction with digital content by people with intellectual disabilities", in *Proceedings of the XVI International Conference on Human Computer Interaction*, ser. Interacción '15, Vilanova i la Geltru, Spain: Association for Computing Machinery, 2015. DOI: 10.1145/2829875.2829897.

[40] H. Saggion, D. Ferrés, L. Sevens, I. Schuurman, M. Ripollés, and O. Rodrıguez, "Able to read my mail: An accessible e-mail client with assistive technology", in *Proceedings of the 14th International Web for All Conference*, ser. W4A '17, Perth, Western Australia, Australia: Association for Computing Machinery, 2017. DOI: 10.1145/3058555.3058567.

[41] B. Kelly, D. Sloan, S. Brown, J. Seale, H. Petrie, P. Lauke, and S. Ball, "Accessibility 2.0: People, policies and processes", in *Proceedings of the 2007 International Cross-Disciplinary Conference on Web Accessibility (W4A)*, ser. W4A '07, Banff, Canada: Association for Computing Machinery, 2007, pp. 138–147. DOI: 10.1145/1243441.1243471.

[42] B. Kelly, S. Lewthwaite, and D. Sloan, "Developing countries; developing experiences: Approaches to accessibility for the real world", in *Proceedings of the 2010 International Cross Disciplinary Conference on Web Accessibility (W4A)*, ser. W4A '10, Raleigh, North Carolina: Association for Computing Machinery, 2010. DOI: 10.1145/1805986.1805992.

[43] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge, "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*, ser. SOUPS '07, Pittsburgh, Pennsylvania, USA: Association for Computing Machinery, 2007, pp. 88–99. DOI: 10.1145/1280680.1280692.

[44] G. D. Moody, D. F. Galletta, and B. K. Dunn, "Which phish get caught? An exploratory study of individuals susceptibility to phishing", *European Journal of Information Systems*, vol. 26, no. 6, pp. 564–584, Nov. 2017. DOI: 10.1057/s41303-017-0058-x.

[45] T. Halevi, J. Lewis, and N. Memon, "Phishing, personality traits and facebook", 2013. DOI: 10.48550/arXiv.1301.7643.

[46] T. Halevi, N. Memon, and O. Nov, "Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks", *SSRN Electronic Journal*, 2015. DOI: 10.2139/ssrn.2544742.

[47] D. Modic and S. E. G. Lea, "How neurotic are scam victims, really? The big five and internet scams", presented at the 2011 Conference of the International Confederation for the Advance-

ment of Behavioral Economics and Economic Psychology, Exeter, United Kingdom, 2011. DOI: 10.2139/ssrn.2448130.

[48] M. Pattinson, C. Jerram, K. Parsons, A. McCormac, and M. Butavicius, "Why do some people manage phishing e-mails better than others?", *Information Management & Computer Security*, vol. 20, no. 1, N. Clarke, Ed., pp. 18–28, Mar. 2012. DOI: 10.1108/09685221211219173.

[49] D. Paraschiv, L. Toader, M. Nitu, and S. Negrea, "Internet fraud and phishing attacks - a european perspective", 7th BASIQ International Conference on New Trends in Sustainable Business and Consumption, Jun. 2021, pp. 394–400. DOI: 10.24818/BASIQ/2021/07/051.

[50] H. S. Jones, J. N. Towse, N. Race, and T. Harrison, "Email fraud: The search for psychological predictors of susceptibility", *PLOS ONE*, vol. 14, no. 1, pp. 1–15, Jan. 2019. DOI: 10.1371/journal.pone.0209684.

[51] A. Vishwanath, T. Herath, R. Chen, J. Wang, and H. R. Rao, "Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model", *Decision Support Systems*, vol. 51, no. 3, pp. 576–586, 2011. DOI: https://doi.org/10.1016/j.dss.2011.03.002.

[52] R. T. Wright, M. L. Jensen, J. B. Thatcher, M. Dinger, and K. Marett, "Research note—influence techniques in phishing attacks: An examination of vulnerability and resistance", *Information Systems Research*, vol. 25, no. 2, pp. 385–400, 2014. DOI: 10.1287/isre.2014.0522.

[53] N. L. Muscanell, R. E. Guadagno, and S. Murphy, "Weapons of influence misused: A social influence analysis of why people fall prey to internet scams", *Social and Personality Psychology Compass*, vol. 8, no. 7, pp. 388–396, 2014. DOI: https://doi.org/10.1111/spc3.12115.

[54] S. F. Verkijika, ""If you know what to do, will you take action to avoid mobile phishing attacks": Self-efficacy, anticipated regret, and gender", *Computers in Human Behavior*, vol. 101, pp. 286–296, 2019. DOI: https://doi.org/10.1016/j.chb.2019.07.034.

[55] J. C.-Y. Sun, S.-J. Yu, S. S. Lin, and S.-S. Tseng, "The mediating effect of anti-phishing self-efficacy between college students' internet self-efficacy and anti-phishing behavior and gender difference", *Computers in Human Behavior*, vol. 59, pp. 249–257, 2016. DOI: https://doi.org/10.1016/j.chb.2016.02.004.

[56] Y. Li, K. Xiong, and X. Li, "Applying machine learning techniques to understand user behaviors when phishing attacks occur", *EAI Endorsed Transactions on Security and Safety*, vol. 6, no. 21, Aug. 2019. DOI: 10.4108/eai.13-7-2018.162809.

[57] R. T. W. Matthew L. Jensen Michael Dinger and J. B. Thatcher, "Training to mitigate phishing attacks using mindfulness techniques", *Journal of Management Information Systems*, vol. 34, no. 2, pp. 597–626, 2017. DOI: `10.1080/07421222.2017.1334499`.

[58] E. Lastdrager, I. C. Gallardo, P. Hartel, and M. Junger, "How effective is anti-phishing training for children?", in *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, Santa Clara, CA: USENIX Association, Jul. 2017, pp. 229–239.

[59] V. Anandpara, A. Dingman, M. Jakobsson, D. Liu, and H. Roinestad, "Phishing IQ tests measure fear, not ability", in *Financial Cryptography and Data Security*, S. Dietrich and R. Dhamija, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 362–366.

[60] C. Jackson, D. R. Simon, D. S. Tan, and A. Barth, "An evaluation of extended validation and picture-in-picture phishing attacks", in *Financial Cryptography and Data Security*, S. Dietrich and R. Dhamija, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 281–293.

[61] P. Kumaraguru, Y. Rhee, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge, "Protecting people from phishing: The design and evaluation of an embedded training email system", in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '07, , San Jose, California, USA, Association for Computing Machinery, 2007, pp. 905–914. DOI: `10.1145/1240624.1240760`.

[62] M. Jakobsson and T.-F. Yen, "How vulnerable are we to scams?", *Black Hat*, 2015.

[63] D. Akhawe and A. P. Felt, "Alice in warningland: A Large-Scale field study of browser security warning effectiveness", in *22nd USENIX Security Symposium (USENIX Security 13)*, Washington, D.C.: USENIX Association, Aug. 2013, pp. 257–272.

[64] O. Sarker, A. Jayatilaka, S. Haggag, C. Liu, and M. A. Babar, "A multi-vocal literature review on challenges and critical success factors of phishing education, training and awareness", *Journal of Systems and Software*, vol. 208, p. 111 899, 2024. DOI: `https://doi.org/10.1016/j.jss.2023.111899`.

[65] C. Ramsten, L. Martin, M. Dag, and L. M. Hammar, "Information and communication technology use in daily life among young adults with mild-to-moderate intellectual disability", *Journal of Intellectual Disabilities*, vol. 24, no. 3, pp. 289–308, 2020. DOI: `10.1177/1744629518784351`.

[66] C. Normand and F. Sallafranque St-Louis, "Risks and benefits of internet use by people with neurodevelopmental disorders", *Annual Review of Cybertherapy and Telemedicine*, vol. 14, pp. 219–222, 2016.

[67] K. A. Ågren, A. Kjellberg, and H. Hemmingsson, "Digital participation? internet use among adolescents with and without intellectual disabilities: A comparative study", *New Media & Society*, vol. 22, no. 12, pp. 2128–2145, 2020. DOI: 10.1177/1461444819888398.

[68] P. Raghavendra, C. Hutchinson, E. Grace, D. Wood, and L. Newman, ""I like talking to people on the computer": Outcomes of a home-based intervention to develop social media skills in youth with disabilities living in rural communities", *Research in Developmental Disabilities*, vol. 76, pp. 110–123, 2018. DOI: https://doi.org/10.1016/j.ridd.2018.02.012.

[69] D. D. Chadwick and C. Fullwood, "An online life like any other: Identity, self-determination, and social networking among adults with intellectual disabilities", *Cyberpsychology, Behavior, and Social Networking*, vol. 21, no. 1, pp. 56–64, 2018. DOI: 10.1089/cyber.2016.0689.

[70] C. Jenaro, N. Flores, V. Vega, M. Cruz, M. C. Pérez, and V. A. Torres, "Cyberbullying among adults with intellectual disabilities: Some preliminary data", *Research in Developmental Disabilities*, vol. 72, pp. 265–274, 2018. DOI: https://doi.org/10.1016/j.ridd.2017.12.006.

[71] C. L. Normand and F. Sallafranque-St-Louis, "Cybervictimization of young people with an intellectual or developmental disability: Risks specific to sexual solicitation", *Journal of Applied Research in Intellectual Disabilities*, vol. 29, no. 2, pp. 99–110, 2016. DOI: https://doi.org/10.1111/jar.12163.

[72] P. C. M. Buijs, E. Boot, A. Shugar, W. L. A. Fung, and A. S. Bassett, "Internet safety issues for adolescents and adults with intellectual disabilities", *Journal of Applied Research in Intellectual Disabilities*, vol. 30, no. 2, pp. 416–418, 2017. DOI: https://doi.org/10.1111/jar.12250.

[73] F. A. Clements, D. D. Chadwick, and L. J. Orchard, "'I'm not the same person now': The psychological implications of online contact risk experiences for adults with intellectual disabilities", *New Media & Society*, 2023. DOI: 10.1177/14614448231217994.

[74] M. Borina, E. Kalister, and T. Orehovački, "Web accessibility for people with cognitive disabilities: A systematic literature review from 2015 to 2021", in *HCI International 2022 – Late Breaking Papers: HCI for Health, Well-being, Universal Access and Healthy Aging*, V. G. Duffy, Q. Gao, J. Zhou, M. Antona, and

C. Stephanidis, Eds., Cham, Switzerland: Springer Nature, 2022, pp. 261–276.

[75] A. Blandford, D. Furniss, and S. Makri, "Qualitative HCI research: Going behind the scenes", in (Synthesis Lectures on Human-Centered Informatics), Synthesis Lectures on Human-Centered Informatics. Springer International Publishing, 2016, ch. 3, pp. 23–31. DOI: 10.1007/978-3-031-02217-3.

[76] J. S. Downs, M. B. Holbrook, and L. F. Cranor, "Decision strategies and susceptibility to phishing", in *Proceedings of the Second Symposium on Usable Privacy and Security*, ser. SOUPS '06, Pittsburgh, Pennsylvania, USA: Association for Computing Machinery, 2006, pp. 79–90. DOI: 10.1145/1143120.1143131.

[77] M. Butavicius, R. Taib, and S. J. Han, "Why people keep falling for phishing scams: The effects of time pressure and deception cues on the detection of phishing emails", *Computers & Security*, vol. 123, 2022. DOI: https://doi.org/10.1016/j.cose.2022.102937.

[78] Bundesamt für Sicherheit in der Informationstechnik (BSI), *Wie erkenne ich Phishing-E-Mails und -Webseiten?*, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/Wie-erkenne-ich-Phishing-in-E-Mails-und-auf-Webseiten/wie-erkenne-ich-phishing-in-e-mails-und-auf-webseiten_node.html (last accessed on Mar. 27, 2024), n.d.

[79] Bundesamt für Verfassungsschutz, *Informationsblatt "Schutz vor Phishing"*, https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/wirtschafts-wissenschaftsschutz/2022-05-31-infoblatt-phishing.pdf (last accessed on Mar. 27, 2024), 2022.

[80] S. Misoch, "Qualitative Einzelinterviews", in *Qualitative Interviews*. Berlin, Germany: De Gruyter, Aug. 2019, pp. 65–136. DOI: 10.1515/9783110545982-201.

[81] M. Bailey, D. Dittrich, E. Kenneally, and D. Maughan, "The menlo report", *IEEE Security & Privacy*, vol. 10, no. 2, pp. 71–75, 2012. DOI: 10.1109/MSP.2012.52.

[82] Netzwerk Leichte Sprache, *Die Regeln für Leichte Sprache*, [Online]. Available: https://www.leichte-sprache.org/wp-content/uploads/2023/03/Regelwerk_NLS_Neuaufl2022_web.pdf (last accessed on Apr. 14, 2024), 2022.

[83] E. I. Obilor, "Convenience and purposive sampling techniques: Are they the same", *International Journal of Innovative Social & Science Education Research*, vol. 11, no. 1, pp. 1–7, 2023.

[84] S. Misoch, “Der Interviewende als Erhebungsinstrument”, in *Qualitative Interviews*. Berlin, Germany: De Gruyter, Aug. 2019, pp. 213–228. DOI: `10.1515/9783110545982-201`.

[85] U. Kuckartz and S. Rädiker, *Qualitative Inhaltsanalyse: Methoden, Praxis, Computerunterstützung*, 5th ed. Weinheim, Germany: Beltz Juventa, 2022, ch. 5, pp. 129–156.

[86] D. Leahy and D. Dolan, “Digital literacy – is it necessary for eInclusion?”, in *HCI and Usability for e-Inclusion*, A. Holzinger and K. Miesenberger, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 149–158.

[87] V. Heitplatz, “Fostering digital participation for people with intellectual disabilities and their caregivers: Towards a guideline for designing education programs”, *Social Inclusion*, vol. 8, no. 2, pp. 201–212, 2020. DOI: `10.17645/si.v8i2.2578`.