Winter 12-11-2022

Too good for malware: Investigating effects of entitlement on cybersecurity threat assessment and piracy behavior

Andrew Bowman
Oklahoma State University, andy.bowman@okstate.edu

Madhav Sharma
Kansas State University

David Biros
Oklahoma State University

Too Good for Malware: Investigating Effects of Entitlement on Cybersecurity Threat Assessment and Piracy Behavior

Andy Bowman[1]
Oklahoma State University
Stillwater, OK, USA

Madhav Sharma
Kansas State University
Manhattan, KS, USA

David Biros
Oklahoma State University
Stillwater, OK, USA

ABSTRACT

When employees use work resources to commit digital piracy, they are putting their employer's security and data at risk. This study investigates the effects of technology entitlement, the belief that one is more deserving of technology resources resulting in an expectation of special privileges in its use. Specifically, we explore the influence of technology entitlement on the relationship between perceived cyber security threat and attitude towards digital piracy. Using technology entitlement, we better understand the perception of risk that goes into a decision to pirate content and commit computer abuse using employer information technology.

Keywords: cybersecurity, piracy behavior, cyber-threat assessment, structural equation modelling.

INTRODUCTION

Digital Piracy is a global economic issue that plagues the software and entertainment industry. Piracy poses an overarching macro-threat to the economics of digital goods leading to loss of 223,000 to 541,000 jobs and $45.7 billion to $111.1 billion in lost GDP (Blackburn et al. 2019). Websites with pirated content (hereinafter, referred to as illegitimate websites) including

[1] Corresponding author. andy.bowman@okstate.edu

software and media (music, tv shows, and movies) are also a major source of cybersecurity threats. These threats include malware (which can infect a computer, delete critical files, corrupt programs, and can also spy on users and gather information with intent to harm), phishing threats, ransomware, and spyware. Thus, users motivated to consume digital entertainment content using illegitimate sites can be targets of various forms of cyber threats and can expose their organizations' network and devices as well (Bossler and Holt 2009).

Post pandemic, many companies are offering their employees opportunities for remote work or hybrid work environment where employees work in the office on some days and may work from home on others (Barrero et al. 2021). Remote work blurs the line between use of devices for work and non-work purposes and has empowered employees with increased technological freedom (i.e., more control over their devices). Non-work purposes for a device include browsing the internet, participating in social media, gaming, and consuming entertainment digitally (McGregor 2022). In a survey conducted by NetMotion, it was found that 74% of employees working from home admitted that they use their work computers for streaming content, primarily from YouTube and Netflix (Chisolm 2020). While paying to consume content either by purchasing legal digital copies or by accessing it via a streaming service is the norm, the statistics mentioned above show that a significant number of bad actors opt for pirating games, movies, and music.

The increased technological freedom afforded to employees by the remote and hybrid work model and an employee centered job market has imbued employees with increased entitlement. Entitlement is defined as sense of inflated self-worth and heightened expectation of special privileges (Campbell et al. 2004). Entitlement has been a strong predictor of counter productive work behavior in organization behavior literature (Joplin et al. 2021; Wheeler et al.

2013). Amo et al. (2022) contextualized entitlement for organizational computer systems and showed that the novel construct technology entitlement predicts computer abuse. Technology entitlement and its effect on specific computer abuses such as digital piracy has not been studied. Even with clear guidelines and policies, computer abuse such as digital piracy is a pervasive counter productive work behavior. Employees who feel the sense of technological freedom are more likely to engage in piracy behavior which can lead to several consequences for the organization including cybersecurity breaches and ransomware that can shut down businesses.

Prior research has studied cybersecurity related threats and piracy behaviors individually. Research in behavioral cybersecurity has focused on phishing susceptibility (Nguyen et al. 2021) information security policy compliance (Chen et al. 2021; Cram et al. 2019), and engaging in voluntary security behaviors (backing up data, anti-malware software use) (Boss et al. 2015). Scholars studying piracy behaviors have also examined the motivation to consume pirated content primarily using theory of planned behavior and social learning theory with ethics and morality as major antecedents(Eisend 2019; Lowry et al. 2017; Tam et al. 2019). Though perceived risks have been a recurring antecedent of attitude towards piracy, it has mostly been used in context of expected legal punishment. Given the low trustworthiness of illegitimate websites, users have to factor in cybersecurity risks while consuming pirated content. Yet, cybersecurity threats as an antecedent of piracy behavior has not been explored to a noteworthy extent. Cybersecurity threat assessment is also influenced by whether an individual is using their personal computer or one belonging to the organization at which they work (Bossler and Holt 2009; Jopin et al. 2021). Technology entitlement, defined as belief that one is more deserving of organizations' technology resources than other individuals, can affect the cybersecurity threat assessment and piracy behavior. To investigate the interplay between entitlement, cybersecurity,

and piracy, we posit the following research questions: (1) How does cybersecurity threat assessment affect piracy behaviors? (2) How does technology entitlement affect the relationship between cybersecurity threat assessment and piracy behavior?

We answer these research questions by proposing and testing a theoretical model for antecedents of piracy behavior based on theory of planned behavior. We test the model by conducting an experimental vignette-based study on participants. This study contributes to literature on piracy deterrence policies and cybersecurity training.

THEORETICAL BACKGROUND

Digital piracy has been a topic of interest for scholars from IS, criminology, and management (Al-Rafee and Cronan 2006; Morris and Higgins 2010; Sundararajan 2004). Though they have examined antecedents and consequences of piracy in from various vantage points, the use of deterrence theory (DT) and the theory of planned behavior (TPB) has been a key commonality in all these strands of literature (Lee et al. 2019; Yoon 2011). DT shows that certain controls can serve as deterrent mechanisms by increasing the perceived threat of punishment for computer abuse (D'Arcy et al. 2009). The theory further suggests that the individual rationally weighs the severity, celerity (speed), and certainty of punishment to better understand the consequences of performing the behavior. The literature has shown that punishment certainty is the most effective at deterring a behavior followed by severity, and celerity (Lowry et al. 2017). Such deterrent controls are used with the goal to deter the behavior from ever happening with the perceived threats or fear of sanctions (Gopal and Sanders 1997). Antecedents of information systems use can be classified as implicit (i.e. implied but not expressed) and explicit (i.e. clearly stated and defined) (de Guinea et al. 2014; Serenko and Turel 2020). While deterrents are successful in predicting explicit factors (punishments and sanctions)

that lead to intention to engage in piracy behaviors, implicit factors such as morality, justifications, entitlement, outcome evaluation can be better understood using TPB (Serenko 2022). Furthermore, the deterrents from DT and implicit factors that drive planned behavior from TPB effect user behavior at different stages of piracy behavior.

Piracy behaviors can be broken down into four stages: visit illegitimate website, browse the website, consider the risk and benefits, and finally intend to engage. These stages are identified based on other online behaviors in contexts such as ecommerce and phishing where behaviors are broken into a series of interrelated activities that occur to accomplish an objective (often represented by funnels) (Abbasi et al. 2021; Kaushik 2009). While there are factors that can motivate or deter the user to move from on stage to the next, in this study, we focus on the consideration of risks and benefits, specifically, consideration of cybersecurity risks. Since the stage being evaluated is in the middle of piracy activities, we argue that by the time a user gets to this stage, effective deterrents would have already deterred some users to engage in piracy.

TPB has been a staple of research investigating information system behaviors such as security, piracy, and other IS-related activities(Ajzen and Fishbein 1977). The TPB suggests that attitude (controlling for subjective norms and perceived behavioral control) has a positive effect on the intention to engage in the specific behavior, which in turn, causes actual behavior. In context of piracy, Yoon (2011) conducted a study comparing TPB based model to another dominant paradigm used to study intentions to participate in piracy behaviors, the Hunt–Vitell ethical decision model and found that TPB explains the piracy intentions better alternative. A meta-analysis conducted by Eisend (2019) further supported the validity of TPB as an appropriate theory to study piracy behavior by analyzing data from 25 relevant studies. Thus, we find it to be of value in our current investigation.

Risk, (i.e. perception of risk associated with the acquisition of pirated products) has been cited as one the key antecedents of attitude towards digital piracy in previous studies (Eisend 2019; Lowry et al. 2017). Eisend (2019)'s meta-analyses showed that risk had a significant negative effect on attitude towards digital piracy. Risk is multifaceted when it comes to the context of piracy. Individuals engaging in piracy behaviors assess risks in various contexts due to legal, social, and technological implications. Individuals being caught while engaging in digital piracy may expose themselves to severe sanctions depending on the regulations of the organization (Higgins 2007; Tam et al. 2019). These can include consequences pertaining to loss of job or termination of internet connection by the service provider (Lee et al. 2019). Additionally, technology implications for engaging in piracy include computer restrictions by organizations and exposure to information security threats found on illegitimate websites. Technological implications, especially pertaining to information security risks have not been studied to a noteworthy extent in piracy literature. Some early studies included the fear of catching a virus as a deterrent to piracy but more recent research has not studied the intersection of piracy and cybersecurity (Wolfe et al. 2008). Our research aims to fill this gap.

Cybersecurity Threat Assessment

Digitization and information system security risks have risen in prominence concurrently. Prior research shows that employees (insiders) within the organization are a major source of information security threats as they have access to the networks (Warkentin and Willison 2009). While malicious insiders can intentionally harm the organization by engaging in deviant behaviors, non-malicious insiders inadvertently expose the organization to security threats via phishing, downloading malware or falling for social engineering(Guo et al. 2011; Liang et al. 2016). Research in behavioral cybersecurity with insiders as level of analyses has focused on

phishing susceptibility (Nguyen et al. 2021) information security policy compliance (Chen et al. 2021; Cram et al. 2019), and engaging in voluntary security behaviors (backing up data, anti-malware software use)(Boss et al. 2015).

Illegitimate websites used for distribution of pirated content are a major source of cybersecurity threats such as malware that can infect a computer, delete critical files, corrupt programs, and can also spy on users and gather information with intent to harm (Bossler and Holt 2009). Users' awareness of the severity and likelihood of being targeted by a cybersecurity threat would affect their attitude towards engaging in piracy. Thus, we posit the following hypotheses:

Hypotheses 1: Perceived cyber-threat has a negative effect on attitude towards piracy.

Technology Entitlement

Technology entitlement is defined as "the persistent belief that one is more deserving of technological resources than other individuals and tends to manifest in expectations of special technology access and privileges" (Amo et al., 2022, p. 1396). It is based on the construct of general entitlement which is a prominent personality trait in psychology literature. People who measure high in general entitlement have an unrealistically positive view of their own capabilities and in turn set unrealistically high expectations for themselves and the way others should treat them. These expectations often result in disappointment (Campbell et al., 2004).

The emotional responses to the failure of these expectations can result in exaggerated levels of psychological distress, violent outbursts, computer abuse, and other deviant behaviors. Nested within general entitlement is other forms of entitlement (Campbell et al., 2004; Amo et al., 2022; Grubbs and Exline, 2016). Technological entitlement follows this line of behavior to the conclusion when people are given control over equipment for work, and what the individual

can do with the resources given to them by their company. Since people who experience general entitlement overestimate their own capabilities and outcomes in subjects, it follows that people who experience technological entitlement estimate their own capabilities and outcomes in the specific focus of that entitlement (technology). With perceived threat having a component of self-estimation and piracy being a form of computer abuse, we posit the following hypotheses:

Hypothesis 2: Technology Entitlement has a negative effect on perceived cyber-threat.

Hypothesis 3: Technology Entitlement has a positive effect on attitude towards piracy.

According to the TPB, attitude towards a behavior is one among the key predictors in the formation of intention. TPB has been heavily used in understanding piracy behavior (Eisend 2019; Yoon 2011). Eisend (2019)'s comprehensive meta-analyses showed that attitude towards piracy was a strong predictor of intention to engage in piracy behavior over 176 studies. Yoon (2011) also showed the attitude towards piracy had a strong positive effect on intention to engage in piracy. Consistent with these strands of literature, we hypothesize:

Hypotheses 4: Attitude towards piracy has a positive effect on intention to consume pirated content.

Based on the proposed hypotheses, we propose a theoretical model for effects of cybersecurity and entitlement on piracy behavior (Figure 2).

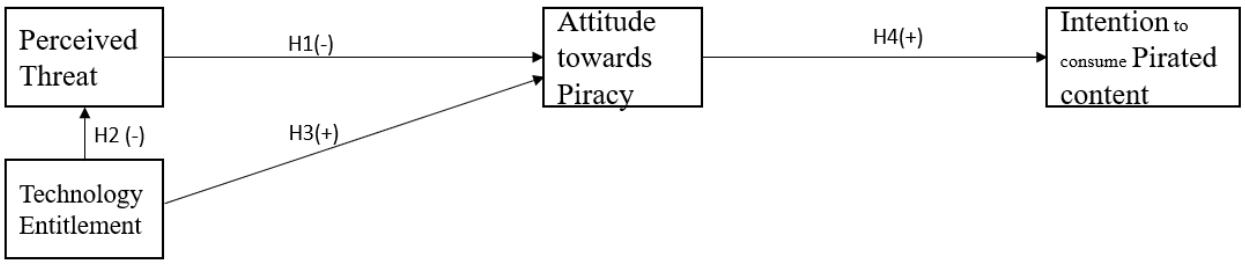

Figure 1. Theoretical Model

METHODOLOGY

We conducted a survey using a scenario-based approach. This approach has been widely used in IS research investigating IT decision making. We opt for a scenario-based approach because it provides two benefits in our context of study. First, this approach provides a decision and behavioral setting that is not easily accessible. In studies related to piracy behavior, ethically, researchers cannot suggest participants to engage in such behaviors (Park et al. 2022). Due to unethical nature of the behavior, researchers cannot recruit participants who partake in the piracy behaviors without undue pressure or implicating them. A scenario-based study sidesteps this dilemma. Second, a scenario helps us create a controlled setting where can test the relationship between constructs proposed in the study without noticeable interference from confounding factors that may otherwise drive piracy behavior. This maximizes internal validity of the study.

Sample

We recruited participants from IS courses of two large midwestern universities. The students were offered extra credit in class for attempting the survey. Our final dataset had 324 observations. Average age of participants was 19.1 (min=18, max=27). 59.5% of the participants identified as males and 23% of them identified as STEM majors.

Scenario and Measures

Consistent with Amo et al., (2022) and Park et al., (2022), we built a scenario based on a plausible case of an employee who may engage in piracy behavior (shown in appendix). We showed an image which was a screen capture of an illegitimate site which can be used to stream pirated content. To not inadvertently give away places to stream pirated content, website name and URL were redacted. This website also had a pop up for updating flash player which was a malware attempt. Based on scenario shown, we asked participants to fill out a questionnaire that contained questions asking about our key constructs: perceived cyber threat (adapted from Chen

and Zahedi, 2016), technology entitlement (adapted from Amo et al, 2021), attitude towards piracy, and intention to engage in piracy (adapted from Al-Rafee and Cronan, 2006). Our main constructs and their sources are summarized in Table 1. Other control measures such as age, major, and gender were also collected.

Table 1. Constructs and Sources

Construct	Definition	Source
Perceived Cyber-threat	User's cognitive assessment of how likely and severely an adverse cybersecurity related incident can affect them.	Chen and Zahedi., (2016)
Technology entitlement	"the persistent belief that one is more deserving of technological resources than other individuals and tends to manifest in expectations of special technology access and privileges"	Amo et al., (2022)
Attitude towards piracy	The degree to which a user has favorable or unfavorable evaluation of piracy behavior.	Al-Rafee and Cronan, (2006)
Intention to engage in piracy behavior	The motivation or level of effort, user will exert, in order to engage in piracy behavior.	Al-Rafee and Cronan, (2006)

RESULTS

We analyzed the data using structural equation modelling (SEM) in Stata. We built a measurement model to assess the validity of our adapted scales. Factor loading for all items for their respective construct was above 0.65. The average variance extracted (AVE) for each construct was greater than 0.5 showing no issues with convergent validity. The AVE was also greater than each Squared correlations (SC) showing no issues with discriminant validity (SCs and AVEs shown in Table 1).

Table 2. Average Variance Extracted and Squared Correlations

	Average Variance Extracted	Technology Entitlement	Perceived Threat	Attitude towards Piracy	Intention to engage in piracy
Technology Entitlement	0.547	1			
Perceived Threat	0.778	0.025	1		
Attitude towards Piracy	0.662	0.139	0.261	1	
Intention to engage in piracy	0.82	0.05	0.233	0.466	1

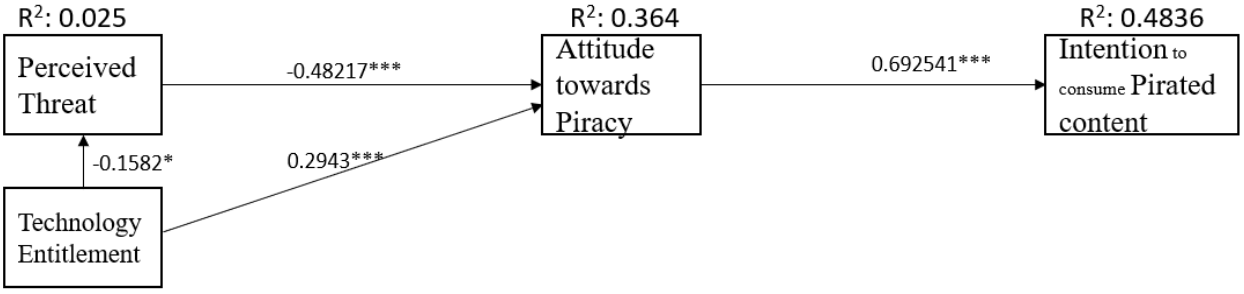

Figure 2. Results of Structural Model and Moderation

The model generated a good fit χ^2 (61) = 146.523, $p < .0001$, SRMR = .057, TLI = .961, CFI = .97, RMSEA = .056 (90% confidence interval, CI: .053, .08), $p = .025$. Figure 2 shows all paths are significant, thus providing support for all our hypotheses. All of these indices are within the threshold for significance in the SEM literature (Kline 2015).

IMPLICATIONS AND LIMITATIONS

Support for H1 demonstrates that people will be less approving of piracy when they see it as being riskier and more dangerous. Technology entitlement had a negative significant effect on perceived threat (supporting H2, albeit with very low explained variance) implying that individuals with high entitlement tend to view threats as less risky than those with low entitlement. Technology entitlement also had a significant positive effect on attitude towards piracy showing that individuals with high entitlement are more likely to participate in such unacceptable behavior (supporting H3). Lastly, we found that attitude toward piracy leads to intention toward piracy, thus supporting H4.

Future research can extend this by exploring further both the unintended dangers of technology entitlement through mechanisms where individuals are more likely to expose their technology resources to cyber threats and may coincide with a higher estimation of one's ability to deal with these threats when they do arise. Researchers should also consider looking at the

other side of the technology entitlement coin and exploring if low levels of technology entitlement may lead to extra caution and safer behavior when dealing with risk filled situations. Potential practical implications from this research can lead to focusing training not just on threat awareness, but also on technology entitlement. When users are aware of threats, but possess high technology entitlement, that training may be less effective due to the moderating effect discovered in this research.

This research has several limitations that need to be considered. For one, we used a convenience sample of college students who may not be as aware of the threats posed by these illegitimate websites, future research should consider using a population of subjects more involved in remote work and subject to disciplinary consequences for failing to comply with information security policies. Common method bias and variance can also affect our results as we use popular adapted scales for all constructs. Second, the scenario and manipulation used a picture of an illegitimate website which does not give the full experience of using the site and being exposed to high number of popup advertisements, this may cause a lower level of perceived threat from the site use. Finally, more understanding needs to be put into the scales for entitlement, while we had strong loadings on the construct, it may not be as easily adapted to the student context and may mean something else to students using university recourses.

CONCLUSION

This study demonstrates a strong potential for the technology entitlement construct to be used in specific computer abuse and cybersecurity contexts and can lead to a deeper understanding of non-malicious insider risks within organizations. IT users who feel more technologically entitled appear to view information piracy more favorably than other thereby

opening organizations to more cybersecurity vulnerability. Continued study of this construct is certainly warranted.

REFERENCES

Abbasi, A., Dobolyi, D., Vance, A., and Zahedi, F. M. 2021. "The Phishing Funnel Model: A Design Artifact to Predict User Susceptibility to Phishing Websites," *Information Systems Research* (32:2), pp. 410-436.

Ajzen, I., and Fishbein, M. 1977. "Attitude-Behavior Relations: A Theoretical Analysis and Review of Empirical Research," *Psychological bulletin* (84:5), p. 888.

Al-Rafee, S., and Cronan, T. P. 2006. "Digital Piracy: Factors That Influence Attitude toward Behavior," *Journal of Business Ethics* (63:3), pp. 237-259.

Barrero, J. M., Bloom, N., and Davis, S. J. 2021. "Why Working from Home Will Stick," National Bureau of Economic Research.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P. 2015. "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors," *MIS quarterly* (39:4), pp. 837-864.

Bossler, A. M., and Holt, T. J. 2009. "On-Line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory," *International Journal of Cyber Criminology* (3:1).

Campbell, W. K., Bonacci, A. M., Shelton, J., Exline, J. J., and Bushman, B. J. 2004. "Psychological Entitlement: Interpersonal Consequences and Validation of a Self-Report Measure," *Journal of personality assessment* (83:1), pp. 29-45.

Chen, Y., Galletta, D. F., Lowry, P. B., Luo, X., Moody, G. D., and Willison, R. 2021. "Understanding Inconsistent Employee Compliance with Information Security Policies through the Lens of the Extended Parallel Process Model," *Information Systems Research* (32:3), pp. 1043-1065.

Chisolm, M. 2020. "Employees Use of Corporate-Owned Devices to Stream Youtube and Netflix Spikes as Remote Work Persists." Retrieved September 15, 2022, from https://www.netmotionsoftware.com/blog/surveys/employees-use-of-corporate-owned-devices-to-stream-youtube-and-netflix-spikes-as-remote-work-persists

Cram, W. A., D'arcy, J., and Proudfoot, J. G. 2019. "Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance," *MIS Quarterly* (43:2), pp. 525-554.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79-98.

de Guinea, A. O., Titah, R., and Léger, P.-M. 2014. "Explicit and Implicit Antecedents of Users' Behavioral Beliefs in Information Systems: A Neuropsychological Investigation," *Journal of Management Information Systems* (30:4), pp. 179-210.

Eisend, M. 2019. "Explaining Digital Piracy: A Meta-Analysis," *Information Systems Research* (30:2), pp. 636-664.

Gopal, R. D., and Sanders, G. L. 1997. "Preventive and Deterrent Controls for Software Piracy," *Journal of Management Information Systems* (13:4), pp. 29-47.

Guo, K. H., Yuan, Y., Archer, N. P., and Connelly, C. E. 2011. "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model," *Journal of management information systems* (28:2), pp. 203-236.

Higgins, G. E. 2007. "Digital Piracy, Self-Control Theory, and Rational Choice: An Examination of the Role of Value," *International Journal of Cyber Criminology* (1:1), pp. 33-55.

Joplin, T., Greenbaum, R. L., Wallace, J. C., and Edwards, B. D. 2021. "Employee Entitlement, Engagement, and Performance: The Moderating Effect of Ethical Leadership," *Journal of Business Ethics* (168:4), pp. 813-826.

Kaushik, A. 2009. *Web Analytics 2.0: The Art of Online Accountability and Science of Customer Centricity*. John Wiley & Sons.

Kline, R. B. 2015. *Principles and Practice of Structural Equation Modeling*. Guilford publications.

Lee, B., Jeong, S., and Paek, S. Y. 2019. "Determinants of Digital Piracy Using Deterrence, Social Learning and Neutralization Perspectives," *International Journal of Comparative and Applied Criminal Justice* (43:4), pp. 295-308.

Liang, N., Biros, D. P., and Luse, A. 2016. "An Empirical Validation of Malicious Insider Characteristics," *Journal of Management Information Systems* (33:2), pp. 361-392.

Lowry, P. B., Zhang, J., and Wu, T. 2017. "Nature or Nurture? A Meta-Analysis of the Factors That Maximize the Prediction of Digital Piracy by Using Social Cognitive Theory as a Framework," *Computers in Human Behavior* (68), pp. 104-120.

McGregor, J. 2022. "Just 4% of Employers Are Making Everyone Return to the Office, Survey Finds." Retrieved September 15, 2022, from https://www.forbes.com/sites/jenamcgregor/2022/05/05/just-4-of-employers-are-making-everyone-return-to-the-office-full-time-survey-finds/?sh=4f50b267e1a2

Morris, R. G., and Higgins, G. E. 2010. "Criminological Theory in the Digital Age: The Case of Social Learning Theory and Digital Piracy," *Journal of Criminal Justice* (38:4), pp. 470-480.

Nguyen, C., Jensen, M., and Day, E. 2021. "Learning Not to Take the Bait: A Longitudinal Examination of Digital Training Methods and Overlearning on Phishing Susceptibility," *European Journal of Information Systems*), pp. 1-25.

Park, E. H., Werder, K., Cao, L., and Ramesh, B. 2022. "Why Do Family Members Reject Ai in Health Care? Competing Effects of Emotions," *Journal of Management Information Systems* (39:3), pp. 765-792.

Serenko, A. 2022. "Antecedents and Consequences of Explicit and Implicit Attitudes toward Digital Piracy," *Information & Management* (59:1), p. 103559.

Serenko, A., and Turel, O. 2020. "Measuring Implicit Attitude in Information Systems Research with the Implicit Association Test," *Communications of the Association for Information Systems* (47:1), p. 17.

Sundararajan, A. 2004. "Managing Digital Piracy: Pricing and Protection," *Information Systems Research* (15:3), pp. 287-308.

Tam, K. Y., Feng, K. Y., and Kwan, S. 2019. "The Role of Morality in Digital Piracy: Understanding the Deterrent and Motivational Effects of Moral Reasoning in Different Piracy Contexts," *Journal of the Association for Information Systems* (20:5), p. 3.

Warkentin, M., and Willison, R. 2009. "Behavioral and Policy Issues in Information Systems Security: The Insider Threat," *European Journal of Information Systems* (18:2), pp. 101-105.

Wheeler, A. R., Halbesleben, J. R., and Whitman, M. V. 2013. "The Interactive Effects of Abusive Supervision and Entitlement on Emotional Exhaustion and Co-Worker Abuse," *Journal of Occupational and Organizational Psychology* (86:4), pp. 477-496.

Wolfe, S. E., Higgins, G. E., and Marcum, C. D. 2008. "Deterrence and Digital Piracy: A Preliminary Examination of the Role of Viruses," *Social Science Computer Review* (26:3), pp. 317-333.

Yoon, C. 2011. "Theory of Planned Behavior and Ethics Theory in Digital Piracy: An Integrated Model," *Journal of Business Ethics* (100:3), pp. 405-417.

APPENDIX A – HEADER OF APPENDIX HERE

The responses for technology entitlement were recorded before the image and scenario was shown. Participants were asked to rate their perceived threat based on the scenario shown below:

> Bill works for CheaprTeez as a supply chain coordinator, CheaprTeez is a startup company that provides workers with a laptop to work from home. Bill's laptop stores all the company's payroll and personnel information. Because Bill is good at his job he is able to get all his work done quickly – finishing a few hours early every day. He is required to stay on his computer and wait to respond to emails or last second changes to orders. During workdays when Bill is finished early, there is nothing left to do so he will browse the internet and watch videos on streaming sites. As a supply chain coordinator at a start-up, Bill's pay is not high and paying for licensed streaming subscriptions (Netflix, Hulu, HBO Max, etc.) is out of his budget. For things he cannot find on the streaming services he has access to, he usually goes to unlicensed streaming sites that host lots of movies for free (like the one shown below). After a software update one day Bill finds that his firewall is blocking access to the unlicensed streaming sites he uses. Bill is able to disable this firewall to access his unlicensed streaming sites.
>
> For the following questions, look at the screenshot of the site below and answer the questions about Bill's browsing habits.