The Role of Heuristics in Information Security Decision Making

Amir Fard Bahreini
University of Wisconsin Whitewater
fardbaha@uww.edu

Ronald T. Cenfetelli
University of British Columbia
cenfetelli@sauder.ubc.ca

Hasan Cavusoglu
University of British Columbia
cavusoglu@sauder.ubc.ca

Abstract

Inadvertent human errors (e.g., clicking on phishing emails or falling for a spoofed website) have been the primary cause of security breaches in recent years. To understand the root cause of these errors and examine practical solutions for users to overcome them, we applied the theory of bounded rationality and explored the role of heuristics (i.e., short mental processes) in security decision making. Interviews with 27 participants revealed that users rely on various heuristics to simplify their decision making in the information security context. Specifically, users rely on experts' comments (i.e., expertise heuristic), information at hand, such as recent events (i.e., availability heuristic), and security-representative visual cues (i.e., representativeness heuristic). Findings also showed the use of other heuristics, including affect, brand, and anchoring, to a lesser degree. The results have practical and theoretical significance. In particular, they extend the literature by integrating bounded rationality concepts and elaborating "how" users simplify their security decision making by relying on cognitive heuristics.

1. Introduction

Information security threats caused by humans fall under two general categories: intentional malicious acts and inadvertent errors [1]. In 2017, it was estimated that inadvertent and irrational human errors (i.e., cognitive biases) are a source of approximately 84% of all breaches [2]. The impact of inadvertent errors has become more significant in recent years, in particular after the COVID-19 pandemic, as more and more people began working from home, away from company assistance and safeguard measures [3]. While a myriad of factors causes cognitive biases, one potential group of mental processes have been often linked to their occurrence: heuristics [4].

"Heuristics are methods for arriving at satisfactory solutions with modest amounts of computation," explains Simon ([5], pg. 11). By using heuristics, people aim "*to reduce the effort associated with decision processes"* (Shah & Oppenheimer, [6], Pg. 207). Heuristics are not inherently problematic. Rather, they act as a double-edged sword. For instance, many experts reach fast and correct decisions by using heuristics to make their decisions. Such usages of heuristics work because they have been based on years of experience [7]. However, in many other situations, they can lead individuals to erroneous judgments and decisions (i.e., biases). Take determining whether an email is phishing as an example. Several criteria can be used to assess whether an email is malicious or not: the address it came from, grammatical error, the urgency of email, title, and signature are a few of those criteria. As defined under normative theories, a rational decision maker will look at all of these factors before deciding. However, by using heuristics, people often do not look at all factors necessary and most likely decide after assessing only a few (and perhaps one) factor(s). Such shortcuts ultimately may lead to inadvertent errors in decisions.

As a specific example, consider password management: As the dominant method of authentication, password management continues to constitute a significant part of current issues in human security practices. the annual Verizon Data Breach Investigation Report noted that 80% of data breaches are linked to compromised, weak, and reused passwords. What makes this threat more problematic is, this number has been fairly consistent in recent years despite the increases in password requirements [8]. When 2,000 individuals in the United States, Australia, France, Germany, and the UK were surveyed, around 90% knew the criteria for strong passwords and the risk of using the same password for multiple accounts [9]. However, 59% of respondents said they use the same password for all their accounts. Convenience, which is one of the primary objectives in the use of heuristics, is noted as a main reason for this behavior [10].

Despite advances in various other fields [6, 11-14], fewer number of studies have investigated the role of heuristics in information security literature [15-19]. Many prior heuristics-related studies include research commentary, review, and call for research studies, which have suggested that heuristics may influence

URI: https://hdl.handle.net/10125/79924
978-0-9981331-5-7

security decision making but have not empirically investigated their role [15, 20].

By some accounts, more than 70 heuristics have been examined in different fields in the prior research [6]. Understanding how users use heuristics in their security decision-making and which types are most dominant can provide great value to companies that spend millions training their employees.

Accordingly, based on the increasing number of threats due to inadvertent errors, potential financial and data losses for the ones committing the errors and their organizations, and the potential role of heuristics in decision making, we argue that examining the concept of heuristics in information security can be highly valuable. Furthermore, the lack of extensive work or theoretical discussions in information security literature creates an opportunity for an exploratory study into the role of heuristics and their resulting biases in information security decision making.

We argue an exploratory study can deliver two main values: a) providing a holistic assessment of the role of heuristics in information security decision making and b) exploring underlying heuristics' sub-themes specific to the information security domain. While there are generally acceptable heuristics that can apply to all domains, scholars over the years have shown that some heuristics are more common in some fields than others [6]. Additionally, there is an inherent difference between IS and other domains, which may lead to the development of the usage of some heuristics. People do not make security decisions in a vacuum. Rather they use technology to make such decisions. Therefore, in IS, there is a human-IT interaction that, in other domains, does not necessarily exist [21]. Furthermore, this interaction can influence how people process information and make security decisions. Therefore, understanding the prevalent heuristics used in information security and underlying heuristics' sub-theme (i.e., specific detail with heuristic usage) can further enhance our understanding. Based on this motivation, we aim to answer the following questions: **RQ1.** Do heuristics comprise an essential part of security decision making? **RQ2.** What heuristics are commonly used in the process of security decision making?

2. Literature Review

Heuristics and bounded rationality were first mentioned in the privacy literature nearly 20 years ago [22, 23]. As Acquisti [22] pointed out, normative models do not properly explain privacy decisions, and *"it is unrealistic to expect individual rationality in this context,"* as users mostly *"resort to simple heuristics."* However, there has been little investigation into the nature and specific role of heuristics in information security [16-19]. Over the years, several studies sporadically delve into the role of bounded rationality and heuristics. Pötzsch [24] found that despite awareness of privacy issues, users utilize simple decision models to make decisions due to their cognitive limitations. In information disclosure, Sundar et al. [18] found that users do not use all the information when disclosing information and rather apply heuristic thinking. This finding was later repeated in an exploratory study [19]. While valuable, these initial studies have focused on privacy and mostly the information disclosure domain and have not delved into theoretical explanations behind such observations. Over the years, seve]ral studies called for an investigation of heuristics and biases in information security decision making [25, 26]. Tsohou et al. [27] provided a review and commentary for the role of heuristics and biases in information security. In the paper, certain heuristics were assumed as influential in information security only because they were important in other domains. While such commentary is valuable, no empirical evidence of whether users actually use these heuristics in security decision making was presented. In another literature review, Acquisti et al. [28] discussed potential biases resulted from heuristics in information security.

Reviewing heuristics literature in information security brings up two points: first, prior research suggests that heuristics appear to play a role in information security. This is based on the theory of bounded rationality and the observation that users' behavior does not follow normative decision models [29]. However, such a proposition has never been supported by empirical evidence in information security. Additionally, even if we assume that heuristics play an essential role in security decision making, the type of heuristics used in the domain so far has only been assumed, mainly adopted based on other literatures' findings [27].

3. Theoretical Background

Human beings judge and make decisions under two modes of cognitive thinking: **System 1** and **System 2** [30]. The former is a **person's intuition** containing thoughts that are effortless and fast, ruled by habit, and influenced by emotion, and the latter is a **person's deliberate thinking** which is slow and controlled (i.e., governed by strategic thinking)[7]. This dual processing model is analogous to Elaboration Likelihood Model (ELM) [31, 32]. As Angst and Agarwal [33] point out, some argue that these models are complementary and similar except that a) there is more empirical evidence, particularly in

IS literature in support of ELM, and b) the persuasion process can work differently in these models. However, we focused on the theory of bounded rationality (and System 1, System 2 thinking models) because despite being less popular in IS, this theory has been rigorously studied and tested in behavioral economics and judgment and decision-making literature [4, 6, 11]. Furthermore, the theory is more applicable and relevant in our research focus, which examines the types of mental shortcuts that people use. Researchers have studied more than 70 heuristics used by people in various contexts [6]. This allows for discovering nuances that may not be possible if we were to apply ELM.

Most theories used in information security assumes users are rational agents [25]. Simply put, they utilize System 2 to make their decisions. Over the years, various theories have examined users' security decision making under this assumption: theory of planned behavior [34, 35], deterrence theory [36], protection motivation theory [37-39], and technology threat avoidance theory [40] are among the most prevalent utilized theories.

With the prevalence of inadvertent human errors [2], examining users' security decisions with the consideration that users may not be completely rational in the process of security decision making has never been more important. Furthermore, such examination can complement prior studies in the domain. Simon first introduced the theory of bounded rationality, in which he argued that people deviate from the normative models because their rationality is limited [29]. Later, he introduced the concept of heuristics as information processing methods to reduce cognitive efforts [41]. According to the theory, the main reason people use heuristics is to **reduce the complexity of information processing.** *"Heuristics methods that make this selectivity [of information search] possible have turned out to be the central magic in all human problem solving that has been studied to date."* discuss Newell and Simon ([41], pg. 147). Under the theory of bounded rationality, individuals do not often process complete information to reach a decision. Rather, under System 1 thinking, they may use heuristics to reduce their cognitive efforts and reach fast decisions. Perhaps, the most well-known and influential are heuristics first discussed by Tversky & Kahneman [4]: **availability** (i.e., making decisions based on the information that are salient or recent)**, representativeness** (i.e., making decisions based on an action, option, or item by the degree which it is resembles another action, option, or item)**,** and **anchoring** (i.e., making decisions based on an available reference point). Another heuristic that was later introduced is **affect** (i.e., making decisions based on positive or negative emotions)[7, 42]**.** Shah & Oppenheimer [6] present an extensive review of prior literature studying heuristics. We will utilize the comprehensive list of heuristics provided by Shah & Oppenheimer [6] to examine which heuristics are most commonly used in information security.

4. Methodology

This study aims to understand if heuristics are an important part of users' security decision-making process (RQ1). If yes, which heuristics are more commonly used in information security decision making (RQ2). Based on the motivation of the study, we used the Framework Analysis to examine the data [43, 44]. Framework Analysis which falls under the thematic methodology, allows for a flexible, structured, and transparent approach to data analysis [45, 46]. The method is specifically useful when analyzing data according to a-priori framework and is most suitable for systematic modeling and mapping of data [45]. Using the Framework Analysis allows for easy comparison between the cases since every case will be coded according to the same codebook. Since the objective of the study is to examine what heuristics are used in the process of security decision making, a framework is already in place (i.e., a list of heuristics) that can be used to analyze the data.

4.1. Study Design

To answer the research questions, we chose interviews as the main approach to data collection in our study design. With each interview, we used process tracing via think-a-loud techniques [47], and semi-structured questioning [48] approaches to collect data as they are among the main approaches to explore heuristics used by individuals ([6], pg. 218). We chose this multifaceted approach in the data collection to utilize their strengths to the fullest and achieve triangulation in the data collection [49], hence increasing the reliability of the results and adhering to the standards of rigor in qualitative studies [50].

A number of questions were designed to elicit decision-making processes using the thinking-aloud technique. As the name suggests, thinking aloud allows users to express their thoughts on topics and questions out loud with no back-and-forth with the interviewers. This technique provides benefits over semi-structured interviews: first, since the interviewer will not interrupt the participants, any priming effect from the interview will be lower than other interview methods. Additionally, the think-aloud technique allows an individual's inner speech to show and enables the researcher to trace their cognitive thinking

[47, 51]. This was followed by semi-structured questioning. For both parts, we inquired about actual previous decisions and hypothetical scenarios. In the former, we aimed to explore users' security decision making in the past and their actual thought processes. The major advantage of asking about actual prior security decisions is that it helps identify decisions with adequate complexity and importance to the individual. The main limitation with inquiring about past decisions is that participants may not recall decision processes fully and accurately [14]. On the other hand, the main advantage of using scenarios is that it allows us to capture the current thought processes of the interviewees. Consequently, discussing the decision-making processes for hypothetical scenarios can address the limitation of inquiring only about past decisions. After allowing participants to give their responses without any interruption, they were asked several questions. The additional semi-structured questioning approach allowed for further exploration of the research question, understanding the responses in more detail, and addressing any gaps and inconsistencies heard in participants' responses [52].

After advertisement on social media, we began interviewing the interested participants. The interviews were designed to run between 45 to 60 minutes and were conducted by one of the researchers. The interviews began by debriefing the participants on the purpose of the study. To avoid priming the users that this is a security-focused study, they were initially told that the purpose of the study was to understand how individuals make IT-related decisions on their devices and online platforms. It was emphasized that honesty is the most critical factor in the responses and whether the decisions are viewed as good or bad is irrelevant. The interviewer started with the think-aloud sections. First, a warm-up exercise was conducted [47, 53]. Ericsson and Simon [47, 53] recommended using mental multiplication (e.g., 24 × 34) to warm up the participants before the think-aloud section. After the warm-up exercise, they first discussed their thought processes during various security decision making scenarios. This was followed by the semi-structured questioning by the interviewer at the end to clarify responses and remove possible ambiguities if needed.

4.2. Data Collection

Overall, 27 interviews during the two phases were conducted by one of the study investigators. The sample included 15 females (56%) and 12 males (44%) between 18 to 40 years old from diverse backgrounds and occupations. During the process, we also captured prior security training, security news exposure, and prior security breach for post-hoc analysis. We reached data saturation in both phases of the interviews. *"Saturation is reached when the researcher gathers data to the point of diminishing returns when nothing new is being added"* discuss Bowen et al. ([54], pg. 140). In each phase of the interviews, after the first ten interviews, responses began to show redundancy (i.e., similar types of heuristics were being used in different tasks). However, the interviewer conducted several additional interviews beyond the point that saturation was reached to ensure no significant findings were lost [55]. Additionally, from the precedence and general guidelines perspectives, this study follows the recommended sample size of 15 to 30 individuals by Marshall et al. [55] for such studies.

14 individuals participated in phase 1 (Shown in online appendices). This initial round of data collection continued until the preliminary results showed saturation and redundancies in the responses. At this stage, we conducted a preliminary assessment to see whether any changes to questions can (and should) be made. The process of iteration is a natural part of qualitative research where initial data collection helps refine and improve the questions [56, 49]. This helps with further answering the research questions. There were two main takeaways from this preliminary assessment:

First, the first-round questionnaire targeted general security decisions. The participants discussed the decision processes they wanted. However, the preliminary assessment showed that users' decisions fall under four general types: account and device security management, password creation, security software selection and usage, and web browsing. Understanding the discussion of these common types of decisions by the users, we decided to refine the questions further. Specifically, instead of asking participants to discuss any security decisions made in the past, we aimed to ask them more targeted questions. Specifically, questions that focus on the four decision types emerged from the preliminary assessment.

Additionally, early results showed that, indeed, most participants use heuristics in their decision making. A common term used by respondents was the importance of "convenience." This is in line with Simon's proposition that people utilize heuristics mainly as a way to reduce their cognitive efforts. Furthermore, early transcriptions showed several heuristics are most commonly used among the users. Among them was availability, affect, anchoring, brand, expertise, and representativeness.

Accordingly, going to the next phase of the data collection, while the interviewer still took notes of any other possible heuristics that may arise in users' responses, he paid particular attention to the usage of those five heuristics that seemed common in the first phase. This allowed us to conduct a more focused investigation into the users' security decision-making process. Based on the early assessment, research questions were refined as for phase 2: **RQ1 (Phase 2).** Are heuristics comprise an important part of security decision making in the following tasks: (a) Password creation, (b) Web browsing, (c) Account and device management, (d) Security software selection and usage? **RQ2 (Phase 2).** What heuristics are commonly used in the process of security decision making? Specifically, how often the following heuristics are used in the process of security decision making? (a) Anchoring, (b) Availability, (c) Brand, (d) Expertise, (e) Representativeness, (f) Affect (definitions are shown in the online appendices). 13 additional individuals participated in phase 2 until results showed saturation.

5. Data Analysis

Data analysis was conducted according to Framework Analysis while adhering to the qualitative research criteria (i.e., credibility, transferability, dependability, and confirmability) [50]. The Framework Analysis involves five consecutive stages: familiarization, identifying a thematic framework (i.e., coding), indexing, charting, and mapping and interpretation.

The analysis begins with **familiarization.** The objective of this stage is for the PI (interviewer in the study) to immerse and familiarize himself/herself with the data. This stage may involve gaining a better understanding of responses and apparent themes within those responses. It also can help with identifying relevant parts of responses (Ritchie et al., 2003). This stage can start during data collection. The interviewer reviewed the transcripts, highlighted parts of the responses that directly discussed the users' security decision making and took notes of the apparent heuristic within those responses. The preliminary assessment of phase 1 of data collection, which led to refining the questionnaire for the second round of data collection, falls under this stage.

The second stage is concerned with **Identifying a thematic framework (i.e., coding).** This stage involves identifying the key themes embedded in the transcripts by several judges. In cases where an a-priori theory is in place, a set of pre-defined codes can be used instead [45, 46]. Since the objective was to identify heuristics that have already been defined in the literature, an a-priori codebook was developed based on Shah & Oppenheimer's list of heuristics [6] (an abbreviated version can be seen in Appendix 3). In addition, if the theme that the judges believed to be present in the decision did not exist in the codebook, they were given the option to identify and label the theme in their own words.

The next stage is **indexing.** This step involves applying back the developed codebook in prior steps to all the transcripts to identify the themes within transcripts [44]. One challenge with indexing is that while one person may see a decision including specific heuristics, others may not agree. To reduce subjectivity in this step as much as possible and integrate quantitative validation for inter-rater agreements and inter-rater reliability, we conducted the indexing in two phases. First, based on interview notes and familiarization during the first stage, we developed a matrix (statements × heuristics) for a modified card sorting assessment. In this matrix, rows were comprised of statements in which participants discuss their security decisions, and each column represents heuristics and includes a brief definition. For this study, unlike a traditional card sorting where judges could only assign a statement to one category (e.g., one statement can be attributed to only one heuristic), judges could have assigned a statement to any number of heuristics they wanted. The resulting table appeared as a mixture of traditional card sorting and MacKenzie, Podsakoff, & Podsakoff's proposed matrix structure for assessing inter-rater agreement where each cell generated a hit ratio [57]. Hit ratio as a measure of inter-rater agreement is the number of item placements in one category to total possible placements. The generally accepted threshold for the hit ratio statistic is .80 [58, 59].

The matrix was independently assessed by fifteen judges. The three investigators evaluated all the 93 statements. Additionally, twelve other researchers, which included Ph.D. students in the higher years of their information systems, computer engineering, and information science programs, participated in this assignment. Due to the large volume of the cases, the matrix was broken to one-third of the original for these judges, leading to each of the external judges to assess 31 statements. Consequently, this resulted in seven responses for each statement: three from study investigators and four from external judges.

This practice allowed us to calculate the hit ratio for each cell. We kept any rows that included at least one cell above the .80 hit ratio threshold. This conservative approach allowed us to obtain the decision-heuristic placement that is generally agreed upon (by 6 out of 7 judges). While a given statement could be assigned to more than one heuristic,

surprisingly, each of the final statements was only placed under one heuristic. After reaching a satisfactory inter-rater agreement among investigators and other external judges during the card sorting assessment, we moved to calculate the Fleiss' kappa for the reliability of agreement among the study investigators [60, 61]. While conservative thresholds mark a value of above .80 as a substantial agreement, values above .60 are considered good [62]. For each heuristic in the matrix, we calculated the Fleiss' kappa, which ranged from .77 to .85, all near and above the acceptable threshold.

The next stage in Framework Analysis is **charting** the results. In this stage, to reduce the volume of data and keep the results and findings within the study, another matrix was developed. This matrix summarizes data by category and helps the researcher with presenting the final interpretation of the results [44, 45]. Table 1 shows the chart of results.

The final stage is **mapping/interpretation** of the results. This involves discussing the findings and their implications. It allows the researchers to discuss the bigger picture [44, 63, 64]. We discuss the results in two subsequent sections.

5.1. Results

Under the theory of bounded rationality, decision makers use heuristics to reduce their mental efforts due to the complexity of information processing. As to how they achieve this, we discussed that prior literature identified various heuristics used to reduce individuals' mental efforts. The data showed that this seems to be the case for many participants; not only participants implicitly or explicitly mentioned that they aim to reduce their mental efforts in their security decision making, but the analysis also showed that they utilize a variety of heuristics to achieve this. Overall, 49 decisions were judged to include the usage of one heuristic. In the results, we saw expertise as the most common heuristic (with 17 items) found in the decisions. However, since the unit of analysis was *a security decision*, this number may not reflect the prevalence of expertise among the sample. Hypothetically, if 7 out of 17 decisions were from responses of one participant, then expertise would not be seen as prevalent as initially thought. Accordingly, to measure the most prevalence heuristic accurately, we needed to assess heuristic usage **per participant**. This gives a clearer picture of which heuristics are more common among various users. To do this, we first mapped which decision belonged to which participant. Table 1 shows the prevalence of heuristics among participants and their distribution with respect to task types. Additionally, the results also showed that heuristics usage in information security varies between various security decisions.

Table 1 Summary of Heuristic Usage

Heuristic	% Usage by Participants (Count)	Used in Decision Types (Count)
Affect	15% (4)	*A/DSM (3), WB (1)
Anchoring	15% (4)	A/DSM (1), SS (3)
Availability	44% (12)	A/DSM (1), PM (9), SS (2)
Brand	15% (4)	A/DSM (3), SS (1)
Expertise	56 % (15)	A/DSM (12), SS (3)
Representat-iveness	19 % (5)	WB (5)

**A/DSM: Account and device management, WB: Web browsing, SS: Security Software, PM: Password Management*

The most prevalent heuristic among participants was **expertise** which was mostly used in account and device security management decisions. In many instances, participants stated that they rely only on the expertise of others to make decisions. While a few would take any source of expertise (e.g., results from an expert on the web), many of those using expertise heuristic discussed relying on family members (e.g., partner, father, or brother). For those people, trust was a contributing factor. A few elaborated that they believe they (i.e., family members) want the best for them, so their advice will undoubtedly be to their benefit. That is why they reach out to the family in the first place during security decision making.

Table 2 Expertise Sample Responses

P10 [On selecting a new security software] "*The very first thing I would do, because I know my dad, he's worked a lot and a lot with security things because he's a mechanical engineer and that's always a very common thing for him. The very first thing I would do is definitely consult with him. Whether he knows it or not, there are definitely people in his company that do."*
P11 [On removing viruses] *"I go to people who are experts in the field. Both my partner and my dad worked in computers. So, both of them have ideas of what is good, tried and true, security programs that I can rely on, so typically, that's how I would go about it because I would want to avoid downloading something that is in and of itself malware."*

The **availability** heuristic was the second-highest used heuristic among the participants. This was mainly due to users' discussions as to how they created their passwords. A closer look at these statements showed that with minor differences, the process is similar among those using the availability heuristic: they create their passwords using a template plus few variable additions. While the template is fixed, the additions could be random or created to adhere to the password requirements of the websites.

Table 3 Availability Sample Responses

P16 [On password selection] *"I have like kind of a template of a password. I use the templates because I find it easier to remember it. Cause if I use a different password for like every single website, I have so many passwords and so many different logins that I would just always forget my password. And then that's just, that just becomes a hassle."*
P18 [On password selection] *"I create a password based on something that is easy to remember. Maybe a combination of a capital letter, a lowercase letter, maybe a special character as well. [For] most of my accounts, I have the same password."*

The data showed that users utilize **representativeness** heuristic primarily during web browsing. While representativeness can be in any form (e.g., text, image), it seems that visual cues represent "secure vs. insecure" options to users. For instance, the padlock in the browser, the perceived quality of website design, and the usage of "https" were brought up during the interviews. With regards to some of these cues, such as the padlock, this is expected because they are designed to convey "connection security." However, some users use this as a sign that the whole website, including its content, is secure, while it may not be the case. This is an instance where using representativeness leads to an error in judgment.

Table 4 Representativeness Responses

P25 [On malicious website detection] *"I mean, I can't say I consciously do it, but if I notice there's no lock, on the URL bar on the top, for example, then it's probably because it's not an HTTPS website for example. I think there's kind of this unconscious process looking as well as like, this a website is littered with ads."*
P19 [On malicious website detection] *"Probably just text and kind of how the website is formatted. Just general formatting in 21st-century websites, kind of a clean, modern look. I would make it. I would assume it's more legitimate."*

With **anchoring**, users make decisions based on an available reference point. Reviewing the answers showed some users do not necessarily look for expertise to make decisions. Rather they search for an anchor to make decisions. This can be an online review, product rating, and word-of-mouth.

Table 5 Anchoring Sample Responses

P8 [On using security software] *"I would do some digging around online, like, just some Googling on what are the best, what are what's considered the best, antivirus software. And I would also ask my friends as to what they use and what they recommend and then use all that info to make a decision."*
P12 [on selecting a security software] *"I would look online to see which ones are best rated. So, like which ones people recommend and have had the most experience with. I would also probably ask my dad for more information and what he thinks I should get."*

When using the **affect** heuristic, users will judge actions that they feel positive (negative) more favorably (unfavorably). Although compared to the availability heuristic, affect was less observed, the pattern seemed to hold. Positive feelings (e.g., feeling better/safer) and negative feelings (e.g., fear) led to users making certain decisions.

Table 6 Affect Sample Responses

P10 [On turning off Bluetooth/location]: *"I don't know [why I do it]. It's just something I do. I don't think about the consequences. I just, you know, in my mind, I think I feel more safe when my GPS is off."*
P15 [on removing a virus] *"I would probably panic. Power off the device or whatever and probably run a scan, try to fix it that way. I probably do my own thing and won't ask anyone."*

Finally, with respect to the **brand**, only one brand played a role in the process of security decision making: Apple. On multiple accounts, users discussed that they see Apple products as more superior with respect to security, thus simplifying their decision making. For instance, they would not take certain actions after a malware incident or download security software just because they have an Apple product.

Table 7 Brand Sample Responses

P16 [On device usage] *"I feel safer [with using a MacBook]. I think overall, they are superior. I guess brand is important in my decisions. I just heard that Apple is generally safer than windows when it comes to viruses and stuff."*
P17 [On using security software] *"I haven't installed any [Security software], especially an antivirus, since it's a Mac and the viruses are significantly less common on them, that would be for, for that reason*."

6. Implications

In this study, we demonstrated how users use various heuristics in their security decision making. To explain this process, we drew upon the theory of bounded rationality, which states that people use heuristics to reduce their thinking efforts [6, 41]. Specifically, expertise, availability, affect, representativeness, anchoring, and brand were shown as heuristics commonly used in the security decision making by users, with task type as a moderator in heuristic utilization.

As discussed in the literature review, over the years, there has been two categories of studies that sporadically studied the usage of heuristics: one group included commentary and reviews which discussed the potential influence of heuristics in information security, and the other group used heuristic as a possible explanation for users' behavior in information disclosure in privacy literature. The current study extends these works in two ways: first, it provides an explanation of users' illogical security decision making which has been a significant source of threat in recent years. Additionally, the study responds to the call to further assess heuristics in information security [1, 20, 25] and presents empirical evidence of actual types of heuristics used in this context (e.g., availability, affect). This study specifically extends the prior work, which suggested heuristics as a general explanation for irrational privacy and security decision making without much contextual investigation [18, 22, 65, 66].

Second, this study contributes to the stream of research focusing on the security-convenience tradeoff, which is most commonly investigated in usable security literature [67]. Under this perspective, secure decisions often cause inconveniences for users. For this reason, in order not to lose their convenience, users often do not make the most secure decisions. This is especially shown to be the case in authentication and password management literature [10, 68]. As a result of this, specific streams of security studies such as usable security investigated changes in user interface design that can increase user security without jeopardizing their convenience [69, 70]. This study contributes to that stream in the following way: this study goes beyond "why" people seek convenience and make somewhat irrational decisions and explains "how" this occurs. Next, we discuss the practical implications in two categories: **direct learning, and interface design/nudging.** A direct approach is to educate users on the role that heuristics play in their decision making. Users consciously or subconsciously use these heuristics. However, increasing awareness on a meta-knowledge level can provide users with a great sense of understanding of their capabilities and security knowledge. A direct learning approach that makes users aware of these heuristics and enables them to understand how they make their security decisions is a plausible way based on this study's findings. For organizational users, this can be integrated into organizations' security awareness programs and security modules, and for personal users, this can be integrated with public educational platforms such as NSA guidelines for the security of home users in the US and the GetCyberSafe program in Canada, which aim to provide educational materials for the public.

In this interface design/nudging approach, security engineers, designers, and administrators can attempt to help users make more secure decisions by either using innovative design, providing feedback, or nudging them towards those decisions. For example, when sending guidelines or providing support to employees, companies can add information about the expertise of the support staff (e.g., education, certificates, year of experience) in the correspondence. Accordingly, rather than seeing the position title of the support team, the employee will see expertise behind the advice that they received. Inclusion of heuristic cues can also be made in the interface design. Designing interfaces that a) make the security decisions more convenient and b) integrate essential heuristic cues (such as including available necessary information without overwhelming the user) is a plausible way to examine and extend the findings of the current study. The findings can also be used to investigate new nudging techniques further [71]. Depending on the decision environment, heuristic cues can be used to nudge users towards more secure decisions. For example, does including available information on proper security behavior in password creation help create stronger passwords?

7. Conclusion

People are still considered the weakest link in information security. Since 2015, while the number of threats from technology vulnerabilities has either remained constant or even decreased in some instances, human errors have been increasing steadily [8]. This study provided an explanation of why and how human errors in information security decision making occur. According to the theory of bounded rationality, human decision making is influenced by various cognitive heuristics. From an effort-reduction perspective, this is because people wish to reduce their cognitive effort and make information processing easier. Accordingly, our study revealed that expertise, availability, representativeness, brand, affect, and anchoring were the most prevalent heuristic used in information security-related decisions by users. Furthermore, the findings showed that no single heuristic is dominant across various decisions. Rather, we discovered that heuristic utilization varies depending on the type of security decisions.

8. References

[1] Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., and Baskerville, R. Future directions for

behavioral information security research. *Computers & Security*, 32 (2013), 90-101.
[2] Sher-Jan, M. Data indicates human error prevailing cause of breaches, incidents. (2018), Retrieved from https://iapp.org/news/a/data-indicates-human-error-prevailing-cause-of-breaches-incidents/.
[3] Milkovich, D. 15 Alarming Cyber Security Facts and Stats. (2020), Retrieved from https://www.cybintsolutions.com/cyber-security-facts-stats/.
[4] Tversky, A., and Kahneman, D. Judgment under uncertainty: Heuristics and biases. *Science*, 185, 4157 (1974), 1124-1131.
[5] Simon, H.A. Invariants of human behavior. *Annual Review of Psychology*, 41, 1 (1990), 1-20.
[6] Shah, A.K., and Oppenheimer, D.M. Heuristics made easy: An effort-reduction framework. *Psychological Bulletin*, 134, 2 (2008), 207.
[7] Kahneman, D. A perspective on judgment and choice: mapping bounded rationality. *American Psychologist*, 58, 9 (2003), 697.
[8] Verizon. Data Breach Investigation Report. (2020), Retrieved from https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf.
[9] LastPass. Psychology of Passwords. (2020), https://www.lastpass.com/resources/psychology-of-passwords-2020.
[10] 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.
[11] Tversky, A., and Kahneman, D. Availability: A heuristic for judging frequency and probability. *Cognitive Psychology*, 5, 2 (1973), 207-232.
[12] Maheswaran, D., Mackie, D.M., and Chaiken, S. Brand name as a heuristic cue: The effects of task importance and expectancy confirmation on consumer judgments. *Journal of Consumer Psychology*, 1, 4 (1992), 317-336.
[13] Ratneshwar, S., and Chaiken, S. Comprehension's role in persuasion: The case of its moderating effect on the persuasive impact of source cues. *Journal of Consumer Research*, 18, 1 (1991), 52-62.
[14] Krabuanrat, K., and Phelps, R. Heuristics and rationality in strategic decision making: An exploratory study. *Journal of Business Research*, 41, 1 (1998), 83-93.
[15] Rosoff, H., Cui, J., and John, R.S. Heuristics and biases in cyber security dilemmas. *Environment Systems and Decisions*, 33, 4 (2013), 517-529.
[16] Garg, V., and Camp, J. Heuristics and biases: implications for security design. *IEEE Technology and Society Magazine*, 32, 1 (2013), 73-79.
[17] Van Schaik, P., Renaud, K., Wilson, C., Jansen, J., and Onibokun, J. Risk as affect: The affect heuristic in cybersecurity. *Computers & Security*, 90 (2020), 101651.
[18] Sundar, S.S., Kang, H., Wu, M., Go, E., and Zhang, B. Unlocking the privacy paradox: do cognitive heuristics hold the key? , *CHI'13 Extended Abstracts on Human Factors in Computing Systems*, 2013, pp. 811-816.
[19] Gambino, A., Kim, J., Sundar, S.S., Ge, J., and Rosson, M.B. User disbelief in privacy paradox: Heuristics that determine disclosure. *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, 2016, pp. 2837-2843.
[20] Furnell, S.M., Bryant, P., and Phippen, A.D. Assessing the security perceptions of personal Internet users. *Computers & Security*, 26, 5 (2007), 410-417.
[21] Burton-Jones, A., and Grange, C. From use to effective use: a representation theory perspective. *Information Systems Research*, 24, 3 (2012), 632-658.
[22] Acquisti, A. Privacy in electronic commerce and the economics of immediate gratification. *Proceedings of the 5th ACM conference on Electronic commerce*, 2004, 21-29.
[23] Acquisti, A., and Grossklags, J. Privacy and rationality in individual decision making. *IEEE Security & Privacy*, 3, 1 (2005), 26-33.
[24] Pötzsch, S. Privacy awareness: A means to solve the privacy paradox? , *IFIP Summer School on the Future of Identity in the Information Society*: Springer, 2008, 226-236.
[25] Dennis, A.R., and Minas, R.K. Security on autopilot: Why current security theories hijack our thinking and lead us astray. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, 49, SI (2018), 15-38.
[26] Dinev, T., McConnell, A.R., and Smith, H.J. Research commentary—informing privacy research through information systems, psychology, and behavioral economics: thinking outside the "APCO" box. *Information Systems Research*, 26, 4 (2015), 639-655.
[27] Tsohou, A., Karyda, M., and Kokolakis, S. Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers & Security*, 52 (2015), 128-141.
[28] Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., . . . Sleeper, M. (2017). Nudges for privacy and security: understanding and assisting users' choices online. ACM Computing Surveys (CSUR), 50(3), 44.
[29] Simon, H.A. Theories of bounded rationality. *Decision and Organization*, 1, 1 (1972), 161-176.
[30] Stanovich, K.E., and West, R.F. Individual differences in reasoning: Implications for the rationality debate? *Behavioral and brain sciences*, 23, 5 (2000), 645-665.
[31] Petty, R. E., and Cacioppo, J. T. 1981. Attitudes and Persuasion: Classic and Contemporary Approaches, Dubuque, IA: Wm. C. Brown.
[32] Petty, R. E., and Cacioppo, J. T. 1986. Communication and Persuasion: Central and Peripheral Routes to Attitude Change, New York: Springer-Verlag.
[33] Angst, C. M., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. MIS quarterly, 339-370.
[34] Ajzen, I. The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50, 2 (1991), 179-211.
[35] Bulgurcu, B., Cavusoglu, H., and Benbasat, I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34, 3 (2010), 523-548.
[36] D'Arcy, J., Hovav, A., and Galletta, D. User awareness of security countermeasures and its impact on information

systems misuse: A deterrence approach. *Information Systems Research*, 20, 1 (2009), 79-98.
[37] Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G.D., and Polak, P. What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, 39, 4 (2015), 837-864.
[38] Johnston, A.C., and Warkentin, M. Fear appeals and information security behaviors: an empirical study. *MIS Quarterly* (2010), 549-566.
[39] Rogers, R.W. A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91, 1 (1975), 93-114.
[40] Liang, H., and Xue, Y. Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly* (2009), 71-90.
[41] Newell, A., and Simon, H.A. *Human Problem Solving*. Prentice-hall Englewood Cliffs, NJ, 1972.
[42] Slovic, P., Finucane, M., Peters, E., and MacGregor, D.G. Rational actors or rational fools: Implications of the affect heuristic for behavioral economics. *The Journal of Socio-Economics*, 31, 4 (2002), 329-342.
[43] Ritchie, J., Spencer, L., Bryman, A., and Burgess, R. Qualitative data analysis for applied policy research. *Analyzing Qualitative Data*, 173 (1994), 194.
[44] Ritchie, J., Spencer, L., and O'Connor, W. Carrying out qualitative analysis. *Qualitative Research Practice: A Guide for Social Science Students and Researchers*, 2003 (2003), 219-262.
[45] Gale, N.K., Heath, G., Cameron, E., Rashid, S., and Redwood, S. Using the framework method for the analysis of qualitative data in multi-disciplinary health research. *BMC Medical Research Methodology*, 13, 1 (2013), 1-8.
[46] Ritchie, J., Lewis, J., Nicholls, C.M., and Ormston, R. *Qualitative Research Practice: A Guide for Social Science Students and Researchers*. Sage, 2013.
[47] Ericsson, K.A., and Simon, H.A. How to study thinking in everyday life: Contrasting think-aloud protocols with descriptions and explanations of thinking. *Mind, Culture, and Activity*, 5, 3 (1998), 178-186.
[48] Schmidt, C. The analysis of semi-structured interviews. *A Companion to Qualitative Research* (2004), 253-258.
[49] Yin, R.K. *Qualitative research from start to finish*. Guilford Publications, 2015.
[50] Lincoln, Y.S. *Naturalistic inquiry / Yvonna S. Lincoln, Egon G. Guba*. Beverly Hills, Calif: Sage Publications, 1985.
[51] Ji-Ye Mao, I.B. The use of explanations in knowledge-based systems: Cognitive perspectives and a process-tracing analysis. *Journal of Management Information Systems*, 17, 2 (2000), 153-179.
[52] Furneaux, B., and Wade, M.R. An exploration of organizational level information systems discontinuance intentions. *MIS Quarterly* (2011), 573-598.
[53] Ericsson, K.A., and Simon, H.A. *Protocol analysis: Verbal reports as data*. the MIT Press, 1984.
[54] Bowen, G.A. Naturalistic inquiry and the saturation concept: a research note. *Qualitative Research*, 8, 1 (2008).
[55] Marshall, B., Cardon, P., Poddar, A., and Fontenot, R. Does sample size matter in qualitative research?: A review of qualitative interviews in IS research. *Journal of Computer Information Systems*, 54, 1 (2013), 11-22.
[56] Gerlach, J., and Cenfetelli, R.T. Constant Checking Is Not Addiction: A Grounded Theory of IT-Mediated State-Tracking. *Management Information Systems Quarterly*, 44, 4 (2020), 1704-1732.
[57] MacKenzie, S.B., Podsakoff, P.M., and Podsakoff, N.P. Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. *MIS Quarterly*, 35, 2 (2011), 293-334.
[58] Cenfetelli, R.T., Benbasat, I., and Al-Natour, S. Addressing the what and how of online services: Positioning supporting-services functionality and service quality for business-to-consumer success. *Information Systems Research*, 19, 2 (2008), 161-181.
[59] Moore, G.C., and Benbasat, I. Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research*, 2, 3 (1991), 192-222.
[60] Fleiss, J., Levin, B., and Paik, M. How to randomize. *Statistical Methods for Rates and Proportions. 3rd ed. Hoboken, NJ John Wiley & Sons* (2003), 86-94.
[61] Fleiss, J.L. Measuring nominal scale agreement among many raters. *Psychological Bulletin*, 76, 5 (1971), 378.
[62] Landis, J.R., and Koch, G.G. The measurement of observer agreement for categorical data. *Biometrics* (1977).
[63] Ross, S.A. The economic theory of agency: The principal's problem. *The American Economic Review*, 63, 2 (1973), 134-139.
[64] Ward, D.J., Furber, C., Tierney, S., and Swallow, V. Using Framework Analysis in nursing research: a worked example. *Journal of Advanced Nursing*, 69, 11 (2013).
[65] Acquisti, A., Brandimarte, L., and Loewenstein, G. Privacy and human behavior in the age of information. *Science*, 347, 6221 (2015), 509-514.
[66] Adjerid, I., Peer, E., and Acquisti, A. Beyond the Privacy Paradox: Objective Versus Relative Risk in Privacy Decision Making. *MIS Quarterly*, 42, 2 (2018), 465-488.
[67] Kim, B.C., and Park, Y.W. Security versus convenience? An experimental study of user misperceptions of wireless internet service quality. *Decision Support Systems*, 53, 1 (2012), 1-11.
[68] Zviran, M., and Haga, W.J. Password security: an empirical study. *Journal of Management Information Systems*, 15, 4 (1999), 161-185.
[69] Furnell, S. Why users cannot use security. *Computers & Security*, 24, 4 (2005), 274-279.
[70] Johnston, J., Eloff, J.H., and Labuschagne, L. Security and human computer interfaces. *Computers & Security*, 22, 8 (2003), 675-684.
[71] Thaler, R. H., & Sunstein, C. R. (2008). Nudge: Improving decisions about health, wealth, and happiness: Yale University Press.

Online Appendicies can be found at https://drive.google.com/file/d/1LdbRETjLFtUZ7m4Y2ioiNtvf9L1exhnm/view?usp=sharing