




ARTICLE



<https://doi.org/10.1057/s41599-021-00746-5>

OPEN

# Exploring cybersecurity-related emotions and finding that they are challenging to measure

Karen Renaud<sup>1,2,3✉</sup>, Verena Zimmermann<sup>4✉</sup>, Tim Schürmann<sup>4</sup>  & Carlos Böhm<sup>4</sup>

This paper reports on a three-part investigation into people's perceptions of cybersecurity, based on their lived experiences. We sought thereby to reveal issues located within the Johari grid's "Blind Spot" quadrant. We utilized research methodologies from both the Arts and Science in order firstly to identify blind spot issues, and secondly to explore their dimensions. Our investigation confirmed a number of aspects that we were indeed aware of, when it came to people's lived cybersecurity experiences. We also identified one particular blind spot issue: widespread, but not universal, negativity towards cybersecurity. We then carried out an investigation using a recognized methodology from psychology, as a first attempt to assess the nature of this negativity and to get a sense of its roots. What our initial experiment revealed was that scoping cybersecurity-related emotions is nontrivial and will require the formulation of new measurement tools. We conclude by reporting on the challenges, to inform researchers who plan to extend the research reported in this paper.

<sup>1</sup>University of Strathclyde, Glasgow, UK. <sup>2</sup>Rhodes University, Grahamstown, South Africa. <sup>3</sup>Abertay University, Dundee, UK. <sup>4</sup>Technische Universität Darmstadt, Darmstadt, Germany. ✉email: [karen.renaud@strath.ac.uk](mailto:karen.renaud@strath.ac.uk); [zimmermann@psychologie.tu-darmstadt.de](mailto:zimmermann@psychologie.tu-darmstadt.de)

## Introduction

The current day and age is characterized by a widespread personal ownership of Internet connected devices (BusinessLine, 2019). This means that most of society now also has to contend with the risk arising from the efforts of a global population of cyber criminals, potentially targeting their devices (Vojinovic, 2019; Eid, 2019). Governments are responding by developing national cybersecurity strategies (US Government, 2018; Her Majesty's Government, 2016; Australian Government, 2016; Public Safety Canada, 2018), organizations are establishing cybersecurity divisions (Vavra, 2019), and universities are funding cybersecurity research (UEU Commission, 2019).

The everyday end users of Internet-enabled devices and services, who vastly outnumber security experts and researchers, are most closely engaged with cybersecurity. Their voices can be drowned out in the general clamour of voices speaking about cybersecurity. When the end users' voices *are* heard, their responses are usually constrained by specific questions that are formulated by the major stakeholders in the field. Yet, it is important to consider the end users' unprompted perspectives, opinions, and perceptions of cybersecurity, so that the social desirability bias does not influence their responses.

Human-centred security researchers study and improve the interface where humans and security-related technologies meet. Their usual research philosophy is *positivist* (Crotty, 1998), i.e. revealing general laws of behaviours and highlighting causal relationships within the research space. As such, the researchers and experts choose the research topics, formulate the research questions, develop studies and design experiments. These researchers are investigating important and crucial aspects of human-centred security, and their solutions make a huge difference to the field as a whole.

Yet, there are additional ways to carry out research: different philosophies that can be used to reveal unexpected and unanticipated dimensions of a research field. These approaches can uncover the meanings everyday computer users construct, instead of testing pre-formulated hypotheses.

Saunders et al. (2016) explain that a purely positivist approach (i.e. hypothesis-led) does not afford a rich and nuanced view of reality, and does not reveal differences in individual experiences. Moreover, it seeks to explain and predict, but not to interpret phenomena (Walsham, 1995).

The *interpretivist* approach, on the other hand, focuses on the *meanings* people attribute to specific phenomena. Crotty (1998) argues that people cannot be studied the way physical phenomena can be studied because people *construct meaning*, and it is these divergent, idiosyncratic and emergent meanings that the interpretivist philosophy seeks to uncover.

Due to our desire to understand how people experience cybersecurity aspects of their world, by considering people's "lived" experiences, embracing an interpretivist philosophy seemed a viable choice for our initial foray. We hoped to explore how the man and woman in the street feels about cybersecurity as a phenomenon. In particular, what puzzles them, what questions they would like to ask (but perhaps do not ask), and what they want researchers to ask them. In essence, we wanted to hear them describe the perceptions they formed based on their lived experiences of cybersecurity.

We planned to use these alternatives to reveal cybersecurity-related issues situated in the upper right quadrant of a version of the Johari window adapted to information needs (Luft and Ingham, 1961; Shenton, 2007) (Fig. 1), i.e. the aspects we, as researchers, are not yet aware of or perhaps only vaguely suspect the existence of. Along these lines, Hand (2020) writes about 'Dark Data': missing data that we might not even know is

missing. The fact that we do not know it is missing means that we do not act to remedy the issues the data would have revealed. The missing data is essentially a *Blind Spot*. Similar to the blind spots in your eyes, you can reveal what is hidden by changing your perspective. This is what we sought to achieve.

To carry out our investigation, we appropriated techniques from the Arts, following up with more traditional scientific techniques to ensure that the research approach was rigorous. We thus crafted a portfolio methodology, blending interpretivist and positivist approaches in order first to identify cybersecurity constructed meanings and responses. Then, we can switch to a positivist approach, to investigate the identified issues using tried and tested techniques from the field of psychology.

Such a portfolio methodology is essentially a departure from our usual purely quantitative and positivist approaches used to embrace a more flexible, open-ended and nuanced investigation. Our research serves multiple purposes:

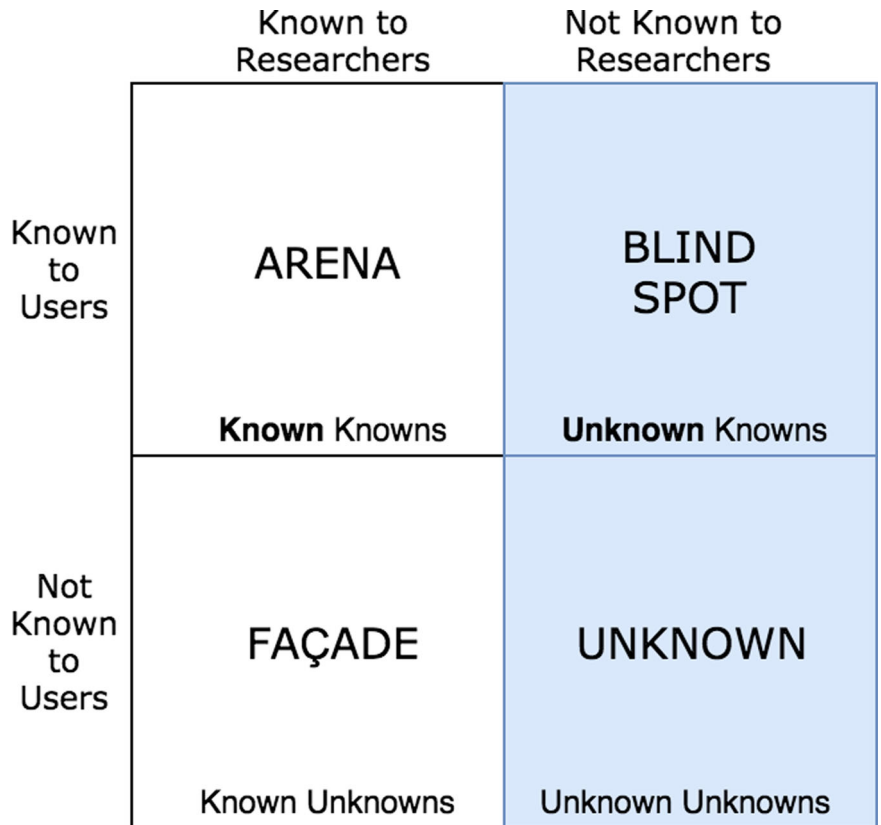
- a. we show the meanings people construct related to cybersecurity, in terms of content, affect and emotion,
- b. we derive a hypothesis to inform future human-centred research, i.e. *People experience negative emotions when confronted with cybersecurity-related terms*,
- c. having formulated the hypothesis, we deploy an appropriate methodology from the field of psychology to test it, and
- d. we outline our "portfolio" research methodology and propose it as an alternative way to carry out this kind of exploratory research, combining interpretivist and positivist approaches to explore constructed meanings in the cybersecurity domain.

We commence by outlining our research methodology (section "Research methodology"). The subsequent sections describe each of the steps in our research methodology, concluding in the section "Outcome and reflection", which reflects, details the limitations of our study, and discusses the challenges of future work. Section "Conclusions, future work and implications" concludes.

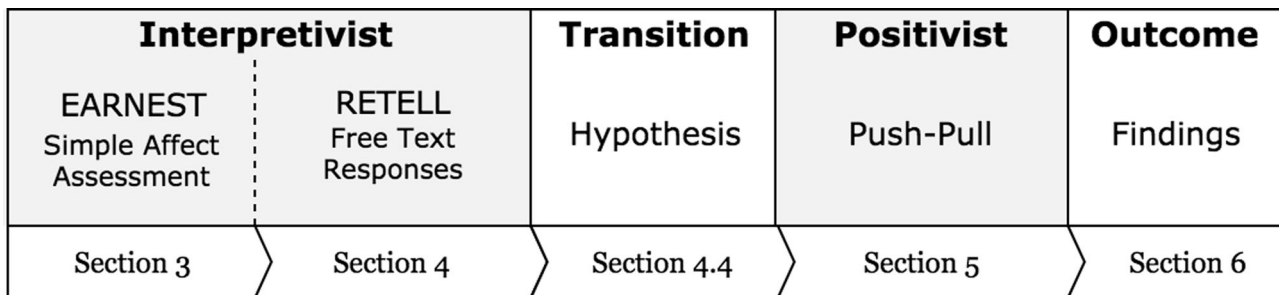
## Research methodology

The aim of this research project was to explore a relatively neglected area: end users' *actual* perceptions based on their lived experiences of cybersecurity. All perceptions, even that of cybersecurity, contain some affective reaction (Zajonc, 1980). Consider, for example, a flower: it is often not merely a flower, but rather a *fragrant* flower, a *beautiful* flower, or a *symbolic* one. Psychological research has shown that perceptions influence people's attitudes towards a topic, their motivation and perceived ability to deal with a certain topic, and finally their behaviour in terms of this topic (Bagozzi et al., 2000). Hence, perceptions of, and emotions related to, cybersecurity might be an important factor influencing cybersecurity attitudes and behaviours. To carry out this research, we constructed an interdisciplinary approach, using a portfolio of methodologies from cybersecurity, psychology and arts. The structure of the portfolio approach is depicted in Fig. 2.

*Study 1: Affect valence (Section 3—EARNEST):* We needed a very simple tool to capture cybersecurity affective responses, one that was both simple to use and obviously afforded anonymity (Fig. 3). We called the tool *EARNEST: affEct RespoNse mEaSurement Tool*. EARNEST allows people to consider a particular question (which is easily replaced). In this case, we are using it to assess how people respond to the question "*When I think about cybersecurity:*". They indicated the response affect on a scale



**Fig. 1 A Johari window adapted from Shenton (2007).** It maps users' knowledge to researchers' knowledge of issues.



**Fig. 2** The paper's research methodology is depicted in this flow diagram.

ranging from “very sad” to “very happy” by inserting a plastic counter into the appropriate cylinder. The cylinders are deliberately opaque so that people would not be influenced by others' choices. We specifically did not “man” EARNEST so that people would feel free to express their genuine feelings when choosing a cylinder to deposit their plastic disc into.

*Study 2: Free text responses (Section 4—RETELL):* We wanted to collect richer data than that afforded by EARNEST. The instrument we chose was an old-fashioned typewriter. This allowed people freely to express their feelings in terms of cybersecurity. This approach was based on a project conceptualized by artist Sheryl Oring (2018). Her project: “*I wish to say*” launched in Oakland, California in 2004. She created a portable public office using a manual typewriter and invited people to dictate postcards, which would be typed and sent to the president of the United States, so that their voices would be heard. To date, more than 3200 postcards have been typed during the course of the project and have been sent to the White House (Torpedo Factory Art Center, 2017). We call this measurement tool *RETELL*: fREe Text

rEsponse coLLector. The beauty of RETELL lies in its affordances. In the *first* place, the relatively slow typing speed and the absence of an ‘undo’ button encourages considered reflection about what they really want to say. The *second* is that it is clearly “offline”. This assures people that they are truly anonymous and encourages frank and honest responses. *Finally*, using a typewriter is sufficiently novel to attract respondents who want to play with a device from a bygone era.

We commenced with a pilot study to help us to refine the experimental set up (section “Pilot study”). We then launched the actual study in two European countries, eliciting responses from a wide range of respondents in different contexts (section “Main study”). We did not aim to reveal cross-cultural or cross-country differences but rather wanted to collect responses from a wide range of respondents due to the nature of this research as being exploratory. We report on our findings in the section “Discussion and reflection”. It is important to mention that we did not collect any demographic information as we would normally do in scientific studies. We did this deliberately, to ensure that people



**Fig. 3** The EARNEST: affEct RespoNse mEaSurement Tool based on Bradley and Lang (1994), with obfuscated images on cylinders from Morris (1995). People choose a cylinder based on their emotional state and deposit a plastic coin in a slot at the top.

knew they could express their real emotions without being concerned about social desirability or the risk of being judged for a less than positive reaction to cybersecurity.

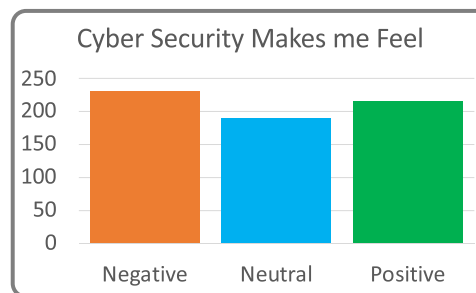
*Formulate hypotheses* (section “Hypotheses”): We reflected on the findings from Study 2, and categorized the identified aspects in terms of whether they were ARENA or BLIND SPOT issues (Fig. 1). This is the point at which the research transitions from an *interpretivist* to a *positivist* philosophy to reveal the dimensions of the identified blind spot issues. To test the affect-related hypothesis, we could not use surveys or interviews because such self-report tools might not accurately reflect people’s affective responses to cybersecurity aspects. We thus appropriated an innovative technique from psychology that did not rely on self-report.

*Study 3: Push/Pull* (Section “Study 3: Push/Pull Study”): Solarz (1960) carried out an experiment that relied on so-called *evaluative reactions* (approaching, avoiding, reaching for, pushing away, etc.) in order to detect people’s positivity or negativity towards a particular concept. We appropriated this method to test the hypothesis. Specifically, we showed participants terms coming from four different word categories: (1) positive, (2) neutral, (3) negative, and (4) cybersecurity. We asked them to operate a commercially available joystick and either pull a term towards them, indicating positive valence, or to push a term away from them, indicating negative valence. We were interested in the extent of cybersecurity-related terms receiving positive or negative evaluations and their positioning, as compared to other, non-cybersecurity-related word categories.

*Outcome* (section “Outcome and reflection”): Having carried out the portfolio research, this section brings everything together to draw final conclusions and reflect on the value of the portfolio approach, our findings, and the implications thereof.

### Study 1: EARNEST—simple affect assessment

To investigate cybersecurity emotions, pictures of sad and happy faces were attached to EARNEST’s cylinders to reflect different affective responses (see Fig. 3). The pictures were taken from the pleasure scale of “SAM”—the Self-Assessment Manikin (Bradley and Lang, 1994), that has been shown to be a suitable tool for measuring affect, can be used with children and adults, and is culture-free and language-free (Morris, 1995), which suited our data collection in two different European countries. The five



**Fig. 4** Study 1’s tallied ranking collected by the EARNEST measurement instrument (Negative, Neutral, Positive).

affect states range from “very sad” to “very happy”. The participant’s task was to put a plastic counter into the cylinder which best reflected their personal cybersecurity affective response. We positioned EARNEST in a number of settings, and left it there for up to 2 weeks before moving it to a new location. The locations included the lobby of our university, a coffee shop in a city centre, Chambers of Commerce meetings, the public library and university events. We tallied the number of counters in each cylinder, and positioned EARNEST in a different location.

*Measurements*: We counted the number of plastic coins in the cylinders corresponding to affect valence in response to the displayed question on EARNEST.

We combined the negative and positive tallies to report coarsely grained affect valence categories: negative, neutral and positive (Russell, 1980).

*Outcome*: Figure 4 shows the final tallies. The outcome is indeterminate. The negative responses outnumber the positive and neutral responses, but the differences are not compelling. The results, while interesting, left us with the realization that responses to cybersecurity cannot be captured meaningfully on a sad-happy scale, but are likely to vary, in terms of context, personal and cybersecurity-related action dimensions. To dig deeper, we explored cybersecurity perceptions in Study 2.

### Study 2: RETELL—free text responses

*Pilot study*. The pilot study took place on the grounds of our university in a publicly accessible building. For a couple of weeks





**Fig. 5** The pilot study setup with the typewriter, posters and yellow box for people to submit their typewritten sheets.

we set up a stall with posters to catch the attention of passersby, general study information, a typewriter (Brand Olympia), and a box for collecting the typed sheets (see Fig. 5<sup>1</sup>). Furthermore we provided emoji stickers to give participants the opportunity to express their emotions related to cybersecurity graphically, along with their typed responses. To ensure that we did not frame their responses, the instruction was phrased as “*Cybersecurity—I want you to have your say*” and “*Cybersecurity—I just want to say...*” on the posters (see Fig. 6<sup>1</sup>). During the first few days, interested parties expressed the need for more information, so we added further instructions on how to use a typewriter and pasted the instruction “*Please type what you would like to say about cybersecurity*” on the typewriter itself.

Participants could type as much as they liked, or abort at any time, by simply discarding their partial response. We did not ask for any personal information to assure anonymity and to encourage frank and honest responses. The sample consisted of people who passed by our stall and participated voluntarily. As soon as they were done, participants were asked to drop the typed sheet in the box. By so doing, they agreed to participate in the study.

The required steps were illustrated on the posters as well as on the corresponding artefacts, i.e. the typewriter and the collection box (see Fig. 5). The stall was unsupervised, but regularly monitored. The researchers’ contact details were provided on the

posters so that we could answer questions or deal with typewriter-related problems when alerted.

*Results and implications for the main study.* The pilot study served the purpose of deriving an initial code book to afford categorization during the subsequent study, as well as informing improvements to the main study design. A total of 43 responses (i.e. sheets of paper) were submitted. Please note that the number does not necessarily align with the number of participants as participants could easily provide multiple responses. Seventeen sheets were excluded because they did not contain study-related information but rather jokes, slogans or indecipherable text.

The analysis was based on Mayring’s inductive content analysis (Mayring, 2004). Typed texts were analysed on two independent code axes: (1) content-wise and (2) in terms of the emotional-affective level of each statement. After the development of an initial code book by one of the authors, all responses were coded by two authors independently. Inconclusive assignments were resolved by means of discussion, and supplementation of the categories, where necessary. A typed text and sentences within the text could be assigned several codes due to the parallel coding in terms of content and affective-emotional level. The content-wise categorization included *what* the person stated or how they understood cybersecurity, and the affective-emotional level *how*

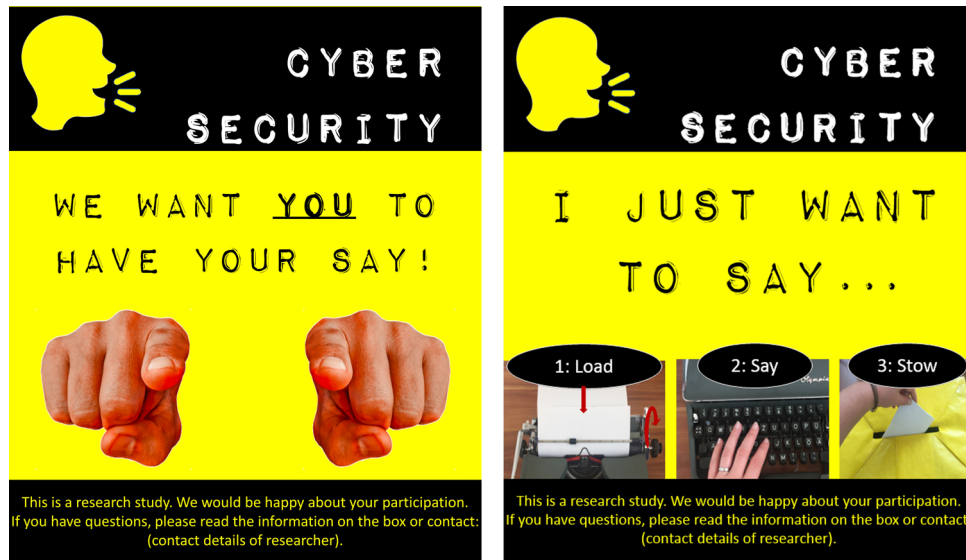


Fig. 6 The attention-catching and instruction posters used in the pilot study, translated to English from German.

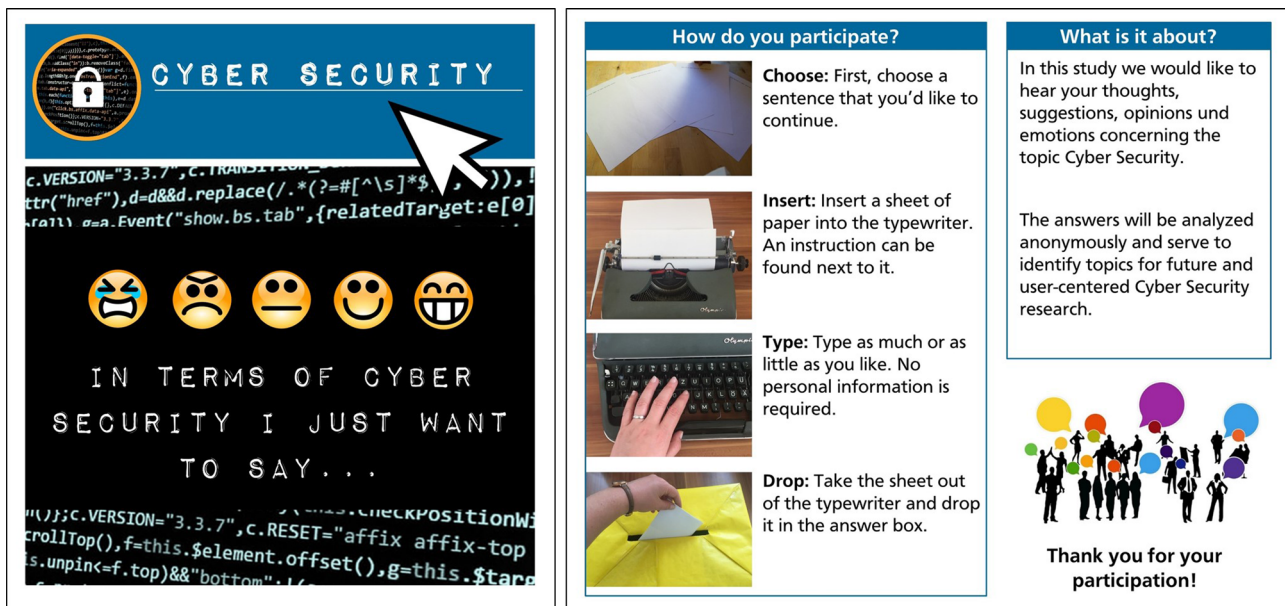


Fig. 7 Anonymized versions of the attention-catching and instruction posters used in the main study. Images used on the posters were from [www.pixabay.com](http://www.pixabay.com).

they felt about the concept. The content-wise categorization covered perceived causes, problems, consequences and suggested measures in terms of cybersecurity. The affective-emotional categorization covered the form of the statement (e.g. question, opinion) and the emotion (e.g. anger, fear, happiness) associated with cybersecurity.

We derived the following refinements for the main study:

- The participants considered the typewriter a good idea and fun to use. For some, the typewriter even initiated the participation in the study. However, some participants requested further instructions on how to use the typewriter. We produced a manual for the main study.
- As a second point, the participants asked for additional information on the study itself and for specific questions to respond to. We thus designed a flyer containing additional study information and provided a selection of incomplete sentences that participants could choose from to complete. To

do so, we made use of the different kinds of statements, i.e. questions, opinions, statements and emotions, that we identified in the pilot study to incorporate the participants' inputs instead of our own research questions. We derived six open-ended sentences such as, "In terms of cybersecurity, I feel...". The complete list can be found in the section "Main study".

- We realized that we had to be present at the stall during the main study to help people struggling with the typewriter and to answer participants' questions directly. With these last two measures we also hoped to reduce the number of nonsense and off-topic responses.

**Main study.** The main study used a similar setting to the pilot study with revised and more detailed posters, instructions and information (see Fig. 7). The stall was mobile and set up in different locations in two European cities: at public fairs and exhibitions of varying content, in canteens, in foyers of publicly



**Fig. 8** The RETELL stall, with three manual typewriters on the back table, with the banners left and right to attract attention. Images used on the posters were from [www.pixabay.com](http://www.pixabay.com).

accessible university buildings, cafés, and libraries. Participants ranged from young to older adults, including students, employed and retired people. We did not collect any demographic information to ensure that participants were assured of full anonymity. The participants were able to choose any of six sheets with different incomplete sentences to prompt a response. The task was to complete the sentence in their own words, with the possibility to add whatever and how much they wanted. The incomplete sentences were derived from the categorization of the pilot study (see the section “Results and implications for the main study”):

1. encourage expression of emotion:
  - (a) “When I think about cybersecurity I feel...”
  - (b) “when someone mentions about cybersecurity, it makes me feel...”
2. personal opinion: “My opinion on cybersecurity is that...”
3. suggesting a measure or improvement: “In terms of cybersecurity, my suggestion would be that...”
4. ask a question: “What I always wanted to ask about cybersecurity is...”
5. a general statement similar to the pilot study’s instructions: “In terms of cybersecurity, I just want to say...”

The participants were encouraged to use the typewriter, but in case of problems or uncertainty, they could dictate a text to the experimenter or write their statement by hand to be typed by the experimenter to ensure that anonymity was preserved (Fig. 8).

**Results.** For the analysis of the typewriter responses, the code book derived from the pilot study results was used, but extended with new categories that had not been mentioned in the pilot study. Thus, a deductive-inductive approach was followed. Again, all responses were coded in terms of content and affective-emotional level of statement.

Participants could submit as many responses as they liked, each of which could lead to several codes, due to the parallel coding in terms of content and affective-emotional level of statement.

Altogether  $N = 215$  responses were collected, including those gathered during the pilot study. Of these 51 were collected in Scotland and 164 in Germany. For the purposes of this publication, all quotes were translated to English.

A total of 61 times, the sheet with the incomplete sentence to express an opinion was chosen. The sheet encouraging a statement was chosen 31 times, the two sheets targeting emotions 48 times, and the sheet encouraging a question 17 times. A total of 32 times, the participants chose to complete the suggestion sentence. The 26 eligible responses from the pilot study were not assigned due to the later introduction of the open-ended sentences.

**Content-wise categorization.** A total of  $N = 420$  codes were assigned in terms of content. The categories concerning content were allocated to the main categories

- “Causes and Problems”, i.e. What are the cybersecurity problems people perceive?, What or whom do they deem responsible for the problems?
- “Effects and Consequences”, i.e. What effects are produced by the perceived cybersecurity problems? What are the consequences of current cybersecurity developments?
- “Suggested Measures”, i.e. What do people suggest to solve cybersecurity issues? What do people wish for in terms of cybersecurity?

The category “Causes and Problems” was the category with the highest number of codes with a total of  $N = 216$ . This category has been divided into six subcategories. For a complete overview, including category descriptions and exemplary codes for each subcategory, see Table 3 in Appendix A.

The subcategory “Lack of Knowledge & Significance” received the highest number of codes ( $n = 114$ ). On the one hand, many participants acknowledged cybersecurity as an important topic in general. On the other hand, many participants stated that people lacked knowledge, did not consider the topic important enough and that cybersecurity had too little significance in society. Some



participants also mentioned that people neglected the topic out of aversion or ignorance. An exemplary quote including several aspects is

“Most people ignoring this topic. It overstrains them and they lack the time to deal with the topic, furthermore they lack knowledge and they do not know how and where they can get infos about the topic” (Response R8).

The second most common subcategory was “Responsible Entities” ( $n = 70$ ) in which the people or organizations that were deemed responsible for cybersecurity problems, were coded. The participants mentioned different responsible groups or entities like hackers, companies, countries or politics, respectively, but also individuals and even themselves. Exemplary quotes are

“[...] data-hungry companies such as Facebook or Google.” (R53) or “Despite this, users’ lack of security awareness very often is the biggest problem” (R10).

The subcategory “Security Vulnerabilities” consisted of  $n = 22$  codes. Several security issues, such as viruses and Trojans, various technical deficiencies or rapid technological development were mentioned. An exemplary quote is

“My opinion on cybersecurity is that the development of AI will undermine cybersecurity efforts” (R83).

The subcategories “Term Cybersecurity” ( $n = 3$ ), “Financing/Costs” ( $n = 3$ ) and “Counter-productive Behaviour” ( $n = 4$ ) received only a few mentions. “Term Cybersecurity” includes texts in which people expressed the idea that the term was chosen poorly. “Financing/Costs” describes cybersecurity financing issues. “Counter-productive Behaviour” encompasses cases in which cybersecurity has been neglected or deliberately reduced to achieve certain purposes. An exemplary quote is

“In terms of cybersecurity, my suggestion would be that one stops trying to weaken IT security to implement non-functioning local policies” (R28).

An overview of the category “Effects and Consequences” ( $n = 80$ ) including category descriptions and exemplary quotes for each subcategory is shown in Table 3.

The subcategory “Societal Damage” ( $n = 45$ ) deals with texts that describe damage to infrastructure, national institutions, businesses and harm for individuals as a result of attacks or poor cybersecurity.

“I fear that contact data will be stolen or hacked” (R3).

“Lack of protection/Insecurity” ( $n = 28$ ) includes texts from people who no longer feel protected, describe security as an illusion, and express a clear desire for more security. Examples would be

“Cybersecurity is a illusion” (R39) or “Every system is vulnerable to a specific type of attack” (R143).

An exemplary code for “Cybersecurity as a field of work and study” ( $n = 7$ ) is:

“Cybersecurity is a great field on which securing a business depends [...] Cybersecurity plays an important role in the security of a business and in the growth of the business” (R107).

For the category “Measures and Suggestions”  $n = 121$  codes were assigned. For a complete overview including category descriptions and exemplary quotes see Table 3. The subcategory “Education & Communication” ( $n = 53$ ) includes topics such as making use of expert knowledge, educating, communicating information, building trust, or improving collaboration.

“More education about the risks of disclosing personal information should be provided. Especially the digital natives should get an understanding of how to generate secure passwords and how to protect themselves on the Internet” (R119) or “The topic should be much more open and much more talked about, or taught” (R174).

Improvements in user-friendliness, software and technology were mentioned and requested in the sub category “Technological Protection & Support” ( $n = 36$ ).

“It [Cybersecurity] should work without you knowing that it is there. It should protect people and their information” (R92).

The subcategory “Laws & Politics” ( $n = 17$ ) contains suggested legal regulations and political measures.

“Politics should finally come to terms concerning the topic realistically and with a clear vision of the future” (R171).

“Personal Security Behaviour” ( $n = 15$ ) includes texts which suggest secure user behaviour on the Internet.

“We should all give less of our data and change the attitude in society” (R145).

*Categorization in terms of affective level of statement.* The “affective level of statement” categorization describes how the participants formulated their responses and what emotions were expressed. In total,  $n = 350$  codes were assigned. The codes were subdivided into the categories “Statements/Opinions”, “Suggestions”, “Questions” and “Emotions/Affective Level”, whereby the “Emotions/Affective Level” category was divided into positive, negative, and neutral feelings and emotions.

A total of  $n = 168$  codes were assigned to “Statements & Opinions”: This category comprises all responses that include a personal statement (i.e. “That’s the way it is”) or a personal opinion (i.e. “I think...”, “In my opinion...”). For example:

“In terms of cybersecurity, I just wanted to say that I find it shocking how little attention we give to it” (R145).

Suggestions were made in  $n = 75$  cases. This category included responses in the form of “One should...”.

“For mobile devices, there should be more information” (R100).

Questions, i.e. every response that was formulated as a question, were asked  $n = 32$  times, e.g.:

“How easy is it really to hack web cams?” (R141)

In “Affective level/Emotions”, most emotions were negative ( $n = 57$ ). Only  $n = 14$  responses were positive, and  $n = 4$  neutral codes could be assigned. A negative code would be:



“When I think about cybersecurity, I feel confused and depressed” (R37).

An example of a positive code would be:

“When I think about cybersecurity, I feel secure” (R70).

**Discussion and reflection.** Figure 9 provides an overview of identified issues. We now discuss them in detail.

*ARENA issues.* Our study confirmed a number of issues known to both researchers and users (Fig. 1):

- *Lack of awareness/knowledge:* People spoke about a perceived lack of awareness and cybersecurity-related knowledge. Specifically, people felt that educational institutions, such as schools, should deliver more cyber education. Examples for research pursuing similar goals include the use of games to increase the users’ motivation to learn about cybersecurity issues (Jin et al., 2018), attempts to generate knowledge and competencies through competition (White et al., 2010), or awareness-raising programmes (Vroom and von Solms, 2002; Susanto and Almunawar, 2012).
- *Uncertainty:* The participants expressed uncertainty and feelings of a lack of security. They wanted to know exactly how they ought to behave and how they could protect themselves. This suggests that people want actionable and concrete, rather than general, cybersecurity-related information. Moreover, cybersecurity research showed that actionable information is more effective in enhancing security-related behaviours compared to general information or pointing out potential negative consequences without providing advice for avoiding these (Witte, 1992; Renaud and Dupuis, 2019).
- *Cyber attack harm:* They also mentioned the societal damage and harm resulting from cyber attacks as acknowledged in many cybersecurity reports (Widup et al., 2018; Cisco, 2018; Symantec Corporation, 2018).
- *Shared responsibility:* It is noteworthy that participants not only acknowledged the importance of cybersecurity, but also their own role in assuring cybersecurity. Most often the participants viewed themselves or other individuals as being responsible for cybersecurity or the lack thereof. In the literature, the role of the end user in terms of cybersecurity has been ambiguous. While some researchers view end users as a vulnerability or weakest link (Wood and Banks, 1993; Schneier, 2011; Kraemer and Carayon, 2007), other more recent approaches emphasize the end users’ ability to be a contributor to cybersecurity and

acknowledge the shared responsibility of all actors to ensure cybersecurity (Sasse et al., 2001; Castelli et al., 2018; Hollnagel et al., 2006; Zimmermann and Renaud, 2019). Because the statements in our study were often framed negatively, the participants’ views seemed to align more with the “human-as-problem” view.

- *Need for law enforcement:* Other actors were mentioned several times: the state or politics in general. People called for tighter legal frameworks in the form of data protection laws to address the actions of cyber criminals. An analysis of 19 national cybersecurity strategies (Luijff et al., 2013) revealed unclear relationships between national cybersecurity strategies and national or international policies in many cases, confirming this. Further, even though the need for society-wide approaches is acknowledged, actions aimed at citizens are often limited to awareness and education campaigns. Thus, some researchers call for better support of citizens by means of law enforcement and tighter regulation (Bauer and Van Eeten, 2009; Renaud and Flowerday, 2018).
- *Usability-security trade-off:* Some mentioned a conflict between usability and security, arguing for an improvement in usability of security tools. This conflict has often been mentioned by researchers in various areas such as encryption (Whitten and Tygar, 1999), smart home technologies (Zimmermann et al., 2019) or password creation (Inglesant and Sasse, 2010) and is targeted, especially by usable security researchers that aim to lessen the trade-off by increasing usability of security technologies and considering human needs (Adams and Sasse, 1999, Zurko, 2005). Attempts include password meters to support usable and secure password creation (Ur, 2017), the development of usable privacy management tools (Gerber et al., 2017), or the design of interfaces to increase the security and usability of e-voting (Marky et al., 2018) or authentication (Lashkari et al., 2009).

*BLIND SPOT issues.* In terms of the emotional-affective coding of the responses, we observed that participants mentioned negative emotions four times as often as positive emotions, when talking about cybersecurity. Feelings of insecurity and uncertainty were mentioned more often than any other. Cybersecurity was described as difficult and complex. People also felt anxious, overwhelmed, or angry, when it came to cybersecurity.

There are an increasing number of interventions available to people, and educational measures, tools and information are all freely available (see the section “ARENA issues”). Our participants wanted better security, but did not know what actual cybersecurity measures to take. This uncertainty had a negative valence.

A potential explanation for this gap is suggested by the emotional-affective categorization of the participants’ responses. It is possible that part of the problem lies neither in unmotivated users nor in a lack of information, but in the feelings of insecurity, uncertainty, frustration and mental overload experienced by participants. Even so, this mostly negative profile of expressed feelings does seem to be something that cybersecurity researchers have not paid much attention to, as yet.

Research from psychology and related disciplines has shown that affect and emotion play an important role in terms of people’s attitudes towards a topic, their motivation and perceived ability to deal with it, and finally their subsequent behaviours (Bagozzi et al., 2000). This is likely to apply to the cybersecurity field too. If users feel uncertain about which information or advice to follow, out of the plethora of available advice, or if they feel overwhelmed by the amount of information, this might

|                | Known to Researchers  | Not Known to Researchers  |
|----------------|---|---|
| Known to Users | <p><b>ARENA</b></p> <p>Lack of Knowledge</p> <p>Uncertainty</p> <p>Cyber Attack Harm</p> <p>Shared Responsibility</p> <p>Need for law enforcement</p> | <p><b>BLIND SPOT</b></p> <p>Negative Cybersecurity Related Emotions</p> |

**Fig. 9** Referring back to Fig. 1, the issues we identified during study 2 are situated within the applicable quadrants of the Johari window.

negatively influence their engagement with cybersecurity issues. The same might happen if they feel insecure due to negative media reports, negative personal experiences or cybersecurity-related fear appeals (Dupuis and Renaud, 2020).

Psychological models describing such negative influences include the Technology Threat Avoidance Theory (TTAT) model proposed by Liang and Xue (2009) and the two-process theory of Mowrer and Lamoreaux (1942). The approaches suggest that people with cybersecurity-related fears, or people who connect a topic with stress and frustration based on previous conditioning, will not engage constructively with a topic, but rather avoid it or even refrain from using new technologies.

In terms of cybersecurity education and skills, a number of psychological theories include affect and emotion as an important factor for learning and understanding new issues: It influences acceptance of new topics and the perceived ability to solve a problem. According to Bandura (1997), who is well known for his work on self-efficacy expectancy, the extent to which one is confident, in terms of ability, has an impact on the actual performance. His findings have also been applied to human-computer interaction: For example, Compeau et al. (1999) investigated the self-efficacy expectancy and expected outcome of using a computer. The investigation showed that desirable and undesirable attributions are important antecedents to computer self-efficacy. It is likely that cybersecurity self-efficacy plays an equally crucial role in triggering secure behaviours.

In terms of carrying out desired cybersecurity-related behaviours, the theory of planned behaviour according to Ajzen (1991) explains how attitude towards a behaviour, control expectation, and social norms are important to initiate a desired behaviour. Uncertainty and aversion towards a topic may thus be counter-productive. For example, a study by Bulgurcu et al. (2010) showed that an employee's intention to comply with the organization's information security policy was influenced by their attitude, normative beliefs, and self-efficacy.

In conclusion, a number of theories that have been successfully applied to human-computer interaction indicate that affect and emotion impact whether and how people engage with new topics, their mastery of new topics, and finally acceptance and actual security-related behaviours. In the next sections, we will thus explore user perceptions of cybersecurity in more detail.

**Hypothesis.** Based on our identification of negative emotional responses to cybersecurity as a blind spot issue, we now transitioned to a more positivist and traditional scientific approach. We propose the following hypothesis for subsequent investigation:

H1: People experience negative emotions when confronted with cybersecurity-related terms.

### Study 3: Push/Pull Study

We wanted to determine the type and magnitude of underlying psychological responses to cybersecurity precautionary terms. Doing so would help us to determine whether these terms are perceived positively or negatively. We benefited from Solarz's (1960) study design, and used it to determine whether participants' first responses would be to draw the term towards them (PULL), or try to push it away, i.e. rejecting the concept (PUSH), using a standard issue joystick.

**Theoretical background.** This test relies on the psychological theory of motivation. Research into the approach-avoidance conflict (Lewin, 1936; Miller, 1944) established a link between the perception of desirable and undesirable outcomes of a given action, on the one hand, and corresponding approach or avoidance behaviour, on the other. Inversely, observing an approaching

behaviour by an individual may allow us to infer the individual's perception of desirable outcomes. Inexperienced users confronted with cybersecurity-related topics may perceive undesirable outcomes of this confrontation, choosing to avoid them. We aim to investigate the extent to which users show approach or avoidance behaviour towards cybersecurity-related concepts.

**Materials.** This experiment required us to display words of different valence, and then to monitor push or pull actions and the valence thereof. We used the original lists of positive, negative and neutral words from Frings et al. (2010) (Table 2 in the Appendix).

To arrive at a list of cybersecurity-related words, we carried out a crowd-sourced survey to determine which security precautions people were aware of, and generally used. We consulted <https://www.cybrary.it/glossary/> to obtain the list. We then gave people two lists: (1) which precautions had they heard of, and (2) which precautions they used regularly. We launched the job with 100 respondents on the online platform CrowdFlower. Table 1 in the Appendix shows the results, demonstrating the usage of the precautions amongst the CrowdFlower participants. We used the top 15 most popular precautions in our study.

Finally, we composed a set of neutral, positive and negative words for the learning stage of the experiment as follows (the responses to these words were not measured or recorded during the learning phase).

Neutral *thick book, small city, blue globe, fountain pen and green bottle.*

Positive *christmas gift, hearty laugh, very tasty, so beautiful and go on a picnic.*

Negative *powerful hate, lose money, hit and run, painful knee and crash and burn.*

**Method.** Participants were asked to operate a commercially available joystick device while being shown words from four categories: positive, neutral, negative, and words related to cybersecurity concepts. The words were displayed in random order.

Measurements included the direction of the joystick operation (towards one's body or away from one's body), the time required to initialize the operation after a word was presented, and the time required to complete the movement and return to the neutral position.

**Sample.** The targeted sample size for this study was specified via an a priori power analysis (Cohen, 2013) using G\*Power (Faul et al., 2007). Assuming a medium sized effect, an alpha level of 0.05, and a power-level of 0.95, 55 participants were required. A total of 61 participants were recruited to compensate for potential outlier removals. Participants were recruited in part as a convenience sample without compensation, while students enrolled in psychology were compensated with course credit. 44 participants were German native speakers, two were English native speakers, and 15 participants indicated "other" as their native language. All were fluent English speakers. 45 participants were currently enrolled as students, with 17 of them being psychology majors. Eleven participants reported being employed in full-time contracts while five participants reported being self-employed. Two participants were excluded from further analysis due to their reaction times in the subsequent task lying outside of the 5th and 95th percentile of data (Ratcliff, 1993). The remaining data consisted of 59 participants (68% female, age mean = 26.83 years, standard deviation = 9.23 years).

**Procedure.** After welcoming a participant to the experiment room, they were seated in front of a computer screen and a joystick on a

desk (Fig. 10). They were asked to give consent concerning the purpose of the study, as well as the data analysis and data retention details after being informed about them in writing. The experimenter then informed the participant about the directional response task and operation of the joystick while instructing them to react as quickly as possible to presented words. Once the participant indicated that they had no more questions about the task, they were presented with a number of learning trials. Subsequently, the main directional response task began. Moving the joystick towards the participant's body was considered a positive reaction toward a presented stimulus, while moving it away from one's body was considered a negative reaction.

All participants saw four total categories: positive, neutral, negative, and words related to cybersecurity concepts (see Fig. 11) in randomized order, controlling for sequence effects. Measurements included the maximum extent of the joystick operation towards one's body or away from one's body (intensity), the time required to initialize the operation after a word was presented (reaction time), and the time required to complete the movement and return to the neutral position (movement time).

**Results.** On average, positive, negative, neutral and cybersecurity-related words received 95%, 11%, 75% and 65% positive reactions, respectively. After checking for statistical assumptions, we conducted a Friedman's ANOVA (Field et al., 2012) to investigate differences in the directional intensity of joystick movements between stimulus categories. The ANOVA revealed significant differences between the groups with  $Chi^2(3) = 124.74$ ,  $p < 0.001$ . Pairwise comparisons using Wilcoxon signed rank tests revealed significant differences for all category combinations. This means that movement intensity significantly differed between neutral and negative ( $V = 1722$ ,  $p < 0.001$ ,  $r = 0.81$ ), neutral and positive ( $V = 54.5$ ,  $p < 0.001$ ,  $r = 0.66$ ), neutral and cybersecurity-related ( $V = 1173.5$ ,  $p < 0.01$ ,  $r = 0.36$ ), negative and positive ( $V = 10$ ,  $p < 0.001$ ,  $r = 0.84$ ), negative and cybersecurity-related ( $V = 22$ ,  $p < 0.001$ ,  $r = 0.83$ ), and positive and cybersecurity-related word categories ( $V = 1559.5$ ,  $p < 0.001$ ,  $r = 0.75$ ). The median movement intensities per stimulus category were 0.60 (neutral), -1.00

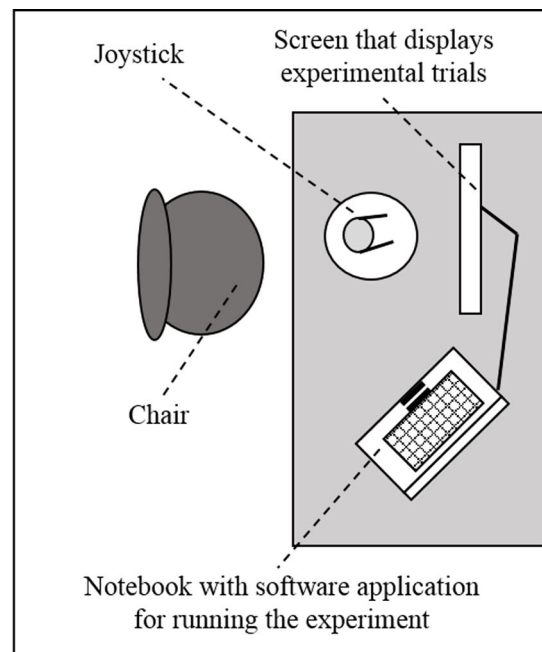
(negative), 1.00 (positive), and 0.33 (cybersecurity-related), with -1 indicating a full push away from the participant and +1 indicating a full pull towards the participant. Movements were counted after crossing an initial intensity threshold of 0.3 in either direction. Thereafter, the maximum movement intensity reached, before returning to a neutral position, was considered for the analysis presented here.

To investigate differences in reaction times between stimulus categories, we first checked whether the data satisfied the necessary statistical assumptions. After finding assumptions for parametric procedures violated, we conducted a nonparametric Friedman's ANOVA (Field et al., 2012) for repeated measures. Results show a significant difference between the four stimulus categories  $Chi^2(3) = 106.02$ ,  $p < 0.001$ . We consequently compared the cybersecurity stimulus category against each other category in a set of planned comparisons via Wilcoxon signed rank tests to determine its reaction time position relative to the other groups. The cybersecurity stimulus category shows a significantly higher reaction time compared to neutral stimuli ( $V = 80$ ,  $p < 0.001$ ,  $r = 0.77$ ), negative stimuli ( $V = 206$ ,  $p < 0.001$ ,  $r = 0.66$ ), and positive stimuli ( $V = 4$ ,  $p < 0.001$ ,  $r = 0.83$ ).

Aside from reaction times required to initiate an action in the experiment, we also investigated movement times required to complete the action once it had been initiated. A Friedman's ANOVA revealed significant differences in movement times between stimulus categories  $Chi^2(3) = 9.10$ ,  $p = 0.028$ . However, no pairwise comparisons between stimulus categories turned out to show significant differences by themselves.

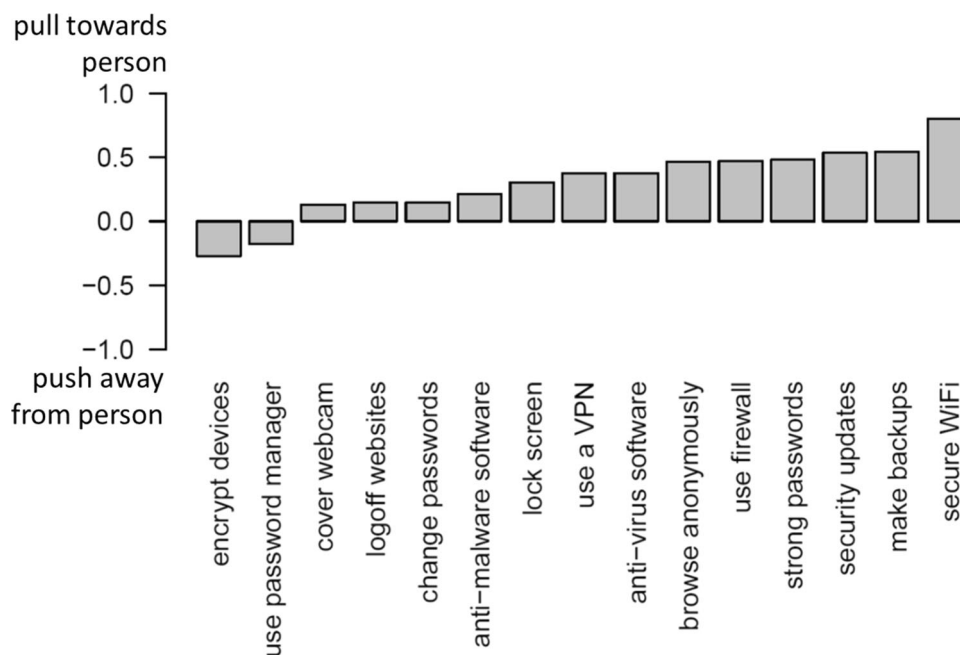
Figure 11 shows the average movement intensity for each cybersecurity-related term. It is interesting to note that the two terms that were pushed away, "encrypt devices" and "use password manager", are those that are not widely adopted (Renaud and Zimmermann, 2019; Sheng et al., 2006). This suggests that familiarity, and perhaps consequent uncertainty, might have played a role in eliciting negativity in this case.

**Discussion.** We observed a clear difference in tendencies to push or pull the words when it came to negative, neutral or positive



**Fig. 10** A depiction of the Push/Pull study. On the left, a photograph of one of the researchers sitting in front of the test computer. On the right is a graphical depiction of the push/pull study setup.





**Fig. 11** The barplot depicting movement directions for the displayed cybersecurity-related terms.

words. Positive words were generally pulled towards the participants, negative words pushed away, and neutral words elicited a generally positive response. Meanwhile, the median response towards cybersecurity words was variable. Consequently, we conclude that participants did not have distinctly avoidance-type reactions towards cybersecurity words, but, on average, slightly approached terms, as reflected in Fig. 11. As such, we cannot support Hypothesis H1. A post-hoc approach to categorizing cybersecurity words did not yield a clearer picture of the data, as cybersecurity words with similar movement directions do not seem to be similar in terms of their implied content.

Yet the RETELL study *had* revealed widespread negativity when we asked people what they wanted to say about cybersecurity. We now consider why RETELL and Push/Pull findings were different.

We did note that the reaction times to the cybersecurity words were significantly longer than reactions to all the other words while movement times were not different. One possible explanation is provided by word length in that the cybersecurity terms were often lengthier than the other words included in the study and thus took longer to process and react to. Another possible explanation for this could be that cybersecurity-related words were less cognitively available to participants, increasing cognitive processing time before an action could be initiated. It might be that the reaction to cybersecurity was not an automated but a reflective one, as compared to the other common terms included in the study. In contrast, people might already have “learned” an association with the other words, so they could react more quickly and “automatically”. This indicates that availability needs to be controlled in order to draw conclusions about valence based on participant reaction times. However, we expect subsequent investigation of the effect of availability on reaction times towards cybersecurity words to resemble general research on word recognition (Moreno and van Orden, 2001). This means that availability may lead to nonlinear, methodologically challenging effects on reaction times in word recognition.

Hence, we have to conclude that this particular tool probably did not have the power to scope the negative emotions that emerged in the RETELL study. It was clearly more complicated than we initially thought it was going to be.

### Outcome and reflection

Our research portfolio approach combined arts and scientific research technologies. The former was used to satisfy the interpretivist approach, with traditional psychological methodologies being used to satisfy the more positivist approach.

The interpretivist stage was inspired by Sheryl Oring’s art-based approach to encourage participants to freely and anonymously express their thoughts on cybersecurity via a typewriter (Oring, 2018). We analysed both content and affective-emotional aspects of statements. The pilot study helped us to tailor our RETELL setup for maximum efficacy in terms of measuring people’s responses to cybersecurity as a topic.

Future research in this direction could consider setting up RETELL in locations that can reach a wider variety of respondents, e.g. shopping centers and public places. The typewriter is a great way to gain attention with many wanting to “play” with it. However, the operation should be simplified for those struggling, e.g. by having someone type for the participants similar to Sheryl Oring’s (2018) approach. The approach of eliciting emotional responses was well received by the participants and many descriptions were provided. Overall, the deployment of this tool was a wise choice.

The Push/Pull test was specifically chosen to test the affect-related hypothesis that emerged from Study 2 and utilize response variables common in psychological investigations of cognitive phenomena. Participants appeared to understand the response variables of reaction times and reaction intensities well and no clarifying questions concerning their meaning were posed. Methodologically, we conclude that the push/pull paradigm was generally appropriate for the task at hand. However, cognitive psychology provides similar experimental paradigms that may be more suitable for measuring emotion in this context. We propose that go/no-go tasks (Gomez et al., 2007) or emotional stroop tasks (Frings et al., 2010) be trialled to determine whether they can provide insights into participants’ reactions to specific cybersecurity-related terms.

**Limitations.** EARNEST attempted to elicit a gut-feel affect response, but did not really give us any helpful information



about the source of the emotion. In retrospect, the tool was a poor measurement tool for this study, both in itself, and in the situations within which it was deployed. In the first place, the question posed on EARNEST was arguably far too much of an umbrella term, and too general to elicit meaningful responses. In the second place, we situated it in busy areas where people would pass by, hoping that many would choose to put a counter in one of the slots. However, this very busyness of the contexts would have made it difficult for people accurately to provide an immediate gut-feel response, and the reason they were passing by might have been more important to them than participating in the study.

The RETELL exploratory study was much better at giving people the opportunity to provide their thoughts, suggestions and questions. Yet the generalizability of the sample might be limited due to the sample probably being mostly young and educated. The stall was set up in different places and events, but mostly in university buildings or their surroundings due to the legal challenges of operating a stall in public venues. So, even though all venues were publicly accessible, most entries probably came from a pool of people with an academic background but due to the focus on anonymity, we cannot describe the sample further. Future approaches of this kind should seek to reach a larger audience, setting up the stall in public places such as shopping centers, parks, stations, libraries or museums, to recruit a more diverse sample.

The Push/Pull test could benefit from enhanced data gathering and experimental design. Additional background information, such as previous exposure to cybersecurity-related threats, could shine light on the general approach-type reactions observed for many of the cybersecurity words. As mentioned in the discussion, a post-hoc categorization approach of cybersecurity words failed, but a careful selection of words to match previously defined categories might alleviate this issue.

**Challenges and future work.** It is challenging to measure emotion without changing it (Bradley and Lang, 1994) because, as Bradley and Lang explain, emotions are part of the human response repertoire. Kassam and Mendes (2013, p. 1) explain that “The awareness and conscious assessment required by self-report of emotion may significantly alter emotional processes”.

Given Schneirla’s (1959) argument that approach-avoidance motivation is deeply embedded in our natures (Schneirla, 1959), further confirmed by (Tooby and Cosmides, 1990), we appropriated a tool that exploited this to measure cybersecurity-related emotions. The tool failed to detect any significant across-the-board negative emotions.

A number of explanations can be advanced for this:

(1) Elliot and Thrash (2010) argue that the strength of approach and avoidance tendencies are personality dependent. Our tool did not factor in personality differences, which might be moderating factors.

(2) Cybersecurity is very new in humanity’s evolutionary history. Unlike many other security-related concepts, cybersecurity is barely decades old. That means people are not as *au fait* with the cybersecurity-related terms. This might have impacted response times by requiring people to engage reflective cognitive processing, instead of tapping into their immediate responsive processing, the two systems of information processing suggested by Dual Process Theories (Kahneman, 2011).

Our initial expectation of cybersecurity-related words being evaluated as quickly and intensely as negative words was not met, possibly because reaction time in the Push/Pull task is

affected by more complex psychological processes than we initially anticipated.

(3) Cybersecurity has two dimensions related to actions to be taken by individuals: the prevention dimension (actions to take to resist attacks) and the recovery dimension (actions taken to respond to and recover from a successful attack). People may feel positive about the first but negative about the second. All of the words in our Push/Pull word list were precautionary actions but in the RETELL study we did not specify the actions. We used cybersecurity as an umbrella term. This might explain the difference between the two studies’ findings.

(4) Cybersecurity terms, as a whole, might well be infused by the fear and dread of being attacked, in addition to the uncertainty of what precautions to take, and not knowing how to implement them. The Push/Pull study did not include any element of uncertainty or fear and so did not tap into these emotions.

We also mentioned the possible role of availability, familiarity and potentially increased cognitive processing required to respond to cybersecurity terms. We deliberately chose the most popular mechanisms, but some might admittedly still not have been particularly familiar to the participants.

We have posited a number of explanations for the failure of our empirical study to confirm the findings of the first study. Future research ought therefore to explore emotional responses towards cybersecurity via less availability-dependent measures and also accommodate the controlled effect of availability on reaction time for emotionally-relevant stimuli.

### Conclusions, future work and implications

We set out to uncover blind spots that we, as cybersecurity researchers, were unaware of. We deployed an exploratory methodology borrowed from the arts to gather insights that were not prompted, framed or triggered, which they would have been if we had applied a traditional positivist approach. What we discovered was that the majority of our respondents felt negatively towards cybersecurity, and expressed these negative emotions when we gave them the opportunity to do so in an unprompted fashion. Yet, this trend could not be confirmed in a follow-up study which aimed to analyse the finding in more detail.

Our paper makes two contributions: (1) we revealed a previously undetected cybersecurity “blind spot” issue: the fact that mention of cybersecurity might well elicit negative emotions; (2) we conclude that traditional psychological tests for measuring emotional responses via words are probably not suitable for measuring emotions in the cybersecurity context.

Detecting the presence of this negativity is merely the first step. The next step is to discern its nature. As future work, it would also be of benefit to uncover the factors contributing to the negative emotions people experience with respect to cybersecurity. In our limitations section, we have already highlighted the need to find more innovative and rigorous ways of measuring these negative emotions in such a way that we do not influence them by measuring them.

The implications of this research are that those who deliver cybersecurity training should be cognisant of the fact that the concepts they are introducing might well trigger negative emotions. They ought to take specific measures to be sensitive to this, and to take the time to explain the terms clearly and carefully to ensure that unfamiliarity does not lead to uncertainty and negativity.

### Appendix

See Tables 1, 2 and 3.

**Table 1 Testing awareness and usage of precautions.**

|                                   | Use | Aware of |
|-----------------------------------|-----|----------|
| Encrypt Devices                   | 7   | 37       |
| Cover WebCam                      | 11  | 23       |
| Use Password Manager              | 17  | 46       |
| Use VPN (Virtual Private Network) | 22  | 62       |
| Logoff Websites                   | 28  | 46       |
| Browse Anonymously                | 32  | 65       |
| Make Backups                      | 37  | 68       |
| Use Firewall                      | 43  | 73       |
| Security Updates                  | 46  | 70       |
| Anti-Malware Software             | 49  | 73       |
| Change Passwords                  | 52  | 65       |
| Secure WiFi                       | 55  | 66       |
| Anti-Virus Software               | 71  | 80       |
| Lock Screen                       | 73  | 81       |
| Strong Passwords                  | 83  | 83       |

**Table 2 Frings words (Frings et al., 2010).**

| Negative |            | Neutral  |           | Positive |               |
|----------|------------|----------|-----------|----------|---------------|
| PANIK    | panic      | STILLE   | silence   | GEDULD   | patience      |
| MORD     | murder     | DAUER    | period    | FEIER    | celebration   |
| ANGST    | fear       | WINTER   | winter    | ALEE     | boulevard     |
| AUFPRALL | crash      | STUHL    | chair     | TRAUM    | dream         |
| VERRAT   | betrayal   | ZUSTAND  | condition | BEGABUNG | talent        |
| AERGER   | annoyance  | QUADRANT | square    | IDEE     | idea          |
| ANGRIFF  | attack     | PAPIER   | paper     | WIESE    | meadow        |
| LAWINE   | snowslide  | FORMAT   | format    | GARTEN   | garden        |
| UNGLUECK | misfortune | ECKE     | corner    | STRAND   | beach         |
| GEISEL   | hostage    | STRUKTUR | structure | CHANCE   | opportunity   |
| TEUFEL   | devil      | FLASCHE  | bottle    | VERSTAND | understanding |
| LUEGE    | lie        | MONAT    | month     | WAHRHEIT | truth         |
| PRUEFUNG | exam       | BRETT    | board     | GESCHENK | gift          |
| FOLTER   | torture    | WOLLE    | wool      | GENUSS   | enjoyment     |
| GEWALT   | violence   | EPOCHE   | era       | BLUETE   | blossom       |
| HASS     | hate       | WINKEL   | angle     | FANTASIE | fantasy       |
| UNFALL   | accident   | BEGRIFF  | concept   | HUMOR    | humour        |
| TUMOR    | tumour     | BEISPIEL | example   | SPASS    | fun           |

Note: German words in uppercase, English words in lowercase.

**Table 3 Overview of the content-wise categories and examples for codes included in the categories (# = number of codes).**

| Sub Category                         | Example  | #   |
|--------------------------------------|--|-----|
| <i>Perceived causes and problems</i> |  |     |
| Lack of knowledge and significance   |  | 114 |
| Lack of knowledge                    | "I also have the feeling to lack the basis to comprehensively understand the topic." (R151)  | 27  |
| Topic is considered important        | "Everyone should be well informed, because it is becoming increasingly important." (R118)  | 31  |
| Lack of significance in society      | "This is a serious issue that everyone should be concerned with. Too often this topic is taken lightly." (R18)   | 26  |
| Difficulty/complexity                | "Cybersecurity is a big and complex topic." (R121)   | 12  |
| Lack of security awareness           | "Nothing in life is safe. However, in cyber many people are less aware of this." (R128)  | 10  |
| Lack of interest/ignorance           | "My opinion on cybersecurity is that it is underestimated and not taken seriously. Too many ignore the topic, especially in terms of politics and not computer scientists." (R172) | 8   |
| <i>Responsible entities</i>          |  |     |
| People/individuals                   |  | 70  |
| People/individuals                   | "My opinion on cybersecurity is that it is severely neglected by most people." (R179)  | 29  |
| Hacker/attacks                       | "I am afraid that contact data will be stolen or hacked." (R3)   | 18  |
| Organizations                        | "People should pay more attention to cybersecurity. Companies do too little to protect their business and their customers." (R27)  | 14  |
| Politicians/countries                | "Most of all, however, I do not think the political will to adopt or implement useful and effective measures or laws." (R8)  | 9   |

**Table 3 (continued)**

| Sub Category                           | Example   | #   |
|--|---|-----|
| Security Vulnerabilities               |   | 22  |
| Usability-Security Trade-Off           | "As far as cybersecurity is concerned, I just wanted to say that with a growth in usability and comfort, security is lost. Because of this, cybersecurity and comfort can not be put together." (R40) | 9   |
| Rapid technological development        | "That Cybersecurity will always lag behind, that there will always be new problems [...]" (R82)   | 7   |
| Diverse vulnerabilities                | "My opinion on cybersecurity is that it should not be an afterthought, it should be considered from the beginning." (R94)   | 6   |
| Counter-productive behaviour           |   | 4   |
| Counter-productive behaviour           | "Instead of solving problems and increasing IT security, it is worked on actively to hide problems and to prevent solutions to these." (R58)  | 4   |
| Financing/cost                         |   | 3   |
| Financing/cost                         | "It is permanently underfinanced." (R54)  | 3   |
| Problematic Term "Cybersecurity"       |   | 3   |
| Problematic Term "Cybersecurity"       | "My opinion on cybersecurity is that it is just a neologism for politicians." (R27)   | 3   |
| Effects and consequences               |   |     |
| Societal Damage                        |   | 45  |
| Companies, infrastructure and politics | "Businesses today are inflicted a high level of damage through industrial espionage." (P 149 Main Study)  | 9   |
| Data Theft                             | "Individuals can lose money or data through insufficient security measures" (R175)  | 17  |
| Data Exposure                          | "One often thinks too little about what is published"(P 181 Main Study)   | 14  |
| Other Damage                           | "Cyber bullying." (R17)   | 5   |
| Lack of Protection/Insecurity          |   | 28  |
| Lack of Protection/Insecurity          | "[...] I have the feeling that in any case I have no serious chances to protect myself, because someone who really wants my private information, will get them." (R124)                               | 28  |
| Field of Work and Study                |   | 7   |
| Field of Work and Study                | "My opinion about cybersecurity is that it is a branch with promising job opportunities." (R50)   | 7   |
| Measures and suggestions               |   |     |
| Education & Communication              |   | 53  |
| Education & Communication              | "This should become a school subject." (R72)  | 53  |
| Technological protection & support     |   | 36  |
| Measures for increasing protection     | "The construction of a "cyber army"." (R20)   | 15  |
| Technical Improvements                 | "The ultimate goal of security policy in a networked society should be to promote free software, close security holes and collaborate on better encryption and security technologies." (R28)          | 15  |
| Usability Improvements                 | "I never read long terms and conditions through, short summaries would be better." (R148)   | 6   |
| Laws & Politics                        |   | 17  |
| Laws & Politics                        | "[...] politics provides clear structures for privacy and protects the people." (R27)   | 17  |
| Personal Security Behaviour            |   | 15  |
| Personal Security Behaviour            | "I can adapt my behaviour in the Internet so that I'm more secure or not. It's up to me." (R71)   | 15  |
| Type of statement                      |   |     |
| Statements & Opinions                  | "In terms of cybersecurity, I just wanted to say that I find it shocking how little attention we give to it." (R145)  | 168 |
| Suggestions                            | "For mobile devices, there should be more information." (R100)  | 75  |
| Questions                              | "How easy is it really to hack web cams?" (R141)  | 32  |
| Emotional-affective level              |   |     |
| Positive                               | "When someone mentions cybersecurity, I feel curious and optimistic." (R87)   | 14  |
| Negative                               | "I also worry about the security of my bank account and online affairs." (R155)   | 57  |
| Neutral                                | "When I think about cybersecurity, I feel relatively neutral." (R147)   | 4   |

**Data availability**

The datasets generated during and/or analysed during the current study are not publicly available due to the fact that many personal details are embedded in the data.

Received: 18 July 2020; Accepted: 26 January 2021;

Published online: 17 March 2021

**Note**

1 Copyright: Image of yellow head: Twitter, CC BY 4.0 <https://creativecommons.org/licenses/by/4.0>, via Wikimedia Commons [https://commons.wikimedia.org/wiki/File:Twemoji2\\_1f5e3.svg](https://commons.wikimedia.org/wiki/File:Twemoji2_1f5e3.svg), Image of pointing finger: [www.pixabay.com](http://www.pixabay.com)

**References**

Adams A, Sasse MA (1999) Users are not the enemy. *Commun ACM* 42(12):41–46  
 Ajzen I (1991) The theory of planned behavior. *Organ Behav Hum Decision Process* 50(2):179–211

Australian Government (2016) Australia's cyber security strategy. <https://cybersecuritystrategy.homeaffairs.gov.au/sites/all/themes/cybersecurity/img/PMC-Cyber-Strategy.pdf>. Accessed 14 Dec 2020  
 Bagozzi RP, Baumgartner H, Pieters R, Zeelenberg M (2000) The role of emotions in goal-directed behavior. In: Ratneshwar S, Mick DG, Huffman C (eds) The why of consumption: contemporary perspectives on consumer motives, goals, and desires. Routledge, pp 36–58  
 Bandura A (1997) Self-efficacy: the exercise of control. Macmillan  
 Bauer JM, Van Eeten MJ (2009) Cybersecurity: stakeholder incentives, externalities, and policy options. *Telecommun Policy* 33(10–11):706–719  
 Bradley MM, Lang PJ (1994) Measuring emotion: the self-assessment manikin and the semantic differential. *J Behav Ther Exp Psychiatry* 25(1):49–59  
 Bulgurcu B, Cavusoglu H, Benbasat I (2010) Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness *MIS Q* 34(3):523–548  
 BusinessLine (2019) Rise in cyber-attacks on smart buildings propels global IT/OT security market: report. <https://www.thehindubusinessline.com/news/real-estate/rise-in-cyber-attacks-on-smart-buildings-propels-global-itot-security-market-report/article29008541.ece>. Accessed 14 Dec 2020  
 Castelli C, Gabriel B, Yates J, Booth P (2018) Strengthening digital society against cyber shocks—key findings from The Global State of Information Security

- Survey 2018. <https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey/strengthening-digital-society-against-cyber-shocks.html>. Accessed 14 Dec 2020
- Cisco (2018) Cisco 2018 annual cybersecurity report. <https://www.cisco.com/c/en/us/products/security/security-reports.html>. Accessed 14 Dec 2020
- Cohen J (2013) Statistical power analysis for the behavioral sciences. Lawrence Erlbaum
- Compeau D, Higgins CA, Huff S (1999) Social cognitive theory and individual reactions to computing technology: a longitudinal study. *MIS Q* 23:145–158
- Crotty M (1998) The foundations of social research. Sage, London
- Dupuis M, Renaud K (2020) Scoping the ethical principles of cybersecurity fear appeals. *Ethics Inf Technol* 1–20. <https://doi.org/10.1007/s10676-020-09560-0>. (In press)
- Eid S (2019) The importance of strong cyber security now and in the future. <https://www.dynamicbusiness.com.au/topics/technology/the-importance-of-strong-cyber-security-now-and-in-the-future.html>. Accessed 14 Dec 2020
- Elliot AJ, Thrash TM (2010) Approach and avoidance temperament as basic dimensions of personality. *J Personal* 78(3):865–906
- Faul F, Erdfelder E, Lang AG, Buchner A (2007) G\* power 3: a flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behav Res Methods* 39(2):175–191
- Field AP, Miles J, Field Z (2012) Discovering statistics using R/Andy Field, Jeremy Miles, Zoë Field. Sage, London; Thousand Oaks
- Frings C, Englert J, Wentura D, Bermeitinger C (2010) Decomposing the emotional Stroop effect. *Q J Exp Psychol* 63(1):42–49
- Gerber P, Volkamer M, Renaud K (2017) The simpler, the better? Presenting the coping android permission-granting interface for better privacy-related decisions. *J Inf Secur Appl* 34:8–26
- Gomez P, Ratcliff R, Perea M (2007) A model of the go/no-go task. *J Exp Psychol* 136(3):389–413
- Hand DJ (2020) Dark data. Princeton University Press, Princeton and Oxford
- Her Majesty's Government (2016) National cyber security strategy 2016–2021. <https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021>. Accessed 14 Dec 2020
- Hollnagel E, Woods DD, Leveson N (2006) Resilience engineering: concepts and precepts. Ashgate Publishing, Ltd
- Inglesant PG, Sasse MA (2010) The true cost of unusable password policies: password use in the wild. In: Fitzpatrick G, Hudson S, Edwards K, Rodden T (eds) Proceedings of the SIGCHI conference on human factors in computing systems. ACM, New York, pp 383–392
- Jin G, Tu M, Kim TH, Heffron J, White J (2018) Evaluation of game-based learning in cybersecurity education for high school students. *J Educ Learn* 12(1):150–158
- Kahneman D (2011) Thinking, fast and slow. Macmillan
- Kassam KS, Mendes WB (2013) The effects of measuring emotion: physiological reactions to emotional situations depend on whether someone is asking. *PLoS ONE* 8(6):e64959
- Kraemer S, Carayon P (2007) Human errors and violations in computer and information security: the viewpoint of network administrators and security specialists. *Appl Ergon* 38(2):143–154
- Lashkari AH, Farmand S, Zakaria OB, Saleh R (2009) Shoulder surfing attack in graphical password authentication. *Int J Comput Sci Inf Secur* 6(2):145–154
- Lewin K (1936) A dynamic theory of personality: selected papers. *J Nerv Mental Dis* 84(5):612–613
- Liang H, Xue Y (2009) Avoidance of information technology threats: a theoretical perspective. *MIS Q* 33(1):71–90
- Luft J, Ingham H (1961) The johari window: a graphic model of awareness in interpersonal relations. *Hum Relat Train News* 5(9):6–7
- Luijff E, Besseling K, De Graaf P (2013) Nineteen national cyber security strategies. *Int J Critical Infrastruct* 6 9(1–2):3–31
- Marky K, Kulyk O, Renaud K, Volkamer M (2018) What did I really vote for? On the usability of verifiable e-voting schemes. In: Perry M, Cox A (eds) Proceedings of the CHI conference on human factors in computing systems, vol 176. ACM, New York
- Mayring P (2004) Qualitative content analysis. In: Flick U, von Kardoff E, Steinke I (eds) A companion to qualitative research, vol 1. Sage Publications, pp 159–176
- Miller NE (1944) Experimental studies of conflict. Ronald Press
- Moreno M, van Orden G (2001) Word recognition, cognitive psychology of. In: Smelser NJ, Baltes PB (eds) International encyclopedia of the social & behavioral sciences. Elsevier, pp 16556–16561
- Morris JD (1995) Observations: SAM: the Self-Assessment Manikin; an efficient cross-cultural measurement of emotional response *J Advert Res* 35(6):63–68
- Mowrer OH, Lamoreaux RR (1942) Avoidance conditioning and signal duration—a study of secondary motivation and reward. *Psychol Monogr* 54(5):1–34
- Oring S (2018) I wish to say. <http://www.sheryloring.org/i-wish-to-say/> Accessed 14 Dec 2020
- Public Safety Canada (2018) National cyber security strategy. <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/ntnl-cbr-scrtr-strtg/index-en.aspx>. Accessed 14 Dec 2020
- Ratcliff R (1993) Methods for dealing with reaction time outliers. *Psychol Bull* 114(3):510–532
- Renaud K, Dupuis M (2019) Cyber security fear appeals: unexpectedly complicated. In: Proceedings of the 2019 New Security Paradigms Workshop (NSPW). ACM, New York, pp 1–15
- Renaud K, Flowerday S (2018) Why governments should treat cybersecurity the way they do infectious diseases. *Behav Sci* <https://behavioralscientist.org/why-governments-should-treat-cybersecurity-the-way-they-do-infectious-diseases/>. (Retrieved 11 Mar. 2021)
- Renaud K, Zimmermann V (2019) Encouraging password manager use. *Netw Secur*, p 20
- Russell J (1980) A circumplex model of affect. *J Personal Soc Psychol* 39(6):1161–1178
- Sasse MA, Brostoff S, Weirich D (2001) Transforming the 'weakest link' a human/computer interaction approach to usable and effective security. *BT Technol J* 19(3):122–131
- Saunders M, Lewis P, Thornhill A (2016) Research methods for business students, 7th edn. Pearson, Essex
- Schneier B (2011) Secrets and lies: digital security in a networked world. John Wiley & Sons, Indianapolis
- Schneirla TC (1959) An evolutionary and developmental theory of biphasic processes underlying approach and withdrawal. In: Jones MR (ed) Nebraska symposium on motivation. University Nebraska Press, pp 1–42
- Sheng S, Broderick L, Koranda CA, Hyland JJ (2006) Why johnny still can't encrypt: evaluating the usability of email encryption software. In: Symposium on usable privacy and security. ACM, pp 3–4
- Shenton AK (2007) Viewing information needs through a Johari Window. *Ref Serv Rev* 35(3):487–496
- Solarz AK (1960) Latency of instrumental responses as a function of compatibility with the meaning of eliciting verbal signs. *J Exp Psychol* 59(4):239–245
- Susanto H, Almunawar M (2012) Information security awareness: a marketing tools for corporate's business processes. *Comput Sci J*. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2124303](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2124303). (Retrieved 11 Mar. 2021)
- Symantec Corporation (2018) Internet security threat report, vol. 23. <https://docs.broadcom.com/docs/istr-23-03-2018-en>. Accessed 14 Dec 2020
- Tooby J, Cosmides L (1990) The past explains the present: emotional adaptations and the structure of ancestral environments. *Ethol Sociobiol* 11(4–5):375–424
- Torpedo Factory Art Center (2017) Sheryl Oring: I wish to say. <http://torpedofactory.org/event/sheryl-oring-i-wish-to-say/>. Accessed 14 Dec 2020
- UEU Commission (2019) Funding opportunities about cybersecurity. <https://ec.europa.eu/digital-single-market/en/newsroom-agenda/funding-opportunity/cybersecurity>. Accessed 14 Dec 2020
- Ur B et al (2017) Design and evaluation of a data-driven password meter. In: Schraefel mc, Hourcade JP, Appert C, Wigdor D (eds) Proceedings of the 2017 CHI conference on human factors in computing systems. ACM, New York, pp 3775–3986
- US Government (2018) NATIONAL CYBER STRATEGY of the United States of America. <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>. Accessed 14 Dec 2020
- Vavra S (2019) NSA to establish new Cybersecurity Directorate to boost defense. <https://www.cyberscoop.com/nsa-cybersecurity-directorate/>. Accessed 14 Dec 2020
- Vojinovic I (2019) 30+ Fear-inducing cyber security statistics. <https://www.smallbizgenius.net/by-the-numbers/cyber-security-statistics/>. Accessed 14 Dec 2020
- Vroom C, von Solms R (2002) A practical approach to information security awareness in the organization. In: Ghonaimy MA, El-Hadidi MT, Aslan HK (eds) Security in the information society. Springer, Boston, MA, pp 19–37
- Walsham G (1995) Interpretive case studies in is research: nature and method. *Eur J Inf Syst* 4(2):74–81
- White C, Williams D, Harrison K (2010) Developing a national high school cyber defense competition. In: Proceedings of the 14th colloquium for information systems security education. Baltimore Marriott Inner Harbor Baltimore, Maryland, CSREA Press
- Whitten A, Tygar JD (1999) Why Johnny can't encrypt: a usability evaluation of PGP 5.0. In: Rubin A (ed) USENIX security symposium, vol. 348. USENIX, Monterey, California, USA, pp 169–184
- Widup S, Spitzer M, Hylender D, Bassett G (2018) Verizon data breach investigations report. [https://enterprise.verizon.com/resources/de/reports/DBIR\\_2018\\_Report\\_execsummary.pdf](https://enterprise.verizon.com/resources/de/reports/DBIR_2018_Report_execsummary.pdf). Accessed 14 Dec 2020
- Witte K (1992) Putting the fear back into fear appeals: the extended parallel process model. *Commun Monogr* 59(4):329–349
- Wood CC, Banks WW Jr (1993) Human error: an overlooked but significant information security problem. *Comput Secur* 12(1):51–60



- Zajonc RB (1980) Feeling and thinking: preferences need no inferences. *Am Psychol* 35(2):151–175
- Zimmermann V, Renaud K (2019) Moving from a “Human-as-Problem” to a “Human-as-Solution” cybersecurity mindset. *Int J Hum-Comput Stud* 131:169–187
- Zimmermann V, Gerber P, Marky K, Böck L, Kirchbuchner F (2019) Assessing users’ privacy and security concerns of smart home technologies. *i-com—J Interact Media* 18:197–216
- Zurko ME (2005) User-centered security: stepping up to the grand challenge. In: 21st Annual Computer Security Applications Conference (ACSAC’05). IEEE, New York

### Acknowledgements

This research work has been co-funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation)—251805230/GRK 2050, and by the German Federal Ministry of Education and Research and the Hessen State Ministry for Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE.

### Competing interests

The authors declare no competing interests.

### Additional information

**Correspondence** and requests for materials should be addressed to K.R. or V.Z.

**Reprints and permission information** is available at <http://www.nature.com/reprints>

**Publisher’s note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The images or other third party material in this article are included in the article’s Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article’s Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/>.

© The Author(s) 2021