Case Study: Exploring Employees' Security Friction & Loss of Productivity

Jonas Hielscher, Jennifer Friedauer, Markus Schöps, M. Angela Sasse
Human-Centred Security, Ruhr University Bochum, Germany

1 Introduction

In organizations, poorly designed security policies and non-usable security mechanisms can cause `security friction` that leads to a drop in productivity among employees [2, 3]. While the burden single security mechanisms cause on users is widely studied in the usable security community, the combination of policies and tools and their effects on employees in an overall organizational context is not [2]. Existing papers primarily discuss a loss of time, e. g., when authentication takes multiple minutes per employee per day [9]. However, we argue that non-usable security tasks can cause friction through different mechanisms, such as a loss of concentration, frustration, stress, or unwillingness to innovate. For non-security-tasks, this has already been discussed and shown [12]. On the journey to measure different aspects of friction with one instrument, we embedded various friction-related questions into an online survey that we distributed to employees in an organization. Here, we report how we measured friction and what we can learn from this case study.

2 Background

Usable security research has the main goal of reducing the effort to use a secure tool or procedure [8] – explicitly and implicitly – and to increase the adoption rate of such [6]. Time-saving and subjective satisfaction of the users is what needs to be achieved [8, 17]. In organizations, employees use a multitude of security tools (e. g., authentication mechanisms, VPNs, encryption tools, digital signature mechanisms) and need to follow policies (e. g., not sharing passwords or using flash drives, even if it is convenient). Hence, some scholars think measuring employees' security behavior within the specific context of their organizations is key [2, 4, 16]. Here, the usability of one tool or aspect is less important than considering the overall effect of security on productivity, whether the multitude of security tasks causes friction with the primary task. While individual productivity is hard to define and is job dependent, it is more complex than counting time spent on a task [11, 12]. Hence, studies about a more comprehensive productivity loss due to security are rare, but it would be necessary to understand how security affects other goals of organizations. Alongside (I) a loss of time, we consider (II) a loss of concentration and mental capacities due to interruption, (III) frustration followed by a loss of motivation, (IV) a loss of the will to innovate, and (IV) the buildup of stress [7, 14] as potential adverse effects of security on employees productivity.

3 Method

We conducted an in-organization case study back in 2022. There, 5 researchers developed an online survey to assess the employees' security awareness on a German automotive supplier's site with 700 employees. The survey contained knowledge and security self-efficacy [5] related questions, but we also embedded multiple questions regarding security friction. Security friction questions were based around productivity research [1, 12, 15] and covered e. g., experienced stress, loss of innovation, perceived time loss, negative side effects, security circumvention [13] etc.

We used Likert-Scales with different scales and open-ended questions. The survey was distributed through the local work council. We got $n = 182$ valid responses for two versions of the survey – an initial extended version ($n = 53$, Appendix A) and a shorter version that led to higher completion rates ($n = 134$). We qualitatively coded open answers and performed descriptive and correlative statistics. This case study aimed to learn whether getting inside the level of security friction employees experienced would generally be possible.

Ethics & Data Privacy: While our institution has no IRB or ERB, we adhered to best practices of security research [18] and the European GDPR. Participants were informed of their rights and gave their explicit consent. Our partner organization's local work council and data protection officer reviewed and approved our survey. We deleted all potential PII after data aggregation and only reported aggregated results back to the organization.

4 Qualitative Results

Here, we present the results of the open-ended questions exemplarily. Appendix B shows the demographics of our participants.

Causes for friction $n = 65$ employees named 125 reasons for friction (from qualitative coding the question: *What rules or procedures do you find disruptive?*). The most often mentioned problems were about authentication ($n = 35$). For example, inconsistent password rules ($n = 7$) – *"[...] the programs have different requirements when creating new passwords. For example, one requires at least 1 special character; the next does not allow such a character. One allows any number of characters, the other only a much too limited number."* — [P29] –, password rotations ($n = 8$), too much authentication in general ($n = 7$), but also the missing integration of Single-Sign-On ($n = 2$) and password managers ($n = 1$). $n = 16$ employees perceived the allowed data transfer methods as too restrictive, e. g., because the necessary software was not allowed (*"Unlike our customers, we do not have access to WhatsApp, WeChat, Zoom, MS Teams and are therefore limited in our communication options."* — [P32]) because data is blocked (*"Download of Excel files from abroad are blocked across the board - even from known, confidential or shared sources"* — [P139], or because the data transfer does not work on the shop floor or in labs (*"The labs are not connected to the intranet, so data transfer is a daily obstacle."* — [P130]). Another $n = 16$ were dissatisfied with the restriction of certain devices or the prohibition of private devices. $n = 15$ named internet content filter as a problem, e. g., *"Blanket blocking of websites in which certain keywords appear. e. g., 'Share'."* — [P62]. Some of the other given friction examples were outdated security tools ($n = 6$), network restrictions ($n = 6$), long IT approval processes ($n = 6$), and, in general, missing security contact persons ($n = 1$) or restrictions in software development ($n = 3$).

Suggested improvements $n = 74$ employees made 78 suggestions on how to reduce the friction. In accordance with the perceived causes, solutions for the reduction of filters and blockers ($n = 10$, e. g.,*"Do not simply delete potentially dangerous files from the attachment, but remove them, scan them and, if 'clean', deliver them to the recipient. Possibly again with a note to only open files from trusted senders."* — [P185]), easier data transfer ($n = 8$, e. g., *"Summary of customer portals for CAD data exchange via a central interface, as it was in the past."* — [135]) and improved password regulations ($n = 8$, e. g., *"Password complexity guidelines and change intervals should be the same between systems to make it easier to comply with them."* — [P92]) were the most often mentioned. Beyond policies and technical measures, some employees made also organizational suggestions, e. g., that security decisions should be made more locally –at the site/ in the teams, not at headquarters – ($n = 6$, e. g., *"Access management within the departments by trained and authenticated employees"* — [P20]), that security personal should be approachable ($n = 6$, e. g., *"The information security officer should be more present in the company."* — [P41]), or that more easily accessible ($n = 7$), e. g., *"rules can be found quickly and easily."* — [P5]). Other suggestions for more usable security included making security invisible ($n = 3$), introducing a password manager ($n = 2$), or using biometric authentication ($n = 1$).

5 Discussion

With this non-representative in-organization case study, we developed an instrument that first gave us insights into the levels of security friction in an organization and employees' perceptions of it. We used too many item scales in the survey, preventing us from comprehensive statistical analysis. Nevertheless, the security friction-related questions can inform the design of future security friction surveys and scales.

We encourage future research on security friction in the context of organizations based on the multiple facets that friction can have, as we did in this case study. One goal of an instrument that reliably measures security friction would be to nudge organizational leadership towards considering employees' time and usable security – something they might currently not consider [10]. From an ethical perspective, improvements for employees must follow such a study. Just uncovering security friction and then ignoring it can be considered unethical. In our case, we offered our partner organization to help them resolve some of the friction causes (e. g., by advising them to introduce password managers), which did not happen in the end due to changes in organizational politics during our study.

One key learning is that we gained insights into the employees' perception of security friction by asking open-ended questions. We were indeed able to uncover different forms of friction that our partner organization should work on. Perhaps not surprisingly, employees described issues with authentication as the primary source of friction.

We were generally surprised at how open the employees were with their critique of existing security rules and policies. While we can not ultimately say what led the employees to be more open than we expected, we attribute it to some combination of (I) the work council distributing the survey as a trusted partner and (II) our appearance as independent academic researchers who will keep employees' data safe.

Acknowledgments

We thank our partner organization and its employees for their openness. We also thank our students Volkan Teterra and Sebastian Bühne for Co-Designing this study with us. Thanks

to Tatiana Mikhaylova for her help. The work was partly supported by the PhD School "SecHuman – Security for Humans in Cyberspace" by the federal state of NRW, Germany, and partly also by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy—EXC 2092 CASA—390781972.

References

[1] Inge Alberts. Challenges of information system use by knowledge workers: The email productivity paradox. *Proceedings of the American Society for Information Science and Technology*, 50(1):1–10, 2013.

[2] Adam Beautement, Ingolf Becker, Simon Parkin, Kat Krol, and Angela Sasse. Productive security: A scalable methodology for analysing employee security behaviours. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 253–270, Denver, CO, June 2016. USENIX Association.

[3] Ingolf Becker. *Measuring and Understanding Security Behaviours*. PhD thesis, UCL (University College London), 2019.

[4] Ingolf Becker, Simon Parkin, and M. Angela Sasse. Measuring the success of Context-Aware security behaviour surveys. In *The LASER Workshop: Learning from Authoritative Security Experiment Results (LASER 2017)*, pages 77–86, Berkely, October 2017. USENIX Association.

[5] Nele Borgert, Luisa Jansen, Imke Böse, Jennifer Friedauer, M Angela Sasse, and Malte Elson. Self-efficacy and security behavior: Results from a systematic review of research methods. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, pages 1–32, 2024.

[6] Deanna D Caputo, Shari Lawrence Pfleeger, M Angela Sasse, Paul Ammann, Jeff Offutt, and Lin Deng. Barriers to usable security? three organizational case studies. *IEEE Security & Privacy*, 14(5):22–32, 2016.

[7] John D'Arcy, Tejaswini Herath, and Mindy K. Shoss. Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems*, 31(2):285–318, 2014.

[8] Simson Garfinkel and Heather Richter Lipford. Usable security: History, themes, and challenges. *Synthesis Lectures on Information Security, Privacy, and Trust*, 5(2):1–124, 2014.

[9] Cormac Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 workshop on New security paradigms workshop*, pages 133–144, 2009.

[10] Jonas Hielscher, Uta Menges, Simon Parkin, Annette Kluge, and M. Angela Sasse. "Employees Who Don't Accept the Time Security Takes Are Not Aware Enough": The CISO View of Human-Centred Security. In *Proceedings of the 32nd USENIX Security Symposium*, USENIX Security '23, Berkeley, 2023. USENIX Association. https://www.usenix.org/conference/usenixsecurity23/presentation/hielscher.

[11] Pamela Karr-Wisniewski and Ying Lu. When more is too much: Operationalizing technology overload and exploring its impact on knowledge worker productivity. *Computers in Human Behavior*, 26(5):1061–1072, 2010.

[12] Young-Ho Kim, Eun Kyoung Choe, Bongshin Lee, and Jinwook Seo. Understanding personal productivity: How knowledge workers define, evaluate, and reflect on their productivity. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, page 1–12, New York, NY, USA, 2019. Association for Computing Machinery.

[13] Iacovos Kirlappos, Simon Parkin, and M Angela Sasse. " shadow security" as a tool for the learning organization. *Acm Sigcas Computers and Society*, 45(1):29–37, 2015.

[14] Chunghun Lee, Choong C. Lee, and Suhyun Kim. Understanding information security stress: Focusing on the type of information security compliance activity. *Computers & Security*, 59:60–70, 2016.

[15] Gloria Mark, Shamsi T. Iqbal, Mary Czerwinski, Paul Johns, Akane Sano, and Yuliya Lutchyn. Email duration, batching and self-interruption: Patterns of email use on productivity and stress. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, page 1717–1728, New York, NY, USA, 2016. Association for Computing Machinery.

[16] James Nicholson, Lynne Coventry, and Pam Briggs. Introducing the cybersurvival task: Assessing and addressing staff beliefs about effective cyber protection. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 443–457, Baltimore, MD, August 2018. USENIX Association.

[17] Ben Shneiderman. *Designing the User Interface: Strategies for Effective Human-Computer Interaction*. Addison-Wesley Longman Publishing Co., Inc., USA, 3rd edition, 1997.

[18] U.S. Department of Homeland Security. The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research, August 2012.

A Questionnaire

The long version of the survey we used in our study was originally in German. All items related to security friction are bold.

Demographic data & Questions to role in organization

1. Please name your Gender [Male; Female; Divers]
2. Please state your Age [Open]
3. Please state your average working hours per week [Open]
4. How much time of your working day do you spend on computer systems on average? [Open]
5. Do you have responsibility for personnel? [Yes; No]
6. Have you worked for your company remotely in the last 2 years? [Yes; No]
7. What is your highest educational qualification? [No school diploma; Comprehensive / secondary school diploma; Secondary school leaving certificate; Completed professional education; (Technical) high school diploma; University degree]
8. Have you completed training or studies in the field of computer science or IT security? [Yes; No]

IT security in the company

1. Where does information security play a role in your daily work? Name the three most important points. [Open Answer]
2. How often have you participated in training or education on information security? [More than twice a year; Once or twice a year; Once, during the training phase when starting the job; Once, at another time; Not at all; I have never heard of such an event]
3. Did you find this training helpful? [Yes, very; Yes, a little; Barely; No, not at all]
4. Who would you contact if you had questions about information security? [Open Answer]
5. Do you fear that you or your colleagues could be the target of a cyberattack? [Yes, often; Yes, sometimes; No]
6. Have you already been the target of a cyberattack in your company? [Yes, and the attack had a negative impact on my work; Yes, but the attack did not have a negative impact on my work; No]
7. **Are there IT security rules in your company that you find disruptive to doing your actual job?** [Yes; No]
8. **What rules or procedures do you find disruptive?** [Open Answer]
9. **Why do you find the rules or procedures disruptive?** [Multiple Choice Answer: Costs too much time; Costs too much concentration; Negatively affects my motivation to work; Prevents me from being innovative; Interferes with teamwork; Does not fit my workflow; Is outdated; Is superfluous; No one else complies; Other]
10. **Would you leave all the information security rules as they currently are, or would you change something?** [Yes, I would leave everything as it is; No, I would change something]
11. **What information security rules and procedures would you change?** [Open Answer]
12. **Do information security rules in your organization prevent you from proposing new ideas, improvements, programs or innovations?** [Yes, regularly I do not suggest something, because I think the rules of the information security rules don't allow it anyway; Yes, I have refrained from proposing something at least once because I thought the Information security doesn't allow it anyway; No, they don't]

IT security for managers

1. Please indicate your personal agreement with the following statements [5-point Likert scale: Strongly disagree - Disagree - Neutral - Agree - Strongly agree]
   - I see myself as a role model for my employees in handling information security at my workplace.
   - **Following the information security rules takes too much time for my employees.**
   - I think that I act in an exemplary manner in information security.
   - I think my employees behave as securely as I show them.
   - **Following the information security rules costs my employees too much nerves/ concentration.**
2. How often do you communicate information security with your employees? [Open Answer]

3. How would you describe information security communication with your employees? [I communicate new rules and technological innovations to my employees, and my employees give me feedback on them; I communicate the rules and technological innovations, but I do not receive feedback or I do not respond to it; There is little or no communication on information security issues.]

4. Are you satisfied with the communication? [Yes, I am satisfied with the communication; No, I would like to see more communication from my employees; No, more communication should emanate from me; No, there is too much communication.]

Prior knowledge of IT security

1. Which of the following terms are you familiar with? [3-point Likert scale: I can explain the term - I have heard of the term before - I do not know the term]

    - Phishing
    - End-to-end encryption
    - Virtual-Private-Network (VPN)
    - SPAM
    - Authentication
    - Digital signature
    - Email encryption
    - Firewall
    - Social engineering
    - Ransomware
    - Two-factor authentication (2FA)
    - Denial of Service (DOS) / Distributed Denial of Service (DDOS)
    - Digital certificate
    - Malware
    - Virus
    - Trojan horse
    - Point-to-point encryption
    - Spear-Phishing
    - Base domain
    - Password manager
    - Keylogger
    - Vishing
    - Makro
    - Emotet

2. Please list any signs of an IT security incident that you are aware of. [Open Answer]

3. Personal assessment of information security rules in your company [5-point Likert scale: Strongly disagree - Disagree - Neutral - Agree - Strongly agree]

    - **I find the rules of information security at my workplace understandably formulated.**
    - I have the necessary knowledge to behave securely at my workplace.
    - **I have the necessary resources to behave securely at my workplace.**
    - I can correctly apply the information security rules I know.

4. Email use [5-point Likert scale: Strongly disagree - Disagree - Neutral - Agree - Strongly agree]

    - I am allowed to open links in emails from senders I know.
    - If I open links in emails whose sender is known to me, this is secure.
    - I do not open links in emails just because the sender is known to me.
    - I do not open links in emails from unknown senders.
    - If I open a link in an email from an unknown sender, nothing bad can happen.
    - I open the links in emails from unknown senders if they look interesting.
    - I may open the attachments in emails from unknown senders.
    - I take a risk when I open the attachment in emails from unknown senders.
    - I do not open email attachments whose senders are unknown to me.

5. Internet use [5-point Likert scale: Strongly disagree - Disagree - Neutral - Agree - Strongly agree]

    - **I may enter information on websites as long as it helps me do my job.**
    - **When I enter information on a website, it doesn't matter what the information is as long as it helps me do my job.**
    - I evaluate the security of websites before I enter information on them.
    - **I may download any file to my work computer as long as it helps me do my job.**
    - I take a risk when I download files to my work computer.
    - **I download any file to my work computer which helps me in my work.**

6. Use of social media [5-point Likert scale: Strongly disagree - Disagree - Neutral - Agree - Strongly agree]
    - If I publicly post my field of work on my social media profile, this is not dangerous.
    - If I post regular status updates about my workday on social media, I am not disclosing any security-related information.
    - If I post about my work colleagues on social media, this is not a potential security risk.
    - I am taking a risk when I publicly state my former employer on my social media profile.
    - Posting something on social media does not create security issues for my company.
    - When I post something on social media, it's important to consider the security of my company.
    - I don't post anything on social media until I've thought about the potential negative consequences.
    - I need to regularly review my privacy settings on my social media accounts.
    - I believe it is important to regularly review my privacy settings on my social media accounts.
    - I do not regularly check my privacy settings on my social media accounts.
7. Security incident reporting [5-point Likert scale: Strongly disagree - Disagree - Neutral - Agree - Strongly agree]
    - I am not obligated to report security incidents in the company of which I have become aware.
    - If I have become aware of security incidents, it is risky to ignore them, even if they seem unremarkable.
    - I would report a security incident in the company if I became aware of it.
8. Password security [5-point Likert scale: Strongly disagree - Disagree - Neutral - Agree - Strongly agree]
    - In my company I need passwords consisting of letters, special characters and numbers.
    - If I use only letters in my passwords in my business, this is secure.
    - I use passwords consisting of letters, special characters and numbers in my work.
9. Two-factor authentication (2FA) [5-point Likert scale: Strongly disagree - Disagree - Neutral - Agree - Strongly agree]
    - I protect my accounts with simple authentication compared to 2FA equally.
    - I think it makes sense to use 2FA to improve the security of my accounts.
    - I use 2FA for all my accounts, for which it is possible.
10. Security on the phone [5-point Likert scale: Strongly disagree - Disagree - Neutral - Agree - Strongly agree]
    - I have to verify the identity of a caller, even if I know the phone number.
    - I consider it unnecessary to verify the identity of a caller.
    - I always verify the identity of every caller.
11. Security while working remotely [5-point Likert scale: Strongly disagree - Disagree - Neutral - Agree - Strongly agree]
    - Working remotely, I must protect my monitor from unauthorized viewing.
    - If I don't protect my monitor from unauthorized viewing when working remotely, I'm not taking a risk.
    - Working remotely, I protect my monitor from unauthorized viewing.
    - Working remotely, I don't have to secure my Wi-Fi connection with the highest possible security standard available to me.
    - If I don't use the highest possible security standard available to me for my Wi-Fi connection when working remotely, nothing bad can happen.
    - Working remotely, I use the highest possible security standard available to me for my Wi-Fi connection.

Email Security

1. Institutional [5-point Likert scale: Strongly disagree - Disagree - Neutral - Agree - Strongly agree]
    - I think the majority of all emails are sent with good intentions.
    - I think that emails are a trusted communication channel.
    - I don't think there is a problem with phishing emails in my company.
    - I know that there is a lot of talk about phishing and emails in my company.
    - I think that emails sent to my work address are more trustworthy than those sent to my home address.

2. Communication partner [5-point Likert scale: Strongly disagree - Disagree - Neutral - Agree - Strongly agree]
    - I think that my email communication partners are generally reliable.
    - I think that I can trust email senders from my own country more than senders from abroad.
    - I usually receive emails only from senders I know.
    - I am generally suspicious of email if I do not know the sender.
    - I can trust emails from senders I know.
3. Email content [5-point Likert scale: Strongly disagree - Disagree - Neutral - Agree - Strongly agree]
    - I evaluate the content of emails regardless of the grammatical and linguistic elaboration.
    - I trust an email more if my name is written in it.
    - I consider long emails more trustworthy than short ones.
    - I am especially careful about emails that ask for confirmation of my account or similar data.
    - I trust emails written in my own native language more than those written in another language.
4. Individual [5-point Likert scale: Strongly disagree - Disagree - Neutral - Agree - Strongly agree]
    - I have enough time to deal with my emails.
    - I feel confident in handling emails.
    - I frequently receive emails that contain links or attachments.
    - I have fallen for a phishing email more often.
    - I am more likely to contact others if I am unsure about the content of an email.

Experience with emails

1. Please indicate your personal agreement with the following statements [5-point Likert scale: Strongly disagree - Disagree - Neutral - Agree - Strongly agree]
    - If I set myself the goal of dealing properly with incoming emails, especially from external senders, I can pursue that goal.
    - If I set myself goals for detecting suspicious emails, I rarely achieve them.
    - When suspicious emails do come up, I have a hard time dealing with them.
    - I try to avoid learning new things for detecting suspicious emails that seem too difficult.
    - If a strategy for spotting suspicious emails doesn't work right away, I increase my efforts.
    - I feel unsure about my ability to recognize suspicious emails.
    - I am fairly confident about my ability to recognize suspicious emails.
    - When I have trouble deciding if an email is suspicious, I give up easily.
    - I don't seem to be able to recognize incoming suspicious emails.
    - I also succeed in recognizing well-made suspicious emails when I make an effort to do so.
    - If I become unsure or suspicious only after opening an attachment or link, I always know what to do.
    - I can find a solution for any email that I am unsure is suspicious.
    - I face suspicious emails calmly because I can always rely on my skills to react correctly.
    - When I am confronted with suspicious emails at work, I usually have several ideas on how to deal with them.
    - When I am confronted with suspicious emails at work, I know how to deal with them.
    - Whatever happens in my email inbox, I will handle it.
    - My experience in handling emails has prepared me well to recognize phishing emails.
    - I am able to respond to suspicious emails according to my expectations.
    - If I am unsure about a suspicious email, I know who I can contact.

Emails in daily work

1. Check emails [5-point Likert scale: Strongly disagree - Disagree - Neutral - Agree - Strongly agree]
    - **I find it stressful to check emails for suspicious features.**
    - **When I check emails for suspicious features, it takes too much time.**
    - I find checking email for suspicious features useful.
    - **When I check email for suspicious characteristics, it distracts me from my real work.**
    - **I feel that checking emails for suspicious features interferes with my daily work.**
    - My colleagues check their emails for suspicious features.

2. **When I check email for suspicious features, I forget what I was doing before.** [Never; Sometimes; Often; Regularly]

3. Reporting suspicious emails [5-point Likert scale: Strongly disagree - Disagree - Neutral - Agree - Strongly agree]

   - **If I report suspicious emails, it costs too much time.**
   - Reporting suspicious emails serves no purpose in my opinion.
   - **The suspicious email reporting process is cumbersome.**

4. **I have already reported an email as suspicious, even though it was legitimate.** [Yes; No; I have not received any feedback on it]

5. Would you like to tell us what you think could be done differently in terms of information security, e. g., rules, programs, communication, or trainings? [Open Answer]

Conclusion

1. In a few weeks, we would like to conduct a follow-up survey and actively approach some participants for this. Would you be willing to participate in such an interview? [Yes; No]

2. In order for us to possibly match your answers from this questionnaire with later interviews/surveys with you, we need a unique ID from you that still guarantees your anonymity.
   Please generate your ID according to the following rules:
   The first two letters of your mother's first name (e. g., ev for Eva) +.
   The last two letters of your father's first name (e. g., er for Peter) +
   The year of birth of your mother (e. g., 50 for 1950) +
   The first two letters of your favorite color (e. g., gr for green).
   The example ID in this case would be: ever50gr [Open Answer]

3. Thank you for your willingness to participate in a follow-up survey in a few weeks. Please leave your email address so that we can send you an invitation to this survey. The email address will not be used for any other purpose and will be deleted after the post-survey is completed. [Open Answer]

4. If you have any comments or feedback about this survey, you can use the following free text field. [Open Answer]

B Participants Demographics

Table 1: The demographics of our participants.

Age	#	*%*	**Gender**	#	*%*
18-30	16	*9*	Male	142	*78*
31-40	46	*25*	Female	37	*20*
41-50	41	*23*	Non-binary	3	*2*
51-60	62	*34*	**Education**		
>60	17	9	Primary Degree or less	4	*2*
Remote work (partly)			Vocational Training	14	*8*
Yes	156	*86*	High School	22	*12*
No	26	*14*	University Degree	142	*78*
Employment			**(Team-)leader**		
Full-time	166	*91*	Yes	34	*19*
Part-time	16	*9*	No	148	*81*