MASARYK UNIVERSITY

JOURNAL OF PSYCHOSOCIAL RESEARCH ON CYBERSPACE
CYBERPSYCHOLOGY

Staggs, S., McMichael, S. L., & Kwan, V. S. Y. (2020). Wishing to be like the character on screen: Media exposure and perception of hacking behavior. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *14*(1), Article 4. https://doi.org/10.5817/CP2020-1-4

Wishing to be Like the Character on Screen: Media Exposure and Perception of Hacking Behavior

Sarah Staggs, Samanta L. McMichael, & Virginia S. Y. Kwan

Department of Psychology, Arizona State University, Tempe, Arizona, USA

Abstract

This research addressed whether exposure to media, which increasingly portrays hacker characters across diverse media domains, may predict perceptions of others' willingness to hack. Specifically, this study assessed how wishful identification with hacker characters may contribute to individuals' perception of hacking behaviors. One-hundred forty-nine North American participants were recruited using MTurk.com. Participants reported (1) their exposure to general media and perceived identification with a fictional hacker character, and (2) their perceived risks, payoffs, and estimated willingness of others to engage in hacker behaviors regarding a specific call to hack. Additionally, this research examined differences in the effects of media exposure on hacking likelihood between two types of hacks: financial hacking attacks and hacktivism attacks. Results show (1) that perceived payoffs of hacking, but not perceived risks, predict individuals' estimation of hacker behaviors, (2) a significant and positive indirect effect between media exposure and estimation of others' willingness to hack passes through wishful identification and perceived payoffs of hacking attacks, and (3) no significant differences in the above relationships between the two types of hacks. Together, these findings highlight that media exposure may increase positive perceptions of hackers and in turn increase the perception of pervasiveness and legitimacy of engaging in hacking behaviors.

Keywords: Wishful identification; game theory; cyber attacks; hacking; hacktivism; computer crimes

Introduction

Cyber-attacks are growing more frequent and are considered to be one of the greatest threats to the United States economy (Graham, 2017; Rainie et al., 2014; The Council of Economic Advisers, 2018). As cyber-attacks are attracting national attention, media portrayals of hacker characters, who engage in unrealistic but thrilling feats, are becoming mainstream (Rosewarne, 2016). Given the increasingly pervasive nature of cyber-crimes, both in reality and on-screen, it is important to consider how media exposure may impact perceptions of hacking behaviors.

The present study explores the relationship between media exposure and perception of others' willingness to engage in socially motivated (i.e. hacktivism) and financially motivated hacks. Within the communications literature, the wishful identification perspective postulates that children and young adults are likely to develop a desire to be like, and behave like, a character portrayed in media (Greenwood, 2007; Hoffner, 1996; Hoffner & Buchanan, 2005). In this research, we argue that exposure to media may predict wishful identification with a hacker character, affect estimates of risks and payoffs associated with hacking behaviors, and ultimately, applying a Game Theoretical model, predict perceptions of willingness to hack. Below, we first briefly introduce the literature on the diverse nature of hacking behaviors. We then discuss the surge in media representations of hackers, provide a rationale for exploring the impact of general media exposure on perceptions of cyber-crimes, and review the tenets of wishful identification. Finally, using a Game Theoretical model, we outline a mechanism by which media exposure may affect estimates of risks and payoffs and influence the perception that others will engage in hacking behaviors.

Hacking Behaviors

As hacking becomes more prevalent and impactful, it is crucial to recognize that hackers as a group are diverse in both their behaviors and motivations. As large-scale cyber-attacks increase, hackers are often vilified as criminals and the term "hacking" is used broadly to encompass all instances of cyber-crimes in the news media (Coleman, 2012). Undoubtably, some hacking behaviors do fall into this clearly criminal realm. For instance, organized crime hackers are generally considered to be motivated by money, the excitement or thrill, and the feeling of power, using social engineering (e.g., phishing emails and planting malware) to target and steal from their victims (Borrett, 2010; Holt & Schell, 2010). However, theorists suggest that traditional hackers are far more complicated; they generally possess expansive technical skills and interest in technology and are often motivated by a moral or political cause (i.e. freedom of information) (Coleman, 2011; Kelty, 2008; Young et al., 2007). These hackers are characterized as "digital activists" or as engaging in "digital civil disobedience" (Sauter, 2013; Züger et al., 2015). The hacker group Anonymous demonstrated this political motivation in 2010 with their highly publicized distributed denial-of-service (DDoS) attacks intended to support WikiLeaks and their endeavor to freely publish classified documents (Sauter, 2013). This type of activism motivated hacking, or "hacktivism," often begins with a "call to hack" through an online forum that draws hackers to participate in the cause (Massa, 2011).

Although hacking behaviors are diversely motivated, it is important to consider the implications of both criminal financial and politically/socially motivated hacking. Both categories of behaviors have the potential to incur great costs. Cyber-attacks in their general form are estimated to cost the U.S. government hundreds of billions of dollars per year (Krawczyk, 2014), far more than annual government expenditures following natural disasters. Distributed denial of service (DDoS) attacks, such as those used by Anonymous, have been characterized as "the networked version of a peaceful sit-in" (Bergal, 2017; Mansfield-Devine, 2011; Milan, 2013). However, Ponemon Institute (2012) estimates that companies lose $22,000 for every minute that their website is taken offline. Additionally, in 2012 alone, hacking for financial gain accounted for more than $100 billion in financial losses to individuals, corporations, and governments (Wiederhold, 2014).

While these financial damages are extensive, commonly, hackers are conceptualized as an elite group of highly technologically skilled actors (Coleman, 2011). Prior to widespread internet and technology access, only individuals with immense technical skills were capable of engaging in hacking, making it less likely that these hacks would take place. That reality is quickly changing. As the use of technology and the internet becomes more mainstream, it is becoming increasingly easier for individuals with a certain degree of familiarity with computers to engage in hacking activities. Individuals without the technical skill to engineer hacks are often able to use code written by more traditionally skilled hackers (Barber, 2001). While these individuals, known as "script kiddies" within hacker communities, lack sophistication, they are capable of inflicting vast financial damage (Gonsalves, 2003). Given this increasingly generalized risk, it is crucial to investigate factors, such as media representations, that may impact perceptions of hacking and the likelihood that individuals may choose to engage.

Media Representations of Hackers

Media representations of hacker characters are significantly increasing. The first computer hackers were portrayed in movies such as *Hot Millions* (1968) and the *Italian Job* (1969) (Gordon, 2010). In order to gain a preliminary understanding of the media portrayal of hacker characters over time, we conducted an exploratory analysis of media from the first instances of hacker portrayals (1968) to the present (2017). Through our preliminary analysis, we found a total of 166 hacker characters portrayed in TV shows and films from 1968 to 2017. For this analysis, only prominent characters were considered. Prominent characters were defined as "a character who appears in all episodes, or are major characters in feature films." To inventory all of these shows, we started with a Wikipedia page that was created for all fictional hacker characters in television shows and film (Wikipedia Contributors, 2020). This list was updated by our team of researchers as well as cross-checked for validity. Notably, forty-five percent (*n* = 74) of the characters were on programs airing in the last decade alone. Popular entertainment programs portraying hackers include *Elementary* (2012-present), *Mr. Robot* (2017-present), *WarGames* (1983), *The Matrix* (1999), and *Girl with the Dragon Tattoo* (2011). Each of the TV series listed above ranged from 8-15 million viewers weekly and the three movies were top box office hits. Although this informal inventory does not replace a thorough content analysis, this analysis provided an initial look at the trend in hacker media representations. Clearly, media portrayals of hackers are on the rise.

In addition to the increasing numbers of media hacker portrayals, there is a trend in the media to present lead hacker characters, including hackers with a previously criminal background, as exciting, skilled, and often of noble intent

(Rosewarne, 2016). These hackers use their skills to assist law enforcement (e.g. Penelope in Criminal Minds) or advance a moral/social cause (e.g. Felicity in Arrow). Even unconventional hacker characters, such as Lisbeth Salander (Girl with the Dragon Tattoo), are substantially ingratiated to the audience. These repeated positive portrayals lead to an overarching theme of hackers as exciting, criminal heroes. As hacker storylines become more prevalent, individuals who consume media (i.e. watch popular movies and television) are increasingly likely to be exposed to positively skewed representations of hacker characters and behaviors. Exposure to shows or movies with leading hacker characters is likely to increase the acceptance and identification with hacking behavior.

General Media Exposure

While many shows do not include leading hacker characters, hacking behaviors/crimes are often a subject of the prime-time shows' extended storylines (e.g., Law & Order SVU, Quantico). Some hacker characters appear on a diverse array of programming domains including characters in popular long-running series such as Kyle on South Park, Casey Parker in Grey's Anatomy, and the Doctor in Doctor Who.

Intuitively, exposure to hacker specific media should impact perceptions of hacking behavior. However, as hacker representations and plotlines spread across diverse media domains, it may be informative to explore whether exposure to general media predicts perceptions of cyber-crimes. Considering a related area of study, media exposure and violence, early research in this area focused on specific exposure to violent media and violent behavior (for a review of early research see Andison, 1977). Later, a landmark study published in the magazine *Science* reported a connection between general media exposure and subsequent violent behavior (Johnson et al., 2002). Importantly, the increasing portrayal of violence in the media called for attention to the impact of general media exposure (American Psychological Association, 1993; Strasburger & Donnerstein, 2000). Moving from specifically violent media to general media exposure also sparked future studies to explore the impact of media exposure in general (e.g., Dworak et al., 2007; Robertson et al., 2013). This line of reasoning is consistent with the research on cultivation theory, which suggests that television programming communicates a general set of repeated messages that shape viewers' beliefs and perceptions (Gerbner et al., 2002). Research findings in this area indicate that time watching media programs in general shapes perceptions of reality related to the acceptance of certain social and sexual behavior (Calzo & Ward, 2009), prevalence of crime (Nabi & Sullivan, 2001), and pervasiveness of drug use (Minnebo & Eggermont, 2007). In recognition of the wide-spread rise in media hacker representations, and learning from the trajectory of the research into the connection between media exposure and violent behavior, the current study explores how exposure to media in general predicts perceptions of hacker characters and hacking behaviors.

Wishful Identification

A potential consequence of the increase in hacking behaviors portrayed in the media is a wishful identification process, or intrigue into hacking (Rosewarne, 2016). Wishful identification is the idea that audience members can watch characters on screen, identify with, take an affinity toward, or even see them as a role model (Greenwood, 2007; Hoffner, 1996; Hoffner & Buchanan, 2005; Konijn et al., 2007; Surette, 2002). Identification with a media character is the process of adopting the perspective of the character and making decisions based on "what the character would likely do" in a given situation (Hoffner, 1996). Researchers have found that young adults and children were more likely to identify with, and model themselves after same-sex characters portrayed on popular television programs (Hoffner & Buchanan, 2005). This same-sex affiliation is due to corresponding character attributes and perceived similarity between the character and the audience member. Additionally, both men and women were more likely to identify with characters who were successful, intelligent, and admired by other characters.

Research suggests that identification with media characters influences behavior modeling in many domains. These include, copy-cat criminal activity (Surette, 2002), aggressive female behavior (Greenwood, 2007), sexual behavior and illegal drug use (Bond, & Drogos, 2014), and risk-taking behaviors, such as binge drinking, participation in extreme sports and risky driving (Fischer et al., 2011; Greenwood, 2007). These risk-taking inclinations may be affected by factors such as a need for excitement, thrill seeking, reducing boredom, and seeking pleasurable experiences (Ben-Zur & Zeidner, 2009). Glorified media presentations of payoffs associated with the risky behaviors have also been shown to exacerbate the associated socio-cognitive yearn to participate in various activities (Fischer et al., 2007; Fischer et al., 2008).

Primarily, past research on wishful identification and media exposure focused on exposure to a specific character and a resulting identification with that character. With the rise of hacker characters and themes in the media, we suggest that general media exposure may stimulate a wishful identification process with hacker characters. Our rationale for this exploration is based on prior research on the mere exposure effect, positive attitudes, and identification. Specifically, research on the mere exposure effect has found that, following repeated exposure, individuals develop a preference for, and positive attitudes toward, a novel stimulus (Zajonc, 1968). Positive feelings toward an object/entity is a defining component of identification (Ryan & Deci, 2000; Henry et al., 1999). Based on this robust and well-established phenomenon and the surge in media portrayals of hacker characters, we argue that individuals with greater exposure to the media are more likely to hold positive attitudes toward, and therefore, wishfully identify with, a hacker character of their choosing.

Therefore, we suggest several specific hypotheses regarding the relations between media exposure, wishful identification, and perceptions of hacking (i.e. risks, payoffs, and willingness to hack). First, following the premises of cultivation theory, mere exposure, and wishful identification, we expect a positive correlation between participant media exposure and wishful identification with a hacker character of their choosing (H1). Additionally, based on the increase in portrayals of hacker characters that emphasize excitement over the more mundane reality of hacking (Rosewarne, 2016), we argue that, for individuals who identify with hacker characters, hacking payoffs will be increasing salient. This leads to our second hypothesis: greater wishful identification will predict increased perceived payoffs for both hacktivism and financial hacks (H2).

Wishful identification suggests that individuals will make decisions based on how the character would likely behave (Hoffner, 1996). Due to social desirability effects, it is difficult to get a straightforward measure of how likely participants are to engage in potentially criminal activities such as hacking. Therefore, this study asked participants to take the perspective of someone else (i.e., report what another person would be likely to think and do). This perspective taking approach has been frequently used in research on stereotypes and prejudice to reduce social desirability concern (see Fiske et al., 2002). Perspective taking generally requires people to ignore their own views. However, research on false-consensus bias shows that people overestimate the extent to which other people share their beliefs, opinions, and preferences (Ross et al., 1977). That is, people generally assumed that others tend to think and behave like they do. Based on the false consensus bias, we hypothesize that individuals who endorse more wishful identification with a hacker character will be more likely to believe other people will engage in hacking behaviors (H3).

A Game Theoretical Approach to Hacking Behavior

Given the implications for perceptions of risks and payoffs based on media exposure and wishful identification, we adopt a Game Theoretical approach to address how these perceptions may influence decision-making for hacking behavior. Game Theory, first founded under the name *minimax theorem* in the late 1920s (von Neumann, 1928), originally stated that within a two-person, zero-sum game with limited possible moves, one can mathematically calculate the strategies that would guarantee the optimal payoffs for each player given the other player's actions. In the near century that followed, the minimax theorem was extended to study a wide range of strategic decision-making contexts that collectively fall under a Game Theoretic framework (Alpcan & Basar, 2003; Reinganum, 1981; Suzuki & Nakayama, 1976). This framework holds that rational decision makers carefully weigh all known consequences of their decisions before acting.

Based on Game Theoretical principles, decisions to hack should consider both the expected benefits of participation (i.e. perceived payoffs) and the potential for negative consequences (i.e. perceived risks). Perceived payoffs of hacking may include factors such as notoriety, personal challenge, benefits to others, raising awareness of a cause, and personal monetary gains. Risks of being caught include not only large financial fines but the possibility of criminal charges and incarceration. Highly publicized examples, such as Edward Snowden and Anonymous, emphasize the validity of both the payoffs and risks associated with hacking. The highly salient nature of these payoffs and risks make Game Theory a useful framework to conceptualize decisions to hack.

A recent study applying Game Theory to hacking behaviors yielded a surprising finding, suggesting that, contrary to the broader theoretical framework of Game Theory, people responding to a call to hack may not always be rational decision-makers (Bodford & Kwan, 2018). In that study, risks were defined as consequences such as getting caught and punished by authorities as an individual or as a group of hackers. In contrast, payoffs were defined as perceived benefits to oneself and/or others as a result of the behavior (Bodford & Kwan, 2018). When asked to predict a third party's action after being presented with a risky (but potentially advantageous) situation, college students' estimations of their willingness to hack stemmed solely from their perceived payoffs of the behavior. Their willingness to hack was not related to their perception of risks underlying the hacking situation. For segments of our population, such risky decisions may be payoff-driven, rather than based on a deliberate calculation of the ratio of benefits to potential risks (Bodford & Kwan, 2018). It should be noted that this study examined willingness to engage in hacktivism (i.e. motivated by social or political beliefs). The present study seeks to replicate Bodford and Kwan's (2018) hacktivism findings, and expand the research to incorporate willingness to engage in hacking for financial gain.

Given these previous findings, we developed several additional hypotheses regarding the application of the Game Theory model to wishful identification and perceptions of hacking behavior. First, as Bodford and Kwan (2018) found, we expect perceived payoffs to be positively correlated with estimations of willingness to hack in both hacktivism and in our added financial hacking condition (H4). Second, we expect perceived payoffs to mediate the hypothesized relation between wishful identification and estimations of willingness to hack (H5). Conversely, given Bodford and Kwan's (2018) findings, perceived risks should not be related to perceived payoffs or estimations of willingness to hack (H6). Finally, we expect to fit a significant model (see Figure 3) that incorporates both the wishful identification and Game Theory framework to display a positive overall relationship between media exposure, wishful identification, perceived payoffs, and estimation of others' willingness to hack in both types of hacking behaviors (H7). While hacktivism and financial gain hacking clearly afford different rewards, rewards in both types of hack are highly salient, thus we do not expect the model to vary by type of hack.

Sex Differences

In addition to our primary analyses, we elected to explore the role of sex differences in our proposed model. The hacker stereotype generally consists of the perception that hackers are "young, white, middle-class males" (Tanczer, 2016). Although female hackers do exist, most highly publicized examples of hackers are male (e.g. Edward Snowden). Tanczer (2016) finds that, within hacker communities, a "Male Oblivious Discourse" is common, meaning that the existence of female hackers is generally ignored.

From our preliminary analysis of media representations of hackers, we also saw an increase in female hacker characters in the last decade. In our exploratory inventory, prior to 2007, female characters made up 22% (*n* = 20) of hacker characters. In contrast, the representation of female hacker characters increased to 43% (*n* = 32) between 2007-2018.

Few empirical studies have addressed sex differences in hacking. While males were found to engage more in gaining access and "tweaking" networks (Jordan & Taylor, 2004), researchers suggest that females may be more tied to hacktivist activities, due to the "fighting for a cause" like nature of the crimes (Segan, 2000). Interviews with three known female hacktivists suggest that females are less interested in breaking into a system for the purposes of exposing a systems' vulnerabilities, and more interested in developing tools to pirate software, helping authorities expose and catch child pornographers (Segan, 2000), and leading political crusades for freedom of information (Alberici et al., 2012). Thus, it is important to ascertain whether there are sex differences in perceptions of hacking activities and willingness to engage in different kinds of hacking activities.

A recent study showed no sex differences among perceived payoffs and willingness to hack associated with a hacktivism manipulation (Bodford & Kwan, 2018). Thus, although we did not expect differences in our model, we examined the possibility of sex differences in perceptions of hacking behaviors throughout our analysis.

Research Overview

To recapitulate, we propose that the wishful identification perspective coupled with a Game Theoretical framework may be a key to understand the relationship between media exposure and perceptions of hacking behaviors. Therefore, the present research aims to (1) replicate Bodford and Kwan's (2018) findings, (2) examine whether there are sex differences among perceptions of hacking activities, (3) extend findings to two types of hacks: hacktivism and financial hacking, (4) apply the Game Theoretical approach to hacking behavior associated with media exposure, and (5) identify a mechanism behind media exposure and hacking related estimations via the wishful identification perspective.

Methods

Participants

Participants were recruited through Mechanical Turk (MTurk), which is a survey host through Amazon.com. Bodford and Kwan (2018) conducted a multiple regression analysis predicting likelihood of engaging in a hack from perceived payoffs and risks; perceived payoffs and risks accounted for 30.5 percent of the variance in the likelihood to hack. Based on this reported effect size, we conducted a power analysis and estimated a minimum of 136 participants, 68 participants per hacking type, to achieve sufficient power in our correlational and mediation analyses (G*Power). Participants were initially screened; only participants who had, or were pursuing, a college degree in the physical sciences, technology, engineering, or math (i.e., STEM fields) were invited to participate in the study. Participants from STEM fields were selected in order to survey individuals who may possess the foundational skills to hack. Many STEM majors, including computer science, require similar introductory courses (e.g. mathematics, physics, introductory computer science). Additionally, although anonymity makes it difficult to get a clear understanding of hacker demographics, IBM's ethical hacking effort suggests that many hackers are computer enthusiasts who come from diverse educational backgrounds including physics, mathematics, and computer science (Palmer, 2001). We also limited our sample to participants residing in North America at the time of data collection due to the questions regarding media exposure to mostly North American media programming.[1] To ensure participant attention, there was one attention check question embedded into each survey (16 participants were excluded from the final analysis for incorrectly answering this question).

The final sample consisted of 149 participants (75 women), with an average age of 30.02 (*SD* = 5.66). Fifty-eight (38.9%) participants held, or were pursing, a degree in technology followed by 48 (32.2%) physical science degrees, 26 (17.4%) engineering degree, and 17 (11.4%) mathematics degree. The majority of our participants were Caucasian (101, 67.8%), then Asian (22, 14.8%), African American (12, 8.1%), Hispanic (6, 4.0%), American Indian (6, 4.0%), other (1, 0.7%), and one person who chose not to disclose his/her ethnicity. Participants took an average of 10.6 minutes (*SD* = 8.9 minutes) to complete the online survey, and were compensated $0.76 for their time and participation. We collected all data during the fall of 2017.

Study Design

The study design included a total of eight versions of the survey. Participants answered the same questions in each survey, however, the sex of the fictional hacker in the hacking scenario was matched to participant sex and the order of the media questions and the type of hack mentioned varied. That is, we used a 2 (sex of fictional hacker) x 2 (media question order) x 2 (type of hack: hacktivism vs. financial) between-subjects design. Participants may have seen the media exposure questions in the beginning or ending of the survey. This variation allowed us to test whether the order of exposure questions affected the results.

After consenting to participation, participants were randomly assigned to one of the survey versions. In all versions, participants responded to questions about their media exposure to TV shows and movies, identified a hacker character they were familiar with, and reported their wishful identification with that character. Next, participants read the hacking scenario and answered questions about their perceived risks, payoffs, and willingness to hack. Finally, in all versions, we collected basic demographic information, and participants were thanked and debriefed.

Measures

Media Exposure

We used six items to measure participants' media exposure. In order to test the impact of general media exposure, we asked participants to report exposure to general media categories rather than exclusively hacker media. Participants responded to six items that asked about media exposure to various types of television and movies. For example, participants were asked, *To what extent do you watch the following types of television and/or movies?* with responses anchored by 1 (*never*) to 5 (*frequently*). The six ratings included: Prime Time Television Shows (e.g., shows like *Criminal Minds, NCIS Los Angeles, Bull, 24, Blue Bloods, Designated Survivor, Scorpion),* Entertainment Crime-Drama Television Shows (e.g., shows like *Criminal Minds, NCIS, NCIS Los Angeles, Blue Bloods, Law and Order SVU, Quantico),* Crime-Drama Movies (e.g., movies like *Girl with the Dragon Tattoo, Live Free Die Hard, Snowden),* Movies and TV shows with lead female characters (e.g., movies like *Hidden Figures, Law and Order SVU, Divergent, Hunger Games series, Nancy Drew),* Female Super-Hero Movies (e.g., movies like *Wonder Woman, Lucy, Electra, Catwoman),* Anime TV shows/Movies (e.g., *Cowboy Bebop, Guilty Crown, Battle Programmer Shirase).* Many of the examples given were of shows and movies that include a hacker main character (e.g. Bull, NCIS, Snowden) or hackers appear as part of the extended narrative (e.g. Law and Order SVU, Quantico). We averaged the six items together to make a composite variable of media exposure (*M* = 2.58, *SD* = 0.92, α = .81).

Wishful Identification

To measure wishful identification, we asked participants to first think about a same-sex fictional technology specialist or hacker character that they knew from television or a movie. Wishful identification researchers contend that identification with characters is predominately same-sex based (Hoffner, 1996; Hoffner & Buchanan, 2005). Participants were given five same-sex visual character examples to help them jog their memory, such as Lisbeth from *Girl with the Dragon Tattoo* and Aram Mojtabai from *Blacklist* (See Appendix A). Participants were asked if they could list the character they were thinking of or the show/movie that character appears in. Approximately, 84% of participants provided the name of a specific character or hacker media example. Of those participants, less than 3% listed a character of a different sex. In total, male participants identified 35 different characters, and female participants identified 26 different characters. The most commonly known male characters were Aram from *Blacklist*, Neo from *The Matrix* and Alec Hardison from *Leverage*. The most commonly known female characters were Abby from *NCIS*, Garcia from *Criminal Minds*, and Felicity from *Arrow*.

Next, participants completed the three-item Wishful Identification scale (e.g., *I'd like to do the kinds of things he/she does on the show*; *He/she is the sort of person I want to be like myself*; *I wish I could be more like him/her*; Hoffner, 1996). Participants indicated their agreement on a 5-point scale, ranging from 1 (*strongly disagree*) to 5 (*strongly agree*). As men and women viewed characters matching their own sex, we averaged the three items separately by sex (Male: *M* = 3.50, *SD* = 1.12, α = .84; Female: *M* = 3.84, *SD* = 0.94, α = .83). The wishful identification aggregates did not significantly differ between males and females, *t*(147) = -1.45, *p* > .05, *d* = 0.24. We therefore aggregated the male and female composites to create one variable of wishful identification (*M* = 3.71, *SD* = 1.03).

Perceived Risks,Payoffs and Estimation of Others' Willingness to Hack

We adopted Bodford and Kwan's "call to hack" scenario to test our hypotheses. The "call to hack" mimics those used in hacker groups to attract hackers to take up a specific cause. The use of a scenario-based guided visualization technique intends to prime each participant to adopt the mindset of an imagined third party who is considering engaging in a hacking attack. Guided visualization techniques were first used in clinical psychology in the mid-1980s to reduce anxiety and enhance work performance by imagining oneself in a situation that is less threatening (Ayres & T. Hopf, 1992; Ayres & T. S. Hopf, 1985; 1990). In the decades since, other areas of behavioral sciences have adopted guided visualization as a strategy to increase the vividness and clarity of participants' mental imagery through text-based prompts.

Our hacking scenario used this third-party, guided visualization approach, that is, one in which participants consider the actions of an imagined other—to avoid the possibility that participants would withhold information or opinions due to concerns about social desirability and legal ramifications of their responses. We also matched the sex of this third-person individual with the participant's sex by first asking the participant to report their sex and other demographic information, and then redirecting to a scenario based on the participant's response (e.g., women were directed to a scenario involving a female subject). Previous studies have used and validated the use of this scenario-based approach to understand risk estimations in the area of insider threat (i.e., employees' intent to carry out a cyber-attack on their own employer's information system; Greitzer et al., 2010; Sinclair & Smith, 2008). Thus, the use of this scenario-based approach toward hacking estimations opens a venue for empirical research in the absence of participants who explicitly identify as hackers, or hacktivists. Respondents were more likely to be truthful in a guided simulation in the comfort of their own space, where hacking is more likely to occur, rather than in a college campus laboratory (Bodford & Kwan, 2018). Depending on the survey version, participants read through one of two different behavioral scenarios (i.e., call to hack for financial gain or call to hack for a cause).

The following are the call to hack scenarios, starting with the financial hack and ending with the hacktivism scenario.[2] Each of the calls were displayed in the survey to match the participant's sex (i.e., females were shown a call to hack with she/her pronouns).

Financial Hack Scenario

> Your friend Jordan is a computer specialist for a National IT company. Jordan has a good job working as a computer software engineer. However, at times s/he finds him/herself bored with the lack of complexity in his/her job and knows that s/he could be making more money using his/her advanced computing skills. During his/her downtime, s/he likes to poke around on other network systems outside of his/her company, allowing his/her to develop his/her programs with better security packages than his/her company's competitors. One day s/he stumbles upon an opportunity to use his/her computer hacking skills for quick and easy profit. S/he discovers that s/he can hack into a large financial investment firm and steal $100 each day from 100 different accounts. If s/he only steals $100 from a different account each day, s/he should go undetected given the large transactions that occur within these types of investments. After only 100 days, s/he would be able to inconspicuously steal $1 million.

Hacktivism Scenario

> Your friend Jordan is a computer specialist for a National IT company. For about two years now, s/he has known about a group of cyber hackers posing as IRS money collectors and targeting the elderly and veterans with their fraud schemes. Their group is known as eLdrSnatch. Their scheme itself can steal up to $1 million dollars from unsuspecting victims, leaving the victims with little money and no retirement funds. Your friend and his/her colleagues have come across a way to use their company's technology to hack into eLdrSnatch's website. S/he knows that using the company's technology to hack is illegal, however, s/he feels that if they can successfully and untraceably hack eLdrSnatch, this group of IT specialists have the ability to shut eLdrSnatch down and retrieve their names and IP addresses. If successful, this would allow law enforcement to find members of eLdrSnatch and seize the money to give back to the helpless elderly victims.

To measure perceived risks, payoffs, and estimation of others' willingness to hack, participants viewed the "call to hack" scenario and then answered three items pertaining to the estimations. To measure perceived risks, we asked participants one question, "*How risky do you think it would be for Jordan to take part in this hack?*" with responses anchored by 1 (*low risk*) to 5 (*high risk*). To measure perceived payoffs, participants answered the question, "*If Jordan is successful, how sizable do you think his/her overall payoffs will be?*" and to measure willingness to hack, we asked participants, "*How likely do you think Jordan is to participate in this hacking opportunity?*" both with responses ranging from 1 (*not at all*) to 5 (*very much*). The descriptive statistics for the financial hack are perceived risks (M = 4.35, SD = 0.90), perceived payoffs (M = 4.08, SD = 1.13), and others' willingness to hack (M = 3.16, SD = 1.08), while the hacktivism scenario are as follows, perceived risks (M = 3.93, SD = 0.99), perceived payoffs (M = 3.22, SD = 1.37), and others' willingness to hack (M = 3.49, SD = 1.05).

Results

Analytical Approach

To test our hypotheses, we used OLS regressions to address the correlational, predictive association between two media variables (i.e., media exposure and wishful identification) and three Game Theoretical parameters (i.e., risks, payoffs, and willingness to hack), involving two types of hacker behaviors (i.e., financial and hacktivism). Separate regression analyses were conducted for each type of hack.

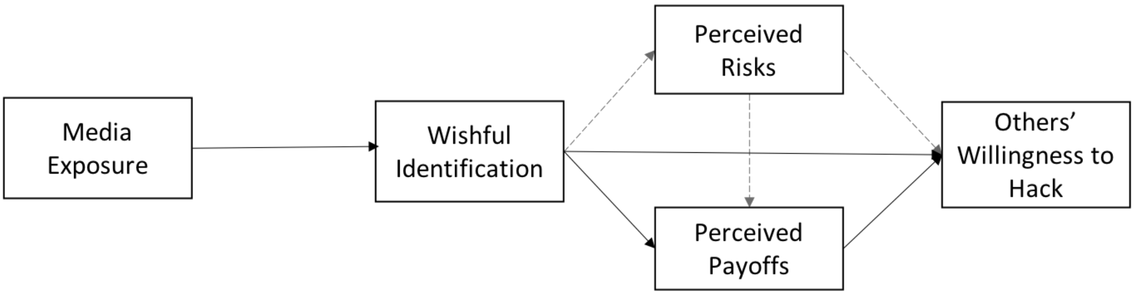


Figure 1. Visual representation of the major predictions.
Note. Dotted lines denote predicted non-significant relationships and the solid lines denote predicted positive relationships.

Tests of Sex Differences and Media Question Order

First, we examined whether there were sex differences in wishful identification and estimations of risks, payoffs, and willingness to hack in each type of hacking behavior. We found only one significant difference between sexes. Specifically, females reported a higher estimation of others' willingness to participate in hacktivism (*M* = 3.74, *SD* = 0.91) than their male counterparts (*M* = 3.17, *SD* = 1.15; *t*(67) = -2.33, *p* < .05, *d* = 0.550) (see Table 1 for the details of *t*-test results). These findings suggest that media exposure, wishful identification, perceived risks, and payoffs were rated equally among sexes. Second, we tested whether there were significant differences in responses between participants who saw the media questions early on in the survey and those who saw the media questions later in the survey, in order to test for ordering differences. Results revealed no differences from the presentation order of the media questions. Given these findings, we aggregated across sex and media question order for the remainder of the analyses.

Table 1. *T-Test Results, A Test of Differences Between Sexes.*

	Male		Female		*t*	Cohen's *d*
	M	*SD*	*M*	*SD*		
Media Exposure	2.54	0.96	2.64	0.88	-0.63	0.109
Wishful Identification	3.59	1.12	3.84	0.94	-1.45	0.242
Risks Hacktivism	3.80	0.92	4.03	1.04	-0.94	0.234
Risks Financial	4.25	0.97	4.47	0.81	-1.09	0.246
Payoffs Hacktivism	3.40	1.40	3.08	1.35	0.97	0.233
Payoffs Financial	4.11	1.10	4.06	1.17	0.23	0.044
Estimation of others' willingness to Hack - H	3.17	1.15	3.74	0.91	-2.33*	0.550
Estimation of others' willingness to Hack - F	3.19	1.19	3.14	0.96	0.18	0.046

Note. Higher numbers indicate: more exposure, higher wishful identification, higher perceived, risks, higher perceived payoffs, higher estimation of others' willingness to hack. **p* < .05.

Hypothesis Testing

Tables 1 and 2 show the descriptive statistics and intercorrelations among our variables of interest. As predicted in hypothesis one (H1), general media exposure and wishful identification with an on-screen hacker character were positively correlated (r = .310, R^2 = .096, p < .001). In support of hypothesis two (H2), there was a positive correlation between wishful identification with a hacker character and perceived payoffs for both hacking types. Perceived payoffs were positively correlated with wishful identification among those participating in the financial hack scenario, (r = .363, R^2 = .132, p < .01), explaining 13.2% of the variance, and in the hacktivism scenario (r = .263, R^2 = .069, p < .05), explaining 6.9% of the variance. In addition, hypothesis three (H3) was only partially supported, such that, estimation of others' willingness to hack was not correlated significantly with wishful identification in the financial hack (r = .156, R^2 = .024, p = .17), but was positively correlated in the hacktivism scenario (r = .345, R^2 = .119, p < .01), explaining 11.9% of the variance.

Table 2. *Descriptive Statistics and Intercorrelations Among Variables of Interests in the Financial Hack Scenario.*

	Media Variables		Financial			*M*	*SD*
	1	2	3	4	5		
1. Media Exposure	—					2.5884	0.9205
2. Wishful Identification	.310**	—				3.7136	1.0376
3. Risks	-.080	.002	—			4.3500	0.9014
4. Payoffs	.015	.363*	.019	—		4.0875	1.1272
5. Estimation of others' willingness to Hack	.288**	.156	-.059	.278*	—	3.1625	1.0843

Note. Higher numbers indicate: more exposure, higher wishful identification, higher perceived payoffs, higher perceived risks, higher estimation of others' willingness to hack. **p* < .05, ***p* < .001.

As predicted in hypothesis four (H4), perceived payoffs were positively correlated with estimation of others' willingness to hack for both the financial hack (r = .278, R^2 = .077, p < .05), explaining 7.7% of the variance, and hacktivism (r = .435, R^2 = .189, p < .001), explaining 18.9% of the variance. As an exploratory analysis, we found a positive correlation between media exposure and willingness to hack for the financial hacking scenario (r = .288, R^2 = .083, p < .01), explaining 8.3% of the variance. See Table 2 and 3 for all associated correlations.

Table 3. *Descriptive Statistics and Intercorrelations Among Variables of Interests in the Hacktivism Scenario*.

	Media Variables		Hacktivism			*M*	*SD*
	1	2	3	4	5		
1. Media Exposure	—					2.5884	0.9205
2. Wishful Identification	.310**	—				3.7136	1.0376
3. Risks	.188	.123	—			3.9275	0.9899
4. Payoffs	.173	.263*	.207	—		3.2174	1.3705
5. Estimation of others' willingness to Hack	.036	.345**	.134	.435**	—	3.4928	1.0519

Note. Higher numbers indicate: more exposure, higher wishful identification, higher perceived payoffs, higher perceived risks, higher estimation of others' willingness to hack. *p < .05, **p < .001.

To address hypothesis five (H5), suggesting mediation, we used model 4 of Hayes' PROCESS macros (Hayes, 2017). The relationship between wishful identification with an on-screen character and estimation of others' willingness to hack was mediated by perceived payoffs in both types of hacks, thus supporting H5 (Financial Hack: R^2 = .081; Hacktivism: R^2 = .2461; Figure 2). We tested the significance of the indirect effect of wishful identification on willingness to hack via perceived payoffs using bootstrapping procedures (1000 bootstrapped samples per testing of the indirect effect). As predicted, this indirect effect is significant in both types of hacks. The standardized indirect effect for the financial hack was .0926, 95% CI [.0007, .2368], and the hacktivism indirect effect was .0973, 95% CI [.0011, .2132].

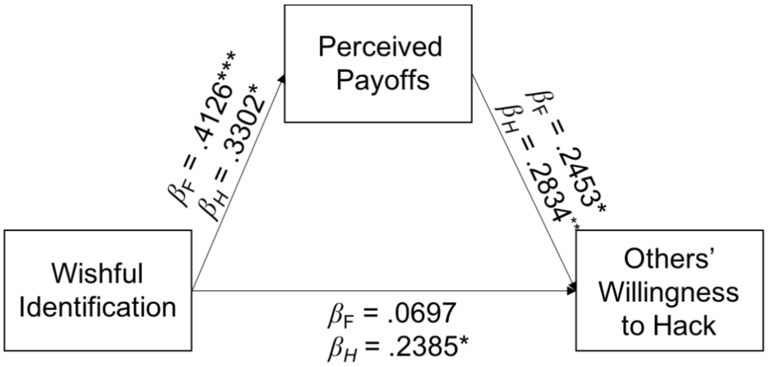


Figure 2. An illustration for H5, positing that wishful identification and willingness to hack is mediated by perceived payoffs in both types of hacking behaviors.

Note. Financial Hack: R^2 = .081; Hacktivism: R^2 = .2461.
Financial hack standardized indirect effect = .0926, 95% CI [.0007, .2368],
Hacktivism standardized indirect effect = .0973, 95% CI [.0011, .2132].
Hacktivism = H, Financial Hack = F.
*p < .05, **p < .01, ***p < .001.

In addition, to address hypothesis six (H6), we tested the relationship of perceived risks with wishful identification, perceived payoffs, and estimation of others' willingness to hack. Wishful identification was not significantly correlated with perceived risks in a financial hack (r = .002, R^2 < .0001, p > .05), nor in hacktivism (r = .123, R^2 = .015, p > .05). Perceived risks were also not significantly correlated with perceived payoffs in a financial hack (r = .019, R^2 < .001, p > .05), nor in hacktivism (r = .207, R^2 = .043, p > .05). Finally, perceived risks were not significantly correlated with estimation of others' willingness to hack in a financial hack (r = -.059, R^2 = .003, p > .05), nor in hacktivism (r = .134, R^2 = .018, p > .05). Consistent with previous research, perceived risks of hacking behaviors did not play an important role in predicting perceptions of hacking behavior.

Testing the Full Model

Analytic Approach

To test hypothesis seven (H7), the overall model, we used AMOS (Version 25.0.x) to test each full model separately. Within the model, media exposure was the exogenous variable, and wishful identification, perceived payoffs, and others' willingness to hack were entered as endogenous variables (see Figure 3). In this model, media exposure predicted an increased wishful identification (path a), wishful identification predicted increased perceived payoffs (path b) and increased estimation of others' willingness to hack (path d), and perceived payoffs predicted an increased estimation of others' willingness to hack (path c). To assess model fit we used the chi-square test, the root mean square error of approximation (RMSEA), and the comparative fit index (CFI). Model fit was considered acceptable when RMSEA < .08 (MacCallum et al., 1996), and CFI > .90 (Hu & Bentler, 1999).

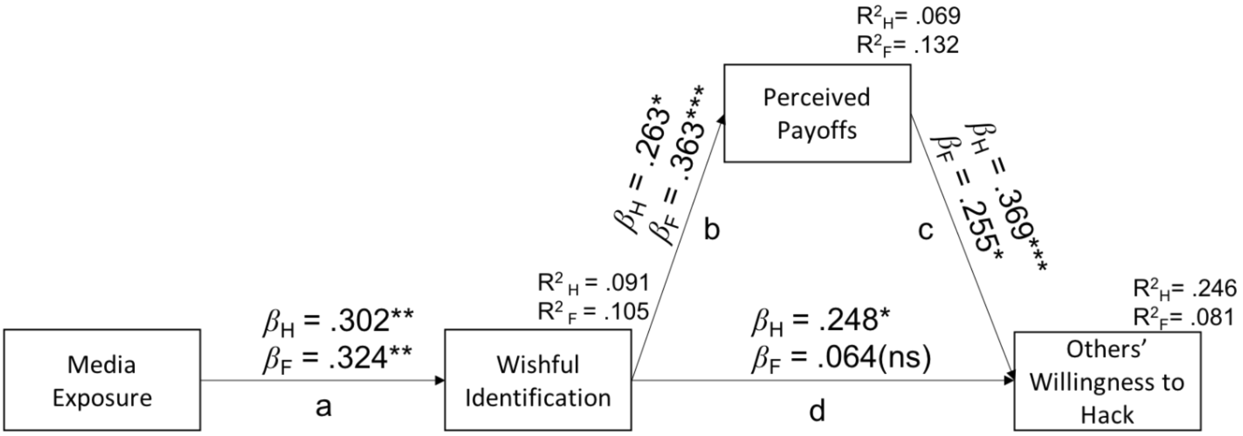


Figure 3. Representation of the full model, and the full indirect effect of media exposure on willingness to hack passing through wishful identification and perceived payoffs.

Note. Hacktivism indirect effect = .029, 95% CI [.007, .133]. Multiple correlations: Wishful Identification: R^2 = .091, Perceived Payoffs: R^2 = .069; Others' Willingness to Hack: R^2 = .246. Model Fit Statistics: $\chi^2(2)$ = 1.766, p = .414, CFI = 1.00, RMSEA = .000 [.000, .231]. Financial hack indirect effect = .030, 95% CI [.003, .102]. Multiple correlations: Wishful Identification: R^2 = .105, Perceived Payoffs: R^2 = .132; Others' Willingness to Hack: R^2 = .081. Model Fit Statistics: $\chi^2(2)$ = 8.188, p < .05, CFI = .785, RMSEA = .198 [.072, .347].
Hacktivism = H, n = 69, Financial hack = F, n = 80.
*p < .05, **p < .01, ***p < .001.

Hacktivism

Results of the full path analysis for the hacktivism scenario were significant and the model fit was satisfactory, $\chi^2(2)$ = 1.766, p = .414, CFI = 1.00, RMSEA = .000 [.000, .231] (see Figure 3). Results showed that media exposure, passing through wishful identification and perceived payoffs, was significantly associated with increased estimation of others' willingness to hack, indirect effect = .029, 95% CI [.007, .133]. As expected, media exposure was associated with increased wishful identification (path a) (β = .302, p < .01). Wishful identification also predicted increased perceived payoffs (path b) (β = .263, p < .05). The relationship between wishful identification and estimation of others' willingness to hack (path d) was also a positive association (β = .248, p < .05). The relationship between perceived payoffs and estimation of others' willingness to hack (path c) was also significant (β = .369, p < .001).

Financial Hack

Results of the full path analysis for the financial hack were significant but not a good fitting model, $\chi^2(2)$ = 8.188, p < .05, CFI = .785, RMSEA = .198 [.072, .347]. Results showed that media exposure, passing through wishful identification and perceived payoffs was significantly associated with an increased estimation of others' willingness to hack, indirect effect = .030, 95% CI [.003, .102]. As expected, media exposure was associated with increased wishful identification (path a) (β = .324, p < .01). Wishful identification also predicted increased perceived payoffs (path b) (β = .363, p < .001). The relationship between wishful identification and estimation of others' willingness to hack (path d) was not a significant relationship (β = .064, p > .05). Finally, the relationship between perceived payoffs and others' willingness to hack (path c) was significant (β = .255, p < .05).

Context of the Hack

To address our overall model, we investigated whether the media variables (media exposure and wishful identification) and perceived beliefs about hacking behaviors were different between hacking contexts (financial and hacktivism). We tested a version of our model with hacking type as the grouping variable, to examine whether the type of hack moderated any of the pathways.

To test for patterned invariance—testing for significant differences between the two groups' paths throughout the model—we fixed the path coefficients for financial and hacktivism groups to be equal and ran a fully constrained base model. Next, using a series of nested models, one constraint was released for each path at a time in order to examine the differences between model fit of each nested model against the base model (see Table 4). None of the nested models significantly differed from the base model. In other words, the change in chi-square from the base model to each nested model did not differ significantly. The only nested model that improved fit was the model that released the constraint on the relation between wishful identification and estimation of others' willingness to hack. This path was estimated freely for both hacking groups while all other paths were held equal for both groups. This result was in line with the aforementioned findings that wishful identification and estimation of others' willingness to hack were not significantly correlated for the financial hacking group but were significantly correlated for the hacktivism group. These findings suggest that wishful identification may have a stronger predictive power of willingness to hack in responding to a call for hacktivism than to a financial hack. Otherwise, the overall model of the effects of media exposure on wishful identification, perceived payoffs, and estimation of others' willingness to hack is similar across hacking contexts.

Table 4. *Examination of the Moderating Effects of Hacking Type in Path Model Through Invariance Testing Using Comparison of Nested Models*.

Model	$\chi^2(df)$	CFI	RMSEA [CI]	$\Delta\ \chi^2(1)$	$\Delta\ \chi^2\ p$
Base model, fully constrained	11.598 (8)	.935	.055 [.000, .120]	n/a	n/a
Release ME on WI	11.596 (7)	.917	.067 [.000, .133]	0.002	.962
Release WI on PAY	11.408 (7)	.920	.065 [.000, .132]	0.190	.663
Release PAY on WH	11.190 (7)	.924	.064 [.000, .130]	0.408	.523
Release WI on WH	10.215 (7)	.942	.056 [.000, .124]	1.383	.240

Note. Each equality constraint was released one at a time. ME = Media exposure; WI = Wishful identification; PAY = Perceived payoffs; WH = Estimation of others' willingness to hack.

Discussion

The present research is the first to call for attention to the potential impact of general media exposure and wishful identification with hacker characters on perceptions of hacking behaviors. Specifically, the present study replicates and extends previous research addressing the willingness to engage in hacker behaviors. We found that perceived risks seem to carry little weight in predicting the willingness to hack. Perceived payoffs and willingness to hack are significantly correlated with each other, such that, one may infer that perceived payoffs may be a driving force in the decision-making process.

This study also confers past results showing little to no sex differences among the estimation of others' willingness to hack, perceived risks, or perceived payoffs. However, in this study the overall sample size for measuring sex differences between each type of hack was small (Hacktivism: n = 69 (39 females) and Financial: n = 80 (36 females)). The mean differences between males and females in our sample were generally not significant but many did produce small effects (see Table 1). Future research should use a larger sample size in order to detect sex differences, if any.

Beyond the replication of past findings, this research broadens the results of past research by examining two types of hacking contexts: financial hacking attacks and hacktivism attacks. Overall, the present findings show that there are no significant differences between the willingness to hack in either context. Additionally, the proposed model is a better explanation of the estimation of others' willingness to hack in the hacktivism context than in the financial context. This suggests that media exposure may have a stronger effect on perceptions of hacking behavior in a prosocial or political-type context. This study included only one example of hacktivism: hacking to prevent crimes against elders. Hacktivism is generally morally or politically motivated. This motivation suggests that individuals will vary in how willing they are to engage in specific "calls to hack" depending on their moral and political beliefs. Future research should attempt to replicate these findings utilizing different examples of hacktivism and taking into account the political ideologies of participants.

The hacker characters portrayed in media are often portraying "hacktivists" rather than a maliciously criminal "hacker". In other words, these characters are using their hacking skills without malicious intent. Our research shows that general media exposure is associated with positive wishful identification with these characters, and in turn, this wishful identification is positively correlated with increased 1) perceived payoffs and 2) estimation of others' willingness to hack. These results add support to the wishful identification prospective such that exposure to media can be affiliated with audience members wanting to "be like" or "act like" characters they see on screen (Hoffner, 1996; Hoffner & Buchanan, 2005). With media representations of these characters on the rise, implications of this research may show a potential increase in hacktivism, or a general willingness to hack among audience members. Importantly, this research is the first to explore the relationship between general media exposure and wishful identification with hacker characters. Future research should seek to replicate these initial results.

Our media exposure measure presented two potential limitations to our study. First, by design, the media exposure aggregate was not focused solely on exposure to hacker media but measured many media domains. While this measure allowed us to explore the relationship between general media exposure and hacking perceptions, this general measure limited our ability to draw conclusions regarding the extent of exposure to exclusively hacker characters. It is possible that individuals scored highly on general media exposure but rarely saw a hacker character. As a preliminary investigation into this possibility, we reran our analyses using two different media exposure aggregates: (1) a four-item aggregate including the items that gave explicit hacker media examples (i.e. Prime Time Television, Entertainment Crime-Drama, Crime-Drama Movies, Anime TV Shows/Movies) and (2) a two-item aggregate including the items that assessed exposure to crime-focused media (i.e. a genre where hacker characters and storylines are widespread). Both of these aggregates were highly correlated with our original six-item aggregate (Four-item: $r = .940$, $p < .001$; Two-item: $r = .862$, $p < .001$). Using each of these revised media exposure aggregates, we found that our overall models held. However, even these revised aggregates do not provide a measure of purely hacker character exposure. Given our finding that general media exposure predicted wishful identification with hacker characters, future research should consider using a direct measure of exclusively hacker media exposure. Secondly, our general media exposure measure is limited by the categories we included in our items. Some of the categories of our measure of media exposure overlapped and provided the same example media to the participant (e.g., Prime-Time Television and Entertainment Crime-Drama both gave NCIS as an example). This overlap of categories limited our ability to measure an expansive scope of general media exposure. Although the similarity and consistency in our findings across all of the potential aggregates (two-, four-, and six-item) suggests that the link between media exposure and wishful identification with hacker characters is robust across domains of media exposure, future research should replicate these findings with alternative, comprehensive media exposure measures.

An interesting direction for future research is to ascertain what predicts wishful identification in the hacker behavior context. Is it purely the quantity of hacker characters, or the portrayal of hackers in specific programing? This type of research would benefit from a thorough content analysis of these hacker portrayals. Our preliminary analysis of media representations of hackers suggests that the number of hacker characters has increased significantly in the last decade. Compared to previous decades, recent media programs portrayed hacker characters as more attractive, successful, and at times admirable. Prior to 2007, research shows that a larger percentage of hacker characters were men. In general, these male characters were portrayed as "geeks" or "nerds," singularly focused on computers, intelligent, tech-savvy, and with an eclectic style and appearance (Rosewarne, 2016). In the last decade alone, female representation has increased in hacker roles and their character profiles are more stylish, attractive, and take on an edgy persona (Rosewarne, 2016). This may explain the little observed sex differences in the estimation of others' willingness to hack, perceived risks, and perceived payoffs. On-screen hacker characters may portray the hacking as more of a "cool" kid behavior, potentially explaining wishful identification patterns. More research is needed to assess the potential impact of these media characters.

Another important direction for future research is to gauge the public opinion of how authentically hacker characters are portrayed in the media. It is possible that individuals vary in how legitimate they feel hacker characters are in their portrayal of hacking. This may be especially true in individuals with advanced technical skills, who are able to identify factual inconsistencies in the portrayals. These differences in perceived authenticity may dampen later wishful identification.

Furthermore, future research could investigate if the portrayals of hackers, and subsequent hacker stereotypes have changed over time. Past research indicates that media representations may have a powerful impact in shaping stereotypes, (i.e., schemas of a category of people based on their group membership). Stereotypes are cognitive heuristics that facilitate information processing, attitudes, and behaviors toward stereotyped targets (Fiske, 1998; Hilton & von Hippel, 1996). Stereotypes regarding certain professions can be learned via media representations (Cheryan et al., 2013). For instance, a content analysis of media portrayals of scientists showed that, regardless of gender, a typical scientist is portrayed as Caucasian, intelligent, nerdy, and geeky (Long et al., 2010). Future research would benefit from an examination of more current perceived stereotypes of hackers to answer the question, *Is the known hacker stereotype changing, and are media responsible*?

Implications

The findings from this study have a number of important implications. First, this research suggests a relationship between general media exposure and the perceived practice of potentially unlawful behaviors. Our research shows that exposure to media and wishful identification with a hacker character is associated with an increase in perceived payoffs and estimation of others' willingness to hack. This may be due to the media's tendency to over dramatize, over glorify, and provide positive outcomes associated with, sometimes, illegal actions (Fischer et al., 2011; Garcia & Arkerson, 2017). Media may also be responsible for showing ease and swiftness (not often portraying a truthful representation) within hacking behaviors (Rosewarne, 2016), leading to behavioral concerns. Individuals with the requisite skills to hack may identify with a character, and in turn may be more willing to behave similarly to the hacker character, seeking payoffs similar to those in the show/movie storyline.

Second, an interesting and concerning finding from this research is that perceived risks may hold less weight in the decision-making process, and perceived payoffs may be a stronger determinant within this type of decision-making behavior. In a recent meta-analysis on media effects of risk-taking behaviors, the researchers concluded that glorification of risky behaviors in media is related to copy-cat behaviors (Fischer et al., 2011). For instance, researchers have attributed an increase in speeding and reckless driving incidents due to an increase in the portrayals of street-racing in advertisements and movies (Vingilis & Smart, 2009). Thus, risk-taking inclinations in hacking behaviors may be propelled by the presumed payoffs, and not the cost-benefit ratio.

Finally, computer games that teach young people how to code are becoming more prevalent (i.e., Code Monkey Island, Kodable) (Crawley, 2014). Our findings suggest that hacking behaviors are driven by perceived payoffs and media exposure. As more young people increase their technical skills, it will become increasingly necessary to employ strategies, such as government and industry sponsored hackathons and cybersecurity competitions, to educate young people about responsible and lawful hacking behavior.

Footnotes

1. We did not collect more specific information about which country in North America the participants reside. Participants indicated which region they live in from the following response items: (1) North America, (2) Europe, (3) Asia, (4) Africa, (5) Latin America, (6) Oceania. Participants who did not select (1) North America were excluded from analysis.

2. The hacktivism scenario provided in this study centers around protecting elderly from financial crimes. In general, hacktivism is politically or morally motivated. Likelihood to participate in specific hacktivism is likely to vary greatly depending on the political or religious ideology of the hacker.

References

Alberici, I. A., Milesi, P., Malfermo, P., Marzana, D., & Canfora, R. (2012). Comparing social movements and political parties' activism: The psychosocial predictors of collective action and the role of the internet. In *1° TAISP (Theory, Action and Impact of Social Protest) Interdisciplinary Conference* (pp. 3-4). Punctum Books.

Alpcan, T., & Basar, T. (2003, December). A game theoretic approach to decision and analysis in network intrusion detection. In *Proceedings of the IEEE Conference on Decision and Control* (Vol. 3, pp. 2595–2600). IEEE.

American Psychological Association. (1993). *Violence & youth: Psychology's response. Volume I: Summary report of the American Psychological Association Commission on Violence and Youth*. https://www.apa.org/pi/prevent-violence/resources/violence-youth.pdf

Andison, F. S. (1977). TV violence and viewer aggression: A cumulation of study results 1956-1976. *Public Opinion Quarterly, 41*(3), 314–331. https://doi.org/10.1086/268390

Ayres, J., & Hopf, T. (1992). Visualization: Reducing speech anxiety and enhancing performance. *Communication Reports*, *5*(1), 1–10. http://dx.doi.org/10.1080/08934219209367538

Ayres, J., & Hopf, T. S. (1985). Visualization: A means of reducing speech anxiety. *Communication Education*, *34*(4), 318–323. http://dx.doi.org/10.1080/03634528509378623

Ayres, J., & Hopf, T. S. (1990). The long-term effect of visualization in the classroom: A brief research report. *Communication Education*, *39*(1), 75–78. https://doi.org/10.1080/03634529009378788

Barber, R. (2001). Hackers profiled – Who are they and what are their motivations? *Computer Fraud & Security, 2001*(2), 14–17. https://doi.org/10.1016/S1361-3723(01)02017-6

Ben-Zur, H., & Zeidner, M. (2009). Threat to life and risk-taking behaviors: A review of empirical findings and explanatory models. *Personality and Social Psychology Review, 13*(2), 109–128. https://doi.org/10.1177/1088868308330104

Bergal, J. (2017, January 10). 'Hacktivists' increasingly target local and state government computers. *The Pew Charitable Trusts: Research & Analysis*. http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2017/01/10/hacktivists-increasingly-target-local-and-state-government-computers

Bodford, J. E., & Kwan, V. S. Y. (2018). A game theoretical approach to hacktivism: Is attack likelihood a product of risks and payoffs? *Cyberpsychology, Behavior, and Social Networking, 21*(2), 73–77. https://doi.org/10.1089/cyber.2016.0706

Bond, B. J., & Drogos, K. L. (2014). Sex on the shore: Wishful identification and parasocial relationships as mediators in the relationship between Jersey Shore exposure and emerging adults' sexual attitudes and behaviors. *Media Psychology, 17*(1), 102-126. https://doi.org/10.1080/15213269.2013.872039

Borrett, L. (2010, August 24). Hackers, crackers, script-kiddies, cyber-spies: Can you spot the bad guy? *Australian Anthill Magazine*. http://anthillonline.com/hackers-crackers-script-kiddies-cyber-spies-can-you-spot-the-bad-guy/

Calzo, J. P. & Ward, L. M. (2009). Media exposure and viewers' attitudes toward homosexuality: Evidence for mainstreaming or resonance? *Journal of Broadcasting & Electronic Media, 53*(2), 280–299. https://doi.org/10.1080/08838150902908049

Coleman, G. (2011). Hacker politics and publics. *Public Culture, 23*(3), 511–516. https://doi.org/10.1215/08992363-1336390

Coleman, G. (2012). *Coding freedom: The ethics and aesthetics of hacking*. Princeton University Press.

Cheryan, S., Plaut, V. C., Handron, C., & Hudson, L. (2013). The stereotypical computer scientist: Gendered media representations as a barrier to inclusion for women. *Sex Roles*, *69*(1-2), 58–71. https://doi.org/10.1007/s11199-013-0296-x

Crawley, D. (2014, June 3). 12 games that teach kids to code — and are even fun, too. *Venture Beat.* https://venturebeat.com/2014/06/03/12-games-that-teach-kids-to-code/

Dworak, M., Schierl, T., Bruns, T., & Strüder, H. K. (2007). Impact of singular excessive computer game and television exposure on sleep patterns and memory performance of school-aged children. *Pediatrics, 120*(5), 978–985. https://doi.org/10.1542/peds.2007-0476

Fischer, P., Greitemeyer, T., Kastenmüller, A., Vogrincic, C., & Sauer, A. (2011). The effects of risk-glorifying media exposure on risk-positive cognitions, emotions, and behaviors: A meta-analytic review. *Psychological Bulletin*, *137*(3), 367–390. https://doi.org/10.1037/a0022267

Fischer, P., Guter, S., & Frey, D. (2008). The effects of risk-promoting media on inclinations toward risk taking. *Basic and Applied Social Psychology, 30*(3), 230–240. https://doi.org/10.1080/01973530802375029

Fischer, P., Kubitzki, J., Guter, S., & Frey, D. (2007). Virtual driving and risk taking: Do racing games increase risk-taking cognitions, affect, and behaviors? *Journal of Experimental Psychology: Applied, 13*(1), 22–31. https://doi.org/10.1037/1076-898X.13.1.22

Fiske, S. T. (1998). Stereotyping, prejudice, and discrimination. In D. T. Gilbert, S. T. Fiske, & G. Lindzey (Eds.), *The handbook of social psychology* (4th ed., Vol. 2, pp. 357–411). McGraw-Hill.

Fiske, S. T., Cuddy, A. J. C., Glick, P., & Xu, J. (2002). A model of (often mixed) stereotype content: Competence and warmth respectively follow from perceived status and competition. *Journal of Personality and Social Psychology, 82*(6), 878–902. https://doi.org/10.1037/0022-3514.82.6.878

Garcia, V., & Arkerson, S. G. (2017). *Crime, media, and reality: Examining mixed messages about crime and justice in popular media.* Rowman & Littlefield.

Gerbner, G., Gross, L., Morgan, M., Signorielli, N., & Shanahan, J. (2002). Growing up with television: Cultivation processes. In J. Bryant & D. Zillmann (Eds.), *Media effects: Advances in theory and research* (pp. 43–68). Lawrence Erlbaum Associates, Inc.

Gonsalves, A. (2003, August 29). *Experts say the MSBlaster author is a 'script kiddie'; experts say that the teen arrested by the FBI is, if guilty, a lightweight, not a highly sophisticated virus writer.* InternetWeek.

Gordon, D. (2010). Forty years of movie hacking: Considering the potential implications of the popular media representation of computer hackers from 1968 to 2008. *International Journal of Internet Technology and Secured Transactions*, *2*(1-2), 59–87. https://doi.org/10.1504/IJITST.2010.031472

Graham, L. (2017, September 20). *The number of devastating cyberattacks is surging – and it's likely to get much worse.* CNBC: Cybersecurity. https://www.cnbc.com/2017/09/20/cyberattacks-are-surging-and-more-data-records-are-stolen.html

Greenwood, D. N. (2007). Are female action heroes risky role models? Character identification, idealization, and viewer aggression. *Sex Roles, 57*(9-10), 725–732, http://dx.doi.org/10.1007/s11199-007-9290-5

Greitzer, F. L., Kangas, L. J., Noonan, C. F., & Dalton, A. C. (2010). *Identifying at-risk employees: A behavioral model for predicting potential insider threats* (Report No. PNNL-19665). U.S. Department of Energy. https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-19665.pdf

Hayes, A. F. (2017). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach*. Guilford Publications.

Henry, K. B., Arrow, H., & Carini, B. (1999). A tripartite model of group identification: Theory and measurement. *Small Group Research, 30*(5), 558–581. https://doi.org/10.1177/104649649903000504

Hilton, J. L., & von Hippel, W. (1996). Stereotypes. *Annual Review of Psychology*, *47*, 237–271. https://doi.org/10.1146/annurev.psych.47.1.237

Hoffner, C. (1996). Children's wishful identification and parasocial interaction with favorite television characters. *Journal of Broadcasting & Electronic Media*, *40*(3), 389–402. https://doi.org/10.1080/08838159609364360

Hoffner, C., & Buchanan, M. (2005). Young adults' wishful identification with television characters: The role of perceived similarity and character attributes. *Media Psychology*, *7*(4), 325–351. https://doi.org/10.1207/S1532785XMEP0704_2

Holt, T. J., & Schell, B. H. (Eds.). (2010). *Corporate hacking and technology-driven crime: Social dynamics and implications.* IGI Global.

Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal*, *6*(1), 1–55. https://doi.org/10.1080/10705519909540118

Johnson, J. G., Cohen, P., Smailes, E. M., Kasen, S., & Brook, J. S. (2002). Television viewing and aggressive behavior during adolescence and adulthood. *Science, 295*(5564), 2468–2471. https://doi.org/10.1126/science.1062929

Jordan, T. & Taylor, P. (2004). *Hacktivism and cyberwars: Rebels with a cause?* Routledge.

Kelty, C. M. (2008). *Two bits: The cultural significance of free software.* Duke University Press.

Konijn, E. A., Nije Bijvank, M., & Bushman, B. J. (2007). I wish I were a warrior: The role of wishful identification in the effects of violent video games on aggression in adolescent boys. *Developmental Psychology, 43*(4), 1038–1044. https://doi.org/10.1037/0012-1649.43.4.1038

Krawczyk, K. (2014, June 10). Cyber crime costs the world more money than some natural disasters do. *Digital Trends.* http://www.digitaltrends.com/computing/new-study-says-cyber-crime-costs-hundreds-of-billions-per-year

Long, M., Steinke, J., Applegate, B., Knight Lapinski, M., Johnson, M. J., & Ghosh, S. (2010). Portrayals of male and female scientists in television programs popular among middle school-age children. *Science Communication, 32*(3), 356–382. https://doi.org/10.1177/1075547009357779

MacCallum, R. C., Browne, M. W., & Sugawara, H. M. (1996). Power analysis and determination of sample size for covariance structure modeling. *Psychological Methods, 1*(2), 130–149. https://doi.org/10.1037/1082-989X.1.2.130

Mansfield-Devine, S. (2011). Hacktivism: Assessing the damage. *Network Security, 2011*(8), 5–13. https://doi.org/10.1016/S1353-4858(11)70084-8

Massa, F. G. (2011). Out of bounds: Anonymous' transition to collective action. *Academy of Management Proceedings 2011*(1). https://doi.org/10.5465/ambpp.2011.65869486

Milan, S. (2013). *Social movements and their technologies: Wiring social change.* Palgrave Macmillan.

Minnebo, J. & Eggermont, S. (2007). Watching the young use illicit drugs: Direct experience, exposure to television and the stereotyping of adolescents' substance use. *Young, 15*(2), 129–144. https://doi.org/10.1177/110330880701500202

Nabi, R. L. & Sullivan, J. L. (2001). Does television viewing relate to engagement in protective action against crime? A cultivation analysis from a theory of reasoned action perspective. *Communication Research, 28*(6), 802–825. https://doi.org/10.1177/009365001028006004

Palmer, C. C. (2001). Ethical hacking. *IBM Systems Journal, 40*(3), 769–780. https://doi.org/10.1147/sj.403.0769

Ponemon Institute. (2012). *2012 cost of cyber crime study: United States*. https://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf

Rainie, L., Anderson, J., & Connolly, J. (2014). Cyber attacks likely to increase. *Pew Research Center: Internet & Technology*. http://www.pewinternet.org/2014/10/29/cyber-attacks-likely-to-increase/

Reinganum, J. F. (1981). On the diffusion of new technology: A game theoretic approach. *The Review of Economic Studies*, *48*(3), 395–405. https://doi.org/10.2307/2297153

Robertson, L. A., McAnally, H. M., & Hancox, R. J. (2013). Childhood and adolescent television viewing and antisocial behavior in early adulthood. *Pediatrics, 131*(3), 439–446. https://doi.org/10.1542/peds.2012-1582

Rosewarne, L. (2016). *Cyberbullies, cyberactivists, cyberpredators: Film, TV, and Internet stereotypes*. ABC-CLIO.

Ross, L., Greene, D., & House, P. (1977). The "false consensus effect": An egocentric bias in social perception and attribution processes. *Journal of Experimental Social Psychology, 13*(3), 279–301. https://doi.org/10.1016/0022-1031(77)90049-X

Ryan, R. M., & Deci, E. L. (2000). Self-determination theory and intrinsic motivation, social development, and well-being. *American Psychologist, 55*(1), 68–78. https://doi.org/10.1037/0003-066X.55.1.68

Sauter, M. (2013). "LOIC will tear us apart": The impact of tool design and media portrayals in the success of activist DDOS attacks. *American Behavioral Scientist, 57*(7), 983–1007. https://doi.org/10.1177/0002764213479370

Segan, S. (2000). *Female hackers battle sexism to get ahead.* Mujeres en Red. El Periódico Feminista. http://www.mujeresenred.net/spip.php?article1543

Sinclair, S., & Smith, S. W. (2008). Preventative directions for insider threat mitigation via access control. In S. J. Stolfo, S. M. Bellovin, S. Hershkop, S. W. Smith, & S. Sinclair (Eds.), *Insider attack and cyber security: Beyond the hacker* (pp. 165–194). Springer.

Strasburger, V. C., Donnerstein, E. I. (2000). Children, adolescents, and the media in the 21st century. *Adolescent Medicine (Philadelphia, Pa.), 11*(1), 51–68.

Surette, R. (2002). Self-reported copycat crime among a population of serious and violent juvenile offenders. *Crime & Delinquency*, *48*(1), 46–69. https://doi.org/10.1177/0011128702048001002

Suzuki, M., & Nakayama, M. (1976). The cost assignment of the cooperative water resource development: A game theoretical approach. *Management Science*, *22*(10), 1081–1086. https://doi.org/10.1287/mnsc.22.10.1081

Tanczer, L. M. (2016). Hacktivism and the male-only stereotype. *New Media & Society, 18*(8), 1599–1615. https://doi.org/10.1177/1461444814567983

The Council of Economic Advisers. (2018). *The cost of malicious cyber activity to the U.S. economy.* https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

Vingilis, E., & Smart, R. G. (2009). Street racing: A neglected research area? *Traffic Injury Prevention, 10*(2), 148–156. https://doi.org/10.1080/15389580802641753

von Neumann, J. (1928). Die zerlegung eines intervalles in abzählbar viele kongruente teilmengen [The breakdown of an interval into a countable number of congruent subsets]. *Fundamenta Mathematicae, 11*, 230–238. https://doi.org/10.4064/fm-11-1-230-238

Wiederhold, B. K. (2014). The role of psychology in enhancing cybersecurity. *Cyberpsychology, Behavior, and Social Networking, 17*(3), 131–132. https://doi.org/10.1089/cyber.2014.1502

Wikipedia contributors. (2020, February 2). *List of fictional hackers*. Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?

Young, R. Zhang, L., & Prybutok, V. R. (2007). Hacking into the minds of hackers. *Information Systems Management, 24*(4), 281–287. http://dx.doi.org/10.1080/10580530701585823

Zajonc, R. B. (1968). Attitudinal effects of mere exposure. *Journal of Personality and Social Psychology, 9*(2, Pt.2), 1–27. https://doi.org/10.1037/h0025848

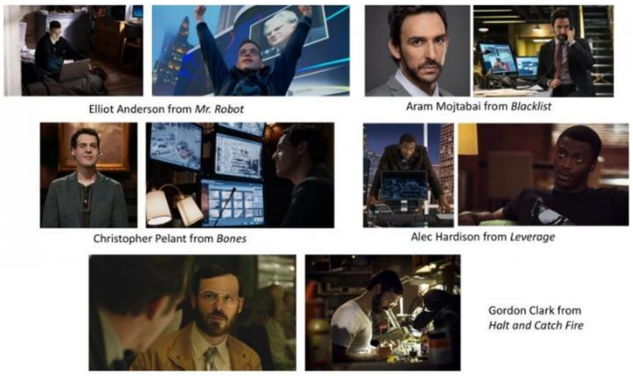
Züger, T., Milan, S., & Tanczer, L. M. (2015). FCJ–192 Sand in the information society machine: How digital technologies change and challenge the paradigms of civil disobedience. *The Fibreculture Journal, 26*, 108–135. https://doi.org/10.15307/fcj.26.192.2015

Appendix A

Media Character Prime and Example Characters

Media Character Prime:

For the next few pages of the survey, we ask you to think about a male/female movie/TV/anime show character who's character is a technology specialist or computer hacker. Please indicate your memory, impression, and likability of that character to the best of your ability. Examples of male/female character computer specialists are below to help jog your memory.


Elliot Anderson from *Mr. Robot*
Aram Mojtabai from *Blacklist*
Christopher Pelant from *Bones*
Alec Hardison from *Leverage*
Gordon Clark from *Halt and Catch Fire*

Abby Sciuto from *NCIS*
Penelope Garcia from *Criminal Minds*
Chloe O'Brian from *24*
Cable McCrory from *Bull*
Lisbeth Salander from *Girl with the Dragon Tattoo*

Can you name this TV show/movie character? Or what show/movie is he/she on?

Correspondence to:
Virginia S. Y. Kwan and Samantha L. McMichael
Department of Psychology,
Arizona State University,
950 South McAllister Avenue,
Tempe, AZ 85287
Email: Virginia.Kwan(at)asu.edu
Email: Samantha.McMichael(at)asu.edu

Editorial record: First submission received on July 18, 2018. Revisions received on April 17, 2019, September 9, 2019 and December 20, 2019. Accepted for publication on January 23, 2020.
Editor in charge: Lenka Dedkova

About Authors

Sarah Staggs received her Ph.D in communication at the University of Arizona and completed a year post-doctoral training with Dr. Virginia Kwan in the Culture and Decision Science Lab at Arizona State University. Her current research focuses on statistical methods to optimize marketing effort and consumer fit. Currently, she is a researcher and data analyst for a global golf company.

Samantha L. McMichael received her B.S. in Psychology at the University of Washington. She currently works with Dr. Virginia Kwan in the Culture and Decision Science Lab as a graduate student of the Ph.D. program in Social Psychology at Arizona State University. Her primary research interests include decision making processes related to future planning, and sex differences in STEM education and the workforce.

Virginia S. Y. Kwan received her Ph.D. at the University of California, Berkeley, served on the faculty at Princeton University, and is now Professor in the Department of Psychology at Arizona State University. Her major research interests revolve around the broad content areas of social perception and decision science. She is the Director of the Culture and Decision Science Laboratory. She has developed a research program that examines social perception using multiple methods, multiple cultures, and multiple species. Her recent research addresses the impact of cyberlife engagement on social cognition and behavior.