Why Do Employees Report Cyber Threats? Comparing Utilitarian and Hedonic Motivations to Use Incident Reporting Tools

Anjuli Franz
Technical University of Darmstadt, franz@ise.tu-darmstadt.de

Why Do Employees Report Cyber Threats? Comparing Utilitarian and Hedonic Motivations to Use Incident Reporting Tools

Completed Research Paper

Anjuli Franz

Technical University of Darmstadt

Hochschulstrasse 1, 64289 Darmstadt, Germany

franz@ise.tu-darmstadt.de

Abstract

Organizational cybersecurity is threatened by increasingly sophisticated cyberattacks. Early detection of such threats is paramount to ensure organizations' welfare. Particularly for advanced cyberattacks, such as spear phishing, human perception can complement or even outperform technical detection procedures. However, employees' usage of reporting tools is scarce. Whereas prior cybersecurity literature has limited its scope to utilitarian motives, we specifically take hedonic motives in the form of warm glow into account to provide a more nuanced understanding of cyber incident reporting behavior. Drawing on a vignette experiment, we test how the design features of report reasoning and risk indication impact users' reporting tool acceptance. The results of our mediation analysis offer important contributions to information systems literature by uncovering the dominant and under-investigated role of hedonic motives in employees' cyber incident reporting activities. From a practice perspective, our findings provide critical insights for the design of cyber incident reporting tools.

Keywords: Organizational cybersecurity, cyber incident reporting, hedonic motives, warm glow

Introduction

Corporate cybersecurity issues challenge both research and practice since they are rooted in complex socio-technical systems, with human actors, technology, and processes acting as interconnected components (Zimmermann and Renaud 2019). Prior information systems (IS) literature has predominantly labelled the human actor as the weakest link in the cybersecurity chain (e.g., Goel et al. 2017; Mitnick and Simon 2003; Turel et al. 2021), that needs to be excluded, controlled, or trained in order to not present a hazard to organizational cybersecurity. On the contrary, researchers have argued that this notion neglects the potential of human actors' capability to contribute actively to protecting and improving security (Kirlappos et al. 2013; Zimmermann and Renaud 2019). Recent works have hence called for a paradigm shift from the human-as-a-problem to a human-as-a-solution cybersecurity mindset (Vielberth et al. 2021; Zimmermann and Renaud 2019). No longer viewing the human "as a problem to control, but rather as a solution to harness" (Zimmermann and Renaud 2019, p. 175) allows to fully tap humans' potential as a vital player in defending organizations against cyberattacks.

One of the most powerful capacities of humans in supporting organizational cybersecurity is the detection and reporting of suspicious activity, such as phishing attempts or anomalous behavior of software or hardware, which we refer to as cyber incident reporting (Heartfield and Loukas 2018). The reporting of such incidents is paramount for organizations since it allows for early cyberthreat detection, which can critically reduce recovery cost and effort (Greene et al. 2018). Since sophisticated cyberattacks often are not automatically detectable (Vielberth et al. 2021), human perception can act as an important source of contextual information, and has even been observed to be a superior security sensor and early warning system compared to technical procedures (Heartfield and Loukas 2018). Over the last years, corporations have hence started to implement reporting tools, such as a phishing reporting button in email software, where employees can effortlessly report suspicious activities to the information security department. Employees' usage of such reporting functionalities, however, is scarce. While social engineering penetration tests have revealed that 78% of all employees never fall for a simulated phishing email and could hence potentially act as cyber incident reporters (Widup et al. 2018), only 7% actually report such a phishing attempt (NCATS 2018).

While understanding what motivates employees to report cyberthreats is crucial for designing effective reporting mechanisms, IS research contributed little insight on this matter as of yet (Briggs et al. 2017; Vielberth et al. 2021). Literature on cyber incident reporting is scant, and first approaches have limited their scope to a utilitarian perspective (e.g., Jensen et al. 2017; Kwak et al. 2020). We argue that this limitation does not account for the complex phenomenon of cyber incident reporting due to two main reasons: First, in the wider field of organizational cybersecurity, the research dialogue has steered towards the role of socio-emotional motivations (e.g., pride, or affective connection to colleagues) in employees' security behavior (e.g., Karjalainen et al. 2019; Posey et al. 2014; Renaud et al. 2021). Imagine, for example, the satisfying and proud emotion of feeling pleased with oneself after detecting and reporting a sophisticated malicious email. These insights have not been employed in cyber incident reporting research as of yet. Second, cyberthreat reporting often takes place through technology, such as reporting tools implemented in email software. Prior works have found hedonic motives to play a crucial role in users' acceptance of technology (Van der Heijden 2004; Wixom and Todd 2005). However, to our knowledge, cyber incident reporting has not yet been studied through the lens of technology acceptance and its hedonic drivers.

We hence argue that, besides utilitarian motives, hedonic desires might play an important and hitherto under-investigated role in employees' reporting activities. From a practice perspective, shedding light on the underlying mechanisms of users' reporting behavior provides valuable insights for the design of cyber incident reporting tools striving to maximize employees' reporting activities. In this research work, we therefore intend to investigate the following two research questions:

RQ1: How do utilitarian vs. hedonic factors influence employees' intention to use cyber incident reporting tools?

RQ2: What are resulting implications for affordances that such reporting tools should offer?

To address these research questions, we conducted an online vignette study. Participants were presented with a self-developed email reporting tool equipped with two different design features, signaling the affordances of report reasoning (RR) (e.g., expounding one's reason to believe that the email is malicious) and risk indication (RI) (e.g., categorizing the report as a priority). The experiment was followed by a questionnaire, where the participants expressed their intention to use the email reporting tool. Furthermore, we measured the two constructs perceived usefulness (Davis 1989) and warm glow of giving (Andreoni 1990; Iweala et al. 2019) as mediators, representing participants' utilitarian and hedonic motives for using the reporting tool, respectively. Our results provide empirical evidence of the mechanism of both perceived usefulness and warm glow in affecting participants' intention to use an email reporting tool, with the hedonic feeling of warm glow contributing more strongly than perceived usefulness.

Our paper contributes to IS literature in general and cyber incident reporting research in particular: First, this research suggests that the concept of warm glow of giving might be a hitherto under-investigated IS continuance construct, which can play a pivotal role to enhance users' acceptance of otherwise utilitarian information systems. Second, this paper provides a novel perspective on organizational cybersecurity by challenging the prevalent assumption that purely utilitarian motives drive employees' intention to support their organization's security efforts (e.g., Herath and Rao 2009; Hsu et al. 2015). By uncovering the dominating role of employees' hedonic motives, we offer an important contribution to our understanding

of why employees report cybersecurity incidents. Lastly, we shed light on affordances that foster both hedonic and utilitarian motives, and hence reveal important implications for the design of cyber incident reporting tools.

Theoretical Background

Behavioral Cybersecurity

Organizational cybersecurity is defined as the "efforts organizations take to protect and defend their information assets [...] from threats internal and external to the organization" (Dalal et al. 2022, p. 5), and is distinguished by its interdisciplinary, socio-technical character (Craigen et al. 2014; Zimmermann and Renaud 2019). While it is an organizational phenomenon, it heavily depends on the individual behavior of each employee, such as choosing secure passwords, locking one's computer screen when leaving one's desk, or not opening suspicious email attachments. Prior research has hence started to study behavioral cybersecurity, investigating, for example, the influence of psychological, social, emotional or cognitive factors on employees' protection of information systems' security (Dalal et al. 2022). On a cognitive level, employees' cybersecurity behavior has been explored through the lens of a rational cost-benefit analysis, studying the role of constructs such as users' perceptions of threat probability, response cost, rewards, or punishment severity in their security behavior (e.g., Herath and Rao 2009; Hsu et al. 2015). By contrast, other research works have discussed users' affective needs as drivers of both compliance as well as noncompliance with information security policies (Karjalainen et al. 2019), or have investigated the role of socio-emotional factors such as ownership, involvement, fear, or personal pride in contributing to organizational security (e.g, Hsu et al. 2015; Posey et al. 2014). Whereas information security professionals seem to think more in terms of extrinsic motivations, such as punishments or rewards, as drivers for employees' security efforts, empirical data suggests that employees themselves are much more likely to be motivated by intrinsic motivations, such as organizational commitment, pride, or perceived responsibility towards their colleagues (Burda et al. 2020; Posey et al. 2014).

When regarding the role of the human factor in cybersecurity in general, previous IS literature has often considered the user to be the weakest link in the security chain, claiming that end-users lack security knowledge and awareness, are unmotivated to take responsibility, or simply lazy (Zimmermann and Renaud 2019). Many research works have hence directed significant efforts to exploring, for example, how the human factor can be constrained and controlled via information security policies (Cram et al. 2019; Li et al. 2021), how users' security knowledge and awareness can be increased via security education, training, and awareness (SETA) programs (Bélanger et al. 2022; Silic and Lowry 2020), or how user-centric design can support employees in engaging in secure behavior (Franz et al. 2021; Volkamer et al. 2017). Revealing intrinsic motives as a major driver for employees' information security efforts, however, opens the way for a new perspective on the human factor within the socio-technical cybersecurity system: The paradigm shift from "human-as-a-problem", who needs to be supported in preventing security incidents, to "human-as-a-solution", who can contribute actively to protecting the organization, allows organizations to fully reap human actors' capability to contribute to maintaining and enhancing cybersecurity (Zimmermann and Renaud 2019). This is in accordance with Kirlappos et al. (2013), who claim that the "comply or die" approach does not work for modern organizations, where employees collaborate and take initiative. In particular, several prior works have highlighted the capacity of human actors in reporting cyber incidents (Heartfield and Loukas 2018; Vielberth et al. 2021), which is the topic of this study.

Cyber Incident Reporting

A cyber incident (or cybersecurity incident) is defined as an occurrence that misaligns the actual ownership and control rights of digital assets (which includes, for example, access, extraction, contribution, removal, or alienation) from the lawful ownership and control rights of these assets (Craigen et al. 2014). Cyber incident reporting describes a user's intentional report of a certain suspicion of, or relevant information about, such a cybersecurity incident, mostly via a computer-based reporting system (Vielberth et al. 2021). Early detection of such threats is paramount for organizations since it allows for fast incident response and containment, which can substantially reduce recovery cost and effort (Briggs et al. 2017; Greene et al. 2018). Prior research has highlighted the capacities of human perception in complementing technical automated procedures (Greene et al. 2018; Heartfield and Loukas 2018; Vielberth et al. 2021). Particularly for social

engineering attacks, that target the human factor via deception or masquerading techniques, human perception often outperforms technical filters: On the one hand, the vast majority of social engineering attackers leave little to no technical traces in their early stages and continuously evolve their attack patterns, exploiting, for example, zero-day vulnerabilities. This leaves technical heuristic detection capabilities with a meager starting basis, and a very limited view of potential threats through user interaction (Heartfield and Loukas 2018; Vielberth et al. 2021). On the other hand, the detection of such attacks requires interpretation of both visual and behavioral information in their specific context, potentially across multiple user-interface platforms (imagine, for example, a spear phishing email that contains a link to a cloud document). This makes human perception a more accurate security sensor than technical security systems, and hence an alluring candidate for actively contributing to cyberthreat detection (Heartfield and Loukas 2018). While there will always be employees that fall for social engineering attacks and hence present a vulnerability for organizational cybersecurity, a single user who correctly detects and reports an incident can severely contribute to protecting the organization as a whole against cyberthreats.

Whereas organizations' cybersecurity can benefit profoundly from their employees' cyber incident reporting, employees' reporting activities are scarce (Briggs et al. 2017; NCATS 2018). Prior works have hence called for research on the underlying motives that drive cyber incident reporting (Briggs et al. 2017; Vielberth et al. 2021). Empirical studies on this question, however, are scant. In the context of phishing reporting, Kwak et al. (2020) have tackled the issue through the lens of Social Cognitive Theory, and have found that users' self-efficacy, cyber security self-monitoring, and expected negative outcomes influence their reporting motivation. Under the umbrella of theory from knowledge management and crowdsourcing, Jensen et al. (2017) have observed that public attribution and validation of successful phishing reports incentivizes employees to report their suspicions of malicious emails more frequently. Qualitative insights by Burda et al. (2020) have suggested that reasons for reporting relate to the perceived sophistication of the attack, where users who assess themselves to have a higher sense of responsibility and threat awareness have expressed the motivation to safeguard less aware colleagues. These insights reflect the findings from the wider field of behavioral cybersecurity research, where both cognitive and affective factors have been observed to play a role in employees' security efforts (e.g., Herath and Rao 2009; Hsu et al. 2015; Karjalainen et al. 2019).

Reporting Tools and Technology Affordances

From a tool perspective, the functionality to report suspicious or anomalous activity has found its way into most email software. This is in accordance with regulations such as ISO 27011, which requires the enablement of employees to report cyber incidents through suitable channels (e.g., A.16.1.2, ISO 2013). Examining the reporting tool landscape in detail, however, reveals that little insights from research have found their way into practice as of yet. Most reporting tools are simple dialogue boxes with the two options to report an email as either spam or phishing, which then results in the email being forwarded to a predefined email address, and the email being deleted from the user's account[1]. The current design hence likely does not acknowledge the underlying motives of employees' usage of such reporting tools, and arguably leaves much room for improvement. Affordance Theory (Gibson 1979) offers a valuable means for user-centered analyses of technologies (Piccoli 2016; Tim et al. 2018; Waizenegger et al. 2020). It relies on the assumption that individuals perceive their environment directly in terms of its potentials for action. Technology affordances are hence action possibilities afforded by a technology to its user (Gaver 1991). If a technology application succeeds to offer salient affordances for users' psychological needs, this will typically motivate the use of such an application (Karahanna et al. 2018). In this work, we test the effect of two reporting tool affordances on employees' usage intention.

User Acceptance and the Constructs of Perceived Usefulness and Warm Glow

Regarding user acceptance of technology in general, numerous research works have confirmed that both utilitarian and hedonic motives play a role in individuals' intention to use a certain technology (Dickinger et al. 2008; Van der Heijden 2004). On the utilitarian side, the construct of perceived usefulness has been

1 For example, Lucy Security's PhishAlert plugin (https://wiki.lucysecurity.com/doku.php?id=phishing_incidents), KnowBew4's Phish Alert Button (https://support.knowbe4.com/hc/en-us/articles/360009629234-How-Do-I-Use-the-Phish-Alert-Button-for-Microsoft-365-), or ProofPoint's PhishAlarm (https://www.proofpoint.com/us/products/security-awareness-training/phishalarm-email-reporting).

a central component of models for predicting user acceptance of technology for decades (Davis 1989; Hu et al. 1999; Venkatesh et al. 2003). Its predictive ability on intentions to use technology has been supported by various research works in utilitarian contexts, and has often been employed as a counterpart to exploring hedonic motives for technology acceptance (e.g., Van der Heijden 2004; Wakefield and Whitten 2006). First introduced in the Technology Acceptance Model (TAM) by Davis (1985), it describes the degree to which an individual believes that using a particular system will increase their job or task performance (Davis 1989). Its theoretical grounding lies in the belief-intention relationships of the Theory of Reasoned Action (Fishbein and Ajzen 1977), which suggests that users' beliefs influence their attitudes, which then lead to intentions, which in turn guide behaviors.

Hedonism refers to pleasure-seeking as motives for action (O'Shaughnessy and O'Shaughnessy 2002). The core principle that distinguishes utilitarian systems from hedonic systems is that the first aim to provide only instrumental value to the user (e.g., enabling them to perform a certain task better), while the latter aim to offer a self-fulfilling value (e.g., experiencing fun or happiness when using the system) (Van der Heijden 2004). Prior IS research has investigated hedonic constructs such as, for example, enjoyment (Dickinger et al. 2008; Van der Heijden 2004), satisfaction (Wixom and Todd 2005), or cognitive absorption (Agarwal and Karahanna 2000) as predictors for technology acceptance. These hedonic constructs are driven by purely egoistic motives, that is, they provide users with enforcement of their own advantage without regard to others. In contrast, the hedonic construct of warm glow is based on altruistic behavior. The concept of "warm glow of giving" is based on Public Goods Theory (Andreoni 1990) and reflects the satisfying "feeling people experience when performing an apparently altruistic act" (Iweala et al. 2019, p. 315). While an individual incentivized by pure altruistic motives is indifferent about the origin of the increased welfare of others, an individual driven by warm glow connects psychosocially with the recipient of the interaction, and receives a personal gain, such as a feeling of pride, enthusiasm, happiness, satisfaction, or boost of self-esteem, through the act of giving (Gleasure and Feller 2016; Iweala et al. 2019). The concept of warm glow has mainly been limited to investigating charitable giving (Gleasure and Feller 2016; Sutanto et al. 2021) and the influence of ethical claims on consumers' purchase intentions (Iweala et al. 2019; Lee and Charles 2021), where warm glow givers have been described as "emotional altruists" (Singer and Ricard 2015). Prior research on organizational cybersecurity has started to study the role of socio-emotional motivations, such as pride, in employees' security behavior (e.g., Karjalainen et al. 2019; Posey et al. 2014; Renaud et al. 2021). Investigating employees' cyber incident reporting behavior through the theoretical lens of warm glow might hence hold interesting insights for IS research.

Research Model and Hypothesis Development

Before presenting our research model, we primarily introduce two affordances of cyber incident reporting tools as potential design features to maximize user acceptance of such tools. The development of the two affordances investigated in this paper has been guided by both research and practice: Spear phishing incidents in our research department have sparked an extensive discussion among colleagues on what it feels like to detect a spear phishing attack in one's inbox, which has yielded results such as a feeling of surprise, excitement or satisfaction, as well as perceived superiority to others who might not be able to identify the email as phishing due to less security knowledge or context awareness. This notion is supported by prior literature, which has observed the role of involvement, ownership, or personal pride in cybersecurity-related behavior (Posey et al. 2014; Zimmermann and Renaud 2019). When identifying a hard-to-detect phishing attack, email users recognize the unique knowledge and valuable capabilities that they bring to this identification process, which neither technical controls nor IT experts might be able to contribute (Wash et al. 2021). Prior research, however, has not yet investigated these socio-emotional factors in the context of cyber incident reporting tools, neither have they been implemented by current phishing reporting tools (e.g., the examples from practice named earlier[1]).

When analyzing which exact psychological needs typically emerge from detecting a spear phishing attack, we agreed on (1) sharing details on the malicious email and how one successfully detected it with others (e.g., by showing colleagues a screenshot of the message, retelling the story of how one was almost tricked by criminals, or describing one's assessment of the specific attack characteristics), and (2) effectively warning others in case one thinks they might likely fall for the phishing attempt (e.g., by reporting the incident to the information security department or by telling colleagues directly about the incident). We then concluded that, out of these two psychological needs, current phishing reporting tools can only partly

cater to the need of warning others (partly, since it remains unclear to the user if their report is handled with sufficient care and priority), and that the need to share one's own assessment of the attack characteristics remains largely unsatisfied. We hence developed two affordances, namely report reasoning (RR) and risk indication (RI), to address these needs. Report reasoning (RR) describes the possibility of explaining why one thinks that the reported occurrence is a cybersecurity incident. Regarding the reporting of a malicious email, for example, RR could be an affordance to explain which part of the email led to the assumption that it might present a security risk. Risk indication (RI) presents a way to indicate that the incident is high-risk, and that precautions should be taken immediately. Applied to the context of phishing, RI could be an affordance to flag a sophisticated attack, which might pose a severe threat to organizational cybersecurity, as a priority report.

To shed light on the effect of the reporting tool affordances RR and RI on our dependent variable intention to use, we propose a research model encompassing utilitarian and hedonic motives as drivers of employees' intention to use a cyber incident reporting tool. In the following, we expound upon each of the posited relationships as depicted in Figure 1.

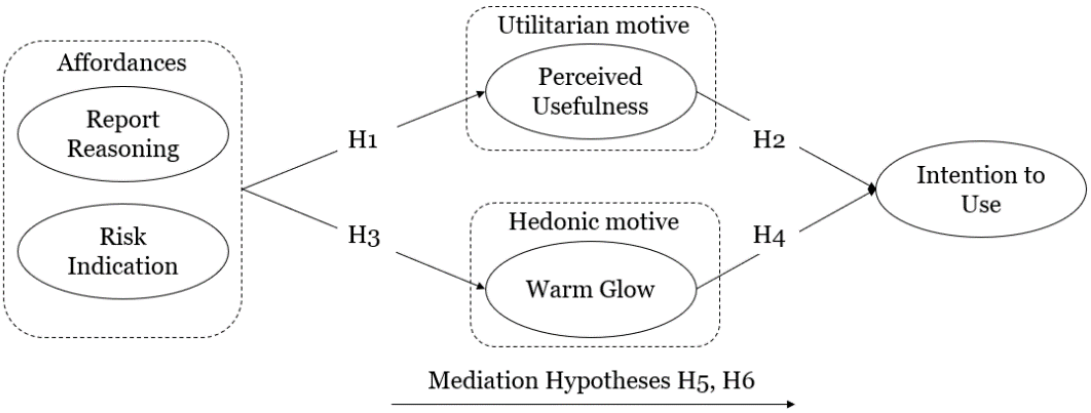


Figure 1. Research Model

On the left side of our model, we present RR and RI as independent variables. From a utilitarian perspective, employees who have detected a cyber incident will perceive the reporting of such an incident as a task they should fulfill in their role as a member of their organization. While RR allows users to pass on potentially important information (such as reporting a legitimately-looking email in a suspicious context), RI enables them to ensure that others will be warned of a sophisticated attack before it spreads. The affordances to provide such relevant information on the incident through a reporting tool gives the tool an instrumental value, since users will feel like the tool helps them to perform the task of incident reporting better. This, in turn, will increase users' perceived usefulness of the reporting tool (Davis 1989).

Furthermore, most employees do not possess expert knowledge on the identification of cyber incidents. We argue that RR and RI can provide guidance through one's own reflection of the security incident, and hence make the task of deciding whether or not to report an incident less difficult. Since prior research has identified users' perceived ease of use of a technology as an antecedent of perceived usefulness (Davis 1989; Karahanna and Straub 1999), we argue this mechanism reinforces the influence of RR and RI on perceived usefulness. Overall, we thus hypothesize that RR and RI have a positive effect on users' perceived usefulness of an incident reporting tool:

> *H1: The presence (vs. absence) of the affordances a) report reasoning, and b) risk indication is related to a higher level of perceived usefulness.*

Perceived usefulness has in turn been confirmed to be a strong predictor of individuals' intention to use a technology (Davis 1989; Hu et al. 1999; Venkatesh et al. 2003). Therefore,

> *H2: A higher level of perceived usefulness increases intention to use.*

Beyond this cognitive rationale, prior research has observed the user-cybersecurity relationship to be driven by emotional and affective needs (Karjalainen et al. 2019; Renaud et al. 2021), such as the need to feel ownership of security decision processes (Hsu et al. 2015; Zimmermann and Renaud 2019), or to feel validated when reporting a cyber incident (Jensen et al. 2017). This holds especially for cybersecurity-aware employees, who tend to feel responsible for safeguarding less aware colleagues (Burda et al. 2020). Both affordances RR and RI address these emotional needs. By enabling employees to interact directly with the information security department, RI and RR signal to users that their task expertise on a cyber incident is valued despite them not officially being security experts. Through RI, employees can take the role of a security advisor who can prompt the information security department to technically analyze a reported incident immediately. Being trusted with such security decisions invokes a feeling of active involvement in, and contribution to organizational welfare, which will enhance their perceived reputation. Furthermore, the affordance of RI will enhance employees' perception that their warning of others was effective, which will foster their satisfaction with the overall reporting process. Beyond that, RR addresses the urge to share one's story of the successful detection of a malicious threat as described at the beginning of this section. This can act as a way to indulge in the feeling of happiness and pride about one's achievement. Overall, we argue that RR and RI will act as a means to evoke and enhance feelings such as pride, satisfaction, happiness, and boost of self-esteem, which are an indication of the experience of warm glow (Gleasure and Feller 2016; Iweala et al. 2019). We hence propose:

> *H3: The presence (vs. absence) of the affordances a) report reasoning, and b) risk indication are related to a higher level of warm glow.*

Hedonic motives, such as satisfaction or enjoyment, have been identified as major drivers for usage intentions (Van der Heijden 2004; Wixom and Todd 2005), since they provide users with the self-fulfilling value of experiencing pleasure through technology usage. Building on IS literature, we hence argue that experiencing warm glow will motivate employees to report cyber incidents, which will result in a higher intention to use a reporting tool. We thus hypothesize:

> *H4: A higher level of warm glow increases intention to use.*

In conclusion, we argue that the underlying motives of employees' cyber incident reporting are twofold. On the one hand, cyber incident reporting can be seen as a utilitarian act, where we assume employees to weigh their personal costs (e.g., spending time and effort) against benefits (e.g., increasing organizational cybersecurity). Since increasing the perceived usefulness of a reporting tool through RR and RI shifts the cost-benefit calculus in favor of the benefit, the presence of these affordances will result in a higher intention to use (Davis 1989). On the other hand, employees' motives to report cyber incidents likely emerge from hedonic ambitions. Similar to a charitable donor giving towards a public good, an employee reporting a cyber incident can experience a feeling of warm glow by psychosocially connecting with the recipient (that is, their organization or colleagues) of their altruistic behavior (Andreoni 1990; Gleasure and Feller 2016). RR and RI augment this psychosocial connection by feeling actively involved in contributing to organizational cybersecurity, which increases employees' feeling of pride, satisfaction, and happiness (Jensen et al. 2017; Posey et al. 2014). The pursuit of the feeling of warm glow hence also drives their usage intention of a cyber incident reporting tool. As such, we suggest that both perceived usefulness and warm glow mediate the effect of our two affordances on intention to use:

> *H5: Perceived usefulness mediates the effect of the affordances a) report reasoning, and b) risk indication on intention to use.*
>
> *H6: Warm glow mediates the effect of the affordances a) report reasoning, and b) risk indication on intention to use.*

Methodology

With the goal to unravel the role of altruistic vs. hedonic motives in employees' intention to use a cyber incident reporting tool, we opted for an online vignette experiment in an email reporting context. We chose the vignette methodology since it permits to control for participants' personal experience and to avoid social desirability bias (Aguinis and Bradley 2014), and because it has been validated as an effective technique for assessing users' perceptions of and reactions to cybersecurity-related conditions (Benlian et al. 2020; Warkentin et al. 2017). In our experiment, participants were asked to imagine they were employed at a

fictional company called TradeFurnishings, which had experienced several cybersecurity issues through phishing or ransomware attacks in the past. Employees were hence asked to report unsolicited emails to the information security department using a reporting tool implemented in their email program. In our experiment, participants were then introduced into the functionalities of the current email reporting tool, which consisted of a report button in the menu bar of their email program, and a dialogue box with two radio buttons "report as spam" and "report as phishing". We decided to use this current tool as a baseline to avoid preconceived attitudes governed by participants' potential past interactions with real-world email reporting tools. In our study, participants were then informed that the information security department had implemented an updated version of the email reporting tool, and were presented with the novel functionalities. Here, we randomly assigned our sample to four conditions, yielding a 2x2 between-subject design.

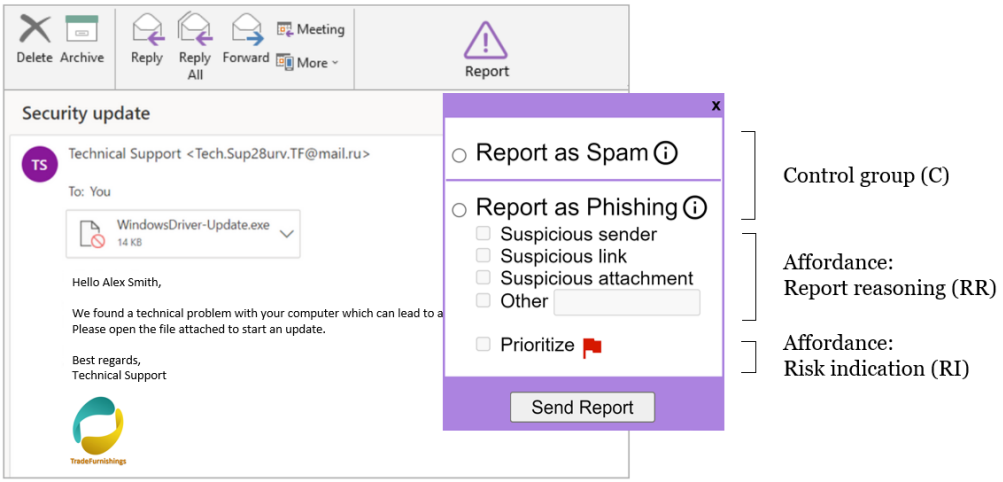


Figure 2. Exemplary Phishing Email with Email Reporting Tool Dialogue

For the control group C as well as all other groups, the previous tool was updated with an element where participants could access brief information on what is spam and what is phishing by hovering over an information icon. The treatment group RR was additionally given the opportunity to multi-select reasons why they thought that this particular email was malicious, e.g., because the sender or link seemed suspicious, hence reflecting the affordance of report reasoning. Participants were informed that their assessment helped the information security department to analyze the email. The treatment group RI could optionally flag the report with a priority tag, signaling the affordance of risk indication. Participants were told to use this priority tag if they believed that they were reporting a sophisticated malicious email that might pose a severe threat to their colleagues and organization, and that their vigilance enabled the information security department to take precautions immediately. Lastly, participants in group RR*RI were presented with a tool that included both affordances RR and RI, as depicted in Figure 2.

After familiarizing themselves with the updated email reporting tool, participants were presented with six consecutive emails, of which three were phishing emails, two were legitimate emails, and one was spam, and were asked to report them via the reporting tool if they perceived them to be phishing or spam. The three phishing emails ranged from mass to spear phishing, with background information from our vignette story (e.g., the TradeFurnishings logo or the name of the CEO) serving as masquerading techniques. The email depicted in Figure 2 was designed to be of medium difficulty to recognize as phishing.

Having processed the emails, participants completed a questionnaire on their perceptions of the email reporting tool. To operationalize our constructs, we used and adapted existing measures. The items for perceived usefulness, warm glow, and intention to use are presented in Table 1. Additionally, we measured demographics (gender, age) and control variables (affinity for technology, phishing identification expertise, average of emails received per day).

Compared with the previous email reporting tool, how do you feel about the new email reporting tool? Please rank your agreement with the following statements.	
Perceived Usefulness (PU) (adapted from Davis 1989) (α = 0.92)	PU1: The new email reporting tool enhances the effectiveness of employees' reports of unsolicited emails. PU2: I find the new email reporting tool more useful. PU3: The new email reporting tool addresses my organization's security-related needs better.
Warm Glow (GLO) (adapted from Iweala et al. 2019) (α = 0.96)	GLO1: Reporting emails with the new email reporting tool gives me a stronger pleasant feeling of personal satisfaction. GLO2: I am more satisfied with myself when I use the new email reporting tool. GLO3: Using the new email reporting tool, I feel happier contributing to TradeFurnishing's security. GLO4: I am more satisfied with myself when I make a contribution towards email security at TradeFurnishings.
Intention to Use (ITU) (adapted from Taylor and Todd 1995; Wixom and Todd 2005) (α = 0.94)	ITU1: I have higher intentions to use the new email reporting tool as a routine part of my job over the next year. ITU2: I plan to use the new email reporting tool more frequently. ITU3: I intend to use the new email reporting tool more often when receiving unwanted emails.
Note: All items were measured on a 7-point Likert scale, ranging from strongly disagree (1) to strongly agree (7). α represents Cronbach's Alpha (Cronbach 1951).	

Table 1. Measurement Items

Our sample was drawn via Prolific, a crowdworking platform for recruiting subjects for scientific experiments (Palan and Schitter 2018). All participants were pre-screened by Prolific as white-collar workers using technology at work more than once a day and speaking English fluently, and were payed US$0.82 for their participation. In total, 277 participants took part in our experiment. Responses from 43 participants who failed at least one of our attention checks were excluded, resulting in our final sample of 234 participants. The distribution across experimental groups is depicted in Table 2. Of the subjects in our study, 54.3% were females, 22.8% were between 25 and 34 years old, and 88.8% lived in the United States. To ensure that our participants were indeed randomly assigned to our four treatment groups, we conducted an ANOVA based on our sample demographics, which yielded no significant difference (all $p>0.05$).

The acceptance of our reporting tool within the experiment was high, participants largely reported phishing correctly at least once during the experiment (90.6%). To illustrate participants' interaction with the reporting tool, we employ the email depicted in Figure 2 as an example: The email was reported as phishing by 81.2% of all participants. Those participants who had the RR element available largely checked the box for suspicious attachment (80.6%), and partly for suspicious sender (53.8%). Of those participants who had the RI element available, 56.8% made use of the priority flag, indicating their assessment that the email is high-risk and should be analyzed by the information security department immediately.

Experimental group	**C**	**RR**	**RI**	**RR*RI**
N	61	60	57	56
Correctly reported phishing at least once	87%	88%	95%	93%

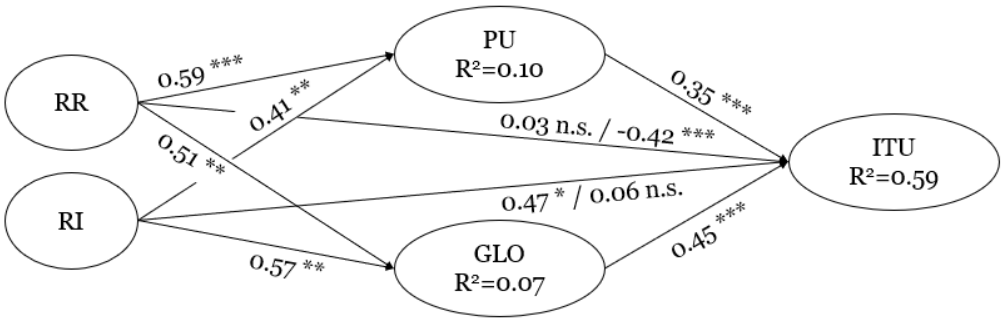
Table 2. Experimental Groups

Results

To analyze our results, we first conducted a linear regression analysis with the presence vs. absence of our two affordances RR and RI as independent variables and intention to use as dependent variable, along with our control variables as covariates. The results indicate a positive direct effect of RI on intention to use ($\beta = 0.47$, $p < 0.05$). In contrast, we find no indication of a significant effect of RR ($\beta = 0.03$, $p > 0.05$), or the interaction term RR*RI ($\beta = -0.02$, $p > 0.05$), on intention to use. As for our control variables, our results suggest a positive effect of participants' affinity for technology ($\beta = 0.24$, $p < 0.001$) as well as gender ($\beta = 0.36$, $p < 0.05$; female = 1).

To test our hypotheses, we then entered perceived usefulness and warm glow as potential mediators in our model. Figure 3 shows the direct and indirect effects of our mediation model analysis. For perceived usefulness (PU), results of our regression model indicate a positive and significant effect of both RR ($\beta = 0.59$, $p < 0.001$) and RI ($\beta = 0.41$, $p < 0.01$). We therefore find **support for H1a and H1b.** The combined variance in perceived usefulness explained by the presence of our affordances RR and RI is 10%.

Furthermore, our analysis confirmed a positive and significant effect of both RR ($\beta = 0.51$, $p < 0.01$) and RI ($\beta = 0.57$, $p < 0.01$) on warm glow (GLO), thus **supporting H3a and H3b**. The regression model explains 7% of the variance in warm glow.



Indirect effects	Coefficient	SE	LLCI	ULCI
RR → PU → ITU	0.21	0.06	0.0886	0.3383
RR → GLO → ITU	0.23	0.08	0.0701	0.4101
RI → PU → ITU	0.14	0.06	0.0390	0.2710
RI → GLO → ITU	0.25	0.09	0.0866	0.4511

Note: N=234; ***p<0.001; **p<0.01; *p<0.05; n.s. not significant.

The first coefficient on a given path represents the direct effect without the mediators in the model; the second represents the direct effect when the mediators are included in the model. Coefficients for indirect effects were computed using bootstrapping with 10,000 samples and a 95% bias-corrected confidence interval. LLCI and ULCI denote the lower bound and upper bound of the confidence interval, respectively. All control variables were included in the analysis.

Figure 3. Direct and Indirect Effects in the Mediation Analysis

For the influence of perceived usefulness on intention to use (ITU), our results indicate a positive and significant effect ($\beta = 0.35$, $p < 0.001$), which is **in support of H2.** Moreover, warm glow has a significant positive influence on intention to use ($\beta = 0.45$, $p < 0.001$), hence **supporting H4**. Our final model explains 59% of the variance in intention to use.

Lastly, we conducted two mediation analyses using Hayes (2018)'s PROCESS macro (version 4.0), which is based on ordinary least squares regression. We provide results based on a bootstrapping approach with 10,000 samples and 95% bias-corrected confidence intervals for the indirect effects.

Our hypothesis H5 posited that the presence of RR and RI affects users' intention to use through perceived usefulness. Results of our mediation analysis reveal a positive indirect effect for both paths RR→PU→ITU (indirect effect = 0.21, CI = [0.09, 0.34]) and RI→PU→ITU (indirect effect = 0.14, CI = [0.04, 0.27]). As such, perceived usefulness mediates the effect of RR and RI on intention to use, **thus supporting H5a and H5b.**

H6 posited that the presence of RR and RI affects users' intention to use through warm glow. Our mediation analysis results indicate a positive indirect effect for both paths RR→GLO→ITU (effect size = 0.23, CI = [0.07, 0.41]) and RI→GLO→ITU (effect size = 0.25, CI = [0.09, 0.45]). Therefore, warm glow mediates the effect of RR and RI on intention to use, **thus supporting H6a and H6b.**

In summary, we find that the effect of RR and RI on intention to use can be explained by a parallel mediation through perceived usefulness and warm glow. Warm glow is likely a more dominant driver of reporting tool acceptance because the coefficient is higher in both the direct and indirect effects. The positive direct effect of RI on intention to use becomes insignificant when entering our two mediators into the model. This means that RI no longer affects intention to use when controlling for perceived usefulness and warm glow, which is often referred to as full mediation (Zhao et al. 2010). While our results indicated no significant direct effect of RR on intention to use, the direct effect becomes negative and significant ($\beta = -0.42$, $p < 0.001$) when entering perceived usefulness and warm glow into the model. This suggests a competitive mediation, and hence the existence of an omitted mediator that is competitive to the positive indirect effects of perceived usefulness and warm glow (Zhao et al. 2010).

Discussion

Organizational cybersecurity hinges on employees' security behavior. While employees have been considered a threat to cybersecurity for a long time (Zimmermann and Renaud 2019), research has started to acknowledge their vast potential in cyber incident reporting (Heartfield and Loukas 2018; Vielberth et al. 2021). Despite their potential, however, employees' reporting activities are scant, which leads to the assumption that current incident reporting tools do not fulfill employees' needs. Although prior works have recognized the importance of studying employees' acceptance of reporting tools, the underlying motives of cyber incident reporting have not yet been unraveled. While prior literature has limited its scope to utilitarian motives (e.g., Kwak et al. 2020), the main objective of our study was to specifically explore hedonic motives. Drawing on donation literature (Andreoni 1990; Gleasure and Feller 2016), we employed the construct of warm glow to operationalize hedonic motives. Our research presents three important findings.

First, our investigation reveals both warm glow and perceived usefulness as key factors for employees' cyberthreat reporting behavior. The strong weight of warm glow (0.45) represents its critical role in reporting tool usage intentions, compared with perceived usefulness (0.35). Second, the results of our mediation analysis indicate that the two design features risk indication (RI) and report reasoning (RR) present a useful extension of current cyber incident reporting tools. For both features, we found significant positive indirect effects on employees' intention to use via perceived usefulness and warm glow. Lastly, our results suggest a competitive mediation for the effect of RR on intention to use. While our findings suggest a positive indirect effect through perceived usefulness and warm glow, the direct effect of RR on intention to use becomes negative when controlling for both mediators. This informs our theorizing of the possible existence of a omitted mediator with a negative sign in our research model (Zhao et al. 2010). While this can be pursued in future research, we speculate that potential candidates might be perceived effort or productivity loss: In comparison to RI, the feature of RR might be associated with higher effort by the user, since it requires more interaction. Conflicts with productivity have been found to be main reasons for non-compliance with security policies (Kirlappos et al. 2013; Sasse 2015). Overall, these results provide a more

nuanced understanding of cyberthreat reporting behavior and shed light on a vast potential for reporting tools to tap into.

Contributions to Theory and Practice

Our research offers two main contributions to the IS literature in general and to cybersecurity literature in particular.

First, this paper investigates the role of hedonic motivation in technology acceptance. While this has been extensively done by prior works, most authors have limited their scope to hedonic motives that are of rather egoistic nature, such as enjoyment (Van der Heijden 2004), user satisfaction (Wixom and Todd 2005), or cognitive absorption (Agarwal and Karahanna 2000). These constructs describe experiences that provide users with an advantage without regard to others. Conversely, the concept of warm glow describes a hedonic experience based on altruistic behavior (Andreoni 1990). To date, IS literature's interest in the role of warm glow has been limited to charitable behavior in purchasing or crowdfunding contexts (Gleasure and Feller 2016; Lee et al. 2018). Drawing on our insights in this work, we argue that warm glow might hold interesting interactions embedded within technology in other research domains. We hence call for research on this hitherto under-investigated IS continuance construct, which can have pivotal influence on users' acceptance of otherwise utilitarian information systems.

Second, this paper provides a new perspective on organizational cybersecurity. Prior IS literature has mostly assumed end-users to lack security knowledge, awareness, and motivation, thus presenting the weakest link in the security chain. While first works have started to acknowledge the power of the user in protecting organizational cybersecurity (Zimmermann and Renaud 2019), most research has limited its scope to the prevailing assumption that purely utilitarian motives drive employees' intention to support their organization's security efforts (Herath and Rao 2009; Hsu et al. 2015; Kwak et al. 2020). While utilitarian motives undoubtedly are a strong predictor of reporting tool usage, our empirical data uncovers the dominating role of hedonic motives in cyberthreat reporting behavior. This challenges the prevailing assumption of why employees report cyberthreats, and answers our research question *RQ1*. With our findings, we additionally contribute to a more nuanced understanding of factors that explain employees' security behavior in general. Our drawing of the analogy between charitable behavior (Gleasure and Feller 2016; Iweala et al. 2019) and organizational cybersecurity behavior can inform future theorizing.

Beyond our theoretical contributions, our paper provides important implications for designers of cyber incident reporting tools. Addressing our research question *RQ2*, our analysis of the underlying motives of employees' reporting intentions uncovers that the design of cyber incident reporting tools should address both utilitarian and hedonic user needs. Informed design decisions can cater to both a strong feeling of perceived usefulness and an experience of warm glow in order to maximize continuance intention. While current reporting tools (such as the one in our experimental control group) do not foster users' hedonic needs, our two design features RR and RI provide a valuable example of how reporting tool design can harness the potential of employees' reporting capacities. While RI (that is, the option to flag reports as a priority) yielded a net positive effect on participants usage intentions and hence represents an attractive candidate for practice, RR apparently needs more finetuning. Furthermore, other mechanisms, such as bonuses or rewards, might be able to stimulate hedonic aspects of reporting cyber incidents.

Limitations and Future Research

We recognize limitations of our research, which hopefully provide opportunities for future works. First, we would like to highlight methodological limitations. Although we measured participants' behavioral intentions, our experimental setup did not allow to measure their actual behavior. While previous studies have observed that the assessment of behavioral intentions provides a reasonable indication of their actual behavior (Venkatesh et al. 2012), we encourage future research to verify our findings through experiments in the field. Furthermore, methodological means such as manipulation checks for our two design affordances as well as the inclusion of further control variables such as perceived ease of use (Davis 1989) would add to the robustness of our experimental data.[2] Second, our study was conducted in the context of email reporting. Although it is likely that our results are applicable to cyber incident reporting in other

2 We would like to thank the Associate Editor of this paper for these valuable suggestions.

contexts, this limits the generalizability of our work. For example, our findings may not be applicable to cybersecurity incidents that require higher degrees of security expertise, or that employees are typically exposed to less frequently than to malicious emails. We therefore call for future research to replicate our findings in other cybersecurity contexts to confirm generalizability.

References

Agarwal, R., and Karahanna, E. 2000. "Time Flies When You're Having Fun: Cognitive Absorption and Beliefs About Information Technology Usage," *MIS quarterly*), pp. 665-694.

Aguinis, H., and Bradley, K. J. 2014. "Best Practice Recommendations for Designing and Implementing Experimental Vignette Methodology Studies," *Organizational research methods* (17:4), pp. 351-371.

Andreoni, J. 1990. "Impure Altruism and Donations to Public Goods: A Theory of Warm-Glow Giving," *The economic journal* (100:401), pp. 464-477.

Bélanger, F., Maier, J., and Maier, M. 2022. "A Longitudinal Study on Improving Employee Information Protective Knowledge and Behaviors," *Computers & Security* (116), p. 102641.

Benlian, A., Klumpe, J., and Hinz, O. 2020. "Mitigating the Intrusive Effects of Smart Home Assistants by Using Anthropomorphic Design Features: A Multimethod Investigation," *Information Systems Journal* (30:6), pp. 1010-1042.

Briggs, P., Jeske, D., and Coventry, L. 2017. "The Design of Messages to Improve Cybersecurity Incident Reporting," *International Conference on Human Aspects of Information Security, Privacy, and Trust*: Springer, pp. 3-13.

Burda, P., Allodi, L., and Zannone, N. 2020. "Don't Forget the Human: A Crowdsourced Approach to Automate Response and Containment against Spear Phishing Attacks," *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*: IEEE, pp. 471-476.

Craigen, D., Diakun-Thibault, N., and Purse, R. 2014. "Defining Cybersecurity," *Technology Innovation Management Review* (4:10).

Cram, A., Proudfoot, J. G., and Bentley, U. 2019. "Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance," *MIS Quarterly* (43:2), pp. 525-554.

Cronbach, L. J. 1951. "Coefficient Alpha and the Internal Structure of Tests," *Psychometrika* (16:3), pp. 297-334.

Dalal, R. S., Howard, D. J., Bennett, R. J., Posey, C., Zaccaro, S. J., and Brummel, B. J. 2022. "Organizational Science and Cybersecurity: Abundant Opportunities for Research at the Interface," *Journal of business and psychology* (37:1), pp. 1-29.

Davis, F. D. 1985. "A Technology Acceptance Model for Empirically Testing New End-User Information Systems: Theory and Results." Massachusetts Institute of Technology.

Davis, F. D. 1989. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly* (13:3), pp. 319-340.

Dickinger, A., Arami, M., and Meyer, D. 2008. "The Role of Perceived Enjoyment and Social Norm in the Adoption of Technology with Network Externalities," *European Journal of Information Systems* (17:1), pp. 4-11.

Fishbein, M., and Ajzen, I. 1977. "Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research," *Philosophy and Rhetoric* (10:2).

Franz, A., Zimmermann, V., Albrecht, G., Hartwig, K., Reuter, C., Benlian, A., and Vogt, J. 2021. "{Sok}: Still Plenty of Phish in the Sea—a Taxonomy of {User-Oriented} Phishing Interventions and Avenues for Future Research," *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, pp. 339-358.

Gaver, W. W. 1991. "Technology Affordances," *Proceedings of the SIGCHI conference on Human factors in computing systems*, pp. 79-84.

Gibson, J. J. 1979. "The Theory of Affordances. The Ecological Approach to Visual Perception," in *The People, Place and, Space Reader*. Routledge New York and London, pp. 56-60.

Gleasure, R., and Feller, J. 2016. "Does Heart or Head Rule Donor Behaviors in Charitable Crowdfunding Markets?," *International Journal of Electronic Commerce* (20:4), pp. 499-524.

Goel, S., Williams, K., University at Albany, S., Dincelli, E., and University at Albany, S. 2017. "Got Phished? Internet Security and Human Vulnerability," *Journal of the Association for Information Systems* (18:1), pp. 22-44.

Greene, K., Steves, M., and Theofanos, M. 2018. "No Phishing Beyond This Point," *Computer* (51:6), pp. 86-89.

Hayes, A. F. 2018. *Introduction to Mediation, Moderation, and Conditional Process Analysis: A Regression-Based Approach*. Guilford Publications.

Heartfield, R., and Loukas, G. 2018. "Detecting Semantic Social Engineering Attacks with the Weakest Link: Implementation and Empirical Evaluation of a Human-as-a-Security-Sensor Framework," *Computers & Security* (76), pp. 101-127.

Herath, T., and Rao, H. R. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18:2), pp. 106-125.

Hsu, J. S. C., Shih, S. P., Hung, Y. W., and Lowry, P. B. 2015. "The Role of Extra-Role Behaviors and Social Controls in Information Security Policy Effectiveness," *Information Systems Research* (26:2), pp. 282-300.

Hu, P. J., Chau, P. Y., Sheng, O. R. L., and Tam, K. Y. 1999. "Examining the Technology Acceptance Model Using Physician Acceptance of Telemedicine Technology," *Journal of management information systems* (16:2), pp. 91-112.

ISO. 2013. "Iso/Iec 27001:2013." Retrieved 12.11.2020, 2020, from https://www.iso.org/standard/54534.html

Iweala, S., Spiller, A., and Meyerding, S. 2019. "Buy Good, Feel Good? The Influence of the Warm Glow of Giving on the Evaluation of Food Items with Ethical Claims in the Uk and Germany," *Journal of cleaner production* (215), pp. 315-328.

Jensen, M., Durcikova, A., and Wright, R. 2017. "Combating Phishing Attacks: A Knowledge Management Approach," *Proceedings of the 50th Hawaii International Conference on System Sciences*.

Karahanna, E., and Straub, D. W. 1999. "The Psychological Origins of Perceived Usefulness and Ease-of-Use," *Information & management* (35:4), pp. 237-250.

Karahanna, E., Xu, S. X., Xu, Y., and Zhang, N. A. 2018. "The Needs–Affordances–Features Perspective for the Use of Social Media," *Mis Quarterly* (42:3), pp. 737-756.

Karjalainen, M., Sarker, S., and Siponen, M. 2019. "Toward a Theory of Information Systems Security Behaviors of Organizational Employees: A Dialectical Process Perspective," *Information Systems Research* (30:2), pp. 687-704.

Kirlappos, I., Beautement, A., and Sasse, M. A. 2013. ""Comply or Die" Is Dead: Long Live Security-Aware Principal Agents," *International Conference on Financial Cryptography and Data Security*: Springer, pp. 70-82.

Kwak, Y., Lee, S., Damiano, A., and Vishwanath, A. 2020. "Why Do Users Not Report Spear Phishing Emails?," *Telematics and Informatics* (48), p. 101343.

Lee, H. C. B., Cruz, J. M., and Shankar, R. 2018. "Corporate Social Responsibility (Csr) Issues in Supply Chain Competition: Should Greenwashing Be Regulated?," *Decision Sciences* (49:6), pp. 1088-1115.

Lee, L., and Charles, V. 2021. "The Impact of Consumers' Perceptions Regarding the Ethics of Online Retailers and Promotional Strategy on Their Repurchase Intention," *International Journal of Information Management* (57), p. 102264.

Li, H., Luo, X. R., and Chen, Y. 2021. "Understanding Information Security Policy Violation from a Situational Action Perspective," *Journal of the Association for Information Systems* (22:3), p. 5.

Mitnick, K. D., and Simon, W. L. 2003. *The Art of Deception: Controlling the Human Element of Security*. John Wiley & Sons.

NCATS, U. S. D. o. H. S. D. N. C. A. a. T. S. 2018. "Phishing Campaign Assessment Summary."

O'Shaughnessy, J., and O'Shaughnessy, N. J. 2002. "Marketing, the Consumer Society and Hedonism," *European journal of marketing*).

Palan, S., and Schitter, C. 2018. "Prolific.Ac-a Subject Pool for Online Experiments," *Journal of Behavioral and Experimental Finance* (17), pp. 22-27.

Piccoli, G. 2016. "Triggered Essential Reviewing: The Effect of Technology Affordances on Service Experience Evaluations," *European journal of information systems* (25:6), pp. 477-492.

Posey, C., Roberts, T. L., Lowry, P. B., and Hightower, R. T. 2014. "Bridging the Divide: A Qualitative Comparison of Information Security Thought Patterns between Information Security Professionals and Ordinary Organizational Insiders," *Information & management* (51:5), pp. 551-567.

Renaud, K., Zimmermann, V., Schürmann, T., and Böhm, C. 2021. "Exploring Cybersecurity-Related Emotions and Finding That They Are Challenging to Measure," *Humanities and Social Sciences Communications* (8:1), pp. 1-17.

Sasse, A. 2015. "Scaring and Bullying People into Security Won't Work," *IEEE Security & Privacy* (13:3), pp. 80-83.

Silic, M., and Lowry, P. B. 2020. "Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance," *Journal of Management Information Systems* (37:1), pp. 129-161.

Singer, T., and Ricard, M. 2015. *Caring Economics: Conversations on Altruism and Compassion, between Scientists, Economists, and the Dalai Lama*. Picador.

Sutanto, J., Wenninger, H., and Duriana, H. 2021. "Warm-Glow Giving, Hedonism, and Their Influence on Muslim User Engagement on Loan-Based Crowdfunding Platforms," *Journal of the Association for Information Systems* (22:2), p. 7.

Taylor, S., and Todd, P. A. 1995. "Understanding Information Technology Usage: A Test of Competing Models," *Information systems research* (6:2), pp. 144-176.

Tim, Y., Pan, S. L., Bahri, S., and Fauzi, A. 2018. "Digitally Enabled Affordances for Community-Driven Environmental Movement in Rural Malaysia," *Information Systems Journal* (28:1), pp. 48-75.

Turel, O., He, Q., and Wen, Y. 2021. "Examining the Neural Basis of Information Security Policy Violations: A Noninvasive Brain Stimulation Approach," *Management Information Systems Quarterly* (45:4), pp. 1715-1744.

Van der Heijden, H. 2004. "User Acceptance of Hedonic Information Systems," *MIS quarterly*), pp. 695-704.

Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. 2003. "User Acceptance of Information Technology: Toward a Unified View," *MIS quarterly*), pp. 425-478.

Venkatesh, V., Thong, J. Y., and Xu, X. 2012. "Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology," *MIS quarterly*), pp. 157-178.

Vielberth, M., Englbrecht, L., and Pernul, G. 2021. "Improving Data Quality for Human-as-a-Security-Sensor. A Process Driven Quality Improvement Approach for User-Provided Incident Information," *Information & Computer Security*).

Volkamer, M., Renaud, K., Reinheimer, B., and Kunz, A. 2017. "User Experiences of Torpedo: Tooltip-Powered Phishing Email Detection," *Computers & Security* (71), pp. 100-113.

Waizenegger, L., McKenna, B., Cai, W., and Bendz, T. 2020. "An Affordance Perspective of Team Collaboration and Enforced Working from Home During Covid-19," *European Journal of Information Systems*), pp. 1-14.

Wakefield, R. L., and Whitten, D. 2006. "Mobile Computing: A User Study on Hedonic/Utilitarian Mobile Device Usage," *European Journal of Information Systems* (15:3), pp. 292-300.

Warkentin, M., Goel, S., and Menard, P. 2017. "Shared Benefits and Information Privacy: What Determines Smart Meter Technology Adoption?," *Journal of the Association for Information Systems* (18:11), p. 3.

Wash, R., Nthala, N., and Rader, E. 2021. "Knowledge and Capabilities That Non-Expert Users Bring to Phishing Detection," *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, pp. 377-396.

Widup, S., Spitler, M., Hylender, D., and Bassett, G. 2018. "2018 Verizon Data Breach Investigations Report."

Wixom, B. H., and Todd, P. A. 2005. "A Theoretical Integration of User Satisfaction and Technology Acceptance," *Information systems research* (16:1), pp. 85-102.

Zhao, X., Lynch Jr, J. G., and Chen, Q. 2010. "Reconsidering Baron and Kenny: Myths and Truths About Mediation Analysis," *Journal of consumer research* (37:2), pp. 197-206.

Zimmermann, V., and Renaud, K. 2019. "Moving from a 'Human-as-Problem" to a 'Human-as-Solution" Cybersecurity Mindset," *International Journal of Human-Computer Studies* (131), pp. 169-187.