This is a repository copy of *Online security attack experience and worries of young adults in the United Kingdom*.

White Rose Research Online URL for this paper:
https://eprints.whiterose.ac.uk/187974/

Version: Accepted Version

Proceedings Paper:
Aldaraani, Najla, Petrie, Helen orcid.org/0000-0002-0100-9846 and Shahandashti, Siamak F. orcid.org/0000-0002-5284-6847 (2022) Online security attack experience and worries of young adults in the United Kingdom. In: Human Aspects of Information Security and Assurance (HAISA 2022)IFIP Advances in Information and Communication Technology. IFIP International Symposium on Human Aspects of Information Security & Assurance, 06-07 Jul 2022 Springer , GRC , pp. 300-309.

https://doi.org/10.1007/978-3-031-12172-2_24

Reuse
Items deposited in White Rose Research Online are protected by copyright, with all rights reserved unless indicated otherwise. They may be downloaded and/or printed for private study, or other acts as permitted by national copyright laws. The publisher or other rights holders may allow further reproduction and re-use of the full text version. This is indicated by the licence information on the White Rose Research Online record for the item.

Takedown
If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.

eprints@whiterose.ac.uk
https://eprints.whiterose.ac.uk/

Online security attack experience and worries of young adults in the United Kingdom

Najla Aldaraani, Helen Petrie, and Siamak F. Shahandashti

University of York, York YO10 5GH, United Kingdom

{nga505|helen.petrie|siamak.shahandashti}@york.ac.uk@york.ac.uk

Abstract. Online security issues continue to grow as a concern, amplified by the coronavirus pandemic. The current cohort of young people (aged 18 – 30, "Generation Z") are the first to have grown up with digital technologies, but to what extent are they worried about online security attacks and what experience do they have of them? An online survey of 81 young UK participants investigated their experience with 12 scenarios presenting online security attacks, asked about their level of worry with 9 online security attacks and their knowledge of computer and online security, and their confidence in their ability to identity an attack. Experience with the online attacks ranged widely, from over 50% of participants experiencing spear phishing to attempt identity theft, to only 2.5% experiencing a spoofed website. A principal components analysis showed that worries clearly fell into two components: Theft Worry and Phishing Worry. Levels of worry on these two components could be predicted from the number of different online security attacks participants had experienced. These relationships may be useful for developing education and advice to encourage better online security behaviour.

Keywords: Experience of online security attacks, worries about online security attacks, young adults, Generation Z.

1 Introduction

Issues of online security continue to grow and have been further amplified by the coronavirus pandemic. In 2020 it was estimated that in the area of identity theft alone, the number of stolen online credentials available for sale on the dark web had quadrupled in two years, with 15 billion sets of credentials available as a result of more than 100,000 data breaches [5]. It is well established that human error or risk-taking is often a source of these security issues [4, 20].

Research some 15 years ago by Furnell and colleagues [9 - 11] showed that users were superficially aware of online security issues, but often lacked detailed knowledge and appropriate strategies to protect themselves online. More recent research suggests the situation has not improved greatly. Furman et al [8] conducted in-depth interviews with 40 American adults and found that they were aware of and concerned about online security, but lacked skills to deal with the issues. Ion et al [13] investigated the practices that novice and expert users considered most important to protect themselves from security attacks. They found that there was little overlap between the groups, with novices relying on antivirus software, changing passwords frequently and visiting only those websites they know, again suggesting that novices lack appropriate strategies. Fagan and Khan [6] found that users were strongly motivated by a convenience/security tradeoff when considering online security, quite possibly to their detriment. A similar result was found specifically in relation to password behaviour, although the relationship between perceived risk and benefit varied between different types of password behaviour [17].

Recent research has also explored the individual characteristics which might predict poor online security behaviour. McCormac et al [14] used the Human Aspects of Information Security Questionnaire (HAIS-Q) to investigate the relationship between knowledge, attitudes and self-reported behaviours in relation to online security and personality traits, age and gender. They found that a number of personality traits predicted online security variables, but age and gender did not. A number of other studies have also found that age is less important that might be expected in relation to online security [2, 15]. However, other studies have found age differences [16, 25], although both these studies were about password-related behaviour in particular, with both showing that younger people were more likely to undertake at least some risky password behaviours.

One factor which may affect online security attitudes and behaviours which does not seem to have been studied is whether people have experience with online security attacks. Given the very robust psychological phenomenon of "optimistic bias" (that people consistently overestimate the likelihood of positive events and underestimate the likelihood of negative events [22]), when people experience online security attacks do they become more worried and more cautious in their behaviour? In this research, we set out to study the first component of that relationship – whether people who have experienced online security attacks are more worried about online security issues.

Given the inconsistent results on age differences in online security attitudes and behaviours, we decided to concentrate on a specific age group of young people, currently aged from 18 to 30 years. This group is also of particular interest, as they are the group often referred to (particularly in the popular media) as "Generation Z", the first generation to grow up with access to the internet and a wide range of personal digital technologies [23]. However, this does not mean that this generation is more expert about digital technologies than older generations. For example, in a large recent survey in the UK, only 28% of 18 to 24 year olds and 34% of 25 to 34 year olds were aware of four main ways in which companies can collect personal data about us on the internet [19].

Compared to previous generations, research is beginning to show that this generation of young people at least perceive themselves as more thoughtful and responsible and less risk-taking than previous generations [21]. Given their familiarity (if not necessarily expertise) with digital technologies, how does this play out in their attitudes to online security? To explore this further, we decided to present participants with a range of different online security attacks, and investigate whether they have experienced them, how worried they are about them and what the relationship between these two sets of variables.

2 Method

2.1 Participants

The inclusion criteria for participation in the study were to be aged 18 – 30 years old and to be a self-defined British person currently living in the United Kingdom. 84 participants were recruited via the Prolific participant recruitment website (prolific.co). Participants were offered compensation of GBP 2.00 for completing an online survey taking appropriately 15 minutes. Data from three participants were omitted as they failed an attention check (see section 2.2), leaving 81 participants. Table 1 summarizes the demographics of the participants. Unfortunately, due to a technical error, participants were not asked their gender. However, a gender balanced sample was requested in Prolific, so we can assume the gender balance is good.

Table 1. Demographics of the participants

Age	
Range (Mean)	18 – 30 years (24.0
Highest educational level	
High school	28 (34.6%)
Bachelors degree	34 (42.0%)
Postgraduate degree	15 (18.5%)
Professional qualification	3 (3.7%)
Prefer not to say	1 (1.2%)
Self-rating of general computer knowledge	
Median (Semi Interquartile range)	5.0 (0.5)
Z score (probability)	6.25 (< 0.001)
Self-rating of online security knowledge	
Median (Semi Interquartile range)	5.0 (1.0)
Z score (probability)	4.90 (< 0.001)
Self-rating of ability to identify an attack from a cybercriminal	
Median (Semi Interquartile range)	5.00 (1.0)
Z score (probability)	5.57 (p < 0.001)

Participants were asked to rate their general computer knowledge, their online security knowledge and their confidence in their ability to identify an attack from a cybercriminal, on 7-point Likert items (scored as 1 = not at all knowledgeable/confident to 7 = very knowledgeable/confident). Ratings were not normally distributed, so non-parametric statistics are reported. Participants rated themselves significantly above the midpoint of the rating item on all three items (Wilcoxon one sample ranked sign test with a H_O that the median rating is 4, midpoint of the scale, Z scores are used as sample size is greater than 25 [12]).

2.2 Online questionnaire

An online questionnaire was deployed through the Qualtrics survey software.

The questionnaire consisted of three parts: a set of 12 short scenarios about online security issues; a set of 9 statements about online security worries; four attention check statements; and a set of demographic questions.

The 12 scenarios were designed to describe in non-technical language the range of online security attacks that young people in the UK may have heard about or experienced (see Table 2). A very simple version of the frameworks from Lockheed Martin (the "intrusion kill chain") [24] and Mitre [18] for describing the lifecycle of security attacks was used to classify the types and stages of attacks. The range of attacks and the concrete examples of these attacks were developed through a reading of the research literature, documents advising people about attacks and how to avoid them, and several brainstorming sessions of the authors. The attacks were then transformed into short scenarios to reflect the experience of users possibly with little technical expertise.

The presentation of the scenarios in the questionnaire all followed the same format. Firstly, presentation of a scenario. Participants were asked "has something like this has ever happened to you?" on a 7-point Likert item (1 = never to 7 = many times). If a participant answered "never", they moved to the next scenario. If this type of scenario had ever happened to them, they were asked a short set of questions, always very similar, but appropriate to the scenario (not analysed for this paper, so not discussed further).

The full set of scenarios is listed in Table 2. For each scenario, we identified the adversarial strategy used for the delivery of the attack and the eventual exploitation phase of the attack following the attack lifecycle frameworks. The order in which the 12 scenarios were presented to participants was randomized to avoid practice and fatigue effects [7].

A set of 9 statements was developed to assess how worried participants were about the various types of security attacks (see Table 4), using a similar method to the development of the scenarios. Participants rated each statement on 7-point Likert items (1 = not worried at all to 7 = very worried).

Demographic questions checked for nationality and location (these were filtered in Prolific), asked for age and highest educational level, and asked participants to rate their general computer and online security knowledge and confidence in their ability to detect an attack from a cybercriminal (all on 7-point Likert items).

Table 2. The 12 scenarios representing online security attacks

Scenario	Attack type and stage
1. I click on a link (e.g. on a website, in social media, in a SMS) and then notice my device acting strangely (e.g. the device freezes, runs slowly or crashes repeatedly). I realise this may have been caused by clicking on the link.	Delivery: *Phishing* (website, social media, SMS) Exploitation: *Denial of Service*
2. I download an attachment (e.g. from an email or website) and then notice my device acting strangely (e.g. device freezes, runs slowly or crashes repeatedly). I realise this may have been caused by downloading the attachment.	Delivery: *Phishing* (email, website) Exploitation: *Denial of Service*

3. I download a free app or game from an unknown or possibly untrustworthy source. Then I notice my device is running slowly or crashing more frequently than normal.	Delivery: *Malicious Code* (in free app or game) Exploitation: *Denial of Service, Trojan Horse*
4. I install some software or a file on my device from a link or attachment I received in an email, then notice the device acting strangely. I can't access some or all of my files and then I am asked to pay a ransom to be able to retrieve these files. I realise this may have been caused by installing that software/file.	Delivery: *Phishing* (attachment in email, website) Exploitation: *Ransomware*
5. I realise that someone has made a purchase using my credit card or bank account details. I remember that I have recently entered these details online and they may have been stolen.	Delivery: unknown Exploitation: *Data Theft*, *Identity Theft*
6. I realise that someone has used my personal information or something I have stored online (e.g. your name, a photo). I remember that I have stored that online and they may have been stolen.	Delivery: unknown Exploitation: *Data Theft*, *Identity Theft*
7. I download some anti-virus/malware software to try to protect my device. But it does not seem to be effective and it keeps showing me advertisements on the device.	Delivery: *Malicious Code* (free app) Exploitation: *Adware*
8. I click on a link (e.g. on a website, in social media, in an SMS) and then notice strange things happening on my device (e.g. pop-ups appearing frequently, unrecognized apps being installed). I realise this may have been cause by clicking on the link.	Delivery: *Phishing* (link on website, social media, SMS) Exploitation: *Malware*
9. My friends report receiving strange messages from me (e.g. requesting money because I'm in trouble, including suspicious links). I realise someone must have illegally used one of my accounts.	Delivery: *Spear Phishing* Exploitation: *Identity Theft*
10. I receive a message or call from what seems to be a trustworthy source (e.g. via email, social media, SMS or phone call) asking me for personal information (e.g. account details, password) for a legitimate reason (e.g. updating data). At some point I realise this is a fake message or call.	Delivery: *Spear Phishing* (email, social media, SMS or phone call) Exploitation: *Data Theft, Identity Theft*
11. I receive a message or call which seems to be from someone I know (e.g. via email, social media, SMS) asking me to give them urgent assistance (e.g. transfer money). At some point I realise this is a fake message.	Delivery: *Identity Theft* (of another person), *Spear Phishing* Exploitation: Theft
12. I need to undertake an urgent task on the government website (e.g. renewing my passport or driving licence). I search quickly for the website in Google. The website asks for personal information (e.g. my name, date of birth or credit card details). After entering my personal information and making a payment, I realise it was not the actual government website, but a fraudulent one with a very similar address and information.	Delivery: *Spoofed Website* Exploitation: *Data Theft, Identity Theft*

3 Results

The 12 scenarios were analysed for whether participants had ever experienced this kind of online security attack, and if they had how frequently they had experienced it, summarized in Table 3. It shows that the scenarios vary greatly in how many participants reported having encountered them, from over half the participants (55.6%, 45) reporting having encountered a spear phishing attack to obtain personal data (Scenario 10) to only 2 (2.5%) who had encountered a spoofed website (Scenario 12). It is notable that the two scenarios which most participants had encountered involved spear phishing and identity theft.

The 9 statements assessing how worried participants were about different security attacks were initially analysed individually, as shown in Table 4. Levels of worry ranged from on average just below the midpoint of the 7-point scale (median of 3.0 for 4 statements, 2, 3, 8, 9) to quite high (median of 5.0 on two statements, 6 and 7). Ratings on all statements were significantly above the "not at all worried" point on the scale, and one of the two statements with ratings of 5.0 was significantly above the midpoint of the scale (Statement 6: Z = 2.09, p = 0.036), the other was not (Statement 7).

A principal components analysis[1] was conducted on the ratings of the 9 statements and produced a very clear result with two components accounting for 71.7% of the variance in the ratings. The first component (which accounted for 58.6% of the variance) included Statements 1, 4, 5, 6 and 7 (factor loadings above 0.74 in all cases) and clearly related to data/identity theft and ransomware (for simplicity we will call this the Theft Worry component). The second component (13.1% of the variance) included Statements 2, 3, 8 and 9 (factor loadings above 0.68 in all cases) and related to phishing and spear phishing (for simplicity we will call this the Phishing Worry component).

Median scores on these two components were calculated for each participant in order to investigate the relationships between these two major worries and experience with the security attacks, as measured by the scenarios and the individual characteristics of self-reported computer and security knowledge and confidence in identifying security threats.

There was no significant relationship between either self-reported computer or security knowledge and scores on either Worry component. However, there was a significant relationship between self-reported confidence in ability to identify security attacks, but only with the Phishing Worry component (Phishing Worry: rho = -0.27, p = 0.015; Theft Worry: rho = -0.15, n.s.). This showed that people who were more confident in their ability to identify security threats were less worried about phishing attacks.

[1] Principal Components Analysis is a technique to reduce a number of variables to the set which describes the data in the smallest possible number of variables with the least loss of information. It is a non-parametric analysis method. A requirement is that at least 5 observations are needed for each variable in the analysis. With 9 statements (i.e. variables), observations from 81 participants comfortably met this requirement.

Table 3. The 12 scenarios by number of participants and frequency of encountering

Scenario No	% (N) participants encountering	Frequency of encountering Median (Semi Interquartile Range)	Type of security threat
10	55.6% (45)	6.0 (2.0)	Spear phishing identity theft
11	38.3%	3.0 (1.5)	Identify theft Spear phishing
1	34.5%	3.0 (1.5)	Phishing, Denial of service
8	29.6%	4.0 (1.5)	Phishing Malware
9	27.2%	3.0 (1.5)	Identity theft
7	24.7%	4.0 (1.0)	Adware
2	23.4%	2.0 (0.5)	Phishing Denial of service
3	21.0%	3.0 (1.5)	Malicious code, Denial of service, Trojan horse
5	17.3%	2.5 (1.5)	Identity theft
6	13.6%	5.0 (1.0)	Identity theft
4	3.7%	5.0 (n/a)*	phishing ransomware
12	2.5% (2)	2.5 (n/a)*	Spoofed website

* Semi interquartile range could not be calculated, as too few ratings

There were also interesting relationships between participants' experience of security attacks and their scores on the Worry components. In terms of whether participants had experienced attacks at all, the more of the scenarios they said they had experienced, the higher their scores on both Worry components (Theft Worry: rho = 0.27, p = 0.027; Phishing Worry: rho = 0.23, p = 0.036). The effect of how frequently participants had experienced an attack was less clear. Linear regressions were conducted to predict Worry scores from the ratings of the frequency of experiencing the different scenarios. The result for the Theft Worry scores was just above standard significance level ($F_{12, 80} = 1.80$, p = 0.066) with Scenarios 1 and 4 being individually significant predictors (Scenario 1: p = 0.008; Scenario 4: p = 0.027). The result for the Phishing Worry scores was significant ($F_{12, 80} = 2.06$, p = 0.031) with Scenarios 1 and 10 being individually significant predictors (Scenario 1: p = 0.014, Scenario 10: p = 0.042). So Scenario 1 is particularly predictive of being worried about security attacks.

Table 4. The 9 statements measuring level of worry about security attacks

	Question	**Attack types**	**Median (SIQR)**
1	My device will be accessed by an attacker and my data will be destroyed	Data theft/ destruction	4.0 (1.5)
2	I will receive an email with a link leading to a fake website	Phishing Website spoofing	3.0 (1.5)

3	I will receive an email with an attachment that may include malicious code	Phishing Malware	3.0 (1.5)
4	Someone will lock me out of my device(s) and demand money to restore access	Ransomware	4.0 (1.5)
5	Someone will access my device(s) or account(s), look at my information and use it to blackmail me	Ransomware	4.0 (2.0)
6	Someone will steal my online identity and misuse it	Identity theft	5.0 (1.5)
7	Someone will access my device(s) or account(s), steal my data and use it for malicious purposes or to their advantage (e.g. make illegal purchases)	Identity theft	5.0 (1.5)
8	I will receive a phone call from someone asking about my confidential data (e.g. password, bank account details)	Spear phishing Identity theft	3.0 (1.5)
9	I will click on a link in a SMS message or email from a source that I cannot verify its origin, whether it is trustworthy	Phishing	3.0 (1.5)

4 Discussion and Conclusions

This study investigated the experience of online security attacks by a sample of young British people ("Generation Z") and their worries about online security, and how these two groups of variables related to each other.

Firstly, we found that this sample of young people rated their knowledge of computers and online security highly and were confident in their ability to identify a security attack, with median ratings on all three aspects significantly above the midpoint of the rating scale. This finding is in agreement with the findings of Cain et al [2] who testing their American participants' "cyber hygiene knowledge" with a multiple choice quiz. Participants in the 18 – 24 and 25 – 29 age groups achieved mean scores of over 80%. However, our results contrast to a very recent survey of over 2750 participants in the UK of 18 to 34 year olds, who were not very aware of how their personal data were collected by companies [19], showing a distinct lack of awareness of security issues.

To investigate the numbers of participants who had any experience of a range of online security attacks, and the frequency of those experiences, we created a set of 12 short scenarios presenting such attacks from the user's perspective in non-technical language. Participants were asked not whether they had experienced exactly the scenario, but "something like" it, to allow for a range of similar experiences. There was a wide range of experience with the security attacks, with over half the participants reporting experience with spear phishing for identity theft purposes (Scenario 10), which was also reported as occurring very frequently, but only a very small number of participants reporting having experienced a spoofed website (Scenario 12).

To investigate what participants are most worried about in relation to online security, a principal components analysis of the 9 statements provided a very clear answer – over 70% of the variance in the ratings was accounted for by two components. The first component was worry about identity and data theft and ransomware, this accounted for over half the variance in the ratings. Identity theft featured in three of the five scenarios reported as experienced by most participants, although ransomware has been experienced by very few participants. However, in the period before and during the coronavirus there was a considerable about of publicity about ransomware attacks, particularly on hospitals in the UK [1, 3]. Of course, these attacks were on large organizations, not individuals, but this publicity may have caused young British people to become more worried about this type of attack. The second component was worry about phishing and spear phishing, this accounted for a smaller proportion of the variance (13%). It may be that participants are more worried about identity/data theft and ransomware as they feel less in control of that aspect of their online security and that the consequences can be very serious. Given their confidence in their knowledge of online security and ability to identity attacks, they may well feel able to identity and deal with phishing and spear phishing attacks. This was borne out by the fact that participants who were more confident in their ability to identify attacks were less worried about phishing (as measured by the Phishing Worry component), but there was no relationship between their rating of their confidence and their worry about identify and data theft (as measured by the Theft Worry component).

There were also interesting results on the relationship between the two Worry components and the reported experience of online security attacks. The measure of the number of different scenarios (therefore the number of different security attacks) participants had experienced was the best predictor of how worried they were, on both Worry components. The frequency of encountering the attacks produced less clear results, with a significant relationship on the Phishing Worry component and a near significant relationship on the Theft Worry component. Thus, the experience of attacks may well mitigate the optimism bias which young people may have about online security. Further analysis of our data may reveal more about these relationships as we also have information on what the consequences of a attack was, which may affect the level of worry. However, at the moment, this suggests that any experience of an online security attack adds to the level of worry about online security.

The challenge for security educators and advisors is how to build on that worry into strong security behaviour. Given that some kinds of online attacks are encountered by many young people, if these could be automatically detected, that may be a very useful opportunity to provide advice and reinforcement of good security practices. On the other hand, even if young people have not experienced an attack personally, creating information in formats that appeal to them might be an effective substitute. For example, TikTok videos about how security attacks occur and the consequences and how to detect them, might help Generation Z become more careful about online security. Further research is needed to test this idea.

References

1. Beaman, C., Barkworth, A., Akande, T.D., Hakak, S., Khan, M.K.: Ransomware: recent advances, analysis, challenges and future research directions. *Computers & Security*, 111, 102490 (2021).
2. Cain, A.A., Edwards, M.E., Still, J.D.: An exploratory study of cyber hygiene behaviours and knowledge. *Journal of Information Security and Applications*, 42, 36 – 45 (2018).

3. Collier, R.: NHS ransomware attack spreads worldwide. *Canadian Medical Association Journal*, 189(22), E786 – E787 (2017).
4. Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., Baskerville, R.: Future directions for behavioural information security research. *Computers and Security*, 32, 90 – 101 (2013).
5. Digital Shadows: From exposure to takeover: the 15 billion stolen credentials allowing account takeovers. https://resources.digitalshadows.com/whitepapers-and-reports/from-exposure-to-takeover. (2020).
6. Fagan, M., Khan, M.M.H.: Why do they do what they do? *Symposium on Usable Privacy and Security (SOUPS),* USENIX Association (2016).
7. Field, A., Hole, G.: *How to design and report experiments*. Sage (2003).
8. Furman, S., Theofanos, M. F., Choong, Y., Stanton, B..: Basing cybersecurity training on user perceptions*. IEEE Security & Privacy*, 10(2), 40-49 (2012).
9. Furnell, S., Bryant, P., Phippen, A.D.: Assessing the security perceptions of personal Internet users. *Computers & Security*, 26(5), 410 – 417 (2007).
10. Furnell, S., Jusoh, A., Katsabas, D.: The challenges of understanding and using security: a survey of end-users. *Computers & Security*, 25(1), 27 – 35 (2006).
11. Furnell, S., Tsaganidi, V., Phippen, A.: Security beliefs and barriers for novice Internet users. *Computers & Security*, 27(7), 235 – 240 (2008).
12. Howell, D.C.: *Fundamental statistics for the behavioural sciences* (8th edn). Cengage (2013).
13. Ion, I., Reeder, R., Consolvo, S.: " … no one can hack my mind": comparing expert and non-expert security practices. *Symposium on Usable Privacy and Security (SOUPS),* USENIX Association (2015).
14. McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. Pattinson, M.: Individual differences and information security awareness. *Computers in Human Behaviour*, 69, 151 – 156 (2017).
15. McGill, T., Thompson, N.: Old risks, new challenges: exploring differences in security between home computer and mobile device use. *Behaviour and Information Technology*, 36(11), 1111 – 1124 (2017).
16. Merdenyan, B., Petrie, H.: Generational differences in password management behaviour. In *Proceedings of the 32nd International BCS Human Computer Interaction Conference (HCI 2018)*. British Computer Society (2018).
17. Merdenyan, B., Petrie, H.: Two studies of the perceptions of risk, benefits and likelihood of undertaking password management behaviours. *Behaviour and Information Technology*, https://doi.org/10.1080/0144929X.2021.2019832 (2022).
18. Mitre Corporation.: MITRE ATT&CK. https://attack.mitre.org/ (2022).
19. Office of Communication (Ofcom): *Adults' media use and attitudes report 2020/21* (2021).
20. Safa, N.S, Maple, C.: Human errors in the information security realm – and how to fix them. *Computer Fraud and Security*, 9, 17 – 20 (2016).
21. Seemiller, C., Grace, M.: *Generation Z goes to college*. Jossey-Bass (2016).
22. Sharot, T.: The optimism bias. *Current Biology*, 21(23), R941 – R945 (2011).
23. Turner, A.: Generation Z: Technology and social interest. *Journal of Individual Psychology*, 71(2), 103 – 113 (2015).
24. United States Senate, Committee on Commerce, Science, and Transportation.: *A "Kill Chain" analysis of the 2013 Target data breach* (2014).
25. Whitty, M., Doodson, J., Creese, S., Hodges, D.: Individual differences in cyber security behaviours: an examination of who is sharing passwords. *Cyberpsychology, Behaviour, and Social Networks*, 18(1), 3 – 7 (2015).