Malcolm Langford, Amelia Svensson, and Tone Wærstad

31 Identify theft

Abstract: Digital identity theft occupies an important place in digital criminology. The proliferation of new identification technologies and ongoing digitalization of the market and state has created a plethora of opportunities for this form of cybercrime. Scholarship on digital identity theft has grown significantly, but there is significant variation in how digital identity theft is defined, mapped, and explained, resulting in sharp divergences over how it should be tackled. In this brief entry, we conceptualize and define the phenomenon, discuss its nature, contrast competing theoretical explanations (victim-centric, offender-centric, and relational), and conclude with a discussion on policy implications and future research.

Keywords: identity theft, digital victimization, identity fraud, routine activity theory, relational cybercrime

Digital identity theft occupies an important place in digital criminology. The proliferation of new identification technologies and ongoing digitalization of the market and state has created a plethora of opportunities for this form of cybercrime (Kjørven, 2020). In 2021, it was estimated that digital identity theft cost American consumers a total of $52 billion, and burdened finance institutions with more than $200 billion in extra costs through fines, reimbursement, and security initiatives (Camplisson, 2022). In Europe, Asia, and Latin America a greater proportion of the population is affected, but the overall losses tend to be lower (Experia, 2022; ICF-SA, 2022). The advent of artificial intelligence is also raising concerns, given the reported effectiveness of machine learning-based methods in carrying out identity theft (Signicat, 2024).

Within cybercrime research, scholarship on digital identity theft has grown significantly (Bossler and Berenblum, 2019). However, there is significant variation in how digital identity theft is defined, mapped, and explained, resulting in sharp divergences over how it should be tackled. In this chapter, we conceptualize and define the phenomenon, discuss its nature, contrast competing theoretical explanations, and conclude with a discussion on policy implications and future research.

Disclaimers and acknowledgments: The chapter is written as part of the SODI project (Societal Security and Digital Identities), financed by the Research Council of Norway (project no. 320785). The authors would like to thank the editors and Marte Kjørven for comments on an earlier version.

 https://doi.org/10.1515/9783111062037-032

Conceptualizing identity theft

The concept of identity theft, whether digital or analog (see Digital by Wernimont), is multivalent. It has been understood and operationalized in numerous ways. In essence, the core difference is between approaches that focus on 'theft-*of*-identity' (i. e., criminal adoption, use, or trading of an identity) and 'identity-*for*-theft' (i. e., the use of identity for other crime). Following Koops and Leenes (2006), a common approach is to delineate as follows:

– *identity-related crime* (e. g., deletion or changing of an identity);
– *identity fraud* (fraud committed with identity as a target or principal tool); and
– *identity theft* (fraud or other unlawful activity in which an identity is used without consent)

The former two approaches put weight on 'theft-of-identity,' while the latter emphasizes 'identity-for-theft.'

This latter and specific approach—identity theft—is the basis of many formal definitions of digital identify theft. For example, the OECD (2009: 16) defined it as when a party without authority "acquires, transfers, possesses, or uses personal information" in connection with fraud or other crimes. Despite such clarifications, public and scholarly discourse is not always consistent, and identity theft is commonly used for all three categories (Golladay, 2020: 982).

To further complicate matters, identity theft is defined sometimes as a distinct legal offense. For instance, the US Identity Theft and Assumption Deterrence Act (title 18, s. 1028(a)(7) U.S.C.) provides that it occurs when a person who:

> [K]nowingly transfers or uses, without lawful authority, of a *means of identification* of another person with the intent to commit, or to aid or abet, *any unlawful activity* that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.

A similar legal definition can be found in Norway (section 202, Criminal Law Act) and an increasing number of states have created a specific offence (ICF-SA, 2022). Yet, legal clarity does not necessarily contribute to conceptual clarity. These legal definitions are both broad in their conception of identity theft (it could cover any of the above analytical categories) and narrow (by creating a specific subsidiary or residual crime of identity theft that comes in addition to the primary crime). Thus, it is important to avoid conflation of criminological and legal conceptions where they co-exist.

Finally, there is a question of what distinguishes *digital* identity theft from its *analog* cousin. Identity theft is nothing new under the sun. It simply metamorphizes with each new technological development, which has been helped by the expansion of the number of digital identities, such as electronic identity devices, usernames, logins, emails, passwords, and biometric data. The idea of digital identity theft emerged as a distinct criminological category as computers and digitalization transformed significantly the nature of the crime. It is thus most commonly invoked in situations where

the *end goal* for the misuse of identity is achieved through *digital means*, e. g., where an electronic identity device of another person is used to apply for a loan or social security benefits or gain access to a social media account to engage in criminal hate speech or blackmail (see Hate Crime and Networked Hate by Powell, Stratton, and Cameron). However, when digital identity misuse is only a *precursor* to the primary crime, it is less clear. In romance fraud, for instance, an offender will often use digital means to steal or fake an identity, but it is the victim themselves that provides, physically or digitally, the benefits, such as sending money or transferring assets (Cross and Layt, 2022). Romance fraud can be thus best understood as a digital identity-related crime.

For the purposes of this essay, we focus on the core of digital identity theft: fraud or other unlawful activity in which an identity is used digitally without consent.

Nature of identity theft

A solid body of scholarly and gray literature has sought to chart the nature of digital identity theft through representative surveys and convenience samples. Besides a focus on temporal variation (Burnes et al., 2020), this research allows cross-sectional insight into the victims of digital identity theft. While there tends to be no overall gender divide (Golladay, 2020; Brataas et al., 2022), most studies show that higher income groups are more at risk (Golladay, 2020). Although, some surveys have shown that low-income groups in high-income countries are also at risk (Williams, 2016).

Younger to middle-aged persons (between the ages of 25 and 54) tend to report more often that they have been victims. This is possibly because they are both financially and digitally active. However, there are questions over the representativity of the survey data given that children are excluded. Some scholars argue that children are the most vulnerable group as many parents inappropriately access their accounts and assets (Navarro and Higgins, 2017).

Survey data on the nature of offenders is less illuminating. Many victims are not aware of the identity of the offender or are too embarrassed or afraid to reveal it. Early US studies indicated that at least a quarter of victims knew the identity of the offender, who was a family member, acquaintance, or work colleague (Newman and McNally, 2005). In the United States, some scholars have examined reports to police and prosecutions to study offenders, and found that minority groups, younger people, and women were more commonly represented compared to physical crimes (Golladay, 2020). However, there is a risk of selection bias, as these groups (especially the former) may be (1) overrepresented in the criminal justice system due to discrimination (Brunson and Weitzer, 2009) and (2) more likely to commit 'low-tech' identity theft (e. g., stealing personal information or 'dumpster diving'—sorting through a victim's trash) —which is easier for police to detect and prosecute than 'high-tech' identity theft (e. g., hacking into websites, purchasing lists of personal information).

Turning to the effects of digital identity theft on victims, the impact is both material and non-material. The direct financial costs tend to be higher on average than

property and violent crime (Golladay, 2020: 987–988), and may be borne by a victim and/or financial institution. Resolving a digital theft incident can involve also significant time costs for all affected, which may be compounded by second-order effects. Victims report having to borrow money, change jobs/housing, and make lifestyle changes, and encountering denial of future credit, service cut-offs, and bankruptcy (ITRC, 2018). As to non-material costs, studies reveal emotional symptoms (depression, anger, anxiety), physical symptoms (headaches, trouble sleeping, high blood pressure), and challenges with trust (Golladay and Holtfreter, 2017). ITRC (2023) found that 16 % of victims considered suicide. When digital identity theft is a relational crime, it may be also accompanied by relationship strain/breakdown or threats of retaliation if the crime is reported (Langford et al., 2024).

Explaining identity theft

In seeking to explain digital identity theft, victimology literature has evolved in its understanding of explanation (see Victimization by Walklate). In our view, the theoretical landscape can be divided into three approaches: (1) victim-centric, (2) offender-centric, and (3) relational.

Victim-centric theories constitute the prevailing paradigm. Building on routine activity theory (RAT) and self-control theory (SCT), and using mostly general survey data, victim-centric approaches focus on how online behavior, personality traits, and degrees of self-guardianship correlate with risks of cybercrime victimization in a digital environment (Williams, 2016; Graham and Triplett 2017). Empirical research has examined whether targeted browsing, exposure to greater phishing through public internet use (deceiving users into revealing personal information), engagement in frequent online shopping/forums, and failure to regularly update passwords increases the likelihood of victimization.

However, the empirical findings are ambiguous (Ngo and Paternoster, 2011). Some RAT-based studies find no or weak significant relationship with certain forms of online self-guardianship, such as installing antivirus software to prevent phishing attacks (Henson, 2020). Others find that many of these guardianship activities provide some, though, limited help (see summary in Langford et al., 2024). As to SCT, Bossler and Holt (2010: 227) find that self-control had a weak relationship with password access, harassment, and having information changed, and no correlation with credit card misuse or malware infection.

A second, and smaller, body of literature is *offender-centric.* Some theories foreground how subcultural engagement encourages and shape motivations to commit cybercrime, including identity theft (Holt et al., 2017). Holt (2020: 522) argues that the "internet serves a vital role in the formation and maintenance of deviant and criminal subcultures." Relatedly, Navarro and Marcum (2020) point to social learning and the role of communication in generating deviant criminal behavior. Debutants learn from others about how to offend successfully, avoid detection, and rationalize their ac-

tions. Others point to theories grounded in cognitive and behavioral psychology, such as internet addiction (Nykodym et al., 2008; Schell, 2020) or neutralization techniques, which often involve denial of responsibility of injury, appeal to higher loyalties, and condemning the condemner (Matza and Sykes, 1957; Brewer et al., 2020).

Empirical evidence for these offender-centric theories is limited. Moreover, such theories may be more relevant to explaining cybercrimes like digital piracy and hacking (Brewer et al., 2020: 553; Holt, 2020: 520; Navarro and Marcum, 2020: 533). Digital identity theft might be simply motivated by more mundane factors. Interviews with convicted offenders, who mostly committed low-tech digital identity theft, indicated that it was driven primarily by easy financial gain, and partly 'thrill-seeking' (Golladay, 2020).

A third approach is what we call *relational cybercrime* (Langford et al., 2024). The relationship between offender and victim inflects the causes, context, and consequences of digital identity theft. Pletcher (2003: 21–22) found that offenders can take advantage of trust in close relationships in order to get a hold of sensitive security information. The intentions of offenders may vary significantly though. They might be malicious, hostile, or irrational, and based on emotional and social circumstances (Hay and Ray, 2020: 588), as would be consistent with general strain theory. Linking strain theory with feminist criminology, Marganski (2020: 636) argues that "Violating others through misogynistic vitriol, degradation, humiliation, etc., for instance, can be viewed as an act of revenge … or a means of gaining control over others so that they comply with demands." Indeed, Bossler and Holt (2010) find that when controlling for close peer victimization, the explanatory power of self-guardianship decreases suggesting that traditional victim-centric theories function poorly when an offender is known to a victim.

A relational approach also orients attention beyond the classical technological focus on phishing, hacking, and keylogging. These techniques occupy just one end of Gordon and Ford (2006)'s classification of cybercrime, so-called type I Cybercrime (which is purely digital in nature). They argued that greater focus is needed on type II Cybercrime "which has a more pronounced human element" (p. 13). This includes email and messenger services. Moreover, such type II or relational cybercrime may carry different burdens for victims. As offenders have greater access to a victim's digital devices, knowledge of their security and financial information, and greater ability to exercise physical and psychological power, they can engage more easily in "social engineering" and commit digital identity theft which has consequences that may be different or even more harmful than type I cybercrime.

Case study

The different patterns of digital identity theft, and their potential causes, can be explored through a brief case study of digital identity theft in Norway. Through our project Societal Security and Digital Identities (SODI), an analysis of the cases of 292 victims

that sought legal aid from three student legal aid clinics[1] between 2015 and 2021 was conducted (Brataas et al., 2023).

In the sample, there was a relatively even distribution of victims across the age deciles from 19 to 60; with a much lower proportion of theft for those over 60. The largest victim group was the youngest decile, with male victims tending to be younger. Overall, 64 % of the victims in the sample were women, but this is partly explained by the fact that one of the clinics only serves female clients. National representative surveys tend to find no gender difference in mere incidence (NorSIS, 2022). Moreover, 68 % of the digital identity theft analyzed was executed using the victim's physical electronic identity device, a single technology owned and developed by the finance industry.

In terms of effects, over half of the fraud (54 %) resulted in a total loss for each victim between US$10,000 and US$500,000. This is significantly higher than the losses in most national surveys of digital identity theft (Golladay, 2020), including in Norway (NorSIS and SODI, 2024). It reflects most likely though the sample selection: victims that sought legal assistance encountered can be expected to have experienced greater harm.

Turning to the explanations and theories traversed above, there were some clear patterns. Two-thirds of victims had a close relationship with the offender: a family member, close friend, or a partner. Using an in-group analysis, we found that this pattern of victimization was gendered. As much as 80 % of women had a close relationship with the offender, which was only the case for 36 % of male victims. For male victims who were victims of relational cybercrime, the offender was often a work colleague. This suggests the importance of integrating feminist and gender perspectives in understanding digital identity theft.

As to technology, it varied according to the relational mode of theft. While 40 % of the victims were unaware as to how their eID was misused, a third reported giving their security information to the offender *in person*, which implies significant trust. Likewise, the effects of digital identity theft also varied according to the relational modes. None of the unknown offenders stood for any fraud with a total loss over US $10,000, while 64 % of the fraud carried by close peers and family resulted in a total loss of US$25,000 or more. When victims reported the case to the police, prosecution was dropped in at least 56 % of the cases, with surprisingly no difference for relational cybercrime, where the identity of the offender was known. This raises questions as to why the prosecution rate is so low even when a victim can identify the offender.

Conclusion and policy implications

This entry has sought to shed light of the ever-present cybercrime of digital identity theft. Understood primarily as fraud or other unlawful activity in which an identity

1 The Law Bus (*Jussbuss*), Women's Law Clinic (JURK), and Street Lawyer (*Gatejuristen*).

is used digitally without consent, the financial and emotional costs have steadily risen during the last three decades. Criminological scholarship sought initially to identify victim behavior as a key explanation for this victimization, but the field has begun gradually to focus also on the motivations of offenders and their diverse relationships with victims.

In this respect, it is worth noting the policy implications of the prevailing victim-centric approach. RAT and SCT theories are drawn commonly on to justify delegating 'guardianship' by state and corporations to individuals (Clough, 2015; Williams, 2016: 22), with these institutions tasked with simply providing advice on how to identify and avoid risks (Hutchings and Hayes, 2009: 437). For type I 'stranger' cybercrime, this is somewhat understandable. However, it risks unnecessarily narrowing policy responses. Even worse, it may cause greater harm through victim-blaming discourses, strengthening a narrative that individuals facilitate their victimization through their lifestyle and activities (Akdemir and Lawless, 2020: 1666), which might help explain the low level of prosecutions for relational cybercrime.

Equally, victim-centric approaches risk being guided by a technological consciousness that reifies digitalization as an artefact, making it a technical challenge that can be addressed independently of systems and society in which it is embedded (Miller, 1978). Kaufmann and Jeandesboz (2017: 309) warn that, "the digital is best examined in terms of folds within existing socio-technical configurations, and as an artefact with a set of affordances that are shaped and filled with meaning by social practice." Notably, in other fields where technology is similarly dispersed and surveillance and prevention of harm is difficult, such deep social integration and the repercussions of new technologies has been acknowledged. As Yoshikawa (2018: 1157) notes, "In select fields, legislatures also augmented or replaced tort law with regulatory regimes, such as the motor vehicle safety regime, and with social insurance schemes, such as workers' compensation, to shift costs and prevent injuries." These private and public insurance-based schemes are based on the premise that the cost of technological harms should not be privatized (see Privatization by Lomell).

In our view, making a move towards a socio-technological consciousness in understanding digital identity theft is long overdue. It would avoid a singular focus on type I cybercrime and a narrow policy repertoire. More research is thus needed on the diverse forms and effects of digital identity theft, the nature of relationships between offenders and victims, and the different policies needed to address this ever-expanding cybercrime.

Suggested reading

Cross, C., Dragiewicz, M., & Richards, K. (2018). Understanding romance fraud: Insights from domestic violence research. *The British Journal of Criminology*, 58(6), 1303 – 1322.

Golladay, K. A. (2020). Identity theft: Nature, extent, and global response. In T. Holt & A. Bossler (eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 981 – 999). Cham: Palgrave Macmillan.

Williams, M. L. (2016). Guardians upon high: An application of routine activities theory to online identity theft in Europe at the country and individual level. *British Journal of Criminology*, 56(1), 21 – 48.

References

Akdemir, N., & Lawless, C. J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. *Internet Research*, 30(6), 1665 – 1687.

Bossler, A., & Berenblum, T. (2019). Introduction: New directions in cybercrime research. *Journal of Crime and Justice*, 42(5), 495 – 499.

Bossler, A., & Holt, T. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice*, 38(3), 227 – 236.

Brataas, E. B., Svensson, A. E., & Stokke, M. (2022). Empiriske funn om misbruk av eID. In M. E. Kjørven, M. A. Hjort, & T. L. Wærstad (eds.), *Bruk og misbruk av elektronisk kommunikasjon* (pp. 115 – 129). Oslo: Karnov.

Brewer, R., Fox, S., & Miller, C. (2020). Applying the techniques of neutralization to the study of cybercrime. In T. Holt & A. Bossler (eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 547 – 565). Cham: Palgrave Macmillan.

Brunson, R. K., & Weitzer, R. (2009). Police relations with black and white youths in different urban neighborhoods. *Urban Affairs Review*, 44(6), 858 – 885.

Burnes, D., DeLiema, M., & Langton, L. (2020). Risk and protective factors of identity theft victimization in the United States. *Preventive Medicine Reports*, 17, 101058.

Camplisson, L. (2022). Time's up: The high cost of weak digital identity. *Future Identity.* https://thefuturidentity.com/rising-fraud-weak-digital-identity/.

Clough, J. (2015). Towards a common identity? The harmonisation of identity theft laws. *Journal of Financial Crime*, 22(4), 492 – 512.

Cross, C., & Layt, R. (2022). "I suspect that the pictures are stolen": Romance fraud, identity crime, and responding to suspicions of inauthentic identities. *Social Science Computer Review*, 40(4), 955 – 973.

Experia. (2022). *2022 Global Identity and Fraud Report.* Experia.

Golladay, K. (2020). Identity theft: Nature, extent, and global response. In T. Holt & A. Bossler (eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 981 – 999). Cham: Palgrave Macmillan.

Golladay, K., & Holtfreter, K. (2017). The consequences of identity theft victimization: An examination of emotional and physical health outcomes. *Victims & Offenders*, 12(5), 741 – 760.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, 2, 13 – 20.

Graham, R., & Triplett, R. (2017). Capable guardians in the digital environment: The role of digital literacy in reducing phishing victimization. *Deviant Behavior*, 38(12), 1371 – 1382.

Hay, C., & Ray, K. (2020). General strain theory and cybercrime. In T. Holt & A. Bossler (eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 583 – 600). Cham: Palgrave Macmillan.

Henson, B. (2020). Routine Activities. In T. Holt & A. Bossler (eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 469 – 489). Cham: Palgrave Macmillan.

Holt, T. (2020). Subcultural theories of crime. In T. Holt & A. Bossler (eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 513 – 526). Cham: Palgrave Macmillan.

Holt, T. J., Freilich, J. D., & Chermak, S. M. (2017). Internet-based radicalization as enculturation to violent deviant subcultures. *Deviant Behavior*, 38(8), 855 – 869.

Hutchings, A., & Hayes, H. (2009). Routine activity theory and phishing victimisation: Who gets caught in the 'net'? *Current Issues in Criminal Justice*, 20(3), 433 – 452.

ICF-SA. (2022). *Study on Online Identity Theft and Identity-Related Crime.* Brussels: EU Commission.

ITRC. (2018). *Identity Theft: The Aftermath 2017.* El Cajon: Identity Theft Resource Center (ITRC).

ITRC. (2023). *Consumer Impact Report 2023.* San Diego: Identity Theft Resource Center.

Kaufmann, M., & Jeandesboz, J. (2017). Politics and 'the digital' From singularity to specificity. *European Journal of Social Theory*, 20(3), 309 – 328.

Kjørven, M. E. (2020). Who pays when things go wrong? Online financial fraud and consumer protection in Scandinavia and Europe. *European Business Law Review*, 31(1), 77 – 110.

Koops, B.-J., & Leenes, R. E. (2006). ID theft, ID fraud and/or ID-related crime-definitions matter. *Datenschutz und Datensicherheit*, 30(9), 553 – 556.

Langford, M., Svensson, A., & Wærstad, T. L. (2024). *Relational Cybercrime.* SODI Working Paper.

Marganski, A. J. (2020). Feminist theories in criminology and the application to cybercrimes. T. Holt & A. Bossler (eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 623 – 651). Cham: Palgrave Macmillan.

Matza, D., & Sykes, G. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review*, 22(6), 664 – 670.

Miller, C. R. (1978). Technology as a form of consciousness: A study of contemporary ethos. *Communication Studies*, 29(4), 228 – 236.

Navarro, J. C., & Higgins, G. E. (2017). Familial identity theft. *American Journal of Criminal Justice*, 42, 218 – 230.

Navarro, J., & Marcum, C. (2020). Deviant instruction: The applicability of social learning theory to understanding cybercrime. In T. Holt & A. Bossler (eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 527 – 546). Cham: Palgrave Macmillan.

Newman, G. R., & McNally, M. M. (2005). *Identity Theft Literature Review.* U.S. Department of Justice, Washington D.C.

Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology*, 5(1), 773 – 793.

NorSIS. (2022). *ID-tyveriundersøkelsen 2022: ID-tyveri rammer fortsatt mange – behov for flere tiltak og økt kunnskap.*

NorSIS and SODI. (2024). *ID-tyveriundersøkelse.*

Nykodym, N., Ariss, S., & Kurtz, K. (2008). Computer addiction and cyber crime. *Journal of Leadership, Accountability and Ethics*, 35, 55 – 59

OECD (2009), *Online Identity Theft.* Paris: OECD.

Pletcher, D. (2003). *Identity Theft: The Aftermath 2003.* San Diego: Identity Theft Resource Center.

Schell, B. (2020). Internet addiction and cybercrime. In T. Holt & A. Bossler (eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 679 – 703). Cham: Palgrave Macmillan.

Signicat (2024). *The Battle Against AI-driven Identity Fraud*, Signicat, Trondheim.

Williams, M. L. (2016). Guardians upon high: An application of routine activities theory to online identity theft in Europe at the country and individual level. *British Journal of Criminology*, 56(1), 21 – 48.

Yoshikawa, J. (2018). Sharing the costs of artificial intelligence: Universal no-fault social insurance for personal injuries. *Vanderbilt Journal of Entertainment & Technology Law*, 21, 1155.