

## Motivation and Demotivation of Hackers in Selecting a Hacking Task

Ken Owen & Milena Head

To cite this article: Ken Owen & Milena Head (2022): Motivation and Demotivation of Hackers in Selecting a Hacking Task, Journal of Computer Information Systems, DOI: [10.1080/08874417.2022.2081883](https://doi.org/10.1080/08874417.2022.2081883)

To link to this article: <https://doi.org/10.1080/08874417.2022.2081883>



Published online: 14 Jun 2022.



Submit your article to this journal [↗](#)




View related articles [↗](#)



View Crossmark data [↗](#)



## Motivation and Demotivation of Hackers in Selecting a Hacking Task

Ken Owen and Milena Head 

McMaster University, Hamilton, ON, Canada

### ABSTRACT

To build a solid foundation on which to understand and combat threats to information systems, researchers need to look past technical security issues and explore why hackers do what they do. Based on General Deterrence Theory and the Theory of Reasoned Action, a structural model is proposed and validated that examines attraction and detraction factors towards a hack. From a motivational perspective, individual characteristics (mastery and curiosity), peer influence and the nature of the task itself are shown to impact hacker's attitudes. Specifically, we uncover an interesting non-linear relationship between hacking task complexity and a hacker's attitude towards a hack. From a deterrence perspective, while hackers consider the likelihood of being caught, the severity of punishment/sanctions does not have a significant effect on hackers' intention to engage in a hacking task. When we better understand what motivates and demotivates these highly skilled users, we gain insights to avoid becoming targets.

### KEYWORDS

Hacker motivation; demotivation; General Deterrence Theory; Theory of Reasoned Action; individual characteristics; task characteristics

### Introduction

Businesses lose billions of dollars every year because of the acts of computer criminals. Damages occur through a broad spectrum of incursions ranging from the covert theft of credit card information to the very public and overt defacement of corporate websites. Modern media is rife with stories of hackers both good and bad. Hackers are seen to steal people's identities, defacing public websites and causing all kinds of computer mischief. It is predicted that cybercrime will cost in excess of \$10.5 trillion USD annually by 2025, up from \$3 trillion in 2015.<sup>1</sup> As the COVID-19 pandemic pushed much of our activities online, it is not surprising that the occurrence of cybercrimes has also increased dramatically<sup>2</sup> and there is no reason to think cybercrime will decrease post-pandemic.<sup>3</sup>

While hackers are often portrayed by the media as evil, they have also been at the center of some positive social projects. For example, the Raspberry Pi Foundation is a charity that turns its profits back into educational programs and developing new products. The Raspberry Pi has opened up opportunities for social good, such as computer training for girls in Afghanistan and children throughout Africa. This foundation was developed by a group of technologically skilled individuals that saw an opportunity to contribute to their community. They used off-the-shelf technology and repurposed it to create credit card sized single board computers. This hack has now sold over 37 million copies worldwide, formed more than 10,000 code clubs of which 42% are girls<sup>4</sup> Annual Review.

Public and private organizations have realized the potential of tapping into the hacker culture to better understand their vulnerabilities. For example, General Motors (GM) has invested \$100 million into cybersecurity per year, including aggressive hiring of hackers to vet and help expose flaws in the complex coding of their self-driving cars.<sup>5</sup> Companies such as IBM, Google, Bank of America and Tesla pay upward of \$150,000 USD annual salary for hackers to detect security gaps and trace potential threats.<sup>6</sup> Governments around the world, like the private sector, are realizing the potential for hackers to provide crucial feedback and expose vulnerability holes that internal employees are not finding. For example, the Department of Defense received over 11,000 valid vulnerability reports from hackers across the globe in a three year time span, estimating to have saved this Department \$64 million.<sup>7</sup> In 2019, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) announced a directive requiring federal agencies to establish a vulnerability disclosure policy, enabling good-faith hackers and citizens to look for and report security vulnerabilities without fear of legal action.

There is no doubt that hacking is an important issue for IS practitioners and thus should be an important issue for IS researchers. To build a solid foundation on which to understand threats and exploit opportunities, researchers need to look past the technical issues of data security and they need to explore why hackers do what they do. To date, very little rigorous research has been conducted on the socio-psychological aspects of hacking as the motives

behind the acts of hacking are often obscure.<sup>8</sup> Specifically, repeated calls have been made for researchers to establish relationships between motivators and hacking behavior.<sup>9–11</sup> This research intends to develop an understanding of how hackers identify and assess hacking tasks. In doing so, this investigation proposes that hackers engage in their activities as a result of two forces working in opposition to one another. On the one hand, hackers experience a number of intrinsic and extrinsic motivations that drive them to pursue their hacking task. On the other hand, there are countervailing forces that limit and mediate the risks a hacker might expose him or herself to by engaging in a hack. These countervailing forces are seen as a hacker's perception of the likelihood he or she would be caught and the severity of any sanctions that may result. The goal of this research is to explore the interplay between the factors that both incite hacking behavior and suppress it. Additionally, this research seeks to understand the contextual factors (e.g., individual and task characteristics) that influence a hacker's attitude and aversion to a specific hacking task. Task characteristics are considered extrinsic contextual factors, which include the type of hacking task being considered as well as the complexity of the task. Thus, the following two research questions are pursued:

- (1) How is the intention of hackers to engage in a hacking task (hack) influenced by motivating and demotivating factors?
- (2) How many contextual factors of individual and task characteristics influence a hacker's attitude toward engaging in a hacking task?

## Background and theoretical foundations

Oliver and Randolph<sup>11</sup> highlight that while researchers have attempted to define the term hacker, such attempts have been inconsistent and incomplete. Influenced by technological development and mainstream media, conceptualizations of hackers have shifted and conflicted in terms of their positive and negative connotations. Several attempts have been made to try to categorize hackers in order to distinguish between conflicting negative characteristics (e.g. exploiting, attacking) and positive characteristics (e.g. learning, helping) of diverse hacker definitions. For example, distinctions as to the ethics of a hacker's intentions have been conceptualized via the color of "hat" these individuals metaphorically wear. Contemporary hacker definitions present three ranges of hackers along an ethical continuum: White Hat, Grey Hat, and Black Hat.<sup>12–14</sup> The term "White Hat" is meant to portray that the hacker only partakes in hacks that are ethical, while Black Hat hacker's works

are characterized by a predacious and malevolent application of his or her skills. The Grey Hat hacker term is then used to pad this dichotomous view of hacker intentions and is essentially used to create a neutral space between the Black and the White.<sup>12</sup> Gaia et al.<sup>13</sup> use this popular hat classification to create scales that help to delineate these three categories in order to correlate personality traits to these colored hats.

The concept of categorizing hackers using hats to define the ethical impacts of their actions, while popularly used, is actually a distraction from the core issues surrounding what motivates a hacker to do the things he or she does. Mahmood et al.<sup>15</sup> make the argument that from a research perspective all hackers should be viewed the same, whereby the focus should be on their motivations and behavior rather than the 'hats' they metaphorically wear. This is the view we adopt in the current research.

Through an extensive inductive qualitative analysis of extant hacker definitions, Oliver and Randolph<sup>11</sup> propose that a hacker be "*defined as a user who wishes to gain access to an identified target in hopes of 1) learning more about the target, 2) exploiting the target for attack or 3) to benefit society*" (pp. 402). This definition acknowledges that hackers are not simple single-minded individuals. Grounded in the spirit of learning, diverse factors may influence a hacker's curiosity, motivation and actions. We adopt this holistic definition as we seek to understand hacker intention. We view the intention to hack as a synthesis of attraction and detraction factors that combine to create a net intention from which a hacker acts. The foundation of this research is grounded in two well-established behavioral theories frequently used in IS research. The first theory, the Theory of Reasoned Action (TRA), describes adoption behavior, i.e., what motivates a particular behavior. The second theory, the General Deterrence Theory (GDT), presents a countervailing avoidance behavioral framework, i.e., what discourages a particular behavior. Integrating TRA and GDT can provide a more complete picture for understanding the complex psyche and behaviors of hackers.

### Motivation: Theory of Reasoned Action

The Theory of Reasoned Action (TRA) has been extensively used to study the relationship between attitudes and behaviors and where choices are of, "... appreciable personal or social significance"<sup>16</sup> p.454. The goal of this research is, in part, to explore the factors that entice an individual hacker to be interested in carrying out a specific task (hacking). TRA is very well suited to this objective. TRA posits that a person's Behavioral

Intention (BI) is the immediate antecedent of behavior.<sup>17</sup> TRA further posits that BI can be considered a function of a person's behavioral beliefs and his or her normative beliefs. Behavioral beliefs are those beliefs that form an individual's attitudes toward a given action, while normative beliefs describe a person's perception of subjective norms.<sup>16</sup> BI is defined as "the degree to which a person has formulated conscious plans to perform or not perform some specified future behavior"<sup>18</sup> p.214. Within the IS domain, there are several theories and models that use BI as their endogenous variable of interest. Examples include the Theory of Reasoned Action,<sup>19</sup> the Theory of Planned Behavior,<sup>20</sup> the Technology Acceptance Model,<sup>21</sup> and the Unified Theory of Acceptance and Use of Technology,<sup>22</sup> among many others. Attitude toward the specified behavior is one construct that is seen to be informing BI. Attitude is a function of belief. In other words, if a person sees that an action leads to a favorable outcome, he or she will develop a positive attitude toward that action and other actions like it.<sup>23</sup> Attitude is "... a learned predisposition to respond to an object in a consistently favorable or unfavorable manner"<sup>19</sup> p.41. As such, attitude evolves over time based on an accumulation of experiences.

TRA also uses subjective norm to capture a person's perception of how people who are important to them think they should or should not perform a specific behavior.<sup>19,24</sup> Subjective norm "... refers to the perceived social pressure to perform or not to perform the behavior."<sup>16</sup> p.43. Subjective norms reflect the social environment surrounding an individual's intentions and beliefs and what an individual believes others would expect of them.<sup>23</sup> This means that what one person believes to be the expectations of others might not be an accurate. Subjective norms represent an internal force that is specific to beliefs held by a person. Ajzen & Fishbein<sup>23</sup> argue that subjective norms are related to intention by means of elements. The first element addresses the question; would influential person X believe some action has value or merit? Secondly, would that influential person X want an individual to act on this belief or intention? These two elements can then be said to impact a behavior in terms of action, target, context and time.

Hackers have been shown to develop their interests through the reinforcement and feedback of other hackers.<sup>8,25,26</sup> Madarie<sup>10</sup> suggests that hacking is a social activity, where hacking frequency is driven by peer recognition. Subjective norm is used to capture a hacker's perception of how people who are important to them think they should or should not perform a specific behavior.<sup>19,24</sup> Social norms also impact

Hackers motivation. Social norms reflect the social environment surrounding an individual's intentions and beliefs.<sup>23</sup> As a result of this adherence to community values and a collective identity, socialized norms are established as part of the framework to identify a community participant. The resulting framework then becomes an additional motivator for hackers.<sup>27</sup> So, as a hacker becomes aware of a community and starts to act as the community's norms dictate, the hacker will become more satisfied with the experience of the community and will further act to align with those norms.

### **Demotivation: General Deterrence Theory**

Deterrence Theory in its simplest form, argues that the knowledge of consequences will effect choices in such a way as to avoid infractions.<sup>28</sup> Deterrence theories function "... when a potential offender refrains from or curtails criminal activity because he or she perceives some threat of a legal punishment for contrary behavior and fears that punishment"<sup>28</sup> p.87. General Deterrence Theory is one of the most widely used criminology theories found in the IS research field.<sup>29</sup> GDT has been used to explore both internal IS misuse and external IS misuse [for examples,<sup>30-33</sup>] The effectiveness of deterrence theory relies on the perception of the certainty and severity of punishment given a planned action. In this research it is assumed that what is typically described in the literature as criminal activity will now encompass any undesirable behavior that risks sanction from an authoritative body. For example, a "criminal activity" in context of a learning institution might include unauthorized access to student records in a computer system. The punishment being risked might include expulsion.

Thus far the theoretical discussion of hacker motivation has exclusively looked at well-situated motivation theories that are used in their natural form without extension. However, as shown in the development of the TPB,<sup>17</sup> the Unified Theory of Acceptance and Use of Technology (UTAUT)<sup>22</sup> and the Unified Model of Information Security Policy Compliance (UMISPC),<sup>32</sup> it is sometimes both necessary and desirable to combine theories and to extend them with new constructs. As previously discussed, to understand hacker motivation, both the attractor elements and the detractor elements need to be considered together to capture a holistic view of their behaviors and to overcome the limitations of applying a single lens to this complex group. In the context of information security policy compliance, Moody et al.<sup>32</sup> and Ameen et al.<sup>34</sup> similarly combine attractor and detractor-based theories to propose their unified model. In this current investigation, the attraction elements

originate in TRA whereas GDT provides the appropriate constructs to evaluate the detractor elements for hacker behavior.

### Context of use

While combining TRA and GDT is expected to give insight into the motivation/demotivation process for hackers, it is of value to consider the unique contextual characteristics (e.g., individual and task characteristics) that may influence this process.<sup>35</sup> When a model is focused on the specific contextual constraints of a given IS artifact, it will have more explanatory power than a theory meant to explain the same phenomenon over a broader spectrum of technologies.<sup>36</sup> Without context, an important part of the hacker story cannot be told and a hacker's interactions with a given situation cannot be understood.<sup>37</sup> This will lead to findings that are incomplete or possibly inconclusive.<sup>38</sup> In response, this research uses the "Single Context Theory Contextualization" approach outlined by Hong et al.<sup>35</sup> This method allows for well-established theories such as TRA or GDT to act as a foundation on which constructs are added or removed. This is done by first separating core constructs from TRA and GDT, then combining them with relevant contextual factors as antecedents.

Brown et al.,<sup>36</sup> suggest there are four contextual factors that influence the intention to use certain types of collaboration technology. These broad contextual factors are: i) technology characteristics, ii) individual or group characteristics, iii) task characteristics, and iv)

situational characteristics.<sup>36</sup> In the case of exploring TRA and GDT and their impact on hacker intentions, the contextual factors of technology characteristics from the Brown et al.<sup>36</sup> list that could be set aside as it is not as meaningful. For example, evaluating a writer's choice of pen when trying to discern what drives that writer's topic selection is analogous to understanding why a choice of technology is not an important contextual concern in understanding hackers. Therefore, this research focuses on the intrinsic motivations of a hacker and not the choice of technology he or she uses. When TRA and GDT are used as lenses, only the internal and external pressures of an individual's motivations are what become important. Those motivations come from how the hacker perceives the hacking task in terms of social merit and risk, as well as the challenge it creates for the hacker. This leaves three of Brown et al.<sup>36</sup> factors relevant to this course of research. First, there are the individual characteristics of the hacker that act as drivers to motivate them to attempt a hacking task. Second, there are the characteristics of the intended task itself. Last, there is the situational context that influences a hacker's actions based on the visibility of the intended hacking task.

### Proposed research model and hypotheses

To better understand the behavioral intentions of a hacker in engaging in a specific hack, a model outlining the theoretical foundations for this research was developed and is shown in Figure 1. The constructs and

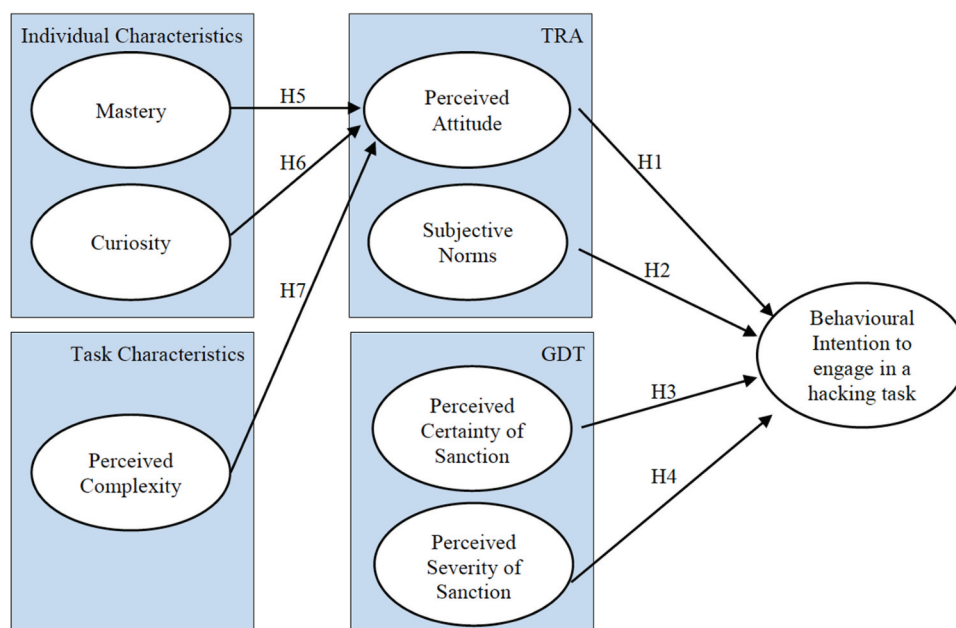


Figure 1. Integrated model for behavioral intention to engage in a hacking task.

hypotheses development of this model are described below. It is important to note that the relationships found in TRA and GDT are well understood and have been repeatedly validated across various contexts. Thus, only a selection of representative work is cited to support each relationship.

This model posits that Behavioral Intentions (BI) for a hacker are consistent with the Theory of Reasoned Action<sup>23</sup> and General Deterrence Theory.<sup>28,39</sup> Thus the model proposes that BI is informed both by motivating factors (attitude; social norms) and demotivating factors (risk assessment of the perceived certainty and severity of sanction for engaging in a hacking task). Furthermore, this model proposes that an individual's perceived attitudes are influenced by the context in which a task is being undertaken.

Behavioral Intention (BI) has been well established through TRA as a direct antecedent of behavior.<sup>40</sup> In accordance with TRA research, BI has been demonstrated to be influenced by perceived attitude and subjective norms.<sup>17</sup> Subjective norms reflect how a person sees his or her relationship with their broader community. It holds the key to a hacker's collective identity.<sup>8,10,25,41-43</sup> From a GDT perspective, BI has also been shown to be influenced by perceived risk (operationalized as the assessment of perceived certainty and severity of sanction for performing an action) in a variety of contexts.<sup>30</sup> Based on the extant literature, we posit that a hacker's behavioral intention will increase if he or she has developed a positive attitude toward carrying out a given hack. The hacker's intention to carry out a hack will also increase if he or she were to believe that those people who make up his or her social network believe that he or she should carry out the intended hack. In Beveren's<sup>44</sup> model of hacker development, peer recognition was identified as a key motivator for hackers' actions. Thus, it is hypothesized that:

**Hypothesis 1:** Perceived Attitude will have a positive impact on Behavioral Intention to engage in a hacking task.

**Hypothesis 2:** Subjective Norms will have a positive impact on Behavioral Intention to engage in a hacking task.

While hackers' intention to engaging in a hacking task was hypothesized to increase based on a positive evaluation of their attitude and perceived social support for the hack, a third, external factor, would be acting as a deterrent to carrying out the hacking task. This third factor is perceived risk for engaging in the hacking task. As the hacker assesses the hacking task, his or her

intention to do the hack will decrease as his or her perception of perceived risk increases. Perceived risk is the degree to which an individual believes that engaging in a specific action will result in an unfavorable outcome. General Deterrence Theory posits that the perceived certainty of detection and the severity of the consequences for a given action are the key elements in perceived risk and influence Behavioral Intention negatively.<sup>30</sup> It is hypothesized that when a hacker assesses the degree of risk a specific hack carries with it, he or she would consider what he or she believes is the certainty of a sanction and how severe the sanction might be. The more likely the hacker perceives that his or her actions would result in a sanction, the more risk they will associate with the specific hack. Furthermore, GDT hypothesizes that the severity of the sanction will also positively correlate with the perceived risk associated with the hacking task.<sup>45</sup> Imagine a hacker is interested in exploring the latest security flaw in a web server. He or she decides to build a server using his or her own equipment. As the activity is completely contained to his or her own server, the hacker would perceive the risk of sanctions to be low. However if this same scenario were carried out with a slightly different context, for example the computer being tested on was a surplus machine at the hacker's place of employment, the hacker might expect that his or her actions would have a greater chance of being noticed by his or her supervisor who might verbally chastise the hacker for misusing his or her time. In this case, there is an elevation in both perceived likelihood of discovery and perceived severity of sanction. Now consider a third scenario where the hacker chooses to explore the latest security flaw in a web server associated with federal income tax processing. In this case, the hacker may believe that federal authorities would likely observe this activity and that if caught he or she would be incarcerated. To the hacker this might represent extreme risk motivating strong avoidance to conduct such a hacking task. Thus, it is hypothesized that:

**Hypothesis 3:** Perceived Certainty of Sanction will have a negative impact on Behavioral Intention to engage in a hacking task.

**Hypothesis 4:** Perceived Severity of Sanction will have a negative impact on Behavioral Intention to engage in a hacking task.

As previously discussed, contextualization can help provide valuable research insights into specific domains of investigation. In the case of hackers, there were three relevant categories of context identified: individual

characteristics; task characteristics; and situational characteristics. Subjective norms were identified as the situational characteristic that influences the behavior of hackers. Given that subjective norms are included within TRA and already hypothesized within the above discussion of behavioral intentions, here we focus on the contextual characteristics of the individual and the task.

Hackers seek gratification through skill development and challenge.<sup>25,42,46</sup> Research shows that hackers have certain individual character traits that can influence their attitudes toward a hacking task. These character traits include curiosity<sup>47,48</sup> and mastery.<sup>25,46,49</sup> Curiosity has been defined as the “degree of receptivity and willingness to engage with novel stimuli.”<sup>50</sup> p.988. This is an essential trait for a hacker to possess. The hacker is driven by curiosity to want to explore and better understand technology in the first place. This also holds true for hackers when considering the individual trait of mastery. Mastery gives the hacker the skills and confidence to try something new. Curiosity encourages reflection and identification of new sources of mastery. As, Jordan & Taylor<sup>49</sup> and Holt et al.<sup>25,51</sup> attest, if a hacker sees a task as a challenge, the hacker will be drawn to it to test and develop his or her skills. This means that when a hacker’s sense of mastery and or curiosity is aroused, his or her attitude toward the hacking task will become positive and heightened. Thus, it is hypothesized that:

**Hypothesis 5:** Need for Mastery will have a positive impact on Perceived Attitude toward engaging in a hacking task.

**Hypothesis 6:** Need for Curiosity will have a positive impact on Perceived Attitude toward engaging in a hacking task.

The tasks that make up a hack have their own qualities. These qualities encompass the specific nature of a task and the perceptions of the person carrying out the task. The key task trait being explored in this research is the complexity of the task.<sup>52,53</sup>

Task complexity refers to the number of inputs, outputs and internal interactions within a task.<sup>53</sup> For example, a simple task for a hacker might be to disable a network switch. To do this there is only one outcome and one type of input. A more complex task for a hacker would be to extract passwords from a database on a remote server. This task may include dealing with attack vectors, web injections, buffer attacks, social engineering, and worms. The outcome being sought is equally complex in that it might be delivered locally to the server through a core dump or remotely through

a SQL query or Web response. To further complicate this task, the intermediary steps and interactions that need to occur on the server may be abundant.

Task complexity can be a double-edge sword for a hacker. If the task is too complex, the hacker’s attitude toward the hacking task may not be positive. This is the case since with increased task complexity, the hacker is more likely at risk of failure, and with the increased likelihood of failure, an individual is less likely to be motivated to attempt the task.<sup>54–58</sup> Conversely, a lack of complexity may also weaken a hacker’s attitude toward doing a hacking task. This is the case since if perceived challenge compared to necessary skills in a computer task (a hacking task in this case) is too low, the users will lose interest in performing that task and the task is deemed boring.<sup>59,60</sup> Thus, it is hypothesized that:

**Hypothesis 7:** Perceived Complexity will have a positive impact on Perceived Attitude.

## Research methodology

### *Procedure and participant recruitment*

Participants in this study were adults over the age of 18 that self-identify as computer hackers.<sup>1</sup> They were contacted through twitter solicitations using hash tags associated with the hacker culture, postings on message boards that were used by hackers, through communications with hacker spaces (organized clubs) located all over the world, and through direct contact at conferences and hacker group events. Upon filling out the survey, participants were asked to reflect on a hacking task that they had considered doing but have not yet tried to execute. Participants were asked to think about a hacking task they had not attempted yet so as to ensure that when they responded to the survey questions, they would be speaking of their expectations and not previously established experiences. This distinction was important since TRA and GDT are both theories that use expectations as predictors of behavior as opposed to actual experience.

This research investigation involved three stages: a pretest; a pilot study; and the main study. The pretest was used to test the understanding of the questions and verify the smoothness of the data collection process to ensure that the main study worked flawlessly. The pilot study was a ‘dress rehearsal’ for the main study where participants were contacted from the intended research population and the process was carried out as it would be done for the main study. The pilot study revealed that

<sup>1</sup>McMaster Research Ethics Board Approval for Human Subjects MREB2014169.

gaining trust of the hacker groups over the Internet presented several unexpected challenges. The questionnaire had to be reorganized twice before the concerns of the hackers were suitably addressed. Specifically, the questions related to GDT had to be moved to the end of the survey to minimize unintentional negative interpretations on the purpose of this research. The final stage was the main study that collected data from the sample population in order to validate the proposed research model.

In total, 107 self-identified hackers participated in this study. Scrutinizing the data for univariate and multivariate outliers, 13 cases were excluded, resulting in a sample size of 94. In order to determine the minimum sample size, a power analysis was conducted to assure a statistical power of 0.80, an alpha of 0.05 and detect a medium effect size ( $f = 0.25$ ).<sup>61</sup> This analysis determined a minimum sample size of 75 for our model. Thus, the final sample size of 94 used for this study was adequate.

### Instrument and model validation

The survey used previously validated instruments to help ensure content validity. Appendix A lists the questions that were used in this study. The questions were appropriately contextualized for the subject of this research and were measured using Likert scales as per the original validated constructs.

Structural Equation Modeling (SEM) was used to validate the proposed research model. Specifically, Partial Least Squares (PLS) was used because of its small sample size requirements and because PLS can be used in research that may be both confirmatory and/or exploratory in nature.<sup>62</sup> Additionally, PLS imposes a minimal demand on data distribution and residual distribution<sup>63</sup> and is more tolerant of small one or two item constructs than covariance-based SEM approaches.<sup>62</sup> The PLS software used in this research was Warp PLS. Warp PLS was selected because of the possibility that the data collected may not satisfy the linearity assumptions of standard PLS software packages. Warp PLS is designed to analyze and test for both linear and nonlinear relationships (e.g., U-shaped and S-shaped functions).<sup>64</sup> Upon examining the relationships in the data collected, a number of nonlinear relationships were detected, validating the use of Warp PLS.

Following, Hair et al.<sup>62</sup> recommendations, a two-step process was followed in evaluating the PLS results. The first step involved evaluating the measurement model to assess the reliability and validity of the measures in the model.<sup>65</sup> This step was then followed by the evaluation of the structural model to determine if there was evidence to support the proposed theoretical model.<sup>65</sup>

**Table 1.** Construct reliability of the constructs in the model.

Construct	AVE	Composite Reliability	Cronbach Alpha
Complexity	0.827	0.905	0.791
Curiosity	0.426	0.869	0.829
Mastery	0.484	0.789	0.644
Subjective Norm	0.834	0.909	0.800
Attitude	0.559	0.792	0.605
Behavioral Intention	0.809	0.927	0.881

## Data analysis and results

### Research model validation

All constructs used in this study were reflective in nature and were adapted from previously validated scales. To assess item reliability, item loading and corrected item-total correlations were examined. The majority of the indicators met minimum thresholds [as per,<sup>66</sup>] however 4 Mastery items and 1 Complexity item had to be dropped from further investigation (as indicated in Appendix 1).

To assess construct reliability in the context of our investigation, Cronbach Alpha composite reliability and Average Variance Extracted (AVE) were calculated and are shown in Table 1. Perceived Certainty and Perceived Severity of Sanction constructs utilized single-item measures [as per,<sup>30</sup>] thus are not included in validation assessments.

Typically, Cronbach's alpha values should be larger than 0.70.<sup>67</sup> However, the instrument used in this research has a number of constructs with few items. According to, Cortina<sup>68</sup> Cronbach's Alpha is sensitive to the number of items in a construct and that constructs with 20 or more items can easily meet the .70 recommendation while smaller constructs will be less likely to achieve the same value. Gliem & Gliem<sup>69</sup> offer an alternative interpretation of Cronbach's alpha in which they expand the criteria for Cronbach's alpha assessment and consider a threshold of 0.60 as tolerable. All multi-item constructs used in this study exceeded this threshold.

The AVE for two constructs (Attitude and Curiosity) fell slightly below the 0.5 recommended threshold<sup>70</sup> but still provide explanatory power. Since this research is exploring a novel phenomenon of hacker motivation, it is believed that these constructs are still able to inform and provide insights into this study's context. In terms of composite reliabilities, all constructs used in this study exceeded the 0.7 threshold<sup>62</sup>

To assess discriminant validity of this study's constructs, it is recommended that indicators load the strongest on their intended construct and that they do not load with an order of magnitude on any other construct.<sup>71</sup> As shown in Table 2, the constructs demonstrate sufficient discriminant validity.



**Table 2.** Cross loadings matrix.

	BI	Attitude	Mastery	Curiosity	Complexity	SN
BI1	<b>0.908</b>	-0.058	-0.009	-0.049	0.057	0.015
BI2	<b>0.853</b>	0.099	0.090	-0.031	-0.041	0.047
BI3	<b>0.936</b>	-0.034	-0.073	0.076	-0.018	-0.058
Attitude1	0.254	<b>0.770</b>	-0.052	-0.169	0.022	0.042
Attitude2	-0.188	<b>0.777</b>	0.107	-0.107	0.107	0.240
Attitude3	-0.071	<b>0.694</b>	-0.062	0.308	-0.095	-0.315
Mastery4	-0.018	-0.315	<b>0.695</b>	-0.134	0.200	0.220
Mastery5	0.055	0.090	<b>0.734</b>	-0.125	0.146	0.130
Mastery6	-0.023	0.149	<b>0.709</b>	0.139	-0.237	-0.186
Mastery7	-0.018	0.074	<b>0.642</b>	0.134	0.121	-0.182
Curiosity1	0.157	0.046	0.030	<b>0.583</b>	0.027	0.049
Curiosity2	-0.009	-0.054	0.058	<b>0.619</b>	0.127	-0.103
Curiosity3	0.221	0.110	0.287	<b>0.542</b>	0.131	-0.132
Curiosity4	-0.001	-0.102	-0.264	<b>0.602</b>	0.012	-0.022
Curiosity5	0.024	0.062	0.088	<b>0.658</b>	-0.122	0.114
Curiosity6	-0.191	0.085	-0.199	<b>0.721</b>	-0.396	0.028
Curiosity7	0.261	0.048	-0.139	<b>0.649</b>	0.210	0.107
Curiosity8	-0.158	-0.048	0.200	<b>0.700</b>	-0.027	0.023
Curiosity9	-0.185	-0.013	-0.018	<b>0.771</b>	0.099	-0.080
Complexity1	0.095	-0.115	0.056	-0.028	<b>0.910</b>	0.076
Complexity2	-0.095	0.115	-0.056	0.028	<b>0.910</b>	-0.076
SN1	0.153	-0.027	0.158	-0.033	0.035	<b>0.913</b>
SN2	0.153	0.027	-0.158	0.033	-0.035	<b>0.913</b>

**Structural model evaluation**

Figure 2 shows the results of the structural model analysis of the proposed research model. Of the seven hypotheses proposed, the structural model shows that there is sufficient evidence to support six of them, two being marginal. A summary of the hypotheses and their support is provided in Table 3. Attitude, Subjective Norm and Perceived Certainty of Sanction had a significant effect on Behavioral Intention ( $p < .01$ ), whereas Perceived Severity of Sanction did not have a significant effect on BI. As antecedents of Attitude, Perceived Task Complexity had a significant impact ( $p < .01$ ) and both Mastery and Curiosity individual traits marginally impacted Attitude at the 0.1 level.<sup>72</sup>

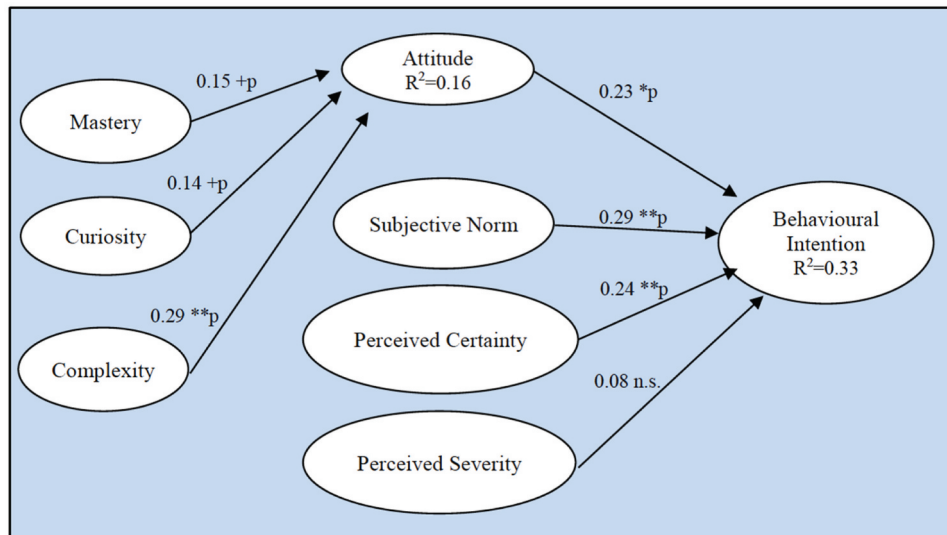
**Table 3.** Summary of findings for supporting the proposed hypotheses.

Hypothesis	Path	Path Coefficient	Significance	Validation
H1	Attitude→BI	0.23	$p < .01$	Supported
H2	SN→BI	0.29	$p < .01$	Supported
H3	Certainty→BI	0.24	$p < .01$	Supported
H4	Severity→BI	0.08	n.s.	Not Supported
H5	Mastery→Attitude	0.15	$p < .1$	Supported
H6	Curiosity→Attitude	0.14	$p < .1$	Supported
H7	Complexity→Attitude	0.29	$p < .01$	Supported

The Tenenhaus Goodness of Fit (GoF) was used to assess both the structural and measurement models' performance.<sup>73</sup> To assess the GoF, the following thresholds were used:  $GoF_{small} \geq 0.1$ ,  $GoF_{medium} \geq 0.25$ , and  $GoF_{large} \geq 0.36$ .<sup>74,75</sup> The model under study in this research scored a GoF of 0.428, which associates it with "large" explanatory power.

**Common method bias**

Common method bias occurs when data is collected using the same method, inadvertently introducing some unexpected biasing effect that changes how participant respond to the measurement instrument. Addressing common method bias requires two strategies. The first strategy is to anticipate biasing influences such as asking potentially identifying information or by inadvertently signaling an outcome bias to the participants. These types of issues are mitigated by providing assurances of steps to anonymize data and by reassuring participants that there are no right or wrong answers. In this study, some procedural remedies as recommended by, Podsakoff, MacKenzie, Lee, and



**Figure 2.** PLS structural model. \* $p < .05$ ; \*\* $p < .01$ ; \*\*\* $p < .001$ ; + $p < .1$ ; n.s.

Podsakoff<sup>76</sup> were used. The second strategy is to test for a biasing effect in the data collected after the data collection is complete.

During the development of the research instrument, a pilot study was conducted. It was very evident by the communications of those involved in the pilot study that an unintentional bias had formed in the research questions. Two questions related to General Deterrence Theory garnered a substantial amount of attention. This was corrected first by substituting the original word “punished” with the word “reprimanded” and then by reorganizing the questions to have the GDT questions appear later in the instrument. This had the effect of allowing participants better overall exposure to the nature of the research without touching on a hot topic before trust was developed. After these changes were made no new comments were received.

To address the chance that a common method bias may still be present in the instrument, two statistical tests were undertaken. The first test was Harman’s single factor test. The procedure for this test involves an unrotated exploratory factor analysis with the factors being constrained to one factor. If the single factor accounts for more than 50% of the variance then a common method bias is present. When this test was conducted on the research data only 17.768% of the variance was explained. This value supports the argument that no common method bias was present. A second analysis was conducted involving the examination of the full collinearity VIFs, where a score of 3.3 or lower suggest no common method bias.<sup>77</sup> The data in this research scored 1.261. Given the strong results from both tests, it can be concluded that common method bias did not impact this investigation.

## Discussion

This research explores hacker motivation and demotivation in regard to target selection through the lenses of the Theory of Reasoned Action (TRA) and General Deterrence Theory (GDT), as well as the effects of context on a hacker’s task selection. Thus, intention to hack is viewed as a synthesis of attraction and detraction factors that combine to create a net intention from which a hacker acts. TRA describes two sources for influencing behavioral intentions: attitude and subjective norms. The research results supported these antecedent to behavioral intentions and thus supported the role of TRA as a framework from which to explore hacker motivations. Public perceptions or personification of hackers tends to depict them as “loners” or averse to socializing. However, this investigation shows that close social associations such as family and peer groups,

represented by the subjective norm construct, have a significant impact on a hacker’s behavioral intentions. Thus, there is evidence to argue that if a hacker’s social environment approves of his or her endeavors or sees his or her goals as valuable then the hacker’s intentions to carry out a hacking task will increase. This supports earlier work from, McHugh & Deek<sup>26</sup> that suggests hackers develop their interests through the reinforcement and feedback of other hackers.

To the best of our knowledge, this research was the first study to utilize GDT to explore the hacker phenomena. In this study, it was determined that hackers do in fact consider the likelihood of being caught when they consider attempting a hacking task. Interestingly the severity of punishment/sanctions did not have a significant effect on hackers’ intention to engage in a hacking task. Thus, it appears that, D’Arcy et al.’s<sup>30</sup> assertion that both the perceived certainty of detection and the severity of the consequences are key elements in risk perception that negatively influence behavioral intention does not apply to hackers. Do hackers assess the degree of risk associated with a particular hack primarily through the probability of getting caught? Perhaps the severity of the reprimand is not as important or a risk they are willing to accept given the nature of behavior. This would be in alignment with, Staggs et al.<sup>78</sup> who recently explored the impact of general media exposure of hackers on perceptions of hacking behaviors. Through this lens, they found that perceived risk carried little weight in predicting willingness to hack. Another potential explanation for this unexpected result pertains to the task itself. Participants were asked to reflect on a hacking task that they had considered doing but have not yet tried to execute when completing the survey. It could have been that most of the participants were contemplating a hack that would not have severe sanctions if caught. For example, if they were contemplating a hack that involved exploiting a security flaw in a web server at their local workplace by using surplus machine, their perceptions of being caught may be moderate to high but expectations of punishment may be low (such as a verbal reprimand). Unfortunately, it was not possible to ask participants to describe the hack they were contemplating, as this would negatively impact their trust and willingness to participate in the study. This is an interesting opportunity for future investigation.

This research also investigates the unique contextual characteristics (e.g., individual and task characteristics) that may influence the motivation/demotivation process. Without context, an important part of the hacker story cannot be told and a hacker’s interactions with a given situation cannot be understood.<sup>37</sup> Based on

extant literature, mastery and curiosity were hypothesized to have direct positive effects on a hacker's attitude toward engaging in a hacking task. While the relationships were not strong, there was marginal support for these individual characteristics impacting hacker's attitudes. However the nature of the task itself was shown to have a strong impact on hacker's attitude toward engaging in a hacking task. Specifically, the more a hacking task is seen as being technically complex to the hacker, the more positive the attitude toward trying the hack. This is a finding that would benefit from further investigation due to its non-linear nature. A hack that lacks complexity is deemed to be boring and does not garner interest among individuals that enjoy the challenge of understanding the internal workings of systems or networks. However, if a task is perceived to be too complex, it may be deemed to be unachievable with a high risk of failure. A deeper understanding of the mechanics that drive this non-linear relationship could provide richer insight into hacker behavior.

## Contributions

This research makes several contributions to both theory and practice. It addresses the need to directly examine the motivations and behaviors of this unique population<sup>9-11,15</sup> by surveying actual hackers that were actively contemplating a hacking task at the time of the research. In examining this unique population, this research used a novel aesthetic lens as an alternative to utilitarianism to view the phenomena. When combined with the intrinsic motivations explored in this investigation, a new group of research questions form. For example, do all attitudes toward actions come from the same logic or goal setting process, or could factors such as attitude be masked by other factors effecting decision making such as aesthetic goals instead of utilitarian goals. The use of an aesthetic lens introduces numerous opportunities to revisit old ideas and apply a fresh perspective. Sören Kierkegaard (1813–1855) posited that people live in the moment; they are moved by the artistry in their lives and not all actions follow ethical principles. Kierkegaard's idea of an aesthetic life superseding the motivation of living an ethical life has proven to be an important foundation for understanding the motivations of hackers. This study has shown that a research lens separated from the orthodoxy utilitarian rationales was an effective approach to investigate this novel population.

The benefits of this research to the professional community are twofold. On one hand the research demonstrates key antecedents that attract hackers toward new tasks. On the other hand, these same antecedents also

hint at strategies to better engage these unique individuals and to leverage their skills in creative product development opportunities.

This research benefits cyber security professionals by providing a better understanding of the motivations of the people behind some of their threats. Based on these findings, practitioners will be able to design strategies to better combat new or developing threats by looking past the technical issues of data security and explore why hackers do what they do. Through the use of a rigorous quantitative methodology, this research introduces an understanding of how hackers identify and assess their tasks. By investigating the motivations of these highly skilled information systems users, new insights into how to avoid harmful actions can be ascertained.

By understanding the impacts that mastery, curiosity and complexity have on hackers' motivations, this research establishes opportunities to engage these IS gurus in fruitful economic activities. By leveraging the results of this research, astute managers can create engaging workspaces replete with appropriate stimuli to attract and benefit from these highly skilled and creative individuals.

The key for industry to leverage this research is to understand that new innovations will attract hackers' attention. Whether it is illegally penetrating a network, controlling a traffic sign or modifying features in an Internet connected car, if it's new and looks like a challenge to hackers, then they will be drawn to it. While some of this type of attention is undesirable, there is an equally desirable side effect for industry. The characteristics that have been identified in this research would also make highly desirable characteristics for product designers. Given that novelty and social contributions have been identified as desirable to hackers, product developers (like those seen on the kickstarter.com website) could be ideal candidates to solicit hackers to contribute to their tasks and tap into their unique skills.

## Limitations and future research

As with any study, this research is constrained by certain limitations. Most notably, this research is limited by the generalizability and size of its sample. While the recommended minimum sample size was exceeded, obtaining 107 usable samples (from which 13 were excluded as outliers) was highly challenging and time consuming. Surveying actual hackers that were actively contemplating a hacking task meant that the sample was naturally skeptical and hesitant to participate. There were an additional 230 responses

to the survey that were not completed that were sourced from hacker groups around the world. This difficulty in obtaining data on motivation perspectives from hackers has been noted by several researchers.<sup>8,79</sup> Regardless of detailed explanation of the purpose of the study, the holistic conceptualization of a hacker and assurances of confidentiality and anonymity, the target group tended to distrust academic motives and highly scrutinize each component of the survey. As such, the sample that chose to complete the survey may not be truly representative of the broader hacker community.

As a result of these limitations there is clearly an opportunity to return to this line of research and build on the foundations it has created. While the current investigation met all its required reliability and validity checks, it would still be desirable to find ways to support its generalizability claims and to increase the depth of the analysis through an expanded sample population. While these issues are a concern, they also represent opportunities for the research community to verify and expand our understanding of this emerging and important hacker phenomenon.

A goal of this research was to identify a select group of key intrinsic motivations and explore their role in how hackers identify the tasks and actions that interest and inspire them to discovery. The research made significant headway in establishing an understanding of the roles of mastery and curiosity in this process. Future research can further explore the role of these intrinsic motivations in a hacker's decision-making process. How and when do curiosity and the desires for mastery mold the hacker psyche and choices he/she makes? Additionally, there is opportunity to investigate other intrinsic motivators in understanding this unique population. For example, Madarie<sup>10</sup> suggest that humbleness and commitment to customs may play a role in understanding hacker motivations.

In parallel to the role of intrinsic motivation on hacker's task selection was the idea that the artifact itself also plays a role in the hacker selection process. Task complexity was explored alongside the personality drivers and represented extrinsic motivation for a hacking task. How a hacker assesses task complexity was not clearly established in this research. The role of this variable as well as the task difficulty needs to be further investigated. According to, Jordan & Taylor<sup>49</sup> a hacking task is not valuable if it is not unique, original and complete. How does complexity play into their definition of a hacking task?

This research was novel in that it took two well-established theories (TRA and GDT) and placed them alongside each other to see if and how they

were relevant to hackers. The use of GDT in this research proved to be challenging as it created unnecessary and unproductive resistance among the participants due to their broader anxiety toward a negative public stereotype. While the connections discovered in this research relating to the roles and interactions of TRA and GDT are compelling, there may be benefit to studying these two concepts separately to enhance the scope of each theories' interaction with the broader hacker community.

## Conclusion

This investigation addressed an important gap in the research on hackers. It explored hacker motivation, demotivation and task selection. It did so by accessing actual hackers and establish relationships between motivators and hacking intention, which have been identified as gaps in extant literature.<sup>10,11</sup> The study also used a novel research lens by looking at hacker motivation not as a function of utility but as a question of aesthetics. This novel lens opened opportunities to explore hacker behavior by looking at the role context played in molding hacker's intentions. The study also addressed the call for context in IS research by exploring individual and task contextual characteristics.

Ultimately this study gave new insight into understanding how the intention of hackers to perform a hacking task is influenced by motivating and demotivating factors, and it added to the understanding of how contextual factors of individual and task characteristics may influence the motivating and demotivating mediators of a hacker's intention to engage in a hacking task.

## Disclosure statement

No potential conflict of interest was reported by the author(s).

## ORCID

Milena Head  <http://orcid.org/0000-0002-4329-3654>

## References

1. Morgan S. Cybercrime to Cost the World \$10.5 trillion annually by 2025. *Cybercrime Magazine*. 2020. [Accessed 2021 01 24]. <https://cybersecurityventures.com/annual-cybercrime-report-2019/>
2. Chng S, Lu HY, Kumar A, Yau D. Hacker types, motivations and strategies: a comprehensive framework. *Computers in Human Behavior Reports*. 2022;5:100167. doi:10.1016/j.chbr.2022.100167.

3. Monteith S, Bauer M, Alda M, Geddes J, Whybrow PC, Glenn T. Increasing cybercrime since the pandemic: concerns for psychiatry. *Curr Psychiatry Rep.* 2021;23(4). doi:10.1007/s11920-021-01228-w.
4. Raspberry Pi Foundation Annual Review. 2020. [Accessed 2021 01 24]. <https://static.raspberrypi.org/files/about/RaspberryPiFoundationReview2020.pdf>
5. Seals T (2020). GM's transportation future hinges on cybersecurity. *RSAC 2020*. [Accessed 2021 01 24]. <https://threatpost.com/gm-transportation-future-cybersecurity/153303/>
6. Mangindin G. Top companies hiring ethical hackers. *Career Karma*; 2022. [Accessed 2022 03 13]. <https://careerkarma.com/blog/best-companies-for-ethical-hackers/>
7. Cable J. Why the U.S. government needs you to hack it. *Fast Company*. 2019. [Accessed 2021 01 24]. <https://www.fastcompany.com/90443829/why-the-u-s-government-needs-you-to-hack-it>
8. Cayubit RFO, Rebolledo KM, Kintanar RGA, Pastores AG, Santiago AJA, Valles PBV. A cyber phenomenon: a Q-analysis on the motivation of computer hackers. *Psychol Stud (Mysore)*. 2017;62(4):386–94. doi:10.1007/s12646-017-0423-9.
9. Crossler RE, Johnston AC, Lowry PB, Hu Q, Warkentin M, Baskerville R. Future directions for behavioral information security research. *Computer Security*. 2013;32:90–101. doi:10.1016/j.cose.2012.09.010.
10. Madarie R. Hackers' motivations: testing Schwartz's theory of motivational types of values in a sample of hackers. *International Journal of Cyber Criminology*. 2017;11:78–97.
11. Oliver D, Randolph AB. Hacker definitions in information systems research. *J Comput Inf Syst.* 2020;62(2):397–409. doi:10.1080/08874417.2020.1833379.
12. Bansal A, Arora M. Ethical hacking and social security. *Radix International Journal of Research in Social Science*. 2012;1:1–16.
13. Gaia J, Ramamurthy B, Sanders GL, Sanders SP, Upadhyaya S, Wang X, Yoo CW. Psychological profiling of hacking potential. *Proceedings of the 53rd Hawaii International Conference on System Sciences*. January 7-10, 2020. Maui, Hawaii, USA; 2020.
14. Georg T, Oliver B, Gregory L. Issues of implied trust in ethical hacking. *The ORBIT Journal*. 2018;2(1):1–19. doi:10.29297/orbit.v2i1.77.
15. Mahmood MA, Siponen M, Straub D, Rao HR, Raghu TS. Moving toward black hat research in information systems security: an editorial introduction to the special issue. *MIS Quarterly*. 2010;34(3):431–33. doi:10.2307/25750685.
16. Ajzen I, Madden T. Prediction of goal-directed behavior: attitudes, intentions, and perceived behavioral control. *J Exp Soc Psychol.* 1986;22(5):453–74. doi:10.1016/0022-1031(86)90045-4.
17. Madden TJ, Ellen PS, Ajzen I. A comparison of the theory of planned behavior and the theory of reasoned action. *Pers Soc Psychol Bull.* 1992;18(1):3–9. doi:10.1177/0146167292181001.
18. Warshaw PR, Davis FD. The accuracy of behavioral intention versus behavioral expectation for predicting behavioral goals. *Journal of Psychology*. 1985;119(6):599. doi:10.1080/00223980.1985.9915469.
19. Fishbein M. Belief, attitude, intention, and behavior: an introduction to theory and research. In: Ajzen I, Ed. Reading (Mass): Addison-Wesley Pub. Co; 1975.
20. Ajzen I. The Theory of Planned Behavior. *Organ Behav Hum Decis Process.* 1991;50(2):179–211. doi:10.1016/0749-5978(91)90020-T.
21. Davis FD. A technology acceptance model for empirically testing new end-user information systems: theory and results [Unpublished doctoral dissertation]. Cambridge: Massachusetts Institute of Technology; 1986.
22. Venkatesh V, Morris MG, Davis GB, Davis FD. User acceptance of information technology: toward a unified view. *MIS Quarterly.* 2003;27(3):425–78. doi:10.2307/30036540.
23. Ajzen I, Fishbein M. Understanding attitudes and predicting social behavior. Englewood Cliffs (N.J): Prentice-Hall; 1980.
24. Venkatesh V, Thong JY, Xu X. Consumer acceptance and use of information technology: extending the Unified Theory. *MIS Quarterly.* 2012;36(1):157–78. doi:10.2307/41410412.
25. Holt TJ, Leukfeldt R, van de Weijer S. An examination of motivation and routine activity theory to account for cyberattacks against Dutch web sites. *Crim Justice Behav.* 2020;47(4):487–505. doi:10.1177/0093854819900322.
26. McHugh JAM, Deek FP. An incentive system for reducing malware attacks. *Commun ACM.* 2005;48(6):94–99. doi:10.1145/1064830.1064833.
27. Lindenberg S. Intrinsic Motivation in a New Light. *Kyklos.* 2001;54(April):317–42. doi:10.1111/1467-6435.00156.
28. Gibbs JP. Deterrence Theory and Research. In: Melton GB, editor. Nebraska symposium on motivation, 1985. Lincoln: University of Nebraska Press; 1986. p. 87–130.
29. Young R, Zhang L. Illegal computer hacking: an assessment of factors that encourage and deter the behavior. *Journal of Information Privacy & Security.* 2007;3(4):33–52. doi:10.1080/15536548.2007.10855827.
30. D'Arcy J, Hovav A, Galletta D. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research.* 2009;20(1):79–98. doi:10.1287/isre.1070.0160.
31. Merhi MI, Ahluwalia P. Examining the impact of deterrence factors and norms on resistance to information systems security. *Comput Human Behav.* 2019;92:37–46. doi:10.1016/j.chb.2018.10.031.
32. Moody G, Siponen M, Pahnla S. Toward a unified model of information security policy compliance. *MIS Quarterly.* 2018;42(1):285–311. doi:10.25300/MISQ/2018/13853.
33. Straub D, Weike RJ. Coping with systems risk: security planning models for management decision making. *MIS Quarterly.* 2008;22(4):441–69. doi:10.2307/249551.
34. Ameen N, Tarhini A, Shah MH, Madichie N, Paul J, Choudrie J. Keeping customers' data secure: a cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. *Comput Human Behav.* 2021;114:106531. doi:10.1016/j.chb.2020.106531.

35. Hong W, Chan FKY, Thong JYL, Chasalow LC, Dhillon G. A framework and guidelines for context-specific theorizing in information systems research. *Information Systems Research*. 2014;25(1):111–36. doi:10.1287/isre.2013.0501.
36. Brown S, Dennis AR, Venkatesh V. Predicting collaboration technology use: integrating technology adoption and collaboration research. *Journal of Management Information Systems*. 2010;27(2):9–54. doi:10.2753/MIS0742-1222270201.
37. Johns G. The essential impact of context on organizational behavior. *Academy of Management Review*. 2006;31(2):386–408. doi:10.5465/amr.2006.20208687.
38. Whetten DA. An examination of the interface between context and theory applied to the study of Chinese organizations. *Management and Organization Review*. 2009;5:29–55.
39. Gibbs JP. *Crime, Punishment, and Deterrence*. New York, NY, USA: Elsevier Ltd; 1975.
40. Ajzen I, Fishbein M, Wicker AW. Attitudinal and normative variables as predictors of specific behavior. *J Pers Soc Psychol*. 1973;27(1):41–57. doi:10.1037/h0034440.
41. Lakhani KR, Wolf B, Bates J, DiBona C. The Boston Consulting Group Hacker Survey. 2002. [Accessed 2021 01 24]. <http://www.bcg.com/opensource/BCGHackerSurveyOSCON24July02v073.pdf>
42. Lakhani KR, Wolf RG. Why hackers do what they do. Understanding Motivation and Effort in Free/Open Source Software Projects. 2005:1–27. [Accessed 2020 05 16]. <https://ssrn.com/abstract=443040>
43. Voiskounsky AE, Smyslova OV. Flow-based model of computer hackers' motivation. *Cyberpsychology & Behavior: The Impact of the Internet, Multimedia and Virtual Reality on Behavior and Society*. 2003;6(2):171–80. doi:10.1089/109493103321640365.
44. Van Beveren J. A conceptual model of hacker development and motivation. *Journal of E-Business*. 2001;1:1–9.
45. D'Arcy J, Herath T. A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *Eur J Inf Syst*. 2011;20(6):643–58. doi:10.1057/ejis.2011.23.
46. Goode S, Cruise S. What motivates software crackers? *Journal of Business Ethics*. 2006;65(2):173–201. doi:10.1007/s10551-005-4709-9.
47. Holt TJ. Subcultural evolution? Examining the influence of on- and Off-Line experiences on deviant subcultures. *Deviant Behav*. 2007;28(2):171–98. doi:10.1080/01639620601131065.
48. Turgeman-Goldschmidt O. Hackers' accounts hacking as a social entertainment. *Social Science Computing Review*. 2005;23(1):8–23. doi:10.1177/0894439304271529.
49. Jordan T, Taylor P. A sociology of hackers. *Sociological Review*. 1998;46(4):757–80. doi:10.1111/1467-954X.00139.
50. Kashdan TB, Gallagher MW, Silvia PJ, Winterstein BP, Breen WE, Terhar D, Steger MF. The curiosity and exploration Inventory-II: development, factor structure, and psychometrics. *J Res Pers*. 2009;43(6):987–98. doi:10.1016/j.jrp.2009.04.011.
51. Holt TJ, Burruss GW, Bossler AM. Social learning and cyber-deviance: examining the importance of a full social learning model in the virtual world. *Journal of Crime and Justice*. 2010;33(2):31–61. doi:10.1080/0735648X.2010.9721287.
52. Campbell DJ. Task Complexity: a Review and Analysis. *The Academy of Management Review*. 1988;13(1):40. doi:10.2307/258353.
53. Ziguers L, Buckland B. A theory of Task/Technology fit and group support systems effectiveness. *MIS Quarterly*. 1998;22(3):313–34. doi:10.2307/249668.
54. de Vries H, Dijkstra M, Kuhlman P. Self-efficacy: the third factor besides attitude and subjective norm as a predictor of behavioral intentions. *Health Educ Res*. 1988;3(3):273–82. doi:10.1093/her/3.3.273.
55. Haid M, Graschitz S, Heimerl P. A matter of motivation—the effects of risk preference and task complexity on the Auditor's motivation. *WSB Journal of Business and Finance*. 2019;53(2):1–14. doi:10.2478/wsbjbf-2019-0017.
56. McGrath JE. *Groups: interaction and performance (Vol.14)*. Englewood Cliffs (N.J): Prentice-Hall; 1983.
57. Shanteau J. Competence in experts: the role of task characteristics. *Organ Behav Hum Decis Process*. 1992;53(2):252–66. doi:10.1016/0749-5978(92)90064-E.
58. Spence JT, Helmreich RL. *Achievement and Achievement Motives: Psychological and Sociological Approaches* Spence, JT. San Francisco, CA, USA: Freeman. 1983. Achievement-Related Motives and Behavior;10–74.
59. Ghani JA, Deshpande SP. Task characteristics and the experience of optimal flow in human—computer interaction. *Journal of Psychology*. 1994;128(4):381–91. doi:10.1080/00223980.1994.9712742.
60. Sepehr S, Head M. Understanding the role of competition in video gameplay satisfaction. *Information & Management*. 2018;55(4):407–21. doi:10.1016/j.im.2017.09.007.
61. Cohen J. *Statistical power analysis for the behavioral sciences*. 2nd. Hillsdale (NJ): Erlbaum; 1988.
62. Hair JF, Ringle CM, Sarstedt M. PLS-SEM: indeed a silver bullet. *The Journal of Marketing Theory and Practice*. 2011;19(2):139–52. doi:10.2753/MTP1069-6679190202.
63. Chin WW. Issues and opinion on structural equation modeling. *MIS Quarterly*. 1998;22:1–8.
64. Guo KH, Yuan Y, Archer NP, Connelly CE. Understanding nonmalicious security violations in the workplace: a composite behavior model. *Journal of Management Information Systems*. 2011;28(2):203–36. doi:10.2753/MIS0742-1222280208.
65. Chin WW. How to write up and report PLS analyses. In: Vinzi VE, Chin WW, Henseler J, Wang H, editors. *Handbook of partial least squares*. Berlin, Germany: Springer; 2010. p. 655–90.
66. Gefen D, Straub D, Boudreau M-C. Structural equation modeling and regression: guidelines for research practice. *Communications of the Association for Information Systems*. 2000;4(August). doi:10.17705/1CAIS.00407.

67. Bernstein IH, Nunnally JC. A catastrophe model for developing service satisfaction strategies. *Journal of Marketing*. In: Oliva T, Oliver R, MacMillan I, editors. *Psychometric theory*. New York, NY, USA: McGraw-Hill; 1994. p. 83–95.
68. Cortina JM. What is coefficient alpha? An examination of theory and applications. *Journal of Applied Psychology*. 1993;78(1):98. doi:10.1037/0021-9010.78.1.98.
69. Gliem JA, Gliem RR. Calculating, interpreting, and reporting Cronbach's Alpha reliability coefficient for Likert-Type scales. 2003 Midwest Research to Practice Conference in Adult, Continuing, and Community Education. Columbus, OH, USA; 2003. 82–88.
70. Mackenzie SB, Podsakoff PM, Podsakoff NP. Construct measurement and validation procedures in MIS and behavioral research: integrating new and existing techniques summary of steps for scale purification and refinement. *MIS Quarterly*. 2011;35(2):1–5. doi:10.2307/23044045.
71. Gefen D, Straub D. A practical guide to factorial validity using pls-graph: tutorial and annotated example. *Communications of AIS*. 2005;2005:91–109.
72. Dimoka A, Hong Y, Pavlou PA. On product uncertainty in online markets: theory and evidence. *MIS Quarterly*. 2012;36(2):395–426. doi:10.2307/41703461.
73. Henseler J, Sarstedt M. Goodness-of-fit indices for partial least squares path modeling. *Comput Stat*. 2013;28(2):565–80. doi:10.1007/s00180-012-0317-1.
74. Akter S, Ambra JD, Ray P. Development and validation of an instrument to measure user perceived service quality of mHealth. *Information and Management*. 2013;50(4):181–95. doi:10.1016/j.im.2013.03.001.
75. Wetzels M, Odekerken-Schröder G, van Oppen C. Using PLS path modeling for assessing hierarchical construct models: guidelines and empirical illustration. *MIS Quarterly*. 2009;33:177–95.
76. Podsakoff PM, MacKenzie SB, Lee JY, Podsakoff NP. Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology*. 2003;88(5):879. doi:10.1037/0021-9010.88.5.879.
77. Kock N, Lynn GS. Lateral collinearity and misleading results in variance-based SEM: an illustration and recommendations. *Journal of the Association for Information Systems*. 2012;13(7):546–80. doi:10.17705/1jais.00302.
78. Staggs S, McMichael SL, Kwan VSY. Wishing to be like the character on screen: media exposure and perception of hacking behavior. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*. 2020;14(1). doi:10.5817/CP2020-1-4.
79. Adam A, Ofori-Amanfo J. Does gender matter in computer ethics? *Ethics Inf Technol*. 2000;2(1):37–47. doi:10.1023/A:1010012313068.

## Appendix A: Measurement Scales

Construct (Source)	Items
Behavioral Intention <sup>22</sup>	<ol style="list-style-type: none"> <li>1. I intend to do this hack in the next 6 months</li> <li>2. I predict I would do this hack in the next 6 months</li> <li>3. I plan to do this hack in the next 6 months</li> </ol>
Attitude <sup>22</sup>	<ol style="list-style-type: none"> <li>1. Doing this hack is a good idea.</li> <li>2. I like the idea of doing this hack.</li> <li>3. Doing this hack will be pleasant.</li> </ol>
Subjective Norm <sup>22</sup>	<ol style="list-style-type: none"> <li>1. People who influence my behavior think that I should do this hack.</li> <li>2. People who are important to me think that I should do this hack.</li> </ol>
Mastery <sup>58</sup>	<ol style="list-style-type: none"> <li>1. I would rather do something at which I feel confident and relaxed than something which is challenging and difficult *</li> <li>2. When a group I belong to plans an activity, I would rather direct it myself than just help out and have someone else organize it. a*</li> <li>3. I would rather learn easy fun games than difficult thought games. *</li> <li>4. If I am not good at something, I would rather keep struggling to master it than move on to something I may be good at.</li> <li>5. Once I undertake a task I persist.</li> <li>6. I prefer to work in situations that require a high level of skill.</li> <li>7. I more often attempt tasks that I am not sure I can do than tasks that I believe I can do.</li> <li>8. I like to be busy all the time. *</li> </ol>
Curiosity <sup>50</sup>	<ol style="list-style-type: none"> <li>1. I actively seek as much information as I can in new situations</li> <li>2. I am the type of person who really enjoys the uncertainty of everyday life</li> <li>3. I am at my best when doing something that is complex or challenging</li> <li>4. Everywhere I go, I am out looking for new things or experiences</li> <li>5. I view challenging situations as an opportunity to grow and learn</li> <li>6. I like to do things that are a little frightening</li> <li>7. I am always looking for experiences that challenge how I think about myself and the world</li> <li>8. I prefer jobs that are excitingly unpredictable</li> <li>9. I frequently seek out opportunities to challenge myself and grow as a person</li> <li>10. I am the kind of person who embraces unfamiliar people, events, and places *</li> </ol>
Perceived certainty of discovery <sup>30</sup>	If I did this hack, I would probably get caught
Perceived sanction severity <sup>30</sup>	If I get caught doing this hack, I will be severely reprimanded
Perceived Complexity(Jarupathirun, Zahedi, <sup>52</sup> )	This task is: (1) Very simple vs. Very complex (2) Very straight forward vs. Very complicated

\*denotes the item was dropped from analysis following measurement model assessments.