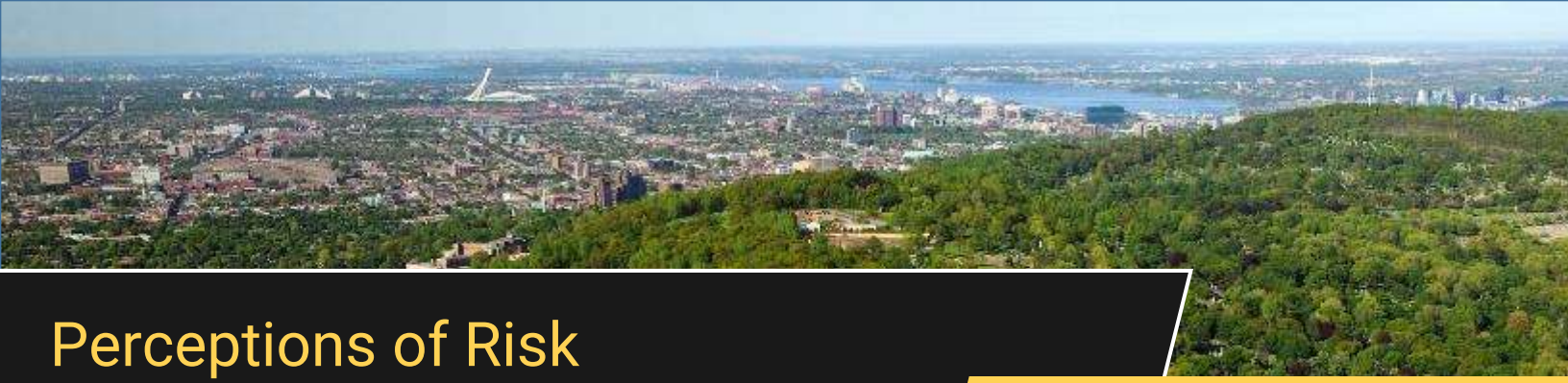
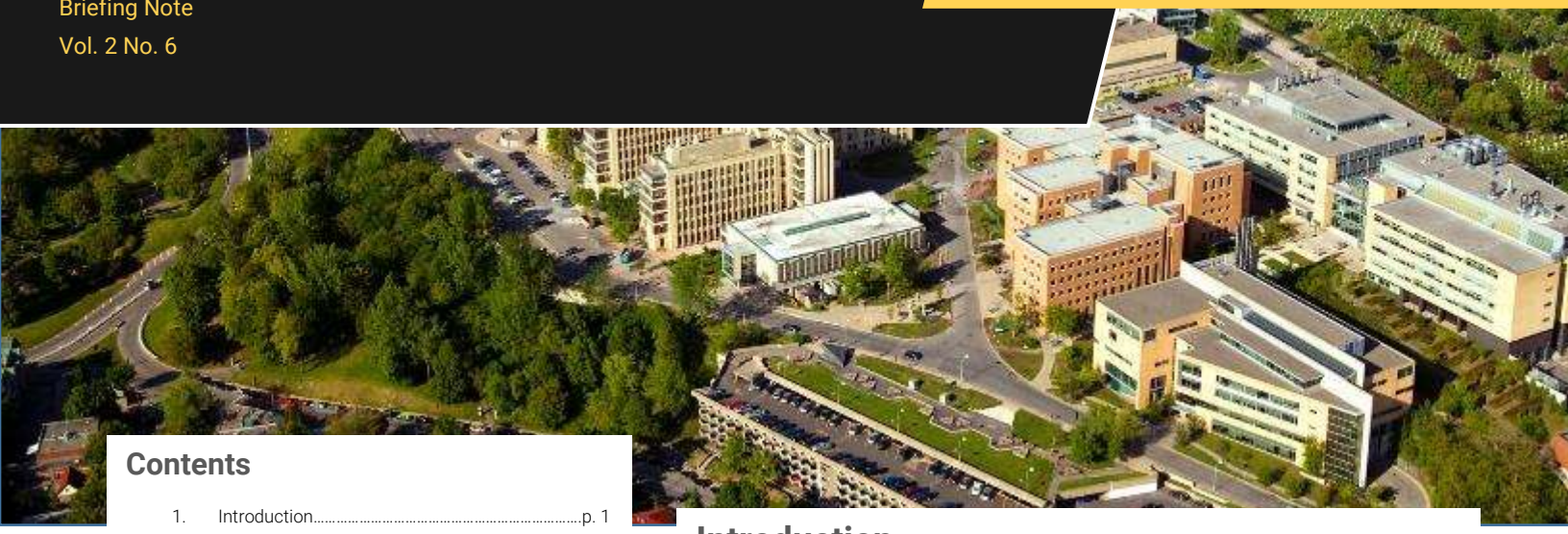


Perceptions of Risk and Security

Lorédane Piris, Master's Candidate

Briefing Note
Vol. 2 No. 6

RCCP | Research Chair in Cybercrime Prevention



Contents

The Research Chair in Cybercrime Prevention was created on the initiative of Université de Montréal, Desjardins and the National Bank of Canada. Headed by Benoît Dupont, a researcher at the International Centre for Comparative Criminology at Université de Montréal, its mission is to contribute to the advancement of research into cybercrime phenomena with a view to prevention.

Introduction

The study of users' perceptions of security and the risks they face falls under various research fields such as public health, psychology and criminology. Criminology is particularly useful for analyzing mechanisms for preventing cybercrime, as it allows us to understand how individuals make decisions and adopt (or not) protective behaviours in uncertain or unpredictable situations. It also helps us understand why users will accept or reject a security measure. To improve cybersecurity for users, we need to focus on the various ways in which users perceive and respond to risks.[1, 2]

Perceptions and risks

Definitions

A perception is a "**cognitive event in which a stimulus or object in an individual's immediate environment is represented in the individual's internal psychological activity, in principle consciously.** "[3]

Risk perception can be defined in a number of ways in theory but is generally "**a person's subjective assessment of the likelihood of a specific event occurring and how they feel affected by its consequences.**"[4]

Variance factors in perceptions

One difficulty in pinpointing risk perception is that it varies by user, and risks do not mean the same thing to everyone. When someone becomes familiar with certain risks, their perceptions may change once they are identified as such, but a multitude of factors also come into play and can change depending on the context.[1, 5, 6]

Differences in perceptions by user profile

Perceptions of security and risk vary according to **age, gender, education, employment status, socio-economic status, computer experience and attitude, and psychological, social or cultural factors.** Studies generally focus on one or more of these variables but do not address them all together. Often the focus is on differences between ordinary and expert users, as those differences commonly result in communication problems between the two groups (for example, in providing or receiving security tips).[1, 4, 6, 7, 8]

Differences in perceptions by risk and target

When assessing risk, people will calculate probability differently depending on whether the risks materialize and affect them directly or potentially affect others. Generally, people feel less concerned about the risks to themselves.[9]

The role of control and the voluntary nature of risk

When a risk is perceived to be voluntary, and under control, it appears **less likely and less severe for the individual,** which will cause users to underestimate risk and therefore decrease their protective behaviours.[1, 8, 9]

Sensitivity to risks and concerns

Some individuals may be susceptible to risks and thus easily worry about all threats, while others remain unshakeable. However, **some risks may be more of a concern than others.** For example, internet users express more concern about threats to information than threats to people or technology. Some consequences are also more worrisome than others for the same threat. For example, when data is stolen that compromises personal information (name, date of birth, address, etc.), individuals are usually most concerned with the theft of their social security number.[4, 9, 10]

Perceived risks and threats

Perceived risks vary depending on the threat, and **users do not appear to have the same perceptions of what seems most dangerous.** Also, while multiple levels of risk and threats can be identified based on online activities, **specific threats will increase user perceptions of risk and vulnerability** (such as a threat that compromises information integrity). Lastly, users may be aware of multiple threats but may choose to **focus their protective measures only on what they understand or know best** (only on passwords, for example). They will prioritize certain risks at the expense of others that are statistically more likely or more severe.[1, 4, 5, 11]

Increase in perceived risk

The potential for catastrophe will increase the perceived level of risk, especially if it has a high impact or serious consequences. Rare risks will cause terror, whereas common risks cause greater harm due to their frequency.[1, 6]

Perceptions and emotions

People will perceive and assess risk based on **their thinking,** using rational and analytical processes, but also **based on how they feel,** as emotions are involved in the perception, management and acceptance of risk. Moods and affects are a backdrop against which perceptions and thoughts about risk fluctuate. For example, a person in a good mood will be less aware of the risks around them and judge the risks as less likely to occur. They will instead focus on the benefits of risky behaviours.[12, 13, 14]

Our perceptions are also affected by the **affect heuristic**, a cognitive shortcut that alters judgment

and hastens decision-making by simplifying an individual's mental operations based on their emotions. Accordingly, technologies perceived as more advantageous will be perceived as less risky and vice versa.[1, 14]

Strong emotions also change risk estimates: **fear will intensify them while anger will minimize them**. The perception of risk will also change if these emotions relate to factors such as perceived severity, immediacy or a sense of being personally affected. For example, users' perception of risk, fear and severity are greater for identity theft than for romance fraud (a fraudulent practice in which scammers lure strangers into intimate relationships online under false pretences to obtain money).[1, 14]

Perceptions and variations: Human beings, their knowledge and calculations

Human nature

Mental models, biases and trust act as **mechanisms to simplify complexity.** They are not only useful for understanding different perceptions but also important to consider, because by understanding them and integrating them into our approaches, we can adapt communication strategies and technology interfaces to help and encourage virtuous behaviour.

Mental models

"**Mental models are depictions of how objects or systems work in people's minds,**" of how they perceive imaginary, hypothetical or real situations or recurring problems.[4] These depictions help us understand the perception of security and risk by highlighting individual reasoning, decision-making and understanding of threats and their likely consequences. **In cybersecurity, users often draw on inaccurate or fragmented mental models of the threats, risks and consequences of their actions on security.**[4, 11, 15]

Biases

Cognitive bias is an **internal mechanism that deviates from rational or logical thinking, impairs judgment and results in skewed decision-making.** A number of cognitive biases can influence perceptions, such as biases of superiority, optimism, invulnerability or the illusion of control. They are interconnected and can put people in risk-taking situations, as these "positive illusions"[2] will make people feel less vulnerable or exposed to negative consequences than their peers. They will therefore underestimate the threats, which will influence their decision-making. For example, in the case of data theft, the individual will think that only those who are better off financially are targeted.[2, 4, 5, 11]

Confidence

Self-confidence can be **cut both ways.** It can make people behave more securely and protect themselves when it comes to controlling perceived threats, especially if they strongly believe in their ability to perform the task (also called "self-efficacy").[11, 16, 17] However, too much self-confidence can have the opposite effect by skewing perceptions of security. Someone who is overly confident in themselves will feel sufficiently protected, let down their guard and no longer perceive the risks adequately (for example, experts will click on attachments in an email sent by an unknown person).[18]

Experience

The experience of users and others influences perceptions of security and risk in several ways.

First, risk-taking experiences that haven't had a negative impact on an individual will cause them to **underestimate the risk to their security.**

Second, **a past negative experience with technology,** whether or not it relates to security, will create **a negative perception that affects future**

choices, including on security. For example, users may decline security updates due to a previous bad experience with operating system updates.

Third, users refer to experiences shared by others (via blogs, web postings, informal stories and so on) for **real examples of positive or negative situations** that they can identify with.[4, 6, 15, 19, 20]

The impact of knowledge, access to information and understanding

Knowledge and understanding of security, risks and threats

Knowledge, understanding and access to information contribute to perceptions of security and risk, hence to decision-making and security behaviour. One, because **knowledge is important to bridging the gap between actual and perceived security,** and two, because what people think they know will affect their security behaviour more than they realize. Thus, if they think they understand the risks, their perceptions of them are diminished.[16, 21]

Also, when it comes to understanding threats, users sometimes have difficulty determining what directly affects them or what affects their security and protective behaviour. **Without a reliable understanding of the threats, their consequences and the advice given, users will choose to ignore them.** Finally, even if a risk is perceived as high, a lack of knowledge can lead to paralysis and inaction when someone should normally be protecting themselves.[4, 22, 23]

Knowledge debate

The lack of user knowledge about security practices and risks is widely debated. Some studies say users understand risks well but actually operate strategically to reduce the burden of applying security tips (for example, reusing passwords for multiple accounts).[24, 25]

This does not seem to solve everything **since having more knowledge and/or understanding does not necessarily lead to more secure behaviour online.** Indeed, the most advanced users sometimes fail to follow the best security practices, take adequate protective measures or pay attention, which can be dangerous and expose them more than inexperienced users.[11, 18]

Many users also report understanding threats but do nothing to protect themselves or may intend to do something but not do it (for example, planning to choose a secure password while continuing to use a weak password.) [11, 26]

Finally, **an adequate understanding of the risks does not automatically promote awareness of appropriate techniques** to protect against them. And keeping up with rapid and constant changes in technology can seem impossible for people who don't have advanced knowledge and aren't interested in acquiring it, leading to a negative perception of security.[4, 17]

Sources of advice

Risk perception is shaped by the information people are exposed to, what they believe and what they have experienced. **Sources of advice also influence security and privacy behaviours, decision-making and behaviour, including taking action.** Users generally follow the advice of people they trust and align their behaviours with family members or people perceived as having more IT experience, even if there is no indication that their advice is valid.[4, 8, 26]

Risk communication

Risk communication can inadvertently reinforce an inaccurate perception of risk. IT security systems often attempt to communicate the risks associated with decision-making, but this is generally ineffective, as users may become accustomed to these messages and no longer pay attention to them. Sometimes **security tips are inadequately justified,** for example, when they do not explain why updates are important and why they should be done regularly.

Finally, good risk communication considers not only the nature of the risk but also how well the user's mental risk model lines up with the conceptual model on which the communication is based. However, **there is a significant gap between security non-experts' and experts' mental models, which hinders effective risk communication.** Users will prioritize certain threats and value certain tips that experts might not.[4, 11, 20, 27, 28]

Calculations and compromises

Another approach looks at the rationale behind the choices people make, that is, their costs and benefits.[15]

Consider the benefits and advantages

People's perceived benefits and advantages greatly influence their perceptions of safety and risk. Often when users appear to act dangerously, it is because they are seeking advantages, since high-risk activities are associated with more benefits and advantages.[11, 14]

Users are generally aware of the costs and benefits involved but perceive them differently, with some seeing more benefits from not adopting the recommended behaviours than from following security policies. **Following security advice is considered too costly by some, who may be more confident in their security mechanisms and wary of what others suggest.** Frequently, the personal benefits are greater than the hypothetical security gain for users who do not follow the advice provided.[15, 29, 30]

Consider costs and consequences

The costs associated with risk management strategies should be considered, as they make users more reluctant to follow advices and protect themselves. **The costs of following security policies and measures may be financial, mental, opportunity, time, effort or access to desired benefits.**[24]

Users may be inclined to ignore advice because they don't see the need for it. They may generally see more benefits in maintaining existing approaches. The consequences may seem hypothetical and abstract and, therefore, difficult to assess. **Individuals may also question the cost-effectiveness of proposed protection** (for example, "Why would I pay for this? Does it protect me?"). Lastly, there is an issue with unbalanced information, with users favouring free and simple solutions as they have trouble distinguishing solution quality.[4, 11, 15, 24]

Consider the effect of timing

Risk perception is also affected by the timing of the risk (immediate, future, near and far). According to the timing effect, "**temporal distance changes responses to future events by changing how people mentally imagine these events.**"[5] A threat will be perceived as high if it is immediate. Conversely, the perceived risk is reduced when the negative consequences are delayed or are likely to be delayed and when the positive effects are immediate. Users may therefore put themselves at risk in situations perceived as having no immediate negative consequences, only benefits (such as choosing a convenient password that reduces the immediate cognitive load but increases the risk of future piracy).[1]

Security rejection—a negative cost-benefit compromise

According to some researchers, it is rational that users reject security tips since **the experts who offer them overestimate their value and benefits, ignoring their costs to users** (including time and effort). While the advice is technically appropriate, the actual indirect costs it generates are too high compared to the potential direct harm it is intended to prevent. Users often perceive the benefits as theoretical. This often leads users to boycott security and/or imperfect strategies that are supposed to reinforce it.[11, 15, 22, 23, 24, 31]

Consider compromises with security

Users often make compromises regarding IT security in terms of time, money, capacity or convenience. Some may be motivated by security features (such as two-factor authentication), while for others, the primary motivation will be convenience. **Perceived convenience is therefore important to consider since it may outweigh security concerns,** as people want simple mechanisms and devices with security appropriate for their needs.[5, 15]

Recommendations

To increase risk perception, work on perceptions and communicate

Build on users' adaptive strategies by trying to make them more secure and limit their negative consequences. For example, adaptive strategies like reuse are common for passwords. In this case, password managers could be developed to facilitate secure reuse.[22]

Thoughtfully design the interfaces and technologies users interact with. This can influence not only their understanding of security, but also their experience and thus their perceptions of security and risk.

Provide effective warnings that **clearly state the risks** and instructions that help users understand and avoid damage.[24]

Present information engagingly and concisely, using plain language.[20]

Increase user self-efficacy with tools and **build user confidence in their ability to secure their data and equipment**[17, 32] by providing practical guidance that users will trust to achieve the expected results.

Use the power of emotions, as they are integral to perceptions and assessments of security and risk.

Consider the timing of consequences, whether real, direct, immediate or long-term, for example, regarding password reuse practices.[22]

Consider the mental models of users, not experts, when communicating risks.[28]

Focus on threats that may have significant negative consequences but are perceived as less risky.[1]

Education and awareness are great, but not enough

Don't spend too much trying to educate users on specific topics, like passwords, because many know what makes a password good, even if few put their knowledge into practice. Instead, one might choose to make people aware of the alternatives, such as password managers.[5]

Educate those who lack knowledge about risks and threats but adapt communication effectively, using persuasive messaging that concretely communicates the risks users and their organizations face and the specific negative impacts of these risks on the organization. Messages about risks must be transparent and clear so that users can judge whether those risks are acceptable.[1, 17, 20]

Tailoring security policies and tools can contribute to more secure behaviours by changing the perception of security.

- Educate by communicating personalized messages and examples of risks and the direct consequences of user choices (such as making people imagine a personal loss).
- Customize dialogue boxes that present security decisions, as non-customized ones are generally ignored and ineffective.[11, 16, 20]
- Educate about biased experiences and inaccurate information.[6]

Consider the advantages and disadvantages for users

Use feedback to understand what people feel is cumbersome, identify potential challenges or costs they may face, what they would be willing to do and anything that could negatively impact their perceptions and uses. This is also important if you want to provide comprehensive information or focus their attention on a particular risk.[26]

Consider what might be both important to users but problematic for security, such as compromises with convenience or ease of use, to motivate more secure behaviour and mitigate negative perceptions. This is especially important because users will often swap security for convenience, since security is not always a primary objective.[5, 15, 24]

Consider the damage—understanding that users often lose more time than money.[24]

Think about what users will find useful, necessary or effective, because if they do not have this perception, they will resist implementing the recommendations.[31]

Highlight the risks and benefits of protective behaviours and work on the disconnect in perception regarding the benefits of following security tips.[1, 15]

Eliminate advice that is no longer relevant to avoid a pileup of advice that leads users to reject security, which they perceive as a burden. [24]

Select and prioritize tips, as users will choose between the recommendations they ignore and the ones they adopt. [24]

If possible, automate protective actions that can be automated or make them as simple as possible to ease the burden on users that can fuel negative perceptions of security.[11]

References

[1] Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J. & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. Computers in Human Behavior, 75, 547–559.

[2] Kouabenan, D. R. (2012). Décision, perception du risque et sécurité. In Traité de Psychologie du Travail et des Organisations(pp. 281–322). Dunod.

[3] https://www.larousse.fr/encyclopedie/divers/perception/78270 :

[4] Zou, Y., Mhaidli, A. H., McCall, A. & Schaub, F. (2018). "I've Got Nothing to Lose ": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach. In Fourteenth Symposium on Usable Privacy and Security ([SOUPS] 2018) (pp. 197–216).

[5] Tam, L., Glassman, M. & Vandenwauver, M. (2010). The psychology of password management: a tradeoff between security and convenience. Behaviour & Information Technology, 29(3), 233–244

[6] Slovic, P., Fischhoff, B. & Lichtenstein, S. (1982). Why study risk perception?. Risk analysis, 2(2), 83–93.

[7] Gunson, N., Marshall, D., Morton, H. & Jack, M. (2011). User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. Computers & Security, 30(4), 208–220.

[8] Furnell, S., Clarke, N., Pattinson, M. R. & Anderson, G. (2007). How well are information risks being communicated to your computer end-users? Information Management & Computer Security.

[9] Sjöberg, L. (2000). Factors in risk perception. Risk analysis, 20(1), 1–12.

[10] Friedman, B., Hurley, D., Howe, D. C., Nissenbaum, H. & Felten, E. (2002, April). Users' conceptions of risks and harms on the web: a comparative study. In CHI'02 extended abstracts on human factors in computing systems (pp. 614–615).

[11] Howe, A. E., Ray, I., Roberts, M., Urbanska, M. & Byrne, Z. (2012, May). The psychology of security for the home computer user. In 2012 IEEE Symposium on Security and Privacy (pp. 209–223). IEEE.

[12] Hogarth, R. M., Portell, M., Cuxart, A. & Kolev, G. I. (2011). Emotion and reason in everyday risk perception. Journal of Behavioral Decision Making, 24(2), 202–222.

[13] Böhm, G. & Brun, W. (2008). Intuition and affect in risk perception and decision making.

[14] Slovic, P. & Peters, E. (2006). Risk perception and affect. Current directions in psychological science, 15(6), 322-325.

[15] Fagan, M. & Khan, M. M. H. (2016). Why do they do what they do?: A study of what motivates users to (not) follow computer security advice. In Twelfth Symposium on Usable Privacy and Security ([SOUPS] 2016) (pp. 59–75).

[16] Sawaya, Y., Sharif, M., Christin, N., Kubota, A., Nakarai, A. & Yamada, A. (2017, May). Self-confidence trumps knowledge: A cross-cultural study of security behavior. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (pp. 2202–2214).

[17] Milne, G. R., Labrecque, L. I. & Cromer, C. (2009). Toward an understanding of the online consumer's risky behavior and protection practices. Journal of Consumer Affairs, 43(3), 449–473.

[18] Kang, R., Dabbish, L., Fruchter, N. & Kiesler, S. (2015). "My Data Just Goes Everywhere": User mental models of the internet and implications for privacy and security. In Eleventh Symposium on Usable Privacy and Security ([SOUPS] 2015) (pp. 39–52).

[19] Bonneau, J., Herley, C., Van Oorschot, P. C. & Stajano, F. (2012, May). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In 2012 IEEE Symposium on Security and Privacy (pp. 553–567). IEEE.

[20] Harbach, M., Hettig, M., Weber, S. & Smith, M. (2014, April). Using personal examples to improve risk communication for security & privacy decisions. In Proceedings of the SIGCHI conference on human factors in computing systems (pp. 2647–2656).

[21] Huang, D. L., Rau, P. L. P., Salvendy, G., Gao, F. & Zhou, J. (2011). Factors affecting perception of information security and their impacts on IT adoption and security practices. International Journal of Human-Computer Studies, 69(12), 870–883.

[22] Stobert, E. & Biddle, R. (2014). The password life cycle: user behaviour in managing passwords. In 10th Symposium on Usable Privacy and Security ([SOUPS] 2014) (pp. 243–255).

[23] Wash, R. (2010, July). Folk models of home computer security. In Proceedings of the Sixth Symposium on Usable Privacy and Security (pp. 1–16).

[24] Herley, C. (2009, September). So long, and no thanks for the externalities: the rational rejection of security advice by users. In Proceedings of the 2009 New Security Paradigms Workshop (pp. 133–144).

[25] Chiasson, S., Forget, A., Biddle, R. & Van Oorschot, P. C. (2009). User interface design affects security: Patterns in click-based graphical passwords. International Journal of Information Security, 8(6), 387.

[26] Furnell, S. M., Bryant, P. & Phippen, A. D. (2007). Assessing the security perceptions of personal Internet users. Computers & Security, 26(5), 410–417.

[27] Vaniea, K. E., Rader, E. & Wash, R. (2014, April). Betrayed by updates: how negative experiences affect future security. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 2671–2674).

[28] Asgharpour, F., Liu, D. & Camp, L. J. (2007, February). Mental models of security risks. In International Conference on Financial Cryptography and Data Security (pp. 367–377). Springer, Berlin, Heidelberg.

[29] Paul, C. L., Morse, E., Zhang, A., Choong, Y. Y. & Theofanos, M. (2011, September). A field study of user behavior and perceptions in smartcard authentication. In IFIP Conference on Human-Computer Interaction (pp. 1–17). Springer, Berlin, Heidelberg.

[30] Althobaiti, M. M. & Mayhew, P. (2014, October). Security and usability of authenticating process of online banking: User experience study. In 2014 International Carnahan Conference on Security Technology (ICCST) (pp. 1–6). IEEE.

[31] Ion, I., Reeder, R. & Consolvo, S. (2015). "... no one can hack my mind": Comparing Expert and Non-Expert Security Practices. In Eleventh Symposium on Usable Privacy and Security ([SOUPS] 2015) (pp. 327–346).

[32] Coventry, L., Briggs, P., Jeske, D. & van Moorsel, A. (2014, June). SCENE: A structured means for creating and evaluating behavioral nudges in a cyber security environment. In International conference of design, user experience, and usability (pp. 229–239). Springer, Cham.

[33] https://www.oxfordreference.com/view/10.1093/acref/9780191803093.001.0001/acref-9780191803093-e-159?rskey=FkcRCi&result=159

[34] Akerlof, G. A. (1978). The market for "lemons": Quality uncertainty and the market mechanism. In Uncertainty in economics (pp. 235–251). Academic Press.