OUR DECISION-MAKING PROCESSES AND HOW THEY IMPACT US IN CYBERSPACE

Leanne Torgersen[1]*, Karen Parish[2], Agnė Brilingaitė[3] and Stefan M. Schulz[1]

[1] Department of Behavioural Medicine and Principles of Human Biology for the Health Sciences, Trier University, Trier, Germany

[2] Department of Educational Studies in Teacher Education, Faculty of Education, University of Inland Norway, Hamar, Norway

[3] Cybersecurity Laboratory, Institute of Computer Science, Faculty of Mathematics and Informatics, Vilnius University, Vilnius, Lithuania

YOUNG REVIEWERS:

ANARA
AGE: 8

MARIA
AGE: 15

As humans, we are very good at processing information quickly and making decisions based on that information. But unfriendly individuals online may take advantage of these factors that make us human by encouraging us to make fast decisions, such as responding to urgent-sounding messages. This article explains the concepts of our intuitive (fast) and rational (slow) decision-making processes. It also discusses a common approach that unfriendly online individuals use in their attempts to hack or gain access to our smart phones or computers and capture our personal information. Finally, readers will learn how mindfulness can help them slow down and be present in the moment, which will help them to decide how best to respond, if at all, to the information they receive online.

LEARNING FROM EXPERIENCES

What factors make us human? These factors include our ability to think, feel, process information, make decisions, and learn from the choices we make. Our human factors help us to make sense of what we are seeing and how we interact with each other and with machines. Imagine you want to cross a street. You learned when you were small never to step into the street without checking first for oncoming cars. That is, you were taught to stop, be mindful of approaching cars, and then cross the street only after deciding it was safe. Once you crossed the street successfully without harm, you learned that this approach worked, and you should repeat it again. If you learned these safety steps as a child, then this knowledge came from personal experience and the wisdom you gained from that experience. Knowledge gained from personal experiences comes from our thinking and decision-making processes, and the consequences we experience.

TWO WAYS OF THINKING

Imagine you are at a fork in the road, and you can either take the shortcut or go the long way. Similar to a fork in the road, we tend to rely on two general types of thinking paths, called Type I and II. These thinking paths help us decide which direction to choose in many situations, including when we are online. One of our thinking paths is fast (intuitive), and the other is slow (rational), and both paths have both positive and negative outcomes (Figure 1). These two thinking paths help us to reason and make judgments and decisions [1, 2].

Figure 1

Both intuitive and rational decision making having pros and cons, as shown in the example here in green and red, respectively.
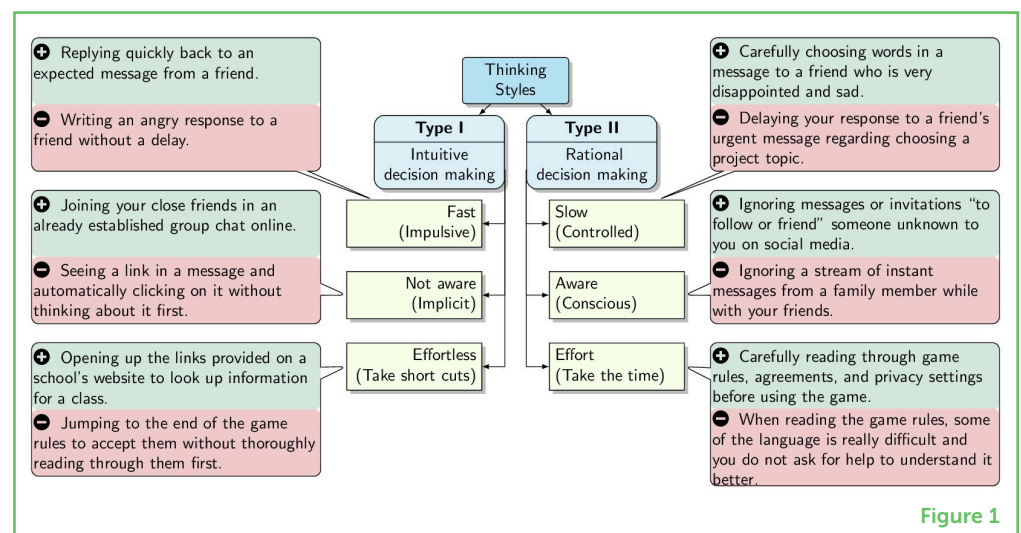

Figure 1

Type I thinking tends to be fast, automatic, and almost effortless. With Type I thinking we are not consciously aware of the information we are receiving and processing. Type I thinking involves

intuitive decision making, which is also known as our "gut feeling" decisions. For example, if a car were speeding toward you, Type I thinking and intuitive decision making would help you automatically move out of the way. However, let us say your friend posts an unpleasant message about you in a group chat. How would you respond? Would you decide quickly and respond defensively, going with your gut feeling? Or would you stop and consider that, instead of posting an angry response, you could talk directly to your friend about the post? This decision to stop and think about the best way to respond, if at all, is Type II thinking.

Type II thinking is controlled, and we are aware or conscious of this type of thinking. Type II thinking involves **rational decision making**, in which we take time and effort to assess and compare the information we have from our prior experiences (i.e., what to do before crossing the road). When using Type II thinking to make a decision, you may analyze the pros and cons of each possible outcome. You may also consider your belief system, which includes the truths that you accept about yourself. Similarly, your values, meaning what is important to you that influences and guides your behavior, can also play a role in this type of thinking.

For example, do you value safety more highly than you value taking risks? Imagine you are thinking of posting your picture online. Before doing so, you may try to figure out how your family or friends would react. To do this, you would most likely use a **mental model** to fill in or guess any missing information. Making a mental model is also part of Type II thinking. Think of it like a puzzle with missing pieces: you make a mental model to complete the puzzle, even if the pieces are not available. Completing the puzzle gives you a better idea how your friends and family would respond to your photo online.

To summarize, with rational decision making, we take our time to evaluate each option, use mental models to fill in missing information, and use our prior knowledge to help us decide. Figure 1 illustrates how our two thinking paths and decision-making processes can affect us both positively and negatively when online.

HOW CAN HUMAN FACTORS CONTRIBUTE TO CYBERATTACKS?

Now you know a bit about each thinking path and how each path affects your decision making. So, when we are online, why do we sometimes not pay attention to the warning signs in cyberspace? When you are online (in cyberspace), do you stop to consider your choices, or do you make quick decisions instead? **Cybersecurity** research has shown that when we do not focus on the information presented and instead make a choice intuitively (using Type I thinking), we have a greater chance of experiencing a negative consequence.

A report from the World Economic Forum identified that 95% of cyberattacks are related to human factors (i.e., the decisions we make) [3]. Consequences from such decisions can include businesses losing control of their computers and people losing money [3]. Like in the real world, not everyone is friendly online. Some unfriendly individuals are interested in finding our weak or vulnerable spots from our online posts so they can gain access to our personal information. By targeting our emotions or catching us when we are not focused, unfriendly online individuals encourage us to respond quickly and decide intuitively. Unfriendly online individuals have found that getting others to use Type I thinking is a successful way to access people's private information [4]. This type of cyber-targeted technique is called **social engineering**. Social-engineered messages sound urgent, like something serious has happened.

These messages make us feel we should respond immediately, without thinking about it first. A socially engineered cyberattack targets our basic psychological needs, including our interest in trusting and helping others and our need for love, acceptance, and belonging. These attacks take advantage of our ways of thinking, making decisions, and behaving, as well as our willingness to pay for something of value. For example, a person may receive a message that a family member was in an accident, and a payment is urgently needed for their medical care [4].

In short, unfriendly online individuals want us to use our intuitive decision making and respond impulsively. Remember: how you decide to respond to the information you receive online (i.e., a request to post your picture or to respond to an unpleasant chat message) can result in a positive or negative outcome. Figure 2 gives an example of friending someone online who then asks for your personal information. What would you do?

SOCIAL ENGINEERING

An online attempt to target a person's emotions and psychological needs, such as an urgent-sounding message that encourages people to respond immediately without thinking it through first.
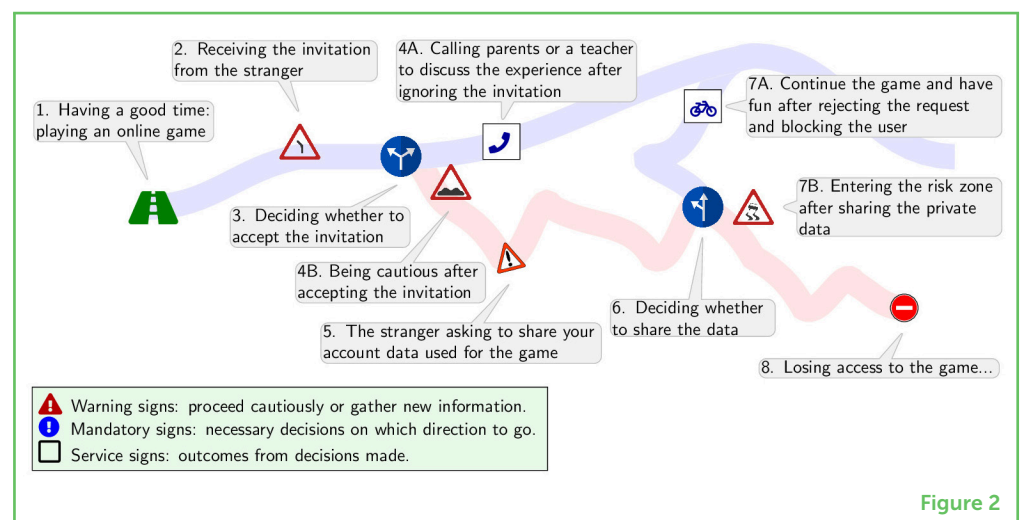
Figure 2

Online decision making represented by common traffic signs seen along the road (Icons designed using Freepik).

Figure 2

1. Having a good time: playing an online game
2. Receiving the invitation from the stranger
3. Deciding whether to accept the invitation
4A. Calling parents or a teacher to discuss the experience after ignoring the invitation
4B. Being cautious after accepting the invitation
5. The stranger asking to share your account data used for the game
6. Deciding whether to share the data
7A. Continue the game and have fun after rejecting the request and blocking the user
7B. Entering the risk zone after sharing the private data
8. Losing access to the game…

⚠ Warning signs: proceed cautiously or gather new information.
ⓘ Mandatory signs: necessary decisions on which direction to go.
▢ Service signs: outcomes from decisions made.

SUPPORTING DECISION MAKING TO AVOID CYBERATTACKS

Metacognition means thinking about the way you think. You could call metacognition your command-and-control center for organizing and managing your information and knowledge [5]. Examples of metacognition include realizing that you are using an easy way to solve a math problem, like trying random numbers, or noticing that you are focused on the rain tapping on the window instead of the actual math problem. You can use your metacognition to change your way of thinking and bring your attention back to the math problem. Thus, metacognition helps with many things, including planning, figuring out what information is missing, using knowledge from past experiences and evaluating the outcome from the choice made (what did I learn from this?). Metacognition can also help you understand how your decisions change when you feel upset or stressed, which can help you stop yourself from deciding at that time [5].

In short, metacognition is a great tool to help us avoid acting impulsively, such as by choosing not to respond immediately to an unpleasant online message [5]. Metacognition makes us aware of the warning signs, nudges us to slow down, encourages us to think about the information presented, and helps us evaluate which direction to go.

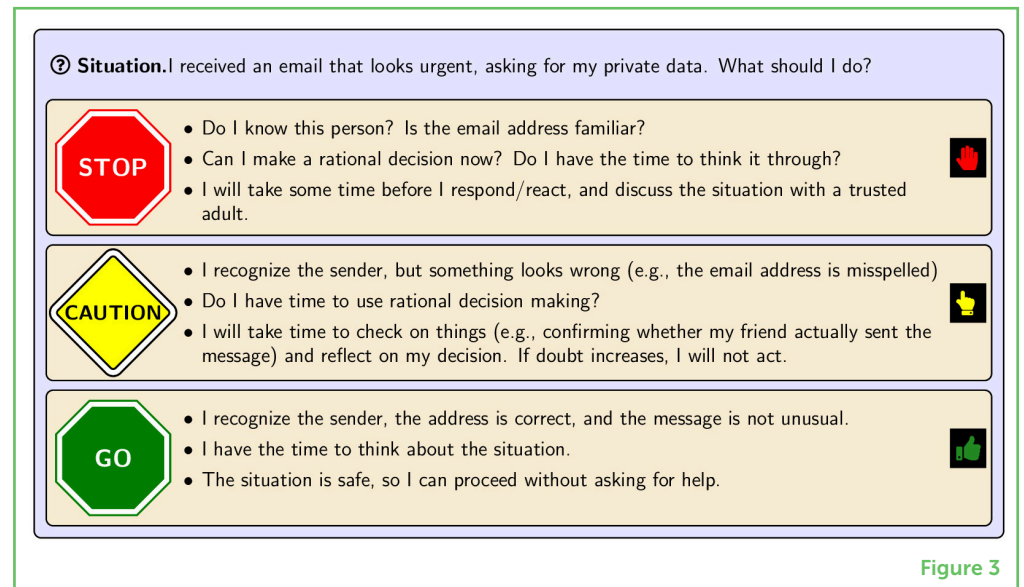## USING MINDFULNESS TO PREVENT CYBER ATTACKS

Mindfulness helps you be present in the moment, such as by noticing how you are feeling. It involves observing what is happening around you (what you are seeing) and reflecting on what it all means (assessing the situation). Mindfulness helps you pause before making a decision.

From what you have learned about Type I and II thinking and how some unfriendly online individuals may try to harm us in cyberspace, it is easy to see how, when we are distracted or upset, we can slip and give away our information. Although we cannot prevent all slips, we can try to slow down and become mindful, reducing the chances of negative outcomes from fast online decisions. Creating your own mindful decision-making streetlight, with red, yellow, and green lights, can help you ask yourself some key questions and decide what to do (Figure 3). Before making any decisions, it is always a good idea to double check with a family member or teacher about any emails, posts, or online requests that seem strange.

In summary, unfriendly online individuals use socially engineered messages to try to gain access to our personal information. Socially engineered messages encourage us to make intuitive decisions and to respond impulsively so we will not realize what information we are

Figure 3

A mindful decision-making streetlight can help you make the best decisions when you are confronted with unusual information or requests online.

Situation. I received an email that looks urgent, asking for my private data. What should I do?

STOP
- Do I know this person? Is the email address familiar?
- Can I make a rational decision now? Do I have the time to think it through?
- I will take some time before I respond/react, and discuss the situation with a trusted adult.

CAUTION
- I recognize the sender, but something looks wrong (e.g., the email address is misspelled)
- Do I have time to use rational decision making?
- I will take time to check on things (e.g., confirming whether my friend actually sent the message) and reflect on my decision. If doubt increases, I will not act.

GO
- I recognize the sender, the address is correct, and the message is not unusual.
- I have the time to think about the situation.
- The situation is safe, so I can proceed without asking for help.

Figure 3

giving away. Both metacognition and mindfulness can help us pause, reflect on what we are observing and prevent us from automatically reacting to urgently sounding messages online. Finally, it is important to understand that whatever you post online, even in a private chat with friends, leaves a "digital footprint"—a personal information trail about you. Therefore, being mindful of what you do online will help you make the right decisions and keep you safe.

ACKNOWLEDGMENTS

REFERENCES

1. Evans, J. S. B. T., and Stanovich, K. E. 2013. Dual-process theories of higher cognition: advancing the debate. *Perspect. Psychol. Sci.* 8:223–241. doi: 10.1177/1745691612460685

2. Strack, F., and Deutsch, R. 2004. Reflective and impulsive determinants of social behavior. *Person. Soc. Psychol. Rev.* 8:220–247. doi: 10.1207/s15327957pspr0803_1

3. Alsharif, M., Mishra, S., and AlShehri, M. 2022. Impact of human vulnerabilities on cybersecurity. *Comput. Syst. Sci. Eng.* 40:1153–1166. doi: 10.32604/csse.2022.019938

4. Nurse, J. R. C. 2019. Cybercrime and you: how criminals attack and the human factors that they seek to exploit. In: Attrill-Smith A, Fullwood C, Keep M, Kuss DJ, editors, *The Oxford Handbook of Cyberpsychology* (Oxford: Oxford University Press), 663–690. doi: 10.1093/oxfordhb/9780198812746.013.35

5. Flavell, J. H. 1976. Metacognitive aspects of problem solving. In: Resnick LB, editor, *The Nature of Intelligence* (London: Routledge), 231–236. doi: 10.4324/9781032646527-16

YOUNG REVIEWERS

ANARA, AGE: 8
I live in the USA. I love reading books, drawing, and playing with my friends. My favorite books are Harry Potter, Wings of Fire, and Keeper of Lost Cities. My favorite subjects in school are art, STEM, and library. When I am not in school, I like to go rock climbing and play the piano. When I grow up, I want to be a scientist or an author.

MARIA, AGE: 15
Hey! I am Maria, a grade 10 student who loves the brain and biology. In my free time, I enjoy traveling and discovering new cultures, hanging out with friends and family, and trying different dishes. I am excited to discover more about the brain and how it works!

AUTHORS

LEANNE TORGERSEN

Leanne is an Ph.D. student in nursing sciences at the Trier University in Germany. She is also a registered nurse from the United States. Her research focuses on human factors in cybersecurity, behavioral psychology, communication, stress, and emotional regulation. Her Ph.D. research project is looking at patients with electronic devices implanted in their hearts and the cyber risks that exist with these devices. Patients need to be educated on these cyber risks, so they can make good decisions on issues affecting their health. A key factor of nursing is to engage, encourage, and empower the patient. Leanne believes that through education, whether with patients at the bedside or with students in the classroom, knowledge empowers people to make the best decisions. *s1letorg@uni-trier.de

KAREN PARISH

Karen is an associate professor at University of Inland Norway. She is an educational scientist, focusing on student's learning. Karen's research focuses on the safe and ethical use of digital technology in educational contexts, such as schools and universities, to promote digital competence. She is involved in several research projects related to the design of creative learning processes in technology-rich environments, which incorporate the use of digital games, virtual and augmented reality, and humanoid robots.

AGNĖ BRILINGAITĖ

Agnė is an associate professor at Vilnius University in Lithuania. She is a computer scientist. Her research involves the application of information technologies in various fields. She develops technological solutions and methods to improve work efficiency in daily routines and the applicability of information systems. Agne educates and trains students and professionals in computer science and cybersecurity—she searches for the best ways to explain technological concepts and designs the learning materials, so they are adapted to the learners' needs to keep them actively engaged.

STEFAN M. SCHULZ

Stefan is a professor at Trier University, Germany. As a clinical psychologist and trained therapist, he leads the Department of Behavioural Medicine and Principles of Human Biology for the Health Sciences and is the managing director of nursing science. Stefan's research focuses on Stress-related mind-body interactions, with a specific interest in heart-related approaches for reducing stress and anxiety in patients and caregivers.