‘Encryption doesn’t matter’: Pitfalls in cybersecurity communications

Florian Meissner, Jan Magnus Nold, Martina Angela Sasse, Rebecca Panskus, and Alexander Wilke

Abstract: Due to digitalisation, cybersecurity is becoming increasingly important for citizens. In Germany, the Federal Office for Information Security (BSI) is the authority responsible for ‘digital consumer protection’. Its aim is to use social media to communicate with the public about cybersecurity. Precisely, this area is an uncharted scientific territory. Theoretical approaches such as **protection motivation theory** (PMT) and **framing** provide useful guidelines for effective communication on protective behaviours. Our study explores the basic characteristics of BSI’s social media communication and analyses to what degree BSI’s posts on Twitter (X) published in 2021 and 2022 correspond with these guiding principles. Based on a computational analysis of n = 3,058 tweets and a qualitative in-depth analysis of the most prominent n = 34 tweets, the results show that BSI’s social media communication is often self-referential and discusses current events related to digital security only to a limited degree. When mentioned, cyber threats and countermeasures are typically presented in a vague manner. Similarly, it is often unclear who might be (potentially) affected by a threat. We conclude that applying a model for designing risk messages that draw on the dimensions of PMT could help cybersecurity-related social media communication.

Keywords: cybersecurity, cybersecurity communication, risk communication, protection motivation theory, framing

1. What are the objectives of communication on cybersecurity?

With the increasing number of digital devices and services, there is value to be had – not least for attackers. This growth has a significant impact on the daily lives of people and businesses, who increasingly need to know about the cybersecurity risks and steps they should take to protect themselves.

Cyberattacks, data leaks, and other security incidents can have serious consequences, ranging from financial losses and a loss of trust in digital systems to the impairment of critical infrastructures. Public communication plays an important role in raising awareness of the risks and available protection measures. The goal is not only to provide details of technical aspects but also to sensitise humans who use digital systems daily. However, awareness-raising measures are not enough to enable secure behaviour.

Research on human behaviour in cybersecurity has concluded that many of the prerequisites for the adoption of secure behaviours are not in place (Sasse et al., 2022). Many humans do not fully understand the risks associated with the use of digital devices and services. They are sometimes unaware of relevant countermeasures or doubt they are effective (Dechand et al., 2019). Such misunderstandings are partly based on media reports that misrepresent the technical reality (Fulton et al., 2019). Furthermore, humans are often overwhelmed by the many different – and sometimes contradictory – pieces of information about cybersecurity (Reeder et al., 2017). At the same time, cybersecurity risks should not be exaggerated. Florencio et al. (2014) identify the negative impact of exaggerated risks by cybersecurity vendors on businesses, and Menges et al. (2023) observe that trainees become dejected and passive after being exposed to worst-case online risks.

When it comes to communicating about IT security, national security agencies need to take a leading role. Effective public communication should create awareness of relevant risks and offer citizens concrete instructions for action to protect themselves against them. To achieve this, communication measures must reach and appeal to the target group and be understandable as well as practicable for them. In Germany, the Federal Office for Information Security (BSI) is the central authority for cybersecurity, which has the task of informing and sensitising citizens (as well as cybersecurity experts and industry professionals). The present work aims to gain insights into what and how the BSI communicates and how effective this is in helping citizens keep safe.

We use the BSI's public communication via Twitter (today X) to examine whether and how this communication can be improved. First, postings by the BSI on Twitter over a period of 20 months were analysed quantitatively. In the second step, the messages with the greatest reach were analysed qualitatively to see if they follow scientific principles for effective communication and are thus likely to be effective. Based on our results,

we derive recommendations for more effective public communication on cybersecurity.

2. State of research on public cybersecurity communication

Communication science in general, and risk and crisis communication research in particular, has so far rarely dealt with cybersecurity. The research that has been carried out reveals an increase in the media coverage of cybersecurity (Alagheband et al., 2020; Boholm, 2021; Buse & Meissner, 2023), which is often driven by key events that have increased public awareness, such as the Snowden revelations or the Cambridge Analytica case. Regarding the use of different media channels for information on cybersecurity, online media have become the primary source of information on cybersecurity for a large proportion of the population (Das et al., 2018). However, differences in demographic characteristics, affinity for technology, and gender must be considered (Herbert et al., 2022).

Another research interest is the analysis of reporting on specific incidents in the context of cybersecurity (Griesbacher & Griesbacher, 2020), as well as the portrayal of the actors, especially hackers, in the media (Buse & Meissner, 2019). Here, we examine how these actors are presented by the media and what effects these representations could have on the formation of public opinion in the field of cybersecurity.

In a prior study, the communication of cybersecurity issues in social media was examined by Vogler and Meissner (2020), who find that people affected by a data leak at a large ticketing provider communicated on Twitter primarily about service aspects and not about security aspects, which could indicate a lower prioritisation of the topic of data security. Bada et al. (2019) uncovers no evidence for the effectiveness of awareness campaigns developed to promote cybersecurity. Reasons for this are that the campaigns depend too heavily on fear-based appeals or are not adapted to the cultural circumstances of their target groups (Sasse et al., 2022). So far, however, there has been a lack of scientific studies analysing the factors for the success or failure of such campaigns to develop suggestions for an improved communication strategy in cybersecurity.

3. Theoretical background: Basic principles for effective security communication

On a theoretical level, a risk and crisis communication perspective offers suitable and instructive approaches that can be applied to communication about cybersecurity. These were developed to support the self-protective behaviour of people who are exposed to certain risks or emergency situations. The present case study is based on the **protection motivation theory** (PMT) approach by Floyd et al. (2000) and the **framing** approach by Entman (1993). Initially proposed by Rogers (1983), PMT posits that messages highlighting personal threats and countermeasures can prompt protective behaviour (Floyd et al., 2000). This theory is particularly relevant when users require added incentives for secure behaviour (Boss et al., 2015). PMT suggests two prerequisites for protective actions: **threat** and **coping appraisals**, each comprising various dimensions.

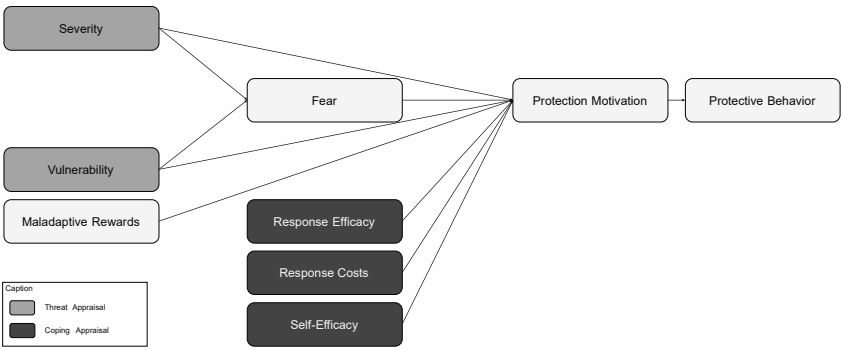

Figure 1. PMT Model, own illustration based on Boss et al. (2015, p. 854)

The threat appraisal involves assessing threat severity and personal vulnerability, with greater weight given to fear over maladaptive rewards (reward for the reaction of not protecting oneself, such as time or cost savings) to stimulate motivation for protection. Coping appraisals include perceived efficacy, self-efficacy, and the response costs of protective measures (Boss et al., 2015). The knowledge that these are key factors in convincing people to implement a certain security behaviour can also be applied to design security communication, for example, in cybersecurity. Prior PMT research highlights self-efficacy's pivotal role in influencing behaviour (Branley-Bell

et al., 2022; Feltz & Öncü, 2014; Mwagwabi & Hee Jiow, 2021; Sasse et al., 2023).

This study also includes the concept of framing, which is widely used in communication science. According to Entman (1993), so-called frames – patterns of interpretation – consist of four elements: a problem description, a causal interpretation, a moral evaluation, and a recommendation for action. For the context of this study, the categories of problem description (here in the sense of a cyber threat) and recommended action (here in the sense of a specific recommended protective behaviour) are particularly relevant. We propose that both approaches – PMT and framing – can be applied to cybersecurity communication.

4. Methodology of data collection and analysis

This case study conducts a two-stage analysis of BSI's Twitter communication on cybersecurity, aiming to assess risk communication practices and identify areas for improvement. BSI's Twitter activity serves as a representative sample of its broader online presence, including platforms like Facebook and LinkedIn, where similar content is shared.

The data for this analysis was extracted from the overall timeline of BSI's Twitter account and retrieved via the Academic Twitter API shortly before it was closed in spring 2023. The period under investigation was 21 April 2021 (two days before a new IT security law was passed in Germany) to 31 December 2022. In total, we analysed 3,058 tweets, looking at the frequency of hashtags, @-mentions, tweet frequency and the most successful (most liked) tweets. The analysis was carried out using RStudio. In addition to the BSI dataset, datasets entailing all tweets in the same time frame by the ethical hacker group Chaos Computer Club (1,145 tweets) and netzpolitik.org (2,854 tweets), a journalistic website on digital policy, were used for comparative purposes.

Then, the study conducted a qualitative analysis of BSI tweets with over 100 likes, a pragmatically set threshold indicating public attention. A category system, aligned with PMT and including problem definition and recommended action, was developed. Following Boss et al. (2015), all PMT dimensions were operationalised and coded as 'High', 'Ambivalent', 'Low', or 'Not available'. Response costs and maladaptive rewards could also be labelled 'Neutral'. Severity and vulnerability were coded only in the presence of a threat, while other PMT elements were coded alongside action

recommendations. Framing categories, inspired by Entman (1993), were established through material review. Threats, action recommendations, and responsibilities were then coded. These categories were utilised in a previous study by Meissner et al. (2024) on cybersecurity reporting in German media, facilitating theoretical comparison. Additionally, categories covering comprehensibility, prominence, target group, and unambiguity were included.

5. Findings of the analysis

a) Quantitative findings

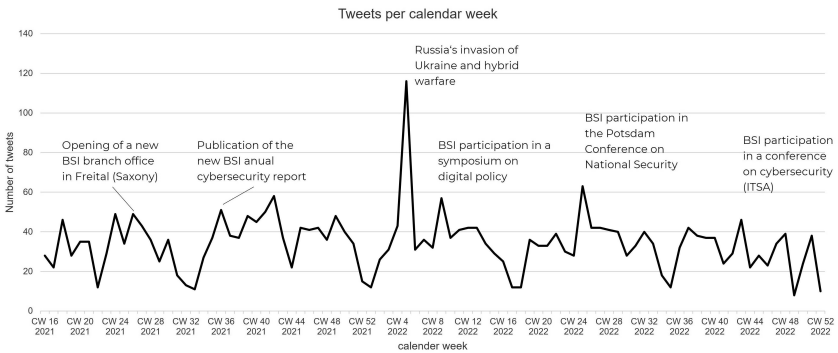

Figure 2. Time course of the number of BSI tweets per week, own illustration

First, the activity of the BSI account was examined over time (Figure 2). On average, the BSI publishes around 35 tweets per week, including individual tweets within threads. Overall, the weekly number of tweets fluctuates to a limited extent. A single clear outlier can be seen in February 2022, which is due to the Russian invasion of Ukraine and the associated hybrid warfare. Smaller peaks can all be attributed to the BSI's organisational communication. This indicates that, at least in quantitative terms, the BSI's communication is less geared towards topical media issues and instead focuses primarily on self-referential messaging.

Table 1. BSI hashtags without #deutschlanddigitalsicherbsi, own illustration

Used hashtags (#)	Amount
#deutschlanddigitalsicherbsi	1203
#bsikongress2022	92
#ransomware	46
#teambsi	41
#bsilagebericht2021	36
#cybersecurity	32
#ki	32
#einfachabsichern	31
#cybersicherheit	30
#coronawarnapp	29
…	

Table 2. Mentions without @BSI Bund and @ArneSchoenbohm, own illustration

Used mentions (@)	Amount
@cyberallianz	128
@bmi_bund	63
@certbund	58
@nancyfaeser	29
@cio_bund	28
@zivilehelden	27
@coronawarnapp	26
@bsi	23
@bka	22
@lilithwittmann	20
…	

The analysis of the most frequent hashtags proved to be less informative in terms of the cybersecurity threats covered. By far, the most frequently used hashtag was '#deutschlanddigitalsicherbsi', followed by further BSI-owned hashtags such as '#bsikongress2022' or '#teambsi'. In addition, there are generic hashtags such as '#cybersecurity' or '#itgrundschutz'; only a few specific topics such as '#ransomware' or '#coronawarnapp' are reflected here (Table 1).

In contrast to non-governmental accounts like Chaos Computer Club (a group of ethical hackers) or netzpolitik.org (a journalistic website on digital policy), analysed for comparison, the BSI account appears not to engage with government surveillance, as evident in hashtag analysis. This omission could be attributed to its status as a state authority under the Ministry of the Interior. The analysis of the most frequent @-mentions shows that almost exclusively official accounts of ministries and politicians are addressed (the accounts of the BSI itself and former President Arne Schönbohm were excluded here because they are replies to their own tweets or routine mutual references). A frequently mentioned account is @cyberallianz, which is a BSI-led initiative designed to communicate and promote dialogue with the corporate sector.

Taken together, both the hashtag analysis and the analysis of @-mentions indicate a self-referential communication approach regarding topics and accounts of state institutions and representatives, while topical issues that

could be more appealing to the public are addressed only to a limited degree.

b) Qualitative findings

In a second step, 34 tweets (the first ten are documented in the appendix below) were filtered out of the total data set (N = 3058) that had at least 100 likes, which we pragmatically considered as a threshold for a minimum amount of public attention. We decided to focus only on likes because, in terms of numbers, they were the most important engagement metric and were also highly correlated with retweets and replies. These tweets were, in a first step, categorised on an inductive basis. Accordingly, the tweets can be roughly divided into three main categories:

1. Tweets that focus on a specific warning about a security threat or another current topic, such as Kaspersky antivirus (Figure 10), Log4j (Figure 6; Figure 7), Ukraine-related phishing waves (Figure 9; Fig 11), a Covid-19 warning app (Figure 3), Wi-Fi vulnerability (Figure 4);
2. Tweets that focus on humorous content with a (sometimes informative) IT reference (Figure 8; Figure 12);
3. Tweets that provide information on cybersecurity topics without any recognisable topical reference, like the explanation of Trojans (Figure 5).

In this context, it has to be noted that none of the self-referential postings (see above) is among the most popular tweets.

In a second step, the tweets were analysed qualitatively based on the categories specified in section 4 (**PMT, framing approach**). A key result is that when it comes to specific threats or security measures, the BSI avoids addressing those affected directly. Quotes such as 'companies and organizations should …' (Figure 6) or 'be vigilant …' (Figure 9) illustrate that the perceived personal vulnerability remains unclear. Therefore, there is only a very abstract perception that a threat is relevant to the individual or the organisation. However, other elements of the PMT are also neglected, which could represent an obstacle to protective behaviour in cybersecurity. Furthermore, the severity of the threat is rarely stated or remains unclear. Only in one tweet was the threat associated with a 'warning level red' (Figure 6), which indicates a high threat. Although suitable security measures were mentioned occasionally within the tweets, these also remained relatively unclear with instructions like 'replace products' (Figure 10) or 'be vigilant

and stay informed' (Figure 9). Only one tweet on phishing in the context of the Russian invasion of Ukraine clearly stated, 'In such cases, don't transfer anything and find out about reputable aid organizations' (Figure 11).

In some cases, the measures were only to be found in a linked press release (Figure 6; Figure 7). However, no information was provided on the effectiveness of the security measures described. The self-efficacy related to the measures (meaning the degree to which they can be implemented effectively by ordinary humans) was also not presented directly. Moreover, the countermeasures that were presented suggest a high level of effort. Vague language such as 'substitute products' (Figure 10), for example, implies that the user first has to make an effort to find out what can be used to replace an existing product.

With reference to framing theory (Entman, 1993), a problem definition was generally given, but only in the further course of the Twitter thread (Figure 11) or in a linked press release (Figure 10). Although the recommended measures were mentioned, they were mainly vague (Figure 4; Figure 10). The analysis also revealed that the comprehensibility of most recommendations for action was only medium to low. In some cases, instructions were only to be found in the press release (Figure 11). Moreover, the target group remained unclear in several cases (Figure 6, Figure 10).

Finally, the qualitative analysis revealed two tweets with the potential for serious misunderstandings or promoting unsecure behaviour. For instance, the mention of replacing 'such products' without guidance on alternatives or the importance of keeping antivirus protection until a replacement is available (Figure 10) may lead users to deactivate Kaspersky antivirus without an immediate replacement, increasing their vulnerability. Another potential misunderstanding concerns the case of WLAN vulnerability (Figure 4). After a prominently placed 'Attention', it was stated that security researchers had found a vulnerability that could affect all WLAN devices. Before a link to a press release followed, the tweet read: 'Encryption doesn't matter', indicating that multiple WLAN standards were impacted. This statement can be misunderstood in the sense that encryption generally offers no protection, reinforcing an existing misconception among many humans (Abu-Salma et al., 2017).

6. Conclusions

The results show that there is room to improve the communication of the BSI on Twitter (now X), both in terms of topicality (to increase outreach) and message design (to support protective behaviour).

Regarding the quantitative results, BSI's communication on Twitter is – to a large degree – self-referential as it revolves around state institutions and representatives and could benefit from focusing more on current topics discussed in journalistic and/or social media to achieve greater relevance among the general public. It became apparent that certain topics, such as state surveillance, are avoided as the BSI is an authority subordinate to the Ministry of Interior.

Looking at the qualitative results, there is usually a threat (problem definition), and in some cases, countermeasures (recommended actions) are mentioned, although the latter often remain vague (including the target group of the recommendation). However, the central elements of the PMT were addressed only to a limited degree. Neither severity, vulnerability, efficacy, nor self-efficacy were clearly presented. Instead, the communication was often unclear and vague.

Against this backdrop, we recommend including a clear mention of target groups and their respective vulnerability in the first sentence. Doing so makes it easier for recipients to understand instantly whether the information given is relevant to them. Also, the severity of the threats should be presented in a more understandable way. Special attention should be paid to self-efficacy in communication as various studies have highlighted the importance of giving an explanation of how individuals can implement secure behaviour (Abroms & Maibach, 2008; Anker et al., 2016; Feltz & Öncü, 2014). Finally, experts should examine tweets for possible misunderstandings before publication to prevent incorrect conclusions and unsecure behaviour. Future work planned for this study will include an assessment of the tweets by cybersecurity awareness experts, who will assess both the correctness and suitability of the tweets. The results will provide further implications for BSI's social media communication.

7. Limitations and outlook

This study has several limitations. First, the study so far focuses only on Twitter (X). Secondly, the qualitative analysis is based on a relatively limi-

ted number of (the most popular) tweets that have been analysed in depth. Thirdly, even though other studies have already shown a positive effect of social media on behaviour (Ghahramani et al., 2022; Laranjo et al., 2015; Scholtz et al., 2016), the actual effect of cybersecurity-related messages on target groups – beyond predictive statements based on theory – still needs to be investigated. In essence, it is reasonable to assume that the federal German cybersecurity authority wields influence. Despite Twitter's relatively limited reach among citizens, it is plausible that political and journalistic stakeholders will carry BSI's messages to other channels. Therefore, further research will be needed to address these desiderata.

References

Abroms, L. C., & Maibach, E. W. (2008). The effectiveness of mass communication to change public behavior. *Annual Review of Public Health*, *29*(1), 219–234. https://doi.org/10.1146/annurev.publhealth.29.020907.090824

Abu-Salma, R., Sasse, M. A., Bonneau, J., Danilova, A., Naiakshina, A., & Smith, M. (2017). *Obstacles to the adoption of secure communication tools*. 2017 IEEE Symposium on Security and Privacy (SP), 137–153. https://doi.org/10.1109/SP.2017.65

Alagheband, M. R., Mashatan, A., & Zihayat, M. (2020). Time-based gap analysis of cybersecurity trends in academic and digital media. *ACM Transactions on Management Information Systems*, *11*(4), 1–20. https://doi.org/10.1145/3389684

Anker, A. E., Feeley, T. H., McCracken, B., & Lagoe, C. A. (2016). Measuring the effectiveness of mass-mediated health campaigns through meta-analysis. *Journal of Health Communication*, *21*(4), 439–456. https://doi.org/10.1080/10810730.2015.1095820

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? https://doi.org/10.48550/ARXIV.1901.02672

Boholm, M. (2021). Twenty-five years of cyber threats in the news: A study of Swedish newspaper coverage (1995–2019). *Journal of Cybersecurity*, *7*(1). https://doi.org/10.1093/cybsec/tyab016

Boss, S., Galletta, D., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, *39*(4), 837–864. https://doi.org/10.25300/MISQ/2015/39.4.5

Branley-Bell, D., Coventry, L., Dixon, M., Joinson, A., & Briggs, P. (2022). Exploring age and gender differences in ICT cybersecurity behaviour. *Human Behavior and Emerging Technologies*, 1–10. https://doi.org/10.1155/2022/2693080

Buse, C., & Meissner, F. (2019). Much ado about hacking? How news media in Germany, the United Kingdom, and the United States report cyber threats. In N. N. (Ed.), GigaNet Annual Symposium. https://www.giga-net.org/2019symposiumPapers/26_Buse_Meissner_Much-Ado-About-Hacking.pdf

Buse, C., & Meissner, F. (2023, 20.05). 'So bleiben Sie sicher im Cyberspace …'. Die Darstellung von Cybersicherheit in deutschen Online-Medien. 68. Jahrestagung der Deutschen Gesellschaft für Publizistikund Kommunikationswissenschaft (DGPuK), Bremen, Deutschland.

Crossler, R., & Bélanger, F. (2014). An extended perspective on individual security behaviors. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *45*(4), 51–71. https://doi.org/10.1145/2691517.2691521

Das, S., Lo, J., Dabbish, L., & Hong, J. I. (2018). Breaking! A typology of security and privacy news and how it's shared. In R. L. Mandryk, M. Hancock, M. Perry, & A. L. Cox (Eds.), *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (pp. 1–12). ACM. https://doi.org/10.1145/3173574.3173575

Dechand, S., Naiakshina, A., Danilova, A., & Smith, M. (2019). In encryption we don't trust: The effect of end-to-end encryption to the masses on user perception. *2019 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 401–415). https://doi.org/10.1109/EuroSP.2019.00037

Entman, R. M. (1993). Framing: Toward clarification of a fractured paradigm. *Journal of Communication*, *43*(4), 51–58.

Feltz, D. L., & Öncü, E. (2014). Self-confidence and self-efficacy. In A. G. Papaioannou & D. Hackfort (Eds.), *Routledge companion to sport and exercise psychology: Global perspectives and fundamental concepts* (pp. 417–429). Taylor & Francis. https://books.google.de/books?id=_zYsAwAAQBAJ

Florencio, D., Herley, C., & Shostack, A. (2014). FUD: A plea for intolerance. *Communications of the ACM*, *57*(6), 31–33. https://doi.org/10.1145/2602323

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, *30*(2), 407–429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Fulton, K. R., Gelles, R., McKay, A., Roberts, R., Abdi, Y., & Mazurek, M. L. (2019). *The effect of entertainment media on mental models of computer security*. USENIX Symposium on Usable Privacy and Security.

Ghahramani, A., De Courten, M., & Prokofieva, M. (2022). The potential of social media in health promotion beyond creating awareness: An integrative review. *BMC Public Health*, *22*(1), 2402. https://doi.org/10.1186/s12889-022-14885-0

Griesbacher, E.-M., & Griesbacher, M. (2020). Cybersecurity im medialen Diskurs. HMD Praxis *Der Wirtschaftsinformatik*, *57*(3), 584–596. https://doi.org/10.1365/s40702-020-00618-7

Herbert, F., Becker, S., Schaewitz, L., Hielscher, J., Kowalewski, M., Sasse, M. A., Acar, Y., & Dürmuth, M. (2022). A World Full of Privacy and Security (Mis)conceptions? Findings of a Representative Survey in 12 Countries. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2212.10382

Laranjo, L., Arguel, A., Neves, A. L., Gallagher, A. M., Kaplan, R., Mortimer, N., Mendes, G. A., & Lau, A. Y. S. (2015). The influence of social networking sites on health behavior change: A systematic review and meta-analysis. *Journal of the American Medical Informatics Association*, *22*(1), 243–256. https://doi.org/10.1136/amiajnl-2014-002841

Meissner, F., Buse, C., & Wilke, A. J. (2024, August 1). Mediated perspectives on cyber risk: A content analysis of news reporting about cyber threats and safety measures. *International Crisis and Risk Communication Conference Proceedings*. International Crisis and Risk Communication Conference. https://doi.org/10.69931/YQNA8053

Menges, U., Hielscher, J., Kocksch, L., Kluge, A., & Sasse, M. A. (2023). Caring not scaring – An evaluation of a workshop to train apprentices as security champions. *Proceedings of the 2023 European Symposium on Usable Security* (pp. 237–252). https://doi.org/10.1145/3617072.3617099

Mwagwabi, F., & Hee Jiow, J. (2021). Compliance with security guidelines in teenagers: The conflicting role of peer influence and personal norms. *Australasian Journal of Information Systems*, *25*. https://doi.org/10.3127/ajis.v25i0.2953

Reeder, R. W., Ion, I., & Consolvo, S. (2017). 152 simple steps to stay safe online: Security advice for non-tech-savvy users. *IEEE Security & Privacy*, *15*(5), 55–64. https://doi.org/10.1109/MSP.2017.3681050

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo & R. E. Petty (Eds.), *Social psychophysiology: A sourcebook* (pp. 153–176). Guildford Press.

Sasse, M. A., Hielscher, J., Friedauer, J., Menges, U., & Peiffer, M. (2022). 'Warum IT-Sicherheit in Organisationen einen Neustart braucht', in Cyber-Sicherheit ist Chefinnenund Chefsache!, online, Feb. 2022: https://www.researchgate.net/publication/358277373_Warum_IT-Sicherheit_in_Organisationen_einen_Neustart_braucht

Sasse, M. A., Hielscher, J., Friedauer, J., & Buckmann, A. (2023). Rebooting IT security awareness – How organisations can encourage and sustain secure behaviours. In S. Katsikas, F. Cuppens, C. Kalloniatis, J. Mylopoulos, F. Pallas, J. Pohle, M. A. Sasse, H. Abie, S. Ranise, L. Verderame, E. Cambiaso, J. Maestre Vidal, M. A. Sotelo Monge, M. Albanese, B. Katt, S. Pirbhulal, & A. Shukla (Eds.), *Computer security*. ESORICS 2022 International Workshops (pp. 248–265). Springer International Publishing.

Scholtz, B., Burger, C., & Zita, M. (2016). A social media environmental awareness campaign to promote sustainable practices in educational environments. In J. Marx Gomez, M. Sonnenschein, U. Vogel, A. Winter, B. Rapp, & N. Giesen (Eds.), *Advances and new trends in environmental and energy informatics* (pp. 355–369). Springer International Publishing. https://doi.org/10.1007/978-3-319-23455-7_19

Vogler, D., & Meissner, F. (2020). How users tweet about a cyber attack: An explorative study using machine learning and social network analysis. *Journal of Digital Media & Policy*, *11*(2), 195–214. https://doi.org/10.1386/jdmp_00016_1

Appendix: List of analysed tweets

Figure A1. Bundesamt für Sicherheit und Informationstechnik (@BSI_Bund). 2021a. 'This is a thread about the numerous requests around the #LucaApp. ▶ We estimate the attack scenario of a code injection via the Luca system to be plausible depending on the specific deployment environment. (1/5)'. Twitter, 28 May 2021. https://twitter.com/BSI_Bund/status/1398195272400920578

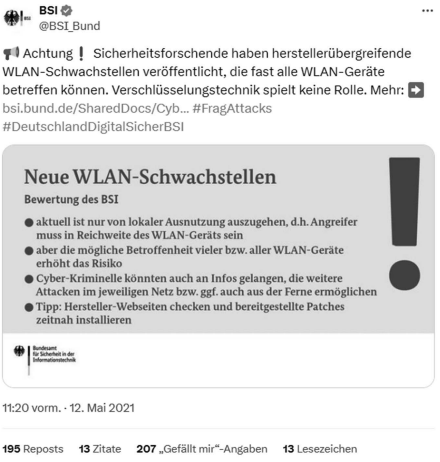

Figure A2. Bundesamt für Sicherheit und Informationstechnik (@BSI_Bund). 2021b. '📢 Attention ❗ Security researchers have published manufacturer-independent Wi-Fi vulnerabilities that can affect almost all Wi-Fi devices. Encryption technology does not play a role. Read more: […]'. Twitter, 12 May 2021. https://twitter.com/BSI_Bund/status/1392409331212210179

Figure A3. Bundesamt für Sicherheit und Informationstechnik (@BSI_Bund). 2021c. 'Disguised malware can infect your devices unnoticed and cause further damage. More information here: 👉 https://bsi.bund.de/DE/Themen/Verbr…'. Twitter, 10 June 2021. https://twitter.com/BSI_Bund/status/1402947681354387459

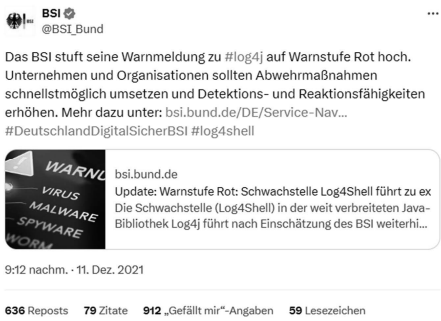

Figure A4. Bundesamt für Sicherheit und Informationstechnik (@BSI_Bund). 2021d. 'The BSI has upgraded its warning message for #log4j to warning level red. Companies and organisations should implement defensive measures as quickly as possible and increase their detection and response capabilities. Find out more at: […]'. Twitter, 11 December 2021. https://twitter.com/BSI_Bund/status/1469761986313564167

Figure A5. Bundesamt für Sicherheit und Informationstechnik (@BSI_Bund). 2021e. 'Update on #log4j warning: compromises are currently being made by crypto miners & botnets. Other forms of attack are likely. Further help regarding detection and (incomplete) list of affected products: […]'. Twitter, 12 December 2021. https://twitter.com/BSI_Bund/status/1470036192112660485

Figure A6. Bundesamt für Sicherheit und Informationstechnik (@BSI_Bund). 2021f. 'To everyone who is helping their loved ones set up and use digital devices over the festive period: Thank you 🥹 For your patience, but also for setting up and explaining the most important IT security settings! 😉 […]'. Twitter, 25 December 2021. https://twitter.com/bsi_bund/status/1474666271438479369

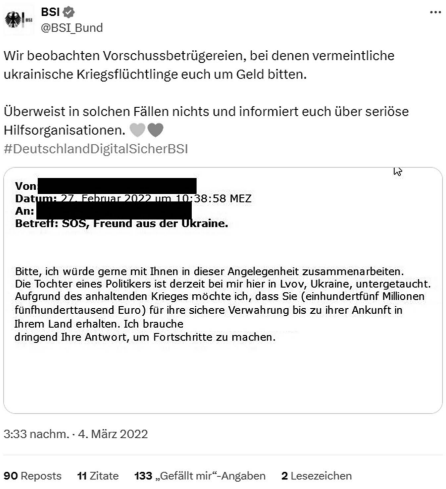

Figure A7. Bundesamt für Sicherheit und Informationstechnik (@BSI_Bund). 2022a. 'We are observing advance payment scams in which alleged Ukrainian war refugees ask you for money. Do not transfer anything in such cases and inform yourselves about serious help organisations. […]'. Twitter, 4 March 2022. https://twitter.com/BSI_Bund/status/1499754995545165829

Figure A8. Bundesamt für Sicherheit und Informationstechnik (@BSI_Bund). 2022b. 'In accordance with §7 of the BSI-Law, we warn against the use of virus protection software from the Russian manufacturer Kaspersky. We recommend replacing such applications with products of other manufacturers. To press release: […]'. Twitter, 15 March 2022. https://twitter.com/BSI_Bund/status/1503643699816845314

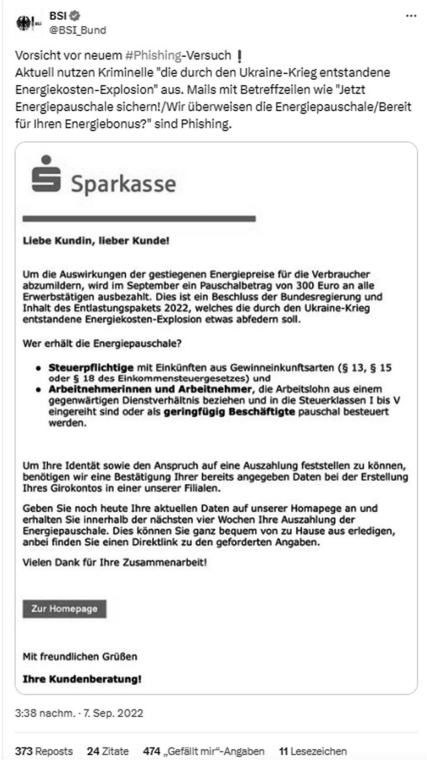

Figure A9. Bundesamt für Sicherheit und Informationstechnik (@BSI_Bund). 2022c. 'Beware of a new #phishing attempt ! Criminals are currently exploiting 'the explosion in energy costs caused by the war in Ukraine'. Emails with subject lines such as 'Secure your energy flat rate now!/We will transfer the energy flat rate/Ready for your energy bonus?" are phishing'. Twitter, 7 September 2022. https://twitter.com/BSI_Bund/status/1567507581496688641

Figure A10. Bundesamt für Sicherheit und Informationstechnik (@BSI_Bund). 2022d. 'We really couldn't resist this one for today's 'Day of Word Games'! 😅 And with that, we wish you all a great #weekend! 😎🤣🤸 […]'. Twitter, 12 November 2022. https://twitter.com/BSI_Bund/status/1591375268710522880