Shacara Pitre

Professor Brian Payne

CRJS 310

June 16, 2022

Identity Theft

Cybercrime is increasing as technology evolves over time. One of the most common is identity theft. Identity theft has been an ongoing problem in our society for years and unfortunately people still fall victim to it. By definition it is "all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain" (United States Department of Justice, 2020). Identity theft occurs more often than we think and can happen to anyone at any time. In addition, it can happen to anyone at any time and there are many examples that can account for this crime. Throughout this paper, I will discuss the dynamics related to identity theft, causes, consequences, strategies to prevent it at the organizational level, and strategies to prevent it at the individual level.

Identity theft has been around for a long time even before we had technology, such as the internet. Criminals would use the more traditional method of collecting people's personal information by "dumpster diving", in which they would look inside trash cans in search of anything that would be of use to them, such as finding documents that identified them and discarded bills. One example of this is "if someone was entering a credit card number or a calling card number in a public place; criminals often used a method called 'shoulder surfing, where they would watch the person from a nearby place in an attempt to capture that information" (Irshad and Soomro, 2018). With technology evolving, it has only become easier for identity

theft to occur because people put so much of the information online already. Identity theft comes in a wide variety of forms. Some of which include: criminal identity theft, medical identity theft, child identity theft, etc.

Criminal identity theft involves someone taking another's identity as their own and using it to commit crimes. Medical identity theft is using someone else's personal information in order to buy medication, medical supplies, and/or presenting false billings to Medicare. Furthermore, child identity theft typically happens because children are not aware of how important that personal information is and that it needs to be protected. Children do not understand the importance of protecting their personal data and that it should not be given out to just anyone. To support this "in 2016, an estimated 26 million persons, or about 10% of all U.S. residents age 16 or older, reported that they had been victims of identity theft during the prior 12 months" (Harrell, 2019).

There are a number of things that can cause identity theft. One of the most common ways that this can happen is in a public setting. Oftentimes, criminals are able to get ahold of personal information just by listening, watching, and observing those around them. For instance, a person could be listening and hear that you are giving your credit card number over the phone or looking as if you are punching in your pin number at the store when you are checking out. Another way of becoming a victim to identity theft is when you receive applications for "pre-approved" credit cards in the mail, but throw them away without taking out the enclosed materials and shredding them. As a result, criminals will go through trash and find these credit cards and will try to activate them without your knowledge using your identity.

It is also possible for criminals to redirect your mail to another location if your mail is already delivered to a place where anyone has access to it. Spam is another way for criminals to

gain access to steal your identity. This is because many people open their spam emails making them fall victim to identity theft and other criminal activity. Our spam folder is not supposed to be open in the first place because it is where emails that are not trustworthy are relocated to. Opening an email that contains spam could be harmful to your computer causing viruses, malware, etc.

People who open spam emails find that the email is going to provide them with some kind of benefit if they give them personal information about them. However, people don't realize that the sender has no intention of giving them what they want. They just sent the email hoping that they can convince someone to give them personal data about themselves, so they can use it to their advantage. When enough information is given to a criminal about an individual, they can take over that person's identity to conduct many other crimes (United States Department of Justice, 2020).

Identity theft is not considered to be a violent crime. Therefore, law enforcement are not willing to use much of their resources for this type of crime and instead use it on more violent offenses. As a result, those detectives who are working on identity theft among other cybercrimes, are left shorthanded (White and Fisher, 2008). In addition, many people do not find out they have been a victim of identity theft until when applying for something, such as a loan, job, mortgage, and they are denied. To clarify, "recent research suggests that more than 80% of victims discover the theft through a negative experience" (White & Fisher, 2008).

If a person becomes a victim of identity theft, there are some important steps that should be taken to ensure that it gets resolved. First, is to call the companies where you know that the fraud occurred. Next, a person should place a fraud alert and get their credit reports. Then, they

should report identity theft to the Federal Trade Commission (FTC). Lastly, they could file a report, if they choose, with their local police department.

Now that we know how identity theft occurs and ways that people can go about getting it resolved, we can now dive into prevention strategies at the organizational and individual level. When it comes to the organizational level, there are many things that companies can do to ensure that their employees and customers are not subjected to identity theft. Encryption, password protection, firewalls, maintaining a console log, and control of paper documents are ways that organizations can help prevent identity theft. Encryption adds another layer of protection to a file. Password protection is another area that a company should consider when protecting their employees. For instance, "organizations should assure that only legitimate users have access to the computer network and associated data" (Gerard et al., 2004).

Firewalls help to protect a company's data stored on a network from unauthorized personnel. There should be policies and procedures in place that will ensure firewalls are evaluated and upgraded to the most up to date software to meet critical risks. In addition, it is important for an organization to maintain a log of all employees when they go to access files that contain sensitive information. As a result, this helps them to detect promptly if a security breach occurs by leaving a trail of everyone who has access. Lastly, having control of paper documents will ensure that companies prevent identity theft. Paper documents should only be stored in areas where employees have to have access since they contain sensitive data. Employees should lock file drawers, cabinets, and offices which contain any paper documents left unattended.

When it comes to preventing identity theft at the individual level, there are things that we can do to protect ourselves. One is to never display details of personal or financial documents on either social media or in a public place for anyone to see. For example, some people post pictures

of them getting their driver's license making them vulnerable to criminals looking to steal their identity. If you are going to post pictures of documents containing your personal information, always make sure to blur out the important details. Another is to turn off automatic log on features that allow browsers to remember your username and password because whoever has your computer or other device can use that to get into your account.

Furthermore, strong passwords are a must when it comes to protecting your identity. It is important to make sure that they are unique and that they contain a mixture of letters and symbols. Lastly, using secure networks or ones that you trust will help significantly (Irshad & Soomro, 2018). It is important to make sure that the network you are accessing is secure by looking to see if it has a locked symbol next to it. If it is public wifi, then you should keep in mind that everyone has access to that wifi and anyone can thus gain access to sites that you visit.

In conclusion, identity theft is a type of cybercrime that will be hard to stop all together, but there are ways that we as individuals and organizations can do to prevent it from occurring as often. Throughout this paper, we have broken down identity theft from the definition to the causes down to the prevention strategies. Identity theft still seems to be a prevalent issue in our society today, especially as technology evolves. We are constantly trying to come up with ways to better protect ourselves from it, but unfortunately criminals are smart and will use tactics to try to trick us into falling for their schemes. However, if we are educated on the ways to protect ourselves from becoming victims of this crime, then we will be a step closer in eliminating these cybercriminals once and for all from stealing our identity.

References

Gerard, G. et.al. (2004, January). Identity Theft: An Organization's Responsibilities. http://ruby.fgcu.edu/courses/cpacini/courses/common/idtheftjoffincrim.pdf

Harrell, E. (2019). Victims of Identity Theft, 2016. U.S. Department of Justice. https://bjs.ojp.gov/content/pub/pdf/vit16.pdf

Irshad, S & Soomro, R. (2018). Identity Theft and Social Media. IJCSNS International Journal of Computer Science and Network Security, VOL.18 No.1 https://www.researchgate.net/profile/Tariq-Soomro-2/publication/323185128_Identity_Theft_and_Social_Media/links/5a850d2aa6fdcc201b9f044c/Identity-Theft-and-Social-Media.pdf

The United States Department of Justice (2020, November 16). What Are Identity Theft and Identity Fraud? https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud

White, M & Fisher, C. (2008). Assessing our Knowledge of Identity Theft: The Challenges to Effective Prevention and Control Efforts, VOL 19 No. 1 https://journals.sagepub.com/doi/pdf/10.1177/0887403407306297?casa_token=ljJgUJAkhc4AAAAA:6vb7jt3Fik7kg_HqAXXBDvpUUzNrpb40XapDwM49rvhiTOJ_s8W00BZLSK10oGkpV-NrRs_IOtfmKQ