Dearden, T. E., & Gottschalk, P. (2023). Convenience theory and cybercrime opportunity: an analysis of online cyber offending. Deviant Behavior, 1-13.
https://doi.org/10.1080/01639625.2023.2246626

Convenience Theory and Cybercrime Opportunity: An Analysis of Online Cyberoffending

Thomas E Dearden

Petter Gottschalk

Abstract

The private nature of business creates opportunities for financial crimes. Convenience theory suggests that this opportunity, accompanied by a willingness and motive explains financial crimes. Newer technologies have created similar private environments, which allow for criminal behavior. For example, cryptocurrencies offer a new way of generating pseudo-anonymous financial transactions. This paper explores criminal opportunity using cryptocurrency and convenience theory. Specifically, we test each convenience dimension, opportunity, willingness, and motive using a sample of adults in the United States. We find all three dimensions explain online financial crimes. Regardless of how cryptocurrency is used, the mere purchase of cryptocurrency is related to an increase in financial cybercrimes. Further, when motive is considered as greed or need, a need is more important than greed. The use of cryptocurrency increases certain opportunities for financial crimes. This may partially be attributed to the crimes itself (e.g., pump-and-dump cryptocurrency schemes) but also to the general opportunity created through cyberspace.

Keywords: Cybercrime, Convenience Theory, Financial Crime,

Convenience Theory and Cybercrime Opportunity: An Analysis of Online Cyberoffending

Convenience theory was introduced by Gottchalk (2017) to explain corporate offending. The overall theme of convenience theory is that white collar criminals find crime as a more convenient opportunity to generate revenue or solve a problem than through other legitimate means. Convenience is divided into three areas, motive, opportunity, and willingness.

In the motive dimension of convenience theory, there are possibilities exploited by crime to satisfy greed of individuals and to achieve goals of corporations, and there are threats avoided by crime to reduce strain of individuals and to compensate for bankruptcy of corporations (Gottschalk, 2022). Cybercrime offenders that are studied in this research represent individuals as illustrated in Figure 1. The greed perspective of individuals is exemplified by people who do whatever it takes to have some of the really expensive things in life. The threat perspective is exemplified by strained people who have financial problems and thus have to deal with money problems. In the opportunity dimension of convenience theory, there are possibilities to commit and conceal crime (Gottschalk, 2022).

Cybercrime offenders that are studied in this research are individuals who have access to resources as illustrated in Figure 1. The specific resource identified is cryptocurrency, where offenders have access to digital arenas to purchase cryptocurrency. In the willingness dimension of convenience theory, there is a choice of crime and a perception of innocence among offenders (Gottschalk, 2022). As a rational choice, cybercrime can simply be worth it, on balance, and cybercrime can benefit offenders. The benefit-cost ratio can be favorable as offenders find it unlikely that they will get caught if they commit cybercrime as cybercrime is not often punished.

The benefits include that friends might think it is cool that offenders commit cybercrime. The willingness is thus dominated by rationality and learning from others as illustrated in Figure 1.

Insert Figure 1 about here

Literature Review

For white-collar offenders, the opportunity generally arises within the course of their occupation. Their specialized accessed provides them greater opportunity for crime than someone who is not within the organization (Benson & Madensen, 2007). However, some financial crimes take place outside the organization. Individuals who scam people do not need specialized access. Instead, they utilize other techniques, such as trust. Still, opportunity theories, such as routine activities theory, suggest that crime will only take place when offenders have access, in some way, to potential victims (Cohen & Felson, 1979).

Cryptocurrency

Cryptocurrency has been defined as "digital assets used as a medium of exchange" (Young et al., 2016). The most common and utilized cryptocurrency today is Bitcoin. First introduced in Satoshi Nakamoto's (likely an alias) original white paper on Bitcoin (Nakamoto, 2008). Bitcoin combines many innovations, to create a decentralized network of information. Some important elements of Bitcoin are a ledger, which stores information about the transactions and virtual locations of Bitcoin, virtual wallets, which allow for possession and protection of Bitcoins located on public facing virtual wallets, and private keys, the passcode required to show ownership and access of a virtual wallet. This model allows for the possession and transfer of

Bitcoin, creating a virtual transaction system. However, cryptocurrencies are specifically not tied to any commodity, currencies, or governments.

It is this freedom from financial institutions that cryptocurrency advocates often tout as a value. Instead of utilizing a third party for transactions (e.g., a bank), Bitcoin operates independently through a decentralized network. The transactions are instead stored on people's computers and connected through a virtual ledger. This technology limits certain forms of financial crimes while creating others. For example, a crooked employee is no longer able to divert funds from one account to another as there is no third-party involved in the transaction. However, cryptocurrency also creates criminal opportunity.

Cryptocurrency is appealing as an accessible tool in the transactions of crime. It serves as a quasi-anonymous (e.g., Bitcoin) or completely anonymous option (e.g., Monero) for financial transactions. Cybercrime is commonly associated with cryptocurrency as it serves as the currency for darknet marketplaces (Chen et al., 2019), and other forms of cybercrime such as ransomware payoffs (Paquet-Clouston et al., 2019).

In this sense cryptocurrency is a convenient opportunity for individuals to carry out cybercrime. Instead of requiring the legitimate access through organizations or positions of power, cryptocurrency serves as an opportunity for concealing the financial aspects of cybercrime. We are not the first to suggest cryptocurrency as a dimension in convenience theory. Nolasco Braaten and Vaughn (2021) analyzed U.S. federal court decisions utilize convenience theory as a framework. Here they specifically focused on cryptocurrency fraud. Given that cryptocurrency is nebulous, somewhere between a commodity and security, fraud schemes abound. These include frauds such as pump-and-dump schemes. In one cause presented by the authors,

> In Greene v. Mizuho Bank, Ltd. (2016), defendant Mizuho, a Tokyo-based bank, was motivated by the desire to continue earning service fees from processing incoming Mt. Gox wire deposits. Mt. Gox, a bitcoin exchange based in Tokyo, Japan started experiencing internal problems because (1) defendant Karpeles (President, CEO, and majority shareholder) was stealing bitcoins belonging to Mt. Gox users and (2) Mizuho was pressuring Karpeles to close the Mt. Gox bank account at Mizuho due to concerns about a U.S. investigation into money laundering on the Mt. Gox account and potential legal liability or reputational harm to Mizuho. When Karpeles refused to close the account, Mizuho stopped processing international wire withdrawals for Mt. Gox, meaning that Mt. Gox users who wired fiat currency to Mizuho could not withdraw their money. Mizuho, however, did not publicly disclose that it had stopped all international wire transfers out of the Mt. Gox account; instead, defendants continued to accept deposits, which earned revenue from service fees. The plaintiffs were U.S. residents who had wired fiat money to Mizuho for trading in Mt. Gox. After Mt. Gox filed for bankruptcy in Japan on February 28, 2014, plaintiffs could not withdraw the U.S. currency that they wired to Mizuho. Plaintiffs filed a class action lawsuit against Mizuho Bank and Karpeles, asserting claims for tortious interference with contract, unjust enrichment, fraudulent concealment, and accounting. Plaintiffs sought to recover financial losses arising from collapse and bankruptcy of the exchange. (970-971)

The stopping of processing of international wire withdrawals for Mt. Gox and the continued acceptance of deposits form MT. Gox shows the economical motive dimension of convenience theory. There were corporate profits from the service fees. Further, it is likely they perceived an opportunity through the jurisdictional issues (Mizuho bank was geographically distant from

victims in the United States). Finally, the Mizuho Bank executives were willing as they argued the issue was an error in the law rather than their fault. In this case and others the authors found general support, suggesting that cryptocurrency serves as a convenient option for cybercrime.

We sought to expand on cryptocurrency and convenience dimensions. Specifically, we wanted to empirically examine each dimension of convenience and whether convenience theory explains financial cyberoffending. This led to our two hypotheses.

H1: Non-cyberoffenders find crime less convenient than cyberoffenders.

H2: Offenders with fewer offenses find crime less convenient compared to offenders with more offenses.

Method

We used an online survey to sample U.S. adults, 18 years or older. Specifically, we fielded a survey using a paid vendor, Dynata. Dynata is a leader in sampling with more than 100 million surveys completed annually. The company acquires lists of participants and creates representative sampling pools based on criteria from the client. Participants complete surveys for small monetary rewards. To ensure data quality Dynata uses machine learning checks via Imperium's QualityScore^{TM}. In addition, participants who speed through the survey who do not complete enough questions were excluded by the authors.

Survey

The survey was part of a larger project and includes several components. First, we obtained ethical approval as required by the lead author's institutional review board (IRB). The first set of questions following ethical approval was a series of demographics questions to help balance the survey in regards to U.S. Census data. Second, several questions about computer use,

offending, and victimization were asked. Finally, a set of scales about criminological questions were asked. Overall, the survey averaged 14 minutes. The survey was built in Questionpro and deployed between April 8, 2022 and April 20, 2022.

Participants

The survey was sent to U.S. adults aged 18 years or older. A total of 1,624 participants started the survey. Of these, 58 did not complete the IRB question (and were removed from the survey) and 172 participants either did not complete the rest of the survey or sped through the questions and were removed. This yielded an overall potential survey of 1,394 participants. We note that no individual question was required, and thus individual models below may include fewer participants if an individual did not complete a question.

The sample yielded similar results to U.S. Census data. While we did not ask race-related questions (due to similar surveys being fielded in non-U.S. countries and having data restrictions) we did ask a series of other demographic questions. For a complete breakdown of demographic variables see table 1. Our sample included roughly equal male and female populations (49.4% and 49.8% respectively). The average age of our participants was 45.9 and range was 18-88. Our sample had slightly higher education compared to U.S. averages, with 31% having a college degree and 16.8% having a professional degree, master's degree, or PhD.

Insert Table 1 about here

Measures

Our key dependent variable was financial cyber offending. We were interested in how many unique types of cybercrimes participants admitted to doing in the past 12 months. Given our focus on adapting the theory of convenience, originally created for financial crimes, we focused only on crimes that can be financially motived. Specifically, these behaviors were, hacking into an unauthorized area of the internet, distributing malicious software, illegally downloading copyrighted files, illegally uploading copyrighted files, and using someone else's personal information on the internet without their permission (i.e., identity theft). Our measure was simply a count of how many of these offenses the participants admitted to. The range was 0-5, where 0 was the most common and represented no cyberoffending over the past 12 months and 5 indicated that they had committed all forms of cyberoffending within the past 12 months.

Unsurprisingly, the majority of people did not admit to having committed a cybercrime in the past 12 months. 272 (19.51%) individuals admitted to at least one cyberoffense. The most common offense was illegally uploading copyrighted files or programs (9.8%) and the least common was hacking into an unauthorized area of the internet (7.9%). For a breakdown of each crime see table 2.

Our independent measures were related to convenience theory. Given that there are numerous possibilities for all aspects of convenience theory, we focused on ones which are most likely in the cybercrime. Specifically for motive we looked at financial need and greed, for opportunity we looked at cryptocurrency use, and for willingness we looked at cybercrime rationalization.

In convenience theory motive is the factors which drive the individual to believe they need to commit crime. In our instance we were focused on a single measurement of possibilities

and threats. For threat, we looked generally at financial problems in the past. Specifically, we asked if they "had to deal with money problems" in the past 12 months. This was measured at a binary variable, yes or no. 545 (42.2%) of our sample reported having to deal with money problems in the past 12 months. For possibilities we asked about their desire, on a five-point Likert scale whether they agreed or disagreed with, "I intend to do whatever it takes to have some of the really expensive things in life." The range for this question was 1-5 with a mean of 2.5 and a standard deviation of 1.3.

Consistent with the theme of this paper we were interested in cryptocurrency as an opportunity for cyberoffending. As such, we utilized a three-point nominal measure of cryptocurrency use. Whether they have purchased cryptocurrency, with the possible outcomes of no, yes – as an investment opportunity, and yes – as a way to purchase goods or services. Within our sample 885 (65.0%) reported not having purchased cryptocurrency. This leaves 333 (24.5%) who purchased cryptocurrency as an investment opportunity and 144 (10.6%) as a way to purchase goods or services.

Finally, Willingness was measured using series of five questions about their belief on cybercrime. These included, committing cybercrime is "worth it", on balance, cybercrime benefits me, generally, I am unlikely to get caught if I commit cybercrime, Cybercrimes are not often punished, and my friends think it is cool that I commit cybercrime. We summated each question, creating a willingness scale. This scale had a mean of 8.65 and a standard deviation of 4.22. See table 2 for a descriptive breakdown of all independent and dependent variables.

Insert Table 2 about here

Results

To test hypothesis one, we utilize a logistic regression to compare individuals who did not offend against individuals who had one or more offenses. For results of all logistics regression see table 3. In our first regression we only used the primary dependents variables. All variables, except possibility - motive were significant at the $p<.001$ level. Using odds ratios, we find that cryptocurrency, both investment and purchase goods and services, increase the likelihood of having committed a cybercrime in the past 12 months by a factor of 2.75. Our motive – threat variable, based on financial trouble in the past, also strongly increased the likelihood of having committed a cyberoffense in that past 12 months (OR=2.29). Finally, our willingness scale was also in the expected direction (OR=1.38). Our motive – possible variable, measured by a willingness to do whatever it takes to get the finer things in life, was not significant. In addition, it was in the opposite direction as expected.

A second model was run to include common demographic variables in addition to the dependent variables. While the dependent variables slightly changed, with cryptocurrency p-values and odds ratios slightly decreasing, everything remained significant with large odds ratios. Of particular interest were the demographic variables. Unexpectedly, gender was not significant. However, Age, Income, and Education were significant ($p<.001$, $p=.021$, $p=017$ respectively). As age and education increased cyberoffending decreased while as income increased cyberoffending increased.

Insert Table 3 about here

To test our second hypothesis, we revised the dependent variable. We dropped all individuals who did not participant in at least one cyberoffense. For the second hypothesis we were concerned with who commits more cybercrimes. We utilized a count variable of the diversity of cybercrime committed in the past twelve months. The range was 1-5, where 1 was an individual who committed only one cybercrime and 5 was an individual who committed all 5 types of measured cyberoffenses.

With this revised version of the dependent variable, we utilized a negative binomial regression, repeating the same procedure as used in hypothesis 1. For a complete breakdown of the two negative binomial regressions see table 4. In this instance only one variable was significant at the $p<.05$ level, motive threat. Participants who reported having financial struggles in the past averaged a higher number of cyberoffenses within the past 12 months. The addition of the demographic variables did increase the p-value of this association to greater than $p=.05$. The only significant variable associated with a greater number of cybercrimes was age. In this case, age is positively associated with number of cyberoffenses within the past 12 months.

Discussion

Our first hypothesis was largely supported. All aspects of convenience theory were associated with an increased likelihood of committing a cyberoffense. In addition, effect sizes were rather high with substantial odds ratios (see table 3). In each category, motive, opportunity, and willingness, at least one subset of variables was significant. Only motive-threat was not significant. While there are numerous possibilities as to why, we believe that this was a measurement issue. There are numerous possibilities of measuring motive. We utilized two, one in the threat category (financial strain) and one in the possibilities category (financial want). It

could be that the question measuring want, that someone is willing to do whatever it takes to have the finer things in life, was not sufficient in measuring possibilities. For example, many people are willing to do whatever it takes to have the finer things in life, but only individuals who are unable to achieve success through legitimate means (e.g., a high paying job) would consider crime as crime carries its own set of risks.

One novel aspect of our study was expanding the understanding of convenience theory to address opportunity beyond the veil of organizations. Instead, we considered the use of cryptocurrency to create opportunity. In some ways this is obvious, an individual attempting to buy drugs online is generally required to utilize cryptocurrency. The association between cryptocurrency and cybercrime purchases (e.g., purchasing illegal software such as viruses or ransomware) is therefore part of the process. However, we want to further add to this notion by suggesting that cryptocurrency is used in the spaces in which cybercrime operates. This can be seen in our data. Any form of cryptocurrency use was associated with an increase in cyberoffending. This not only includes utilizing cryptocurrency as a tool to purchase a product or good, but purchasing cryptocurrency as an investment. Instead of just a tool for purchasing illegal goods, we believe that cryptocurrency is highlighting the opportunity, through participation in online spaces, which provides an avenue for cybercrime. We see potential ties to situational opportunity theories, such as routine activities theory (Cohen & Felson, 1979) or crime pattern theory (Clarke & Cornish, 1985). Rather than a physical space being the environment in which routines happen, cyberspace has now offered a digital environment in which crime can take place (Choi, 2008)

Our second hypothesis was not supported. Utilizing only individuals who had committed at least one cybercrime, we failed to find any strong association between our dependent variables

or our demographics. The only consistent association was age, where the older the individual was the more likely they were to have committed more cyberoffenses. While this is generally inconsistent with some general crime literature, such as street crime, we think it makes sense in the context of cybercrime. The diversity of cybercrimes measured lead to some degree of needed computer knowledge to commit said crimes. Having the knowledge to hack into unauthorized spaces, commit identity theft, distribute malicious software, and pirate material would require a working knowledge of several different areas of computers including networks, operating systems, internet of things (IOT), and cybersecurity. This will require time for an individual to learn these skills.

The development of most criminological theories stem from street crime. Given that that cyberspace is a relatively new concept, much work has been done to see how traditional criminological theories work in cyberspace. These are diverse and include routine activities theory (Choi, 2008; Graham & Triplett, 2017; Hawdon et al., 2019; Leukfeldt, 2015; Reyns, 2013), social learning theories (Al-Garadi et al., 2016; Dearden & Parti, 2021; Holt et al., 2010; Weulen Kranenbarg et al., 2021) self-control (Donner, 2016; Holt et al., 2018; Kerstens & Jansen, 2016; Reisig et al., 2009) neutralization (Brewer et al., 2020; Chua & Holt, 2016; Holt et al., 2019; Nolasco Braaten & Vaughn, 2021) anomie and strain (Dearden et al., 2021; Hay & Ray, 2020; Hutchings & Collier, 2019) critical criminology (McCarthy & Steinmetz, 2020; Owen & Marshall, 2020) and others. However, convenience theory has only received scant attention (Gottschalk & Hamerton, 2022). We offer an empirical test of convenience theory, additionally considering cryptocurrency as a new opportunity for offenders.

Our paper offers several contributions to the literature. First, convenience theory suggests that offenders will only commit crimes if they see them as convenient amongst the options

visible to them (Gottschalk, 2017). While this theory is generally applied in the context of white-collar crime, we extend the convenient notion to cybercrime. Certainly, committing crime without leaving one's own home is the epitome of convenient. This theory can help explain why we have seen a general increase in the volume of cybercrime taking place. For example, the National Gang Intelligence Center (2011) released a bulletin in 2011 suggesting that gangs were utilizing tax fraud as a source of income. One can easily see how filling out tax forms and receiving return checks is an easier and more convenient criminal option that traditional street crime, such as selling drugs.

Part of the convenience is that the opportunities for cybercrime are occurring in virtual spaces. We empirically assessed one of these virtual spaces, cryptocurrency. While there are direct ties to cryptocurrency and cybercrime, through illegal purchases, there are also indirect ties. In our research we found that purchasing cryptocurrency as a tool for investing led to an increased likelihood of cyberoffending. We suggest that operating in the cyberspaces with cryptocurrency leads to opportunity for cybercrime, much like being in a geographic region high in crime or vices increases the opportunity for crime.

We also offer additional insight in the both the willingness and motive for cybercrime. We assess each empirically. First, we discover that a threat motive is more important than a possibility motive. Financial issues within the past 12-months led to an increased chance of having committed a cyberoffense by a factor of 2.29. We also discover that willingness to commit cybercrime is a risk factor for cyberoffenses.

Although not part of our research question or hypotheses, we also should address the findings from the demographic variables. We find that age, income, and education all correlate with cyberoffending. Both age and education are negatively correlated, indicating a decrease in

cyberoffending as age increases and higher educational attainment. While educational attainment is consistent in literature generally about crime, age has mixed results and appears to depend, at least in part, on the type of cybercrime being committed. For example, the typical digital privacy offender was younger than 19 (Hinduja & Higgins, 2011) whereas the average international male cyber offender was 35 and the average female international cyber offender was 45 (Hadzhidimova & Payne, 2019). As a predictor, age has been mixed (e.g., Weulen et al, 2019 for null results, Hawdon et al., 2020 for positive results). Finally, income was positively correlated with cyberoffending. This certainly brings into question the exact nature of feeling a financial threat. We suggest that the threat, having experienced a financial strain in the past 12 months, is relative. It could be that a high-income earner experiences a threat when they struggle to maintain their lifestyle. This does not mean that they struggle to have the basic necessities, but they struggle to maintain the standard which they are accustomed to. This seems to be consistent with literature on strain, where relative strain is more important than absolute strain (Zhou et al., 2019).

Limitations

Each dimension of convenience, motive, opportunity, and willingness could have been measured using additional or different variables. The conceptualization of each area of the theory provides numerous operationalization opportunities. As such, as some point we had to pick what is most likely in cybercrime. A different paper operationalizing any of the dimensions differently may yield different results. We encourage other authors to consider other potential combinations of the dimensions of convenience and how they can empirically assess said theory.

The choice of our dependent variable, a series of potential financial cybercrimes was also carefully considered. One could argue that any of these cybercrimes could be done for a

multitude of reasons, including personal consumption, boredom, and revenge. However, each crime fits as part of the cybercrime as a service notion (Manky, 2013), where cybercrime has become a commodity to buy and sell. For example, online vendors not only sell drugs, but also the malware needed to infect victims' computers.

Our survey methodology, especially our use of online sampling carries limitations. While some studies find that online polling yield similar results to more rigorous random sampling (e.g., Weinberg et al., 2014; Simmons & Bobo, 2015; MacInnis et al., 2018) others find non-probability online sampling to be less reliable (e.g., Einarsson et al., 2022; Lehdonvirta et al., 2021; Pickering & Blaszczynski, 2021). Consistent with prior data as well, our study showed a slight propensity for higher educated and higher income brackets than the average U.S. sample (Singer & Kulka, 2002).

Conclusion

The potential profile of a cyberoffender emerges from this research. First, the motive is threats rather than possibilities. Threats are associated with urgency, difficulty, and high stakes. Threats involve a negative situation in which loss is likely and over which one has relatively little control. Strains from threats most likely to result in crime are those seen as unjust and high in magnitude. Strains are events and conditions that individuals dislike. Strains lead to negative emotions and thereby create pressure for corrective action. Crime is one possible action. Sources of strain include failure to achieve inspiration, failure to achieve aspiration, and failure to achieve fair and just outcome. Individuals who suffer such failures that increase their reflected appraisal, will tend to commit crime because they want to reclaim their power of advantage.

Second, the opportunity is to commit rather than to conceal wrongdoing. The opportunity to commit derives from access to resources. A resource is an enabler applied and used to satisfy

human needs. A resource has utility and limited availability. The cyberoffender has access to resources that are valuable (application of the resource provides desired outcome), unique (very few have access to the resource), not imitable (resource cannot be copied), not transferable (resource cannot be released from context), combinable with other resources (results in better outcome), exploitable (possible to apply in criminal activities), and not substitutable (cannot be replaced by a different resource). Access to resources equates access to power.

Third, the willingness is based on rationality and learning. The rational choice assumption about offending is based on a normative foundation where advantages and disadvantages are subjectively compared. When there is no perceived likelihood of detection, then there is no deterrence effect to prevent offences. If there is a certain perceived likelihood, then willingness might depend on the perceived consequences. Learning is an outcome of differential association where the cyberoffender makes a decision to associate with those who agree with him or her, and distance himself or herself from those who disagree. This perspective suggests that whether individuals engage in crime or not depends on their socialization within certain peer groups.

Financial crimes are often conducted under within the shroud of a private organization. However, online environments have created similar opportunities for newer financial crimes. We show that cryptocurrency can create opportunity for financial cybercrimes. Using convenience theory, we find that all aspect of convenience also empirically explains online financial crimes. Our results support and extend the validity of convenience theory.

References

Al-Garadi, M. A., Varathan, K. D., & Ravana, S. D. (2016). Cybercrime detection in online communications: The experimental case of cyberbullying detection in the Twitter network. *Computers in Human Behavior*, *63*, 433–443. https://doi.org/10.1016/j.chb.2016.05.051

Benson, M. L., & Madensen, T. D. (2007). Situational crime prevention and white-collar crime. In *International handbook of white-collar and corporate crime* (pp. 609–626). Springer.

Brewer, R., Fox, S., & Miller, C. (2020). Applying the Techniques of Neutralization to the Study of Cybercrime. In *The Palgrave handbook of international cybercrime and cyberdeviance* (pp. 547–565). Springer.

Chen, X., Hasan, M. Al, Wu, X., Skums, P., Feizollahi, M. J., Ouellet, M., Sevigny, E. L., Maimon, D., & Wu, Y. (2019). Characteristics of Bitcoin Transactions on Cryptomarkets. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *11611 LNCS*, 261–276. https://doi.org/10.1007/978-3-030-24907-6_20

Choi, K. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology*, *2*(1).

Chua, Y. T., & Holt, T. J. (2016). A cross-national examination of the techniques of neutralization to account for hacking behaviors. *Victims & Offenders*, *11*(4), 534–555.

Clarke, R. V, & Cornish, D. B. (1985). Modeling offenders' decisions: A framework for research and policy. *Crime and Justice*, *6*, 147–185.

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, *44*(4), 588–608. https://doi.org/10.2307/2094589

Dearden, T. E., & Parti, K. (2021). Cybercrime, differential association, and self-control: knowledge transmission through online social learning. *American Journal of Criminal Justice*, *46*(6), 935–955.

Dearden, T. E., Parti, K., & Hawdon, J. (2021). Institutional Anomie Theory and Cybercrime—Cybercrime and the American Dream, Now Available Online. *Journal of Contemporary Criminal Justice*, *37*(3), 311–332.

Donner, C. M. (2016). The Gender Gap and Cybercrime: An Examination of College Students' Online Offending. *Victims and Offenders*, *11*(4), 556–577. https://doi.org/10.1080/15564886.2016.1173157

Einarsson, H., Sakshaug, J.W., Cernat, A., Cornesse, C., & Blom, A.G. (2022). Measurement equivalence in probability and nonprobability online panels. International Journal of Market Research, 64(4), 484-505. https://doi.org/10.1177/14707853221085206

Gottschalk, P. (2017). Convenience in White-Collar Crime: Introducing a Core Concept. *Deviant Behavior*, *38*(5), 605–619. https://doi.org/10.1080/01639625.2016.1197585

Gottschalk, P., & Hamerton, C. (2022). Online Convenience. In *White-Collar Crime Online* (pp. 37–61). Springer.

Graham, R., & Triplett, R. (2017). Capable Guardians in the Digital Environment: The Role of Digital Literacy in Reducing Phishing Victimization. *Deviant Behavior*, *38*(12). https://doi.org/10.1080/01639625.2016.1254980

Hadzhidimova, L. I., & Payne, B. K. (2019). The profile of the international cyber offender in the US. *International journal of cybersecurity intelligence & cybercrime*, *2*(1), 40-55.

Hawdon, J., Bernatzky, C., & Costello, M. (2019). Cyber-Routines, Political Attitudes, and Exposure to Violence-Advocating Online Extremism. *Social Forces*, *98*(1), 329–354.

https://doi.org/10.1093/sf/soy115

Hawdon, J., Parti, K., & Dearden, T. E. (2020). Cybercrime in America amid COVID-19: The initial results from a natural experiment. *American Journal of Criminal Justice*, *45*(4), 546-562.

Hay, C., & Ray, K. (2020). General Strain Theory and Cybercrime. In T. J. Holt & A. M. Bossler (Eds.), *Palgrave Handbook of International Cybercrime* (pp. 583–597).

Hinduja, S., & Higgins, G. E. (2011). Trends and patterns among music pirates. Deviant Behavior, 32(7), 563-588.

Holt, Thomas J., Burruss, G. W., & Bossler, A. M. (2010). Social learning and cyber-deviance: Examining the importance of a full social learning model in the virtual world. *Journal of Crime and Justice*, *33*(2), 31–61. https://doi.org/10.1080/0735648X.2010.9721287

Holt, Thomas J., van Wilsem, J., van de Weijer, S., & Leukfeldt, R. (2018). Testing an Integrated Self-Control and Routine Activities Framework to Examine Malware Infection Victimization. *Social Science Computer Review*, 089443931880506. https://doi.org/10.1177/0894439318805067

Holt, Thomas J, Brewer, R., & Goldsmith, A. (2019). Digital drift and the "sense of injustice": Counter-productive policing of youth cybercrime. *Deviant Behavior*, *40*(9), 1144–1156.

Hutchings, A., & Collier, B. (2019). Inside out: Characterising cybercrimes committed inside and outside the workplace. *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 481–490.

Kerstens, J., & Jansen, J. (2016). The Victim–Perpetrator Overlap in Financial Cybercrime: Evidence and Reflection on the Overlap of Youth's On-Line Victimization and Perpetration. *Deviant Behavior*, *37*(5). https://doi.org/10.1080/01639625.2015.1060796

Lehdonvirta, V., Oksanen, A., Räsänen, P., & Blank, G. (2021) Social media, web, and panel surveys: Using non-probability samples in social and policy research. Policy & Internet, 13(1), 134-155. https://doi.org/ 10.1002/poi3.238

Leukfeldt, E. R. (2015). Comparing victims of phishing and malware attacks Unraveling risk factors and possibilities for situational crime prevention. *International Conference on Cyber Security*, 1–7. http://arxiv.org/abs/1506.00769

MacInnis, B., Krosnick, J. A., Ho, A. S., & Cho, M. J. (2018). The accuracy of measurements with probability and nonprobability survey samples: Replication and extension. Public Opinion Quarterly, 82(4), 707-744. https://doi.org/10.1093/poq/nfy038

Manky, D. (2013). Cybercrime as a service: a very modern business. *Computer Fraud & Security*, *2013*(6), 9-13.

McCarthy, A. L., & Steinmetz, K. F. (2020). Critical Criminology and Cybercrime. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 601–621). Springer.

Nakamoto, S. (2008). Re: Bitcoin P2P e-cash paper. *The Cryptography Mailing List*.

Nolasco Braaten, C., & Vaughn, M. S. (2021). Convenience Theory of Cryptocurrency Crime: A Content Analysis of U.S. Federal Court Decisions. *Deviant Behavior*, *42*(8), 958–978. https://doi.org/10.1080/01639625.2019.1706706

Owen, T., & Marshall, J. (2020). *Rethinking Cybercrime: Critical Debates*. Springer.

Paquet-Clouston, M., Haslhofer, B., & Dupont, B. (2019). Ransomware payments in the bitcoin ecosystem. *Journal of Cybersecurity*, *5*(1), tyz003.

Pickering, D. & Blaszczynski, A. (2021): Paid online convenience samples in gambling studies: Questionable data quality. International Gambling Studies, 21(3), 516-536.

https://doi.org/10.1080/14459795.2021.1884735

Reisig, M. D., Pratt, T. C., & Holtfreter, K. (2009). Perceived risk of internet theft victimization: Examining the effects of social vulnerability and financial impulsivity. *Criminal Justice and Behavior*, *36*(4), 369–384. https://doi.org/10.1177/0093854808329405

Simmons, A. D., & Bobo, L. D. (2015). Can non-full-probability internet surveys yield useful data? A comparison with full-probability face-to-face surveys in the domain of race and social inequality attitudes. Sociological Methodology, 45(1), 357—387. https://doi.org/10.1177/0081175015570096

Singer, E., & Kulka, R. A. (2002). Paying respondents for survey participation. In M. V. Ploeg, R. A. Moffitt, & C. F. Citro (Eds.), Studies of welfare populations: Data collections and research issues. (pp. 105-129) National Academy Press.

Reyns, B. W. (2013). Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses. *Journal of Research in Crime and Delinquency*, *50*(2), 216–238. https://doi.org/10.1177/0022427811425539

Weinberg, J. D., Freese, J., & McElhattan, D. (2014). Comparing data characteristics and results of an online factorial survey between a population-based and a crowdsource-recruited sample. Sociological Science, 1(19), 292—310. https://doi.org/10.15195/v1.a19

Weulen Kranenbarg, M., Holt, T. J., & Van Gelder, J. L. (2019). Offending and victimization in the digital age: Comparing correlates of cybercrime and traditional offending-only, victimization-only and the victimization-offending overlap. *Deviant Behavior*, *40*(1), 40-55.

Weulen Kranenbarg, M., Ruiter, S., & Van Gelder, J. L. (2021). Do cyber-birds flock together? Comparing deviance among social network members of cyber-dependent offenders and

traditional offenders. *European Journal of Criminology*, *18*(3), 386–406. https://doi.org/10.1177/1477370819849677

Young, M. D., Donley, M. A., Rubin, G. A., & Kneller, T. M. (2016). *Bitcoins and the Blockchain : The CFTC Takes Notice of Virtual Currencies Bitcoins and the Blockchain : The CFTC Takes Notice of Virtual Currencies*. https://www.skadden.com/-/media/files/publications/2016/01/bitcoinsandtheblockchainthecftctakesnoticeofvirtua.pdf

Zhou, Q., Zhang, J., & Hennessy, D. A. (2019). The role of family absolute and relative income in suicide among Chinese rural young adults: Mediation effects of social support and coping strain. *Journal of Public Health*, *41*(3), 609–617.

Figure 1: Convenience themes for cybercrime

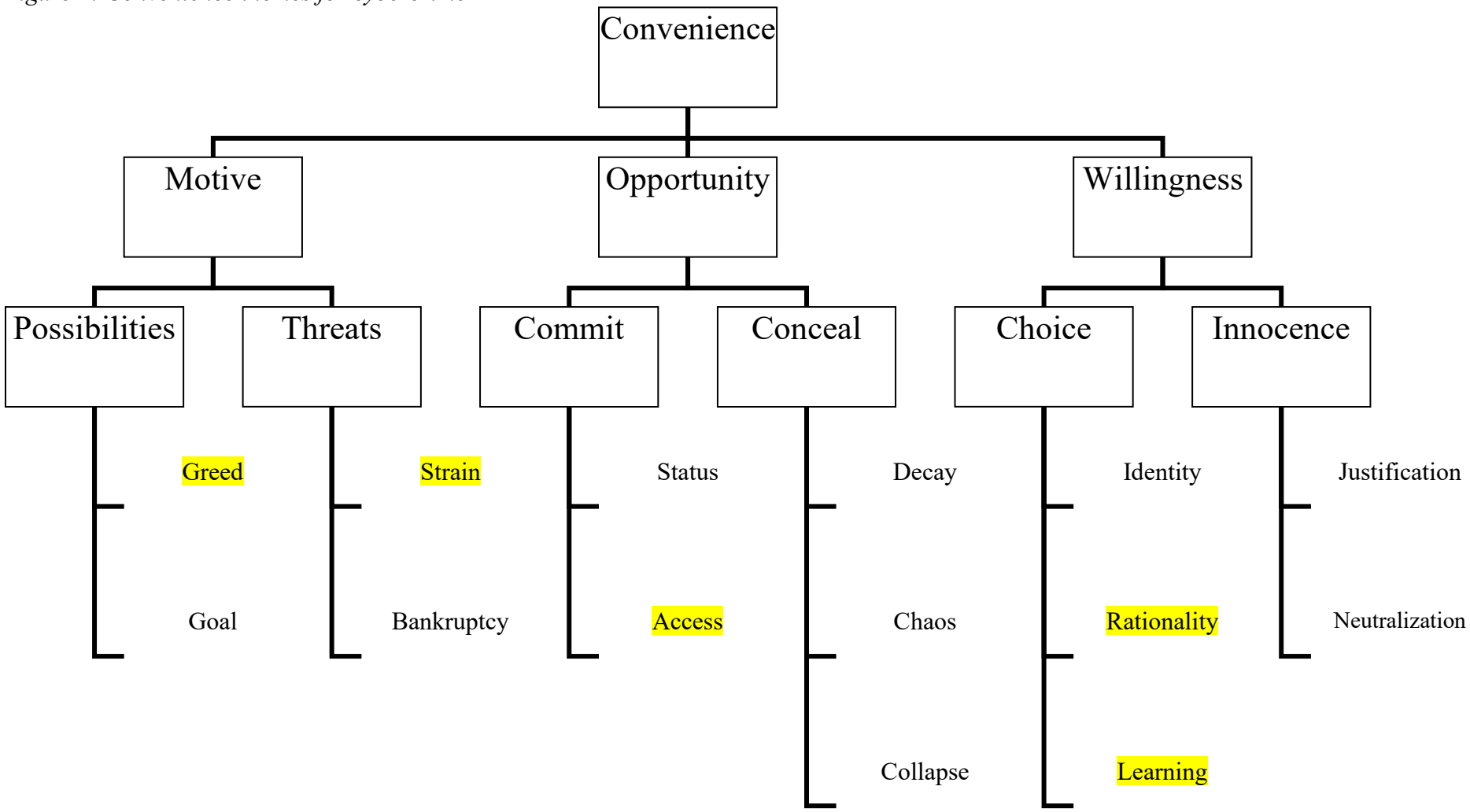

Table 1: Demographic Variables

Gender	Male	Female	LGBTQ/Non-Binary	No answer			
	683 (49.4%)	688 (49.8%)	5 (.4%)	7 (0%)			
Education	Less than High School	High School	Some College	College Degree	MA/ Professional/ PhD		
	65 (4.7%)	647 (25.1%)	311 (22.5%)	428 (31.0%)	232 (16.8%)		
Household Income	< $25k	$25k-$50k	$50k-$75k	$75k-$100k	$100k-$150k	$150k-$250k	>$250k
	273 (20.6%)	295 (22.2%)	235 (17.7%)	181 (13.6%)	199 (15.0%)	105 (7.1%)	40 (3.0%)
Age	Mean	Median	SD	Min	Max		
	45.9	43	17.5	18	88		

Table 2: Independent and Dependent Variables

Dependent Variable (Sum of Below)	Yes	No
Hacked into an unauthorized area of the internet	108 (7.9%)	1,262 (92.1%)
Distributed malicious software	127 (9.3%)	1,237 (90.7%)
Illegally downloaded copyrighted files or programs	131 (9.6%)	1,234 (90.4%)
Illegally uploaded copyrighted files or programs	133 (9.8%)	1,230 (90.2%)
Used someone else's personal information on the internet without their permission	126 (9.2%)	1,243 (90.8%)
Independent Variables		
Motive Threat	545 (42.2%)	746 (57.8%)
Cryptocurrency Purchase - None	885 (65.0%)	
Cryptocurrency Purchase - Investment	333 (24.5%)	
Cryptocurrency Purchase – Goods or Service	144 (10.6%)	
	Mean	SD
Willingness	8.65	4.22
Motive Possible	2.53	1.29

Table 3: Logistics Regression Predicting Cybercrime

	Theory Model				Full Model			
Variable	*B*	*SE(B)*	*p*	OR	*B*	*SE(B)*	*p*	*OR*
Crypto Investment*	1.01	.22	<.001	2.75	.75	.34	.002	2.12
Crypto Purchase*	1.01	.29	<.001	2.75	.76	.31	.014	2.13
Motive Threat	.83	.19	<.001	2.29	.81	.21	<.001	2.25
Motive Possible	-.03	.09	.719	.97	-.12	.09	.192	.89
Willingness	.32	.03	<.001	1.38	.31	.03	<.001	1.36
Gender (Male)					-.13	.20	.535	.88
Age					-.04	.01	<.001	.96
Income					.16	.07	.021	1.17
Education					-.25	.10	.017	.78
Constant	-5.57	.33	<.001	.00	-3.08	.51	<.001	.046
Pseudo R^2	.35				.39			
LR Chi^2	411 (n=1,231)				464 (n=1,154)			

Notes: *Base comparison was no cryptocurrency purchase

Table 4: Negative Binomial Regression Predicting Cybercrime Volume

	Theory Model				Full Model			
Variable	*B*	*SE(B)*	*p*	OR	*B*	*SE(B)*	*p*	*OR*
Crypto Investment*	-.18	.11	.113	.83	-.17	.12	.156	.84
Crypto Purchase*	-.12	.13	.371	.89	-.09	.14	.541	.92
Motive Threat	.18	.09	.047	1.19	.16	.09	.075	1.18
Motive Possible	.05	.04	.187	1.06	.06	.04	.134	1.07
Willingness	.02	.01	.089	1.02	.02	.01	.157	1.02
Gender (Male)					-.07	.09	.476	.94
Age					.01	.00	.040	1.00
Income					.05	.03	.072	1.05
Education					-.08	.04	.075	.92
Constant	.53	.18	.003	1.70	.33	.24	.180	
Pseudo R^2	.02				.03			
LR Chi^2	14 (n=196)				20 (n=193)			

Notes: *Base comparison was no cryptocurrency purchase