Knowledge about Identity Theft

Spotting Signs of Identity Theft: Learning how to recognize signs of personal data compromise, the implications of identity breaches, and the necessity of reporting such incidents. Include where to report.

Introduction: Definition and relevance of identity theft

Identity theft (ID-theft) is a crime where an adversary uses another person's identity for illegal purposes, such as fraud and theft (Bose and Leung, 2013). Typically, an identity thief will attempt to steal a victim's Social Security number, driver's license number, credit card numbers, ATM cards, and date of birth information. With these data in hand, it is relatively simple for the identity thief to impersonate the victim. The thief then spends as much of the victim's money as possible in a short period and moves on to the next victim (Ingram, 2005). The most common ID-theft are phishing attacks, in which people receive spam or fake e-mails that attempt to access confidential data to commit fraud. The phishing attacks are fraudulent e-mail messages appearing to come from legitimate enterprises to access the private information and to commit identity theft. These similar-looking web pages are designed to steal information or to perform a social engineering-based attack (Bojjagani et al., 2020).

Although ID-theft is not a new crime, the magnitude of the problem has increased with society's growing dependence on digital storing and sharing of personal information across all forms of services (Burnes et al., 2020). This means that many people nowadays have access to information on the identities of others (Hinde, 2005).

In line with this, a recent study from the Swedish National Council for Crime Prevention (BRÅ, 2023) have identified a number of technical and structural vulnerabilities that facilitate fraud:

- Readily available information such as name, address, age, family situation and vehicle ownership enable fraudsters to identify potential victims and prepare their deception.
- The ability to manipulate who is displayed as the sender of calls, text messages and emails makes the fraudster appear credible in their contact with the victim.
- The ability to publish fraudulent adverts, register fraudulent domains and companies, and use intermediaries to represent them allows fraudsters to establish credibility via seemingly legitimate websites, companies and adverts.
- A digital banking and payment market imply both insufficient transaction monitoring and considerable opportunities for fraudsters to make money untraceable quickly.
- Access to specific skills to prepare and carry out the fraud (e.g. technical know-how) and to people who can be used as money launderers facilitates fraud.
- Digital ignorance and unfamiliarity, stress, a lack of critical thinking, risk tendency, the need for excitement, greed, desperation, loneliness and the need for affirmation, understanding, closeness and love are all vulnerabilities that are associated with potential victims. Digital illiteracy, susceptibility to stress and a lack of critical thinking are vulnerabilities that are particularly associated with older people.

- The lack of accessible alternatives to digital services means that people who lack digital skills, knowledge and perhaps the motivation to learn are forced to use services they do not master.

The identified vulnerabilities largely reflect people’s behavioural patterns. What people do, how they do it and which alternatives are available, combined with human capabilities and characteristics, determine how fraud can be carried out and who is affected. (BRÅ, 2023)

Identification: How individuals and organizations can detect identity theft

According to Information Commissioner’s Office (ICO), there are a number of signs to look out for that may indicate you are or may become a victim of identity theft:

- You have lost or have important documents stolen, such as your passport or driving licence.
- Mail from your bank or utility provider doesn’t arrive.
- Items that you don’t recognise appear on your bank or credit card statement.
- You apply for state benefits, but are told you are already claiming.
- You receive bills or receipts for goods or services you haven’t asked for.
- You are refused financial services, credit cards or a loan, despite having a good credit rating.
- You receive letters in your name from solicitors or debt collectors for debts that are not yours.

Immediate Actions: What to do when you've identified identity theft

Identity theft can occur not only due to computer-related threats (e.g., phishing, spoofing, and viruses) but also due to consumers' conventional behaviours. It is important for individuals to fight identity theft using technological and conventional behavioural countermeasures (Lai et al., 2011).

If suspicious activities are discovered, the crime should be reported as soon as possible (Swedish Police Authority, 2021). According to the Swedish Police Authority, additional actions for victims of ID-theft to take are to:

- Report the incident to the police.
- Dispute any fraudulent invoices.
- If possible, block your social security number with the credit reference company if credit information has been taken in your name that you did not request.
- Call your bank and monitor your accounts.
- Verify that no changes have been made to your civil registration address.
- Verify that you are registered at the correct address.
- Verify that no mail has been forwarded to another address.
- Block your ID-card, if it is lost. Contact the authority that issued the card.

Preventive Actions: What to do to minimize the risk of identity theft

Studies by Burnes et al. (2020) shows that individuals engaging in a higher number of proactive, routine protective behaviours, were less likely to experience identity theft victimization with each additional protective behaviour. The study looked at individuals who; checked credit reports; changed passwords on financial accounts; purchased credit monitoring services or identity theft insurance; shredded or destroyed documents containing personally identifying information; checked bank or credit card statements for unfamiliar charges; used computer security software; or purchased identity theft protection services.

According to Sule et al. (2021), most ID-thefts that have been carried out have been socially engineered to prey on people's fears, habits and, ultimately, their personal details. In this "Covid-19 era" and beyond, it is important to refocus security best practices on "Security Hygiene". It can be argued that the human errors are the weakest link in a secure identity system.

The Swedish Police Authority (2021) published a list of advice on how to minimize the risk of ID-theft. Those include:

- Never send personal or login information via e-mail without establishing that the relevant company, authority or organization has requested the information.
- Use services that notifies you directly on your mobile phone or via e-mail if someone has taken a credit report on you. Then you have the chance to act quickly by contacting the relevant credit company and stopping the credit or loan from being granted.
- Ensure that no unauthorized persons have access to your mail.
- If you have lost an identity document, report it to the Police and to credit bureaus.
- Do not open emails or links that are unknown to you. There is a risk that unknown links contain viruses that are transferred to your computer that for example copy your login details.
- Have up-to-date virus protection on your computer and mobile phone.
- Do not download new apps without checking if they have been around for a while and have received positive reviews and ratings.
- Be careful where you save your login details for different accounts.
- Use strong passwords for your most important accounts.
- Securing you passwords. Keep you passwords safe by following these tips:
  - Never give out your passwords.
  - Use strong passwords, preferably a password phrase, with many characters and a large variety of characters.
  - If possible, use a password manager that helps you create and manage strong passwords.
  - Use different passwords for different services, especially your most important services.
  - Use two-factor login where possible.

Europol has collected similar Do's and Don'ts in a PDF file, and adds the instruction to never give away more of your personal information than necessary, for example while filling out a form etc.

Reporting Protocols: Who and how to report the incident to authorities or internal IT departments

Research reveals that a lot of ID-thefts and cybercrimes goes unreported in the EU. According to Bidgoli (2021), one of the reasons for this is the victim simply being unaware of the crime. Similarly, Tcherni et al. (2015) report that some victims might not lose their details so much as "share" them with the criminal. According to Cross (2019), victims of cybercrime often experiences challenges and negativity surrounding their attempts to initiate a police response, and a lack of willingness on the part of the police to accept a complaint from the victim, and might therefore be discouraged to report. The last factor behind the gap of reporting cybercrimes is that victims do not know where to report incidents (de Kimpe et al., 2021). A lack of knowledge about cybercrime mechanisms, or who to report contributes to crimes not being reported at all (Bidgoli, 2021).

To combat the crime of identity theft, government legislation, consumer education, and corporate security policies are crucial (Bose and Leung, 2013). According to Europol, victims are encouraged to immediately report ID-theft to their local police and to the company affected (i.e. bank or online service).

References

Bidgoli, M. (2021). If You See Something Suspicious Online, Report It: An Investigation into Addressing and Overcoming the Challenges in Cybercrime Reporting. The Pennsylvania State University ProQuest Dissertations Publishing. https://www.proquest.com/pagepdf/2576934024?accountid=14581

Bojjagani, S., Brabin, D., Rao, V. (2020). PhishPreventer: A Secure Authentication Protocol for Prevention of Phishing Attacks in Mobile Environment with Formal Verification. Procedia Computer Science, 171, 1110-1119. https://doi.org/10.1016/j.procs.2020.04.119

Bose, I., Leung, A. C. M. (2013). The Impact of Adoption of Identity Theft Countermeasures on Firm Value. Decision Support Systems, 55(3), 753-763. https://doi.org/10.1016/j.dss.2013.03.001

Burnes, D., DeLiema, M., Langton, L. (2020). Risk and Protective Factors of Identity Theft Victimization in the United States. Preventive Medicine Reports, 17. https://doi.org/10.1016/j.pmedr.2020.101058

Cross, C. (2019). 'Oh we can't actually do anything about that': The problematic nature of jurisdiction for online fraud victims. Criminology and Criminal Justice, 20(3), 358-375. https://doi.org/10.1177/1748895819835910

Europol. Infographic – ID Theft. https://www.europol.europa.eu/sites/default/files/documents/infographic_-_id_theft.pdf

Hinde, S. (2005). Identity Theft: Theft, Loss and Giveaways. Computer Fraud & Security, 5, 18-20. https://doi.org/10.1016/S1361-3723(05)70215-3

Information Commissioner's Office (ICO). Licensed under the Open Government Licence. https://ico.org.uk/for-the-public/identity-theft/

Ingram, D. M. (2006). How to Minimize Your Risk of Identity Theft. Optometry – Journal of the American Optometric Association, 77(6), 312-314. https://doi.org/10.1016/j.optm.2006.03.012

de Kimpe, L., Walrave, M., Snaphaan, T., Pauwels, L., Hardyns, W., Ponnet, K. (2021). Research Note: An Investigation of Cybercrime Victims' Reporting Behaviour. European Journal of Crime, Criminal Law and Criminal Justice, 29(1), 66-78. https://doi.org/10.1163/15718174-bja10019

Lai, F., Li, D., Hsieh, C-T. (2012). Fighting Identity Theft: The Coping Perspective. Decision Support Systems, 52(2), 353-363. https://doi.org/10.1016/j.dss.2011.09.002

Sule, M-J., Zennaro, M., Thomas, G. (2021). Cybersecurity Through the Lens of Digital Identity and Data Protection: Issues andTrends. Technology in Society, 67. https://doi.org/10.1016/j.techsoc.2021.101734

Swedish National Council for Crime Prevention (Brottsförebyggande rådet, BRÅ), Fjelkegård, L., Horgby, A. (2023). Fraud Against Individuals. https://bra.se/bra-in-english/home/publications/archive/publications/2023-10-06-fraud-against-individuals.html?lang=sv
Swedish Police Authority (2021). Id-kapning – skydda dig. https://polisen.se/utsatt-for-brott/skydda-dig-mot-brott/bedrageri/identitetsintrang/
Swedish Police Authority (2021). Identitestintrång – utsatt. https://polisen.se/utsatt-for-brott/olika-typer-av-brott/bedrageri/identitetsintrang/

This project was funded by the European Union's Internal Security Fund - Police Programme under Grant Agreement No 101038738