Security Mental Models and Personal Security Practices of Internet Users in Africa

Enock Samuel Mbewe and Josiah Chavula

Computer Science Department
University of Cape Town, South Africa
{embewe, jchavula}@cs.uct.ac.za

Abstract. Recent trends show an increase in risks for personal cyberattacks, in part due to an increase in remote work that has been imposed by worldwide Covid-19 lockdowns. These attacks have further exposed the inefficiencies of the *paternalistic* design of Internet security systems and security configuration frameworks. Prior research has shown that users often have inadequate Internet security and privacy mental models. However, little is known about the causes of flawed mental models. Using mixed methods over a period of nine months, we investigate Internet security mental models of users in Africa and the implications of these mental models on personal security practice. Consistent with prior research, we find inadequate Internet security mental models in self-reported expert and non-expert Internet users. In addition, our mental modelling and task analysis reveal that the flawed security practice does not only result from users' negligence, but also from lack of sufficient Internet security knowledge. Our findings motivate for reinforcing users' Internet security mental models through personalised security configuration frameworks to allow users, especially those with limited technical skills, to easily configure their desired security levels.

Keywords: usable security · security mental models · Internet security · privacy

1 Introduction

Over the years, improving end-users security has proven to be a challenging task. Generally, users perceive security as a secondary task that they must complete before performing a more relevant primary task. Such mental models hinder the acceptance of security awareness initiatives and inhibit users' perception and adoption of security [12]. A *mental model* is defined as "psychological representations of real, hypothetical, or imaginary situations." [9]. Research has shown that users have incomplete or vague information on security mechanisms, systems, the Internet, and information flow in many circumstances[23]. Recent cybersecurity trends reveal a huge increase in cyberattacks targetting both enterprises and individuals [36]. The COVID-19 pandemic has forced the remote workforce increasing the risks of online attacks on personal devices. This influx of attacks has revealed how unprepared users are to combat these attacks.

The "*partenalistic*" or "*stupid user*" [2, 38] design of Internet security systems has not prepared users to have proper mental models about Internet security protocols and configuration frameworks. As a result, users have remained the weakest link in the security ecosystem. Cranor and Garfinkel [12] report that security is taken as a "by the way" by many users, while other users perceive security mechanisms as an annoyance. Other studies attribute these security perceptions to lack of security awareness and propose interventions to instil a security culture in Internet users and to engage them in security decision-making [1, 2, 10]. Despite these interventions, many users keep making suboptimal security decisions. We argue that the current implementation of Internet security services leaves users, especially those with limited computing skills, out of the security decision-making process. This is because security configuration parameters are often specialised, hidden from the user, or the security decisions are implemented in a top-down fashion where those with power (e.g. Internet Service Providers (ISPs), content providers) make security decisions on behalf of users. This pyramidal implementation of Internet security services often disregards user security and privacy preferences. As a result, many users do not develop proper mental models of Internet security and consequently fail to configure the required security level to meet the required protection. Mental models with negative consequences include an erroneous understanding of the Internet structure, the flow, security and storage of their online information [23, 29].

Usable Internet security research reports that users with technical skills exhibit better mental models of the Internet. For example, a study conducted by Kang et al. [23] found that users with technical knowledge had more articulate mental models of the Internet. In contrast, those with little technical knowledge displayed simple Internet models. Despite these differences, the authors did not find a direct relationship between people's technical background and their actions to control their privacy or increase their security online. However, their work does not investigate why users have disparities between mental models and security practices. Understanding the reasons behind users' flawed security mental models is important in ensuring that usable online security solutions are designed to accommodate varying technical skill levels. This study investigates the factors that influence users' security and privacy mental models and practice. Drawing from Internet users in Africa, our work tries to explain the relationship between users' computing skill levels, general Internet mental models, Internet security models, and practice. Developing regions, such as Africa, have seen rapid Internet penetration over recent years, which has provided risks for different kinds of online attacks. Therefore, understanding personal security readiness is fundamental to ensuring that proper security tools are developed that reinforce users' Internet security mental models. Specifically, we aim to answer the following questions:

1. *What is the relationship between users' computing skills levels, security knowledge, security preferences and Internet security practice?*
2. *What mental models of the Internet and online security do users have?*
3. *Which mental models interfere with secure and private Internet usage?*

The contribution of our work is three-fold; first, we use a comprehensive mixed-methods (survey, open-ended questionnaire, mental modelling and task analysis) user study with participants drawn from the understudied African Internet userbase. Using individual methods, prior research has focused much on the developed regions where the Internet is developed. Secondly, our work provides further evidence that flawed mental models and poor online security practice are also caused by insufficient Internet security knowledge. Our findings suggest that the inadequate security mental models are exacerbated by delegated or ”stupid user” implementation of Internet security services, which advocate for expert-friendly security configuration services. Finally, concurring with prior research, our study identifies generally weak explainable relationships between users technical knowledge, Internet security mental models and their security practice. We provide insight into how these relationships can be strengthened to reinforce users' security mental models and their online security practice.

2 Related Work

Three areas of usable security research are essential to our work: i) studies on users security preferences, ii) studies on human in the security loop and iii) studies on security education.

2.1 Usable security

Security is ordinarily defined as a collection of all measures to prevent loss of any kind. The concept of security is as old as humankind and peoples' physical safety, and their possessions have always been at risk from a deliberate attack or accidental damage [33]. The increased user base on the Internet and other digital platforms imply that peoples' physical and digital assets are at risk [12]. Decades ago, access to the Internet and online communication was a corporate privilege due to the high cost of access devices and data services. On the contrary, recently, we have witnessed a surge in the uptake of ICT-enabled services and Internet access from developing regions. To meet the increasing demand for online security, the research communities and the IT industry have developed many security mechanisms and theories to counter digital attacks. Despite these interventions, online exploitation and security breaches of businesses, governments, and individual Internet users keep blossoming [26]. Cranor and Garfinkel [12] reported that security mechanisms are mostly too obscure for users to comprehend, i.e., not usable. Whitten and Tygar [41] reported in their work that there exists an antagonism between security and usability, exposing mutual trade-offs between these properties. A common opinion is that users should sacrifice usability to achieve sufficient security [11]. On the other hand, Fagan and Khan [15] found that users, despite being aware of existing dangers, often put usability before security, exposing themselves to many risks.

2.2 Human in/out of-the-loop philosophies

Over the years, many usable security variants have emerged. They can be classified as a human in the loop [16], and human out-of-loop [14, 34]. These philosophies continue to shape usable security research. With the notion that humans are the weakest link in the security chain, some security mechanisms are fully automated and do not include humans [16]. This kind of security design is known as a paternalistic approach or Human-out-of-the-loop[2, 8, 27]. The paternalistic security research paradigm reports that automated systems are generally more accurate and predictable than humans and that automated systems do not get tired or get bored [16, 38].

Although some paternalistic security systems work, other variants of Usable Security research report that these systems can be too restrictive, inconvenient, expensive, or slow in some cases. Edwards [14] argue that it is unreasonable to automate all privacy and security management decisions due to numerous technical and social factors that limit such automation's efficacy and acceptance. This line of thought supports two approaches to involving humans in decision making: strict libertarian and soft paternalistic that require users to be involved in security decision-making [19]. Historically, these approaches do not guarantee that users will make competent security decisions due to human limitations resulting from inexperience and cognitive limitations, among others [2].

2.3 User's Internet and Internet security mental models

The mental modelling approach is becoming more common in usable security research. It is used to understand users' perception of the Internet, Information and Communication Technologies (ICTs), and Internet-related systems such as cybersecurity [5, 10, 20, 25, 37, 38, 39], Mobile App security and privacy [28], online banking and Internet of Things (IoT). The mental models are regarded as an important framework for describing user behaviour [31].

Renaud et al. [32] investigated the reasons why users do not implement email security. In their work, they argued that the non-adoption of end-to-end encryption might not be entirely due to usability issues as reported by Whitten and Tygar [41]. Instead, they found incomplete threat models, misaligned incentives, and a general absence of understanding of the email architecture as some of the factors contributing to the non-adoption of security. Their research proposed building more comprehensive end-user mental models related to email and email security. This is counter-intuitive to the *Paternalistic or 'stupid user' approaches* that assume that security is too complicated for average users to comprehend and try to implement security mechanisms for the users. Asgharpour et al. [5] evaluated expert and naïve mental models of computer security and found that the models differed with expertise. They also found that security models in the form of common metaphors (e.g. viruses, zombies, or keys) did not reconcile well with understanding in either group.

The definition of an expert user differs among different studies. For example, Bravo-Lillo et al. [7] defines *expert* users as having taken a graduate-level security course or worked for at least a year in the field; while Ion et al. [20] define a security expert as having a minimum of five years of experience. In their work, Bravo-Lillo et al. [7] reported a difference in how expert and novice users interpreted the context of security warnings. Similarly, Ion et al. [20] observed differing security preferences between experts and novices. A recent study by Krombholz et al. [25] assessed HTTPS mental models of both end-users and administrators and found that misconceptions about security benefits and threat models existed in both groups. In particular, they found that end-user mental models are more conceptual, while administrator models are protocol-based.

In summary, prior research has shown that users of ICTs have poorer security mental models leading to a more inadequate online security culture. Complementing prior research, our study investigates the factors that lead to the flawed mental models. We focus on identifying hurdles users face when interacting with the Internet security configuration frameworks such as web security, DNS, VPN and web filtering configuration tools. Africa has seen a surge in the Internet user base over the last ten years. However, security research has focused much on American and European Internet users. Thus, our study focuses on Africa to understand the human element of security and privacy.

3 Methodology

This study uses a mixed-methods approach in a multi-stage approach to obtain an in-depth understanding and explanation of users' Internet security culture. We begin with a close-ended, exploratory baseline online survey to get an insight into Internet users' knowledge, preference, usage and perception of Internet security and security configuration tools found in Internet access platforms commonly used. We follow up the online survey with an open-ended questionnaire. To alleviate limitations of self-reported responses [13, 40], we run user experiments (mental modelling and tasks analysis) based on our online survey and questionnaire results. Finally, we complement the user experiments with iterative follow-up interviews. We required the participants to be active Internet users, primarily based in Africa. The African population is particularly of interest because most Usable Security research has focused on North American and European populations, even though the number of internet users in Africa has grown at the fastest rate in recent years. The surge in the Internet user base has significantly been accelerated by smartphone uptake and social network platforms. In the following subsections, we describe the study design in detail.

3.1 Quantitative Study (Online Survey)

The exploratory survey's primary aim was to get a general insight into the relationship between users' computing skill levels and their knowledge of the Internet and online security. It also aimed to explore the general online security practice of users. In addition to questions about computer knowledge, we included questions that enabled us to categorise participants into expert and non-expert categories. Following the principle of cognitive interviews [30], we pre-tested the survey to identify and correct all the ambiguities. Participants were asked to provide their honest opinions, which we used to fine-tune the questions iteratively. We pre-tested ($n = 30$) the survey internally with our research group members and other colleagues and friends until a satisfactory convergence was reached.

Recruitment and Inclusion Criteria Study participants were recruited through social media, personal contacts and professional mailing lists. The aim of using diverse sources was to capture a representative sample among Internet users in Africa and to include participants with different levels of computing skills. We posted the invitation (in English) on LinkedIn, Twitter, WhatsApp groups, and African Network Operators Groups' (NOG) mailing lists.

A total of 298 responded to the survey. However, our quantitative evaluation only considers the responses of 240 participants who completed all the questions in the survey. These participants represent a diversity of self-reported computing skills, ranging from basic, intermediate, advanced and expert. We structured the survey to allow participants to provide their general and personal picture of Internet security mechanisms and preferences. The survey had five sections; *Internet access and usage, Internet security knowledge, Internet Security preferences* and *Demographics.*

3.2 Qualitative Study

Self-reported studies suffer various biases, including over-reporting and under-reporting [13, 40]. To alleviate this problem, we used the survey to recruit participants for subsequent follow-up studies. A total of 155 participants agreed to be included in our follow-up studies. We sent out an online open-ended questionnaire to these 155 participants, of which 60 participants completed the questionnaire. We also recruited 32 individuals to participate in the mental modelling and task analysis activities.

Open-ended Questionnaire We designed an online questionnaire to validate the participants' self-reported technical skills and to uncover further details that would have been missed during the exploratory survey, such as the level of familiarity with Internet security protocols and concepts. The questionnaire was also used to recruit participants for the interactive sessions.

Mental modeling The exploratory surveys provided some insight into participants' Internet and security mental models. However, self-reported responses do suffer over-reporting biases [13, 40]. To qualify the survey responses, we tested participants' knowledge of Internet infrastructure and its security features. Gentner and Stevens [17] has shown that users act in line with their mental models of a phenomenon. We therefore gave drawing tasks to participants, following a methodology employed by Kang et al. [23]. We first asked participants to draw the Internet and its components. To put the tasks into perspective, we asked participants to draw the processes of sending an email and making an online payment. These tasks were identified as most common (See Figure 4) and were mostly rated as critical and requiring strict security and privacy (See Figure 2). We asked the participants to label the direction of information flow and to identify entities that would have access to user data. Participants were further encouraged to identify vantage points that require security and describe the kind of security required. We encouraged participants to verbalise their thought process in line with think-aloud protocols [6, 21].

Task analysis We undertook a task analysis exercise where we asked participants to configure security using tools available in their preferred Internet access platforms, such as operating systems, web browsers and mobile applications. The aim was to investigate how users' mental models interfere with the security practice of participants. We also aimed to identify factors that influence security mental models and practice. The task analysis session was also used to validate self-reported studies and mental models. We used lab experiments and online video conferencing sessions using Zoom to observe the participants do the configuration tasks.

We specifically asked the participants to take us through their usual way of configuring security or privacy on their preferred Internet access platform. This was necessary to allow the participants to demonstrate their mental models without an imposed configuration type. We then asked the participants to configure security and privacy in their preferred browser. We decided to use a browser-based security configuration because it was the platform most highly ranked by participants in the exploratory survey. In addition, we asked the participants to demonstrate how they would block ads, phishing sites and adult content. We also asked the participants whether they knew how to configure DNS and asked them to demonstrate how they would configure secure DNS protocols. We chose DNS because it is a more straightforward protocol that can be implemented at the endpoint. Also, DNS has been exploited recently, exposing the user to unwanted content and poor QoE.

We video-recorded the drawing and configuration sessions with participants' permission without capturing any participants' identifying information. Each recording was assigned a unique random code for easy referencing in this paper. Throughout the process, we were able to go back to the participants for clarification interviews. These iterative interviews allowed us to identify emerging concepts and their relationships. We carried out the interviews until we reached the saturation of the theoretical constructs.

3.3 Data analysis

We used non-parametric statistical tests (Chi-square ($\tilde{\chi}^2_{(DF)}$), Cramer's Phi (ϕ_C, Correlation) and Likelihood ratio) to analyse the quantitive results. We mainly looked for the relationship between computing skills and participants' perception, knowledge and practice of Internet security configuration. We iteratively analysed the qualitative data using content and narrative analysis methods. We transcribed the results verbatim and coded the data with the aid of NVivo12 software [1]. The initial coding was done independently between two researchers and compared and sorted at a research meeting. We then looked for patterns, connections and relationships among the codes and assigned them to more high-level predefined categories. Throughout the process, we could go back to the participants to seek clarification on emerging themes. This iteration continued until we reached saturation. Finally, we organised the themes into a relationships model to answer our research questions 2 and 3.

[1] https://www.qsrinternational.com/nvivo-qualitative-data-analysis-software/home

4 Results

Our results show that, generally, users with better computing skills have better Internet mental models. To a considerable extent, we observe that better Internet mental models imply stricter security and privacy requirements. However, we note that stricter security requirements do not imply better self vulnerability assessment or better security practice. We observe that expert users with security experience had better mental models for both the Internet and security. We find that, among other factors, lack of proper knowledge of Internet security and its configuration frameworks is the leading cause of flawed security practice among many participants.

4.1 Online Survey Results

Demographics: Table 1 shows demographics for survey participants, identified predominantly as male at 82.92%, followed by females at 15%. We attribute this to the divide between males and females in terms of Internet usage or technology usage in general [3, 4, 7, 22]. Figure 1 shows the countries of residence for our survey participants. In terms of educational level, participants identified overwhelmingly as tertiary institutions graduates (97.08%). The survey targeted participants who use the Internet regardless of educational background; hence, we focus more on participants' computing skill levels (Fundamentals (0.42%), Basic (8.33%), Intermediate (20.83%), Advanced (34.17%) and Expert (36.25%).

Demographic	
Gender	
Male	199 (82.92 %)
Female	38 (15.83%)
Transgender	1 (0.42%)
Prefer not to say	2 (0.83%)
Higest Qualification	
Tertiary	233 (97.08)
High/Secondary	4 (1.67)
None	3 (1.25%)
Computer Skill level	
Expert (Systems /network administration and security, Programming, e.t.c)	87 (36.25%)
Advanced (Internet, Email, Office applications, Databases, Programming)	82 (34.17%)
Intermediate (Internet, Email, Office applications, databases)	50 (20.83%)
Basic (Internet, Email, Office applications (Word, Spreadsheet, PowerPoint)	20 (8.33%)
Fundamentals (Internet,Typing)	1 (0.42%)

Table 1: Survey participants' demographics

Internet Access and Use: To understand the participants' Internet use, we asked them to choose from a list of use categories. Figure 4 shows a stacked bar chart for the internet use frequencies. The seven most common uses are productivity/office, communication, information search, social networking, entertainment, e-Financial services and virtual meetings. Comparing levels of computing skills and internet usage, we find a statistically significant relationship only

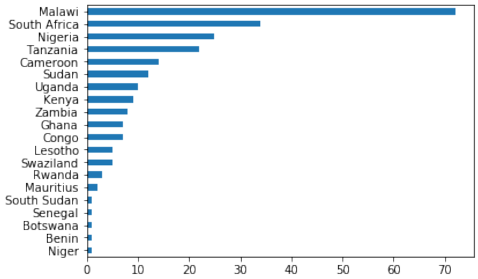


Fig. 1: Participants' country

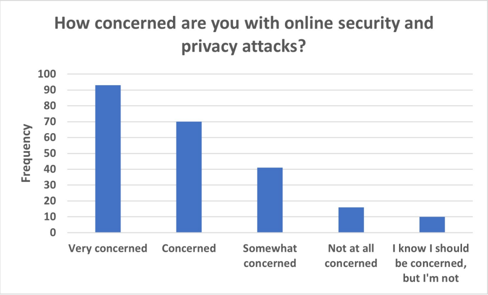


Fig. 2: Participants' concerns on security and privacy attacks

on two uses; e-Services ($\tilde{\chi}^2_{(4)}$: 9.847, LR : 10.904, ϕ_C : 0.203, $p = 0.043$) and Productivity ($\tilde{\chi}^2_{(4)}$: 16.002, LR : 14.307, ϕ_C : 0.258, $p = 0.003$). Overall, this suggests no major differences in how users use the Internet, whether one is an expert or not. The results further show that participants mostly use smartphones, laptops, desktops, tablet computers, and Kindle devices (See Figure 3). We found that many participants access the Internet via mobile broadband ($\approx$ 58%) followed by office network ($\approx$ 25%) using web browsers and mobile apps installed on their smartphones and laptops. We consider this information useful for designing usable security interventions.

Our results show that the Internet is a significant part of participants' daily lives, with over 78% of them reporting to access the Internet for over four (4) hours daily.

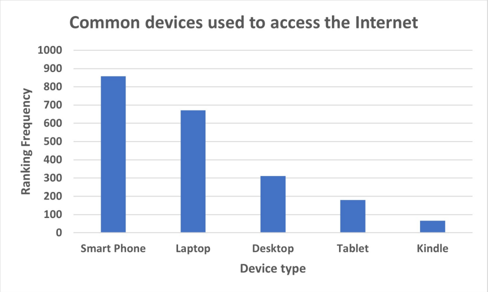


Fig. 3: The devices that participants use to access the Internet

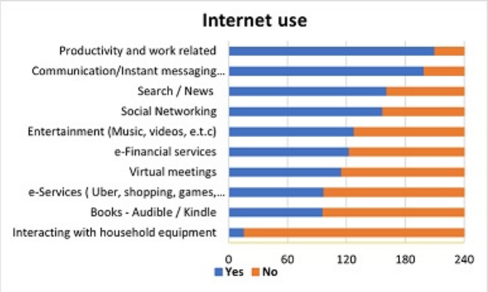


Fig. 4: What participants indicated they use the Internet for

Users' Internet security knowledge and preference: The study further sought to understand participants' Internet security configuration and preferences. We asked a series of questions, including VPN usage, and priority ranking between convenience and performance, security, privacy, confidentiality, integrity, and availability. We also asked them about what they would consider an ideal security configuration tool. The follow-up questions particularly aimed to solicit ideas on what users deem useful information that an *ideal* security configuration tool should provide. We find that 94 (39.17%) of the participants indicate to have used VPN. Among the reasons for using VPN, participants indicated the need for enhanced privacy/security, remote access, bypassing censorship, and accessing geo-restricted content. We find a statistically significant relationship between computing skill level and VPN usage ($\tilde{\chi}^2_{(4)}$: 42.428, LR : 45.699, ϕ_C : 0.420, $p < 0.001$), gender and VPN usage ($\tilde{\chi}^2_{(3)}$: 24.432, LR : 30.943, ϕ_C : 0.319, $p < 0.001$).

We asked participants to indicate their level of concern for their online safety and privacy, such as pervasive monitoring, unsolicited emails, and unwanted adverts. Most of the participants (40.43%) indicated that they were very concerned (they feel vulnerable), 30.43% indicated that they were concerned, (17.83%) were somewhat concerned, 6.96% were not concerned at all and finally, 4.35% indicated that they knew they should be concerned, but they chose not to be concerned. The participants were further asked to rank their security, convenience, and performance preferences during any browsing session. We asked this question in three ways to ensure that users are not coerced by order of the items or question phrasing. Firstly, we just asked for ranking according to preference with which they ranked security, performance, and convenience, respectively. After some questions, we asked participants to indicate which of the three (security, performance, and convenience) they would compromise if their connection was vulnerable to attacks and, secondly, if their network was slow. In both scenarios, participants indicated that they would rather compromise convenience and performance. In all three cases, participants indicated taking security seriously, even if it meant trading off with performance and convenience. In addition to these three options, we asked participants to rank security confidentiality, Integrity, Availability and Privacy according to their preference. Generally, these three security goals are achieved using different mechanisms that impact performance differently. Therefore this question solicited the most preferred goal. This could inform the design of security mechanisms by highlighting which security mechanisms *must* be available to the users and which ones can be optional. We provided definitions of these concepts in advance to ensure that the participants could make an informed ranking decision. The results indicate confidentiality, privacy, availability and integrity as the general preference order.

We required the participants to indicate whether they knew of security configuration tools available in their Internet access platforms. A majority 143(59.6%) indicated that they were of such. Of those, 120 indicated to have ever configured security using these configuration tools. Finally, of those participants who indicated to have ever configured Internet security using the available tool, over 70% found the tools to be simple enough. The rest reported that the tools were either difficult to use or confusing. We asked the participants how they wished the tools improved. Among other features, the participants indicated correct information on the tools' interface, including security information of their browsing session, the performance impact of their security configuration, and general connection information.

What and how information should be protected? To determine what kind of information participants would keenly consider protecting online, we asked the participants to indicate the level of importance for each asset requiring protection. Figure 5 shows a Likert plot for eight different digital assets. We observe that for most of the assets, the responses are skewed towards the critical side of the scale. Of the eight sample digital assets tested, online banking, passwords, data and identity were rated *Very critical* by at least 70% of the participants. Except for news content and browsing history, we observe that over 96% of participants rate the digital assets as critical. The lowest is news content. This implies that not all digital assets are the same, and hence protection requirements will differ. Given an option to define intent and its associated costs, users may protect one asset and not the other.

In addition to the digital assets, we asked participants to indicate the level of agreement to seven statements about their online security and privacy preferences. Figure 6 shows Likert

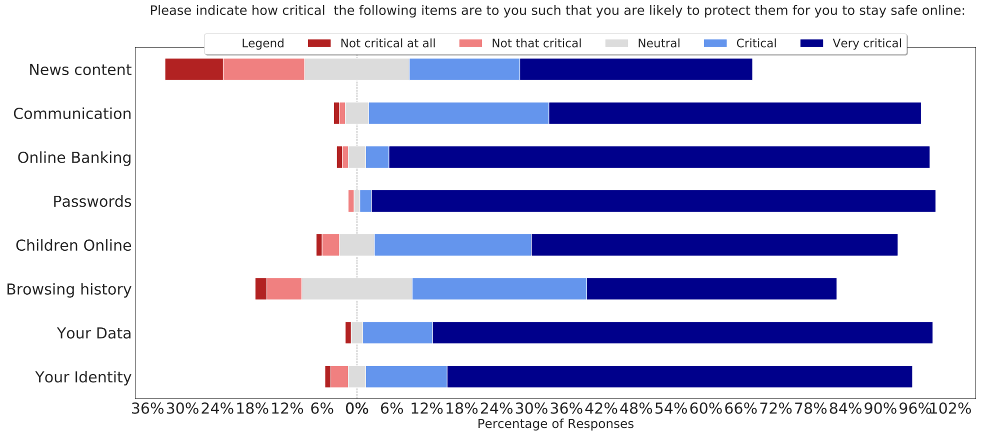


Fig. 5: Criticality of participants' digital assets that require protection

plot for the seven statements, where we observe that over 90% of the participants indicated they prefer to browse confidentially and anonymously. Over 65% of the participants strongly agreed that users should control their security and privacy online using simple Internet security configuration tools capable of keeping the user informed of the security or performance impact of their security configuration. Surprisingly, we observe that ≈ 75% of the participants agree that ISPs ought to be able to monitor users' browsing activities. This contradicts the requirement to browse anonymously.

4.2 Qualitative Analysis

This section presents results from the three qualitative studies we conducted; open-ended questionnaire, mental models drawing exercises, and security configuration task analysis. The task analysis method was used to validate the claims and observations made in the quantitative studies and in mental modelling.

Internet and security mental models The Internet mental models described by participants varied substantially across computing skill levels. We observe that increase in computing skill level comes with an increase in complexity and clarity of models, which we classify into simple, moderate, and complex or representative models. For example, participants with basic and intermediate computing skills presented the Internet as a central node represented with a rectangle, cloud, globe or a big server (See Figure 7). Other participants' models of the Internet included big technology companies, such as Google and Facebook. One participant (P0044) said "*I really don't know, but the possible structure could be the Website like Google*". To such a class of participants, the Internet is pretty much defined by the applications they use. Figure 8 shows one of the simplistic views of the Internet drawn by a participant. On one extreme, the experts displayed a complete understanding of the Internet, mentioning underlying telecommunication structure, applications, protocols, and standards (See Figure 9). Due to space limitations, we present users' Internet models using a code frequency graph in Figure 7. We observe that to many participants, the Internet model is the communication infrastructure represented by a green bar in Figure 7. Advanced and expert users also mentioned technical

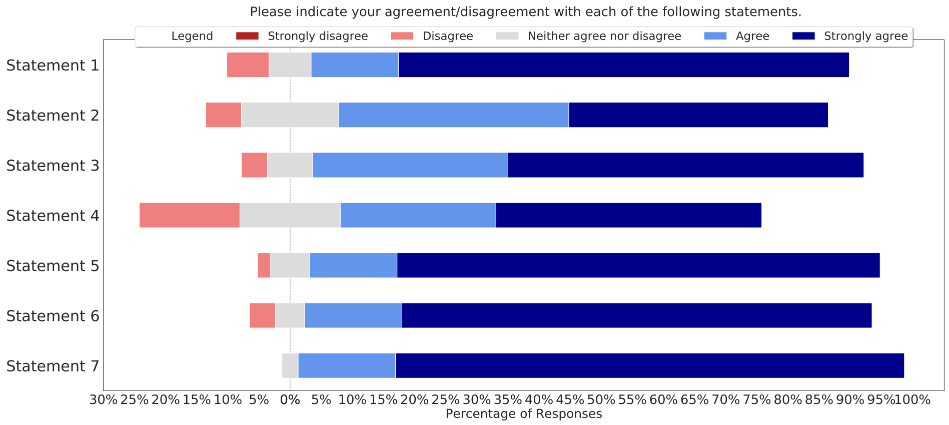


Fig. 6: Agreement/Disagreement to security and privacy statements. Refer to the following key for statements:
Statement 1 - I ought to be able to communicate over the Internet without people being able to read/access the content.
Statement 2 - I ought to be able to take on different aliases/roles at various times on the Internet.
Statement 3 - I value being able to visit websites on the Internet in an anonymous manner.
Statement 4 - Internet Service Providers ought to monitor Internet user's browsing activity
Statement 5 - There ought to be more straightforward Internet security configuration tools to protect one's privacy on the internet.
Statement 6 - Users ought to have complete control over which websites/Apps get personal information.
Statement 7 - Users should be informed of the possible security/performance impact of one's security configuration.

and web standards and end-users as being part of the Internet structure. We identified similar patterns in the email and online payment drawings.

The study asked the participants to explain the risks associated with Internet browsing. Many participants mentioned hackers, password and information theft, among others. However, many non-expert participants failed to explain how they mitigated against the mentioned risks. This was contrary to the quantitative study results where many participants responded that they were very concerned (see Figure 2) about their security and that they configure security on their Internet access devices. Expert participants mentioned advanced measures such as VPN, encryption, incognito and third-party plugins.

Impact of Mental models on Security Practice The second interactive activity was the task analysis experiment. In this experiment, we observed participants as they configured security in response to three questions about online privacy, browser/app security and DNS security. We designed the questions based on responses given in the two surveys and the drawing exercises. In all tasks, we observed that participants with little to moderate computing skills had a vague idea of Internet security. Most of the participants in these categories referred to passwords and antivirus as their primary means of security. For example, one participant

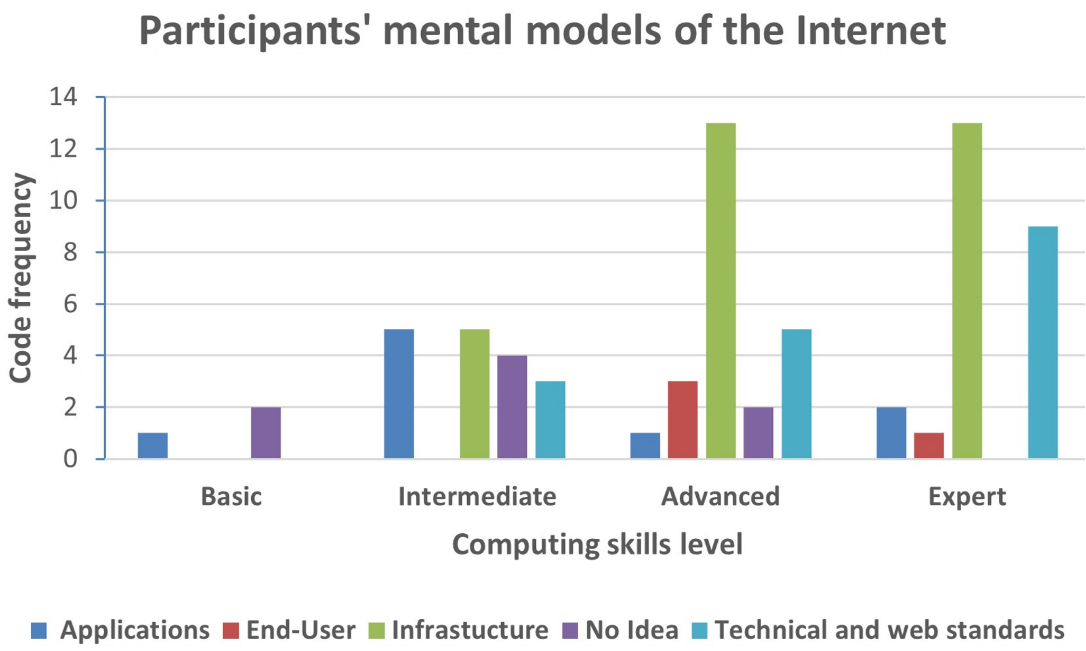


Fig. 7: Code frequency for the internet mental model

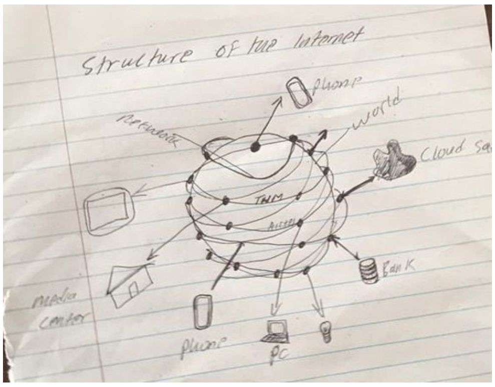
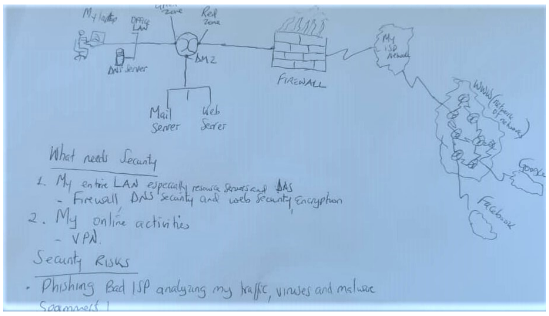


Fig. 8: Simplistic structure of the Internet



What needs Security

1. My entire LAN especially resource Servers and DNS
   - Firewall, DNS security and web Security, Encryption
2. My online activities
   - VPN.

Security Risks

- Phishing Bad ISP analyzing my traffic, viruses and malware Scammers !

Fig. 9: A more detailed structure of the Internet

(P0039) said, "*I feel very secure because I use a personal laptop which is secured with a password and an antivirus.*"

Observing how participants went about configuring security, we noted that many non-expert participants did not know the Internet security configuration frameworks. For example, others were quick to admit that they did not know Internet security configuration tools, and therefore, they did not customise security on their Internet access platforms. When we followed up on what they thought Internet security was and why they had indicated that they had ever configured security, many referred to passwords and phone locking mechanisms as security measures. We demonstrated some of the configurations to such participants and asked them to repeat the configurations. Finally, we asked them to describe the difficulty level for the procedure. Some users felt that the procedure was simple enough but indicated that the tools were hidden for an average user.

Many Advanced and expert users used advanced security methods such as adblocking and made use of browser-based privacy configuration, incognito mode and third-party plugins. A few expert level participants used VPN, Encryption, and DNS filtering. However, we note that some self-reported advanced and expert users had a simplistic view of security, just like intermediate users. The study required the participants to demonstrate if they knew and used various Internet security mechanisms such as VPN and DNS privacy protocols. These protocols, especially DNS, can easily be configured from the endpoint running almost all kinds of operating systems and web browsers. All non-expert users indicated that they did not know about VPN and DNS. Many advanced and expert users indicated that they only use security and privacy services provided by their ISPs. Few expert users indicated awareness of DNS privacy protocols such as DNS over TLS (DoT), DNS over HTTPS (DoH), and DNSSEC.

We expected that the results from the self-reported activities would translate into actual practice in the configuration exercise. Surprisingly, we identified disparities between the participants' self-reported activities and the actual configuration through the task analysis activities. For example, while participants indicated knowledge of the Internet configuration tools, a few used them to configure security and privacy. Also, despite concerns over security and privacy risks, only a few implemented correct and sufficient security measures to curb the risks. We also noted that participants confused Internet security with device security by frequently referring to antivirus, passwords, PINs and patterns. This is in contrast to the self-reported responses where most participants indicated they knew Internet security configuration.

In summary, we observe relationships between computing skills, Internet security mental models, and security preferences. The results suggest that in addition to cognitive biases reported by Acquisti et al. [2], lack of sufficient security knowledge leads to distorted security mental models which, in turn, leads to more flawed online security practice. Concurring with prior research, this study also shows that while users have higher security needs, their actions do not reflect those needs. For example, some participants felt they had all the security. Others felt that they had nothing of interest to the attackers, while others were willing to give up on their security and privacy to get *free* stuff from the Internet.

Relationship between technical knowledge, security mental models and security practice We summarised our results through a relationship model (See Figure 10), which describes the connections between the main themes in this study. In this model, the continuous lines show strong relationships between the entities. In contrast, the dotted lines show a weaker relationship between the entities. The arrows define the implication of the relationship. Generally, the results show a strong relationship between the participants' technical skills and their Internet mental models (including the knowledge of online attacks). This agrees with the findings by Kang et al. [23]. However, better Internet models do not always imply better security mental models and online security practice, as revealed by the task analysis experiment. For example, we found that some participants who had better Internet models exhibited a distorted self vulnerability assessment. Both quantitative and qualitative studies do not show significant differences in internet needs across computing skill levels.

Concurring with Kang et al. [23], we found that users either have a simple, moderate or complete model of the Internet. The users with a complete model of the Internet generally have matched security mental models and security practice. On the other hand, users with moderate Internet models show moderate security mental models. Lastly, users with basic mental models show basic security mental models. However, regardless of their Internet security

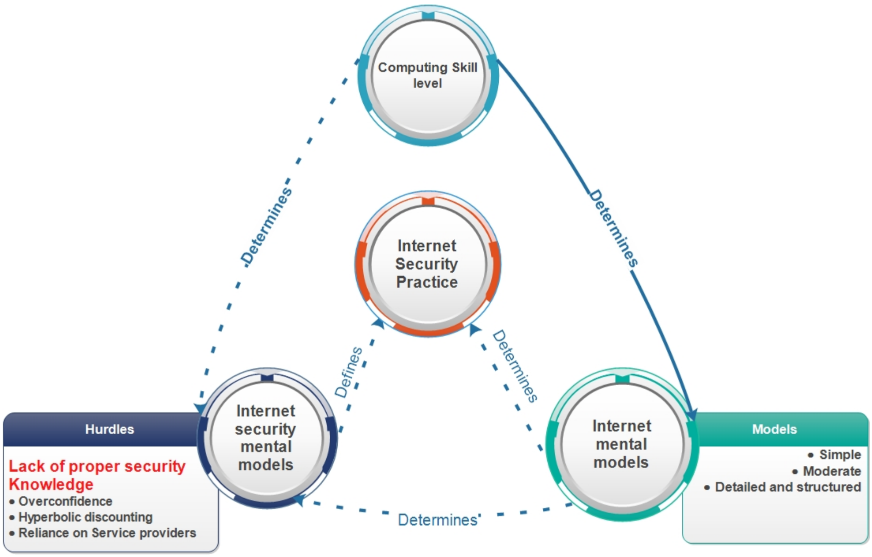


Fig. 10: The relationship model between Internet user's computing skills, metal models, self vulnerability assessment and security preferences

mental models, most of the participants showed flawed security mental models leading to poor online security practice. The results show that security preferences do not translate to good security practice. Prior research calls this scenario a (security) privacy paradox. Our study finds that apart from the cognitive biases that are known to cause the paradox, lack of sufficient security attack vectors and security configuration knowledge is the leading cause of the flawed mental models among Internet users.

5 Discussion

This study used multi-step mixed methods to identify users' difficulties in interacting with Internet security mechanisms and configuration tools. This approach provides a unique way to identify hurdles and disparities in the participants' security mental models. The usage of drawing and configuration experiments aimed to triangulate the rich narrative of descriptive and contextual data provided by surveys and interviews. The approach successfully enabled us to pinpoint the source of hurdles and their respective impact on participants' Internet security practice.

Our results generally show a relationship between users' technical knowledge, mental models, and security practice. However, we note flawed self vulnerability assessment and a mismatch between users' self-declared technical competence and security preferences and practice. Prior research has tried to explain this disparity, especially in privacy and social economics research. The two theories we relate to our findings are Privacy Paradox, a dichotomy between privacy attitude and practice, [18], and Cognitive Biases, especially overconfidence, optimism bias, and hyperbolic discounting [2].

Overconfidence and optimism bias are instances of incorrect estimates of subjective probabilities [2]. People with optimism bias underestimate the chances that they might be subject to an adverse event. On the other hand, overconfidence is an overestimation of one's judgments. The results show that some advanced and expert participants would be easy targets of online attacks due to cognitive biases. For example, one advanced user (P0035) indicated that he did not think anyone could attack him. When followed up, he said, "*I use a strong antivirus, and I refrain from clicking unknown links.*" This participant and other participants built their security mental models around antivirus software, heeding security warnings, and incognito web browsing. Much as these are possible prevention measures, the participant did not realise that attacks can be automated and come in different forms, such as social engineering, phishing, and SMishing. Other participants thought they had nothing of interest to the attackers, while others felt powerless to protect themselves. For example, one participant (P0050) said "*I do not think I have anything, apart from my banking app password, which the attackers can target me for.*" We further noted that some participants were willing to give up on their security online to access "free" Internet resources. When asked about how the participants manage personal information online or respond to security warnings, some participants indicated that they decide based on the type of activity and weigh the benefits: "*When my information is required, I weigh the benefits. For example, if a website requests my information to download a scarce book or movie, why not? I give it away. After all, my information is already in public.*" This is referred to as hyperbolic discounting in social economics literature [2], trading long-term better benefits with short-lived rewards. Attackers exploit such human vulnerabilities to launch attacks.

Interestingly, these participants indicated that they were very concerned about online security and privacy breaches, reaffirming the Privacy Paradox theory, which attempts to explain discrepancies between user attitude and their actual behaviour. Through task analysis, our study aimed to establish the potential cause of such risky behaviours across different technical skill levels. When compared to the Western-centric research on the topic, we note that the Internet users in both the western world and Africa suffer from cognitive biases and overreliance on the service providers [5, 23, 32]. Peculiar to the African Internet users described in this study, we find that lack of proper security orientation, including security protocols and configuration frameworks, is the leading cause of poor Internet security mental models. Thus, security remains a mystery to many users, which might be why humans are still considered the weakest link in the security ecosystem.

We argue that the "stupid user" implementation of Internet security services has robed users of their ability to learn and build proper security mental models. In particular, research in this area argues that humans may not remember or may not be interested in the underlying security protocols such as encryption, hash functions, among others. Through the findings of this study, we argue that if Internet users are given the right tools, information and engagement, it might be possible to change this narrative. We find that participants were comfortable using passwords and antiviruses because they interact with these tools daily, and have become inherent in Internet usage. Another good example could be taken from the security of physical assets, which require personal responsibility. Over time, humans have built mental models around it and can implement complex physical security systems.

We also observe that due to the paternalistic nature of Internet security implementation, many users do not have these critical Internet security services in their Internet models. For example, participants mentioned DNS, encryption and VPN fewer times across all the security configuration activities than passwords and antivirus. This lack of awareness might allow DNS attacks, for example, to succeed with less difficulty. The prevalent remote work enforced by COVID-19, for example, requires personal security enforcement. However, most Internet users are still not equipped to take personal responsibility for security online, allowing for cyberattacks to succeed. More practical human-centred Internet security interventions are needed to improve Internet security mental models.

This study does not show a strong colleration between computing skills and internet needs. However, we find that users would endeavour to protect some Internet transactions but not others (see Figure 6). For example, some participants indicated they would sacrifice performance to secure e-banking, communications, and identifying information.

In section 4.2, we presented a model showing the relationships among computing skills, Internet mental models, security mental models and Internet security practice. In this model, we show weak relationships between most of the entities. However, for complete protection online, there is a need to have strong connections among the entities. Several interventions have been proposed in recent years to improve the security landscape. One example is the Security Configuration Management (SCM) tool [24]. SCM is defined as the management and control of configurations for an information system to enable security and to manage risk. Such tools are useful in corporations where a single point of control is possible. However, this study shows that many participants used personal devices for Internet access. This suggests that more personalised security configuration tools are needed to protect Internet users from various attacks. One of such tools is personal DNS privacy configurators from Cloudflare [2], AdGuard [3] and DNSCrypt [4]. Much as these tools are effective, they focus on one aspect of the security puzzle and mostly proprietary and expert-oriented.

This study calls for further research to reinforce users' security mental models and improve their security practice. We suggest data-driven security configuration models and personal security configuration tools. Such tools could combine various interventions responsible for educating, informing, feedback, and configuring security protocols on users' devices. For example, a data-driven approach would provide users with accurate information on the performance cost of various protocols with an easy to use interface; and provide feedback and vulnerability information to the user regardless of their technical background. The generated cues and the properly framed nudges [2, 35] could help reinforce computing skills, mental models and security practice.

6 Limitations

The potential limitation of this study lies in the language used to collect data and the type of the participants. We used the English language only. This left out other potential participants based on educational background and geographic region. Also, as described in the results section, most of the participants had at least a bachelor's degree working in ICT-related fields. This skewness may affect the generalisation of the results. Nonetheless, we argue that our findings provide an overview of users' security mental models and their impact on users' online security practice. Future work could employ multi-lingual, expanded studies that consider participants from all the African regions with diverse educational backgrounds.

7 Conclusion and future work

This study employed a mixed-methods approach to understand and investigate the relationship between Internet users' computing skill level, Internet security mental models, and security practice. The study further aimed to establish the possible cause for Internet users' distorted security mental models. Our results show that computing skill levels significantly influence users' security knowledge and preferences. However, the technical skills do not necessarily

[2] See https://blog.cloudflare.com/1111-warp-better-vpn/

[3] See https://adguard.com/en/adguard-android/overview.html

[4] See https://github.com/DNSCrypt/dnscrypt-proxy

influence online security practice due to challenges that users experience when interacting with Internet security configuration tools. Our study design, especially mental modelling and task analysis methods, uniquely establishes that users' poor security mental models are often caused by insufficient Internet security knowledge. This lack of technical know-how for security configuration is fueled by "stupid user" security implementation, which advocates for expert-friendly security configuration tools. Our future work will explore how data-driven, user-centric Internet security configuration framework would reinforce users' security mental models and improve their security practice.

Acknowledgements

The authors are grateful for the financial support received from the Hasso Plattner Institute for Digital Engineering through the HPI Research School at the University of Cape Town. In addition, the authors would like to thank Reuben Moyo for the help rendered during data collection, themes formulation and validation. Finally, we thank all the participants for their time and willingness to provide information published in this study.

References

[1] Jemal Abawajy. User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, 33(3):237–248, mar 2014. ISSN 0144-929X. https://doi.org/10.1080/0144929X.2012.708787. URL http://www.tandfonline.com/doi/abs/10.1080/0144929X.2012.708787.

[2] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, Yang Wang, and Shomir Wilson. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys*, 50(3), aug 2017. ISSN 15577341. https://doi.org/10.1145/3054926.

[3] Nicholas O Alozie and Patience Akpan-Obong. The digital gender divide: Confronting obstacles to women's development in africa. *Development Policy Review*, 35(2):137–160, 2017.

[4] Amy Antonio and David Tuffley. The gender digital divide in developing countries. *Future Internet*, 6(4):673–687, 2014.

[5] Farzaneh Asgharpour, Debin Liu, and L Jean Camp. Mental models of security risks. In *International Conference on Financial Cryptography and Data Security*, pages 367–377. Springer, 2007.

[6] Silvia Bernardini. Think-aloud protocols in translation research: Achievements, limits, future prospects. *Target. International Journal of Translation Studies*, 13(2):241–263, 2001.

[7] Cristian Bravo-Lillo, Lorrie Faith Cranor, Julie Downs, and Saranga Komanduri. Bridging the gap in computer security warnings: A mental model approach. *IEEE Security & Privacy*, 9(2):18–26, 2010.

[8] Colin Camerer, Samuel Issacharoff, George Loewenstein, Ted O'donoghue, and Matthew Rabin. Regulation for conservatives: Behavioral economics and the case for" asymmetric paternalism". *University of Pennsylvania law review*, 151(3):1211–1254, 2003.

[9] Kenneth James Williams Craik. *The nature of explanation*, volume 445. CUP Archive, 1952.

[10] Lorrie Faith Cranor. A framework for reasoning about the human in the loop. *Usability, Psychology, and Security, UPSEC 2008*, 2008.

[11] Lorrie Faith Cranor and Norbou Buchler. Better together: Usability and security go hand in hand. *IEEE Security & Privacy*, 12(6):89–93, 2014.

[12] Lorrie Faith Cranor and Simson Garfinkel. *Security and usability: designing secure systems that people can use.* " O'Reilly Media, Inc.", 2005.

[13] Diane Dodd-McCue and Alexander Tartaglia. Self-report response bias: Learning how to live with its diagnosis in chaplaincy research. *Chaplaincy Today*, 26(1):2–8, 2010.

[14] W Keith Edwards, Erika Shehan Poole, and Jennifer Stoll. Security automation considered harmful? In *Proceedings of the 2007 Workshop on New Security Paradigms*, pages 33–42, 2008.

[15] Michael Fagan and Mohammad Maifi Hasan Khan. 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)*, pages 59–75, Denver, CO, June 2016. USENIX Association. ISBN 978-1-931971-31-7. URL https://www.usenix.org/conference/soups2016/technical-sessions/presentation/fagan.

[16] Ivan Flechais, Jens Riegelsberger, and M Angela Sasse. Divide and conquer: the role of trust and assurance in the design of secure socio-technical systems. In *Proceedings of the 2005 workshop on New security paradigms*, pages 33–41, 2005.

[17] Dedre Gentner and Albert L Stevens. *Mental models.* Psychology Press, 2014.

[18] Nina Gerber, Paul Gerber, and Melanie Volkamer. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior, aug 2018. ISSN 01674048.

[19] Pelle Guldborg Hansen. The definition of nudge and libertarian paternalism: Does the hand fit the glove? *European Journal of Risk Regulation*, 7(1):155–174, 2016.

[20] Iulia Ion, Rob Reeder, and Sunny Consolvo. "...No one can hack my mind": Comparing expert and non-expert security practices. *SOUPS 2015 - Proceedings of the 11th Symposium on Usable Privacy and Security*, pages 327–346, 2019.

[21] Riitta Jääskeläinen. Think-aloud protocol. *Handbook of translation studies*, 1:371–374, 2010.

[22] Linda A Jackson, Yong Zhao, Anthony Kolenic III, Hiram E Fitzgerald, Rena Harold, and Alexander Von Eye. Race, gender, and information technology use: The new digital divide. *CyberPsychology & Behavior*, 11(4):437–442, 2008.

[23] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. "My data just goes everywhere:" User mental models of the internet and implications for privacy and security. In *SOUPS 2015 - Proceedings of the 11th Symposium on Usable Privacy and Security*, pages 39–52, 2016. ISBN 9781931971249.

[24] Klaus Keus and Thomas Gast. Configuration management in security related software engineering processes. *Bundesamtfür Sicherheit in der Informationstechnik Postfach*, 20: 03–63.

[25] Katharina Krombholz, Karoline Busse, Katharina Pfeffer, Matthew Smith, and Emanuel Von Zezschwitz. 'If HTTPS Were Secure, i Wouldn't Need 2FA' - End User and Administrator Mental Models of HTTPS. *Proceedings - IEEE Symposium on Security and Privacy*, 2019-May:246–263, 2019. ISSN 10816011. https://doi.org/10.1109/SP.2019.00060.

[26] George Kurtz. Sophos 2021 threat report: Navigating cybersecurity in an uncertain world. https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-2021-threat-report.pdf, 2021. Accessed: 24 February 2021 - 19:15.

[27] Thomas C Leonard. Richard h. thaler, cass r. sunstein, nudge: Improving decisions about health, wealth, and happiness, 2008.

[28] Jialiu Lin, Norman Sadeh, Shahriyar Amini, Janne Lindqvist, Jason I. Hong, and Joy Zhang. Expectation and purpose. page 501, 2012. https://doi.org/10.1145/2370216.2370290.

[29] Alexandra Mai, Katharina Pfeffer, Matthias Gusenbauer, Edgar Weippl, and Katharina Krombholz. User mental models of cryptocurrency systems - A grounded theory approach. *Proceedings of the 16th Symposium on Usable Privacy and Security, SOUPS 2020*, pages 341–358, 2020.

[30] Becky Milne, Andy Griffiths, Colin Clarke, and Coral Dando. The Cognitive Interview. *Evidence-Based Investigative Interviewing*, (February):56–73, 2019. https://doi.org/10.4324/9781315160276-4.

[31] Don Norman. *The design of everyday things: Revised and expanded edition.* Basic books, 2013.

[32] Karen Renaud, Melanie Volkamer, and Arne Renkema-Padmos. Why doesn't jane protect her privacy? In Emiliano De Cristofaro and Steven J. Murdoch, editors, *Privacy Enhancing Technologies*, pages 244–262, Cham, 2014. Springer International Publishing. ISBN 978-3-319-08506-7.

[33] M. Sasse and I. Flechais. Usable security: Why do we need it? how do we get it? 2005.

[34] Bruce Schneier. *Beyond fear: Thinking sensibly about security in an uncertain world.* Springer Science & Business Media, 2006.

[35] Kavya Sharma, Xinhui Zhan, Fiona Fui-Hoon Nah, Keng Siau, and Maggie X. Cheng. Impact of digital nudging on information security behavior: an experimental study on framing and priming in cybersecurity. *Organizational Cybersecurity Journal: Practice, Process and People*, ahead-of-p(ahead-of-print), sep 2021. ISSN 2635-0270. https://doi.org/10.1108/ocj-03-2021-0009.

[36] Rob Sobers. 134 cybersecurity statistics and trends for 2021. https://www.varonis.com/blog/cybersecurity-statistics/, January 2021. Accessed: 15 February, 2021.

[37] Blase Ur, Jonathan Bees, Sean M Segreti, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Do users' perceptions of password security match reality? In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 3748–3760, 2016.

[38] Rick Wash and Emilee Rader. Influencing mental models of security: A research agenda. *Proceedings New Security Paradigms Workshop*, 09 2011. https://doi.org/10.1145/2073276.2073283.

[39] Rick Wash and Emilee Rader. Too much knowledge? Security beliefs and protective behaviors among United States internet users. *SOUPS 2015 - Proceedings of the 11th Symposium on Usable Privacy and Security*, pages 309–325, 2019.

[40] Rick Wash, Emilee Rader, and Chris Fennell. Can people self-report security accurately? agreement between self-report and behavioral measures. In *Proceedings of the 2017 CHI conference on human factors in computing systems*, pages 2228–2232, 2017.

[41] Alma Whitten and J D Tygar. Usability of Security : A Case Study. *Computer Science*, (102590):1–41, 1998.