**Identity Theft in Information Security**

Corbin Osman

American Public University System

ISSC422 – Information Security

Mike Instructor

04/23/2023

**Abstract**

Personally identifiable information is a common target for attackers who search for the information of others. With the development and progression of technology and the online world a lot of personal information is shared throughout networks and systems. Much of our personally identifiable information is both stored and shared online, with or without our knowledge. This increases the risk that our personal information may be viewed or accessed by others who are not authorized to do so, which can result in problems and issues for those who the information belongs to.

This paper focuses on understanding what identity theft is and how it is performed online and in a digital environment. The scope and goal are to gain a greater knowledge and understanding of why identity theft is prevalent, what types of information and data are commonly targeted, how identity theft is performed online and ways to recognize it, and methods of protecting information from the attacks of others. The purpose and intent of this paper are to help readers gain an understanding of how identity theft is performed, know why they should work to protect themselves and their information, and learn about strong practices in securing their personal information in the online world.

**What is Identity Theft?**

Throughout history there have been many features and characteristics used to identify individuals and the differences between them and others. Some identifiers are biological whereas others may be numerical. Examples of biological identifiers are fingerprints, DNA, and physical traits whereas a few numerical identifiers are social security numbers, medical record numbers, and account numbers. Additional information such as a date of birth, address, or phone number can also be used to identify an individual.

Much of this information is confidential and sensitive in nature, only being shared with those who need access to it. Identity theft occurs when this information is accessed and stolen by unauthorized parties which attackers then usually utilize for personal gain and benefit. Personally identifiable information can be used to open utility accounts, open or access credit accounts, withdraw funds from debit accounts and open bank accounts, and perform many other large life actions (Henson, 2017). Identity theft has been occurring for decades and continues to affect the lives of millions whose information is compromised.

Identity theft affects millions of individuals each year. The Identity Theft Research Center reports that there were over four hundred and twenty million victims of identity-related crimes in the year 2022 (ITRC, 2023). Further, they share that the top five pieces of personally identifiable information compromised through data breachers were the individual’s name, full social security number, date of birth, current home address, and driver’s license or state ID number (ITRC, 2023). These statistics help portray the amount of information that is compromised each year and how many individuals are affected by identity theft.

**How is Identity Theft Performed?**

Identity theft can be performed in a variety of different ways. One method thieves often use is to collect mail that may be thrown out. Mail correspondence often contains some form of personal information such as an address, the receivers’ name, and even a part of an account number. Another method that is common is stealing items that contain confidential information such as a wallet or purse. Most people keep forms of ID, credit and debit cards, and medical cards within a wallet or purse, which are prime targets for thieves looking to steal information for use in identity theft. For the intent of this paper, we will explore ways that identity theft is performed in the digital and online world.

With the world relying on and heavily utilizing technology and digital networks, a lot of our personal and sensitive information is shared across the world. Whether it is known to us or not, our information is being shared with advertisers, employers, and even strangers through social media interactions, online forums, email and text message communications, and other digital avenues. Our information may deliberately be shared with others, though there are times when it is accessed and obtained without authorization or consent.

Once personal information is obtained by others, identity theft occurs when this information is used without authorization or consent. As previously mentioned, this information is commonly used to open new credit accounts, access pre-existing fund accounts, take over online accounts, and other forms of identity theft (Ravichandran, 2023). There are quite a large number of ways identity theft can occur, and we will now look further into different ways personal information can be compromised and used for identity theft.

**Identity Theft Through the Use of Technology**

There are many ways attackers gain access to information and systems that they do not normally have access to, and a lot of these similar actions are used for stealing personal information to be used in identity theft. One avenue of attacks is through social engineering, which is the act of deceiving an individual or group into sharing information that they may not otherwise share. An example could be an attacker convincing their target to share their address and phone number in order to deliver a package they recently ordered. This can appear to be a legitimate inquiry, but the party behind it may be collecting the information for other purposes. Other examples of social engineering can be pressuring a target to send money to help someone in need, having a user log in to a fake website that appears to be legitimate to capture login credentials, and requesting information be shared with an attacker who is threatening the target through various means.

The above methods often involve one individual or party communicating with another, though there are other methods which are more passive in nature. Network and device scanning and monitoring can occur without a target’s knowledge, resulting in the attacking party capturing confidential and sensitive information that is being transmitted or received by the target. Personal and business networks and systems can also be targeted, and an attacker who has gained access to a network can utilize software to monitor communications and access files that contain sensitive information and data. Additionally, spyware can be planted on networks or devices to capture information and relay it to the attacker (Webroot).

Networks and devices can also be attacked through more active methods such as hacking and attacking a router. A personal or business network can be the target of such an attack where the malicious actor intentionally hacks a device or network to search for and capture confidential information (Masjedi, 2022). This is often commonly performed on public network connections where many users connect their devices. In utilizing the public connection an attacker is able to search for and capture traffic that contains sensitive information that can be used in identity theft. A similar attack is through an evil-twin or rogue access point attack. These both utilize a network connection that is meant to appear legitimate and deceive users into believing they are connected to a secure trusted network. When they instead connect to the fake access point, the malicious actor is able to locate and steal important information.

With many individuals saving their personal data and card information on website shopping accounts, there is a risk of someone gaining access to the account and utilizing the saved card information to make purchases of their own. This is commonly known as online shopping fraud, which occurs when an account that has saved card information is accessed by an unauthorized individual who makes purchases using the saved card details (Hayes, 2020). This is considered a form of card and fund identity theft is common across shopping websites that allow users to save their payment information for ease of access.

One additional way personal information can be compromised is through data hacks and breaches. Each year many businesses and organizations that hold client and employee information are attacked, and as a result there are times when this personal information is captured by the attackers. Depending on the severity of the attack, upwards of millions of individuals can be affected and have their personally identifiable information leaked for others to access and use it. An unfortunate factor with data breaches is that clients and employees rely on those who have their information saved to utilize strong security and protect the information from malicious actors. In other words, the safety of their personal information and data may be out of their hands.

These are a few of the many methods malicious actors can access and steal personally identifiable information to then later use for identity theft. With a better knowledge of different attacks that could be performed we will now explore ways and methods to detect signs of identity theft and how to protect against it in the digital world.

**Recognizing and Protecting Against Digital Identity Theft**

When one knows how an enemy will attack, they can prepare for the attack and look for signs of it occurring. In the digital world, however, attacks can occur without a target’s knowledge, and the effects of identity theft can present themselves after it is too late to respond. For this reason, it is critical that users know what to look out for while online and what they can do to protect themselves and those around them.

In following the previously mentioned attacks, let us look at strong practices to utilize in combatting these methods of identity theft. For phishing and social engineering attacks it is important to monitor digital communications such as emails and text messages to ensure that they are received by and sent to recognized parties. Be wary as well about sharing confidential and sensitive personal information, as these could be intercepted by attacks in transmission. When possible, it is safer to share personal information in-person to ensure that the intended recipient receives it. Additionally, utilize trusted and secured networks and devices when communicating and working with personal information online to ensure that encryption and protection are offered.

To help protect against both passive and active network and device attacks it can be beneficial to install anti-virus and security software. Utilizing device security features and protection software can help prevent the attacks of malicious actors who may try to steal information and data (Ramsey Solutions, 2023). Furthermore, it is important to ensure that both devices and networks are updated regularly to ensure that the most recent patches and updates are installed. This will help to ensure that potential system and network vulnerabilities are patched, thus increasing the level of security around the information contained within.

As previously mentioned, it is important to utilize trusted networks and devices when sharing personal data. If there are times where this is not possible, there are still actions one can take to better secure themselves while accessing and sharing information. When navigating the web or communicating on an untrusted device or network, utilizing a browser’s incognito mode will help to ensure that your history and log in credentials are not saved. When using a personal device on an untrusted network it can be helpful to install and use a virtual private network (VPN) to secure and encrypt online interactions. In all circumstances, it is best practice to use a secured internet connection point when possible (Ramsey Solutions, 2023).

When shopping online and using personal accounts, it is good practice to avoid saving your information to use at a later time. While this can be convenient and makes logging in or purchasing items easier, it also presents a vulnerability. When your information is saved by a website to an account, attackers may be able to use that information if they can access the account. Similarly, if login credentials are saved to a browser, an attacker might be able to access personal accounts if a device is stolen. For these reasons, it is recommended to avoid saving personal information in an online environment.

Due to data breaches and hacks being unpredictable, as well as multiple businesses and organizations having access to client and employee personal information, it can be difficult for users to protect themselves against its occurrence. One practice users can implement to their routine is regularly monitoring their accounts and information. Identity thieves often open credit or debit accounts with information they receive, so routinely monitoring one’s credit report and pre-existing accounts can help show if any have been opened fraudulently. Similarly, it can be helpful to monitor notices for unrecognized logins or activity. Many social media and website accounts will notify you if there are login attempts from unrecognized locations or devices as well as any attempts to update information. These can be signs that someone is attempting to access and take over accounts.

The following are additional good practices to aid in protecting against identity theft. Enable two-factor or multi-factor authentication on devices and accounts. Avoid sharing personal information online via social media accounts, forum accounts, and other online public sites. Do not interact with email or text communications that seem out of the ordinary or are asking for personal information.

**Protecting Against Digital Identity Theft in Business Environments**

Many identity thieves target individuals when searching for personal information, though there are also times where attackers will target large groups such as organizations or businesses. As previously mentioned, data breaches and hacks are a common way that the personal information of clients and employees is compromised. The Insurance Information Institute recorded that there were nearly two-thousand data breaches in the year of 2022, resulting in the aforementioned four hundred and twenty million individuals impacted through compromised information (III). This often occurs due to security policies and procedures not being followed and vulnerabilities being exploited in systems and infrastructures.

In addition to the practices to protect against identity theft mentioned in the previous section there are many strong practices that can be implemented into business and enterprise policy to help secure confidential and sensitive information. All locations that contain this important information should utilize a strong wireless network and form of encryption. Access to such information should be restricted to those who do not need it in order to perform their functions. This limits the number of vulnerabilities created by granting access to all users (Nead, 2021). Access and permissions should regularly be audited to ensure that users only have access to what they need to fulfill their roles, and permission hierarchies can help to organize the levels of permissions granted to each employee.

Employees should be trained and educated about the risks the business faces should security policies and procedures not be followed (Nead, 2021). It is critical that all employees, no matter what position they hold, understand the importance of following proper policies to ensure that both their and client’s information and data are protected from unauthorized access. Humans are often considered the weakest link in regard to security, and many breaches occur due to employees making mistakes that create vulnerabilities which can be exploited by malicious actors.

A few areas employees should be educated in are recognize and responding to phishing attacks, creating strong login credentials, utilizing two-factor or multi-factor authentication for accounts and systems, maintaining devices and networks up to date, and downloading and installing software only from trusted sources. These practices can help to increase the level of security within an enterprise environment and ensure that client and employee information and data is further secured from unauthorized individuals. Practicing these strategies will help a business as a whole, even if the employees implementing them do not have access to the confidential information themselves.

**Limitations and Difficulties in Detecting Identity Theft**

Due to its online nature, identity theft can be difficult to detect and protect against. Many who experience its effects do so following the incident and find that there may have been no warning signs to alert them of its potential. Because it can occur so suddenly, many do not know how to respond to identity theft when they fall victim to it. Depending on the severity of the breach and compromise of information, one may need to work a lot harder to recover from the incident.

In the instance of identity theft occurring where a malicious actor utilizes personal information to open fraudulent credit accounts, victims can experience damage to their credit scores and reputability. If one does not routinely review their credit and accounts they have opened, they may not realize an account has been opened for a long period of time. Once a fraudulent account is found, the impacts can often be reversed when it is proven that the individual is a victim of identity theft, though this process can take a long period of time.

When data breaches occur and the personal information of millions is leaked, it can be difficult to know how to respond. It is possible that one’s information is never used fraudulently, though with it being compromised there is always a chance due to the information being in the hands of malicious parties. Due to this factor, one may not experience the effects of identity theft for a time after an initial data breach.

As technology has advanced and identity thieves have moved their operations to the digital world it has become more difficult to find and catch the perpetrators. By utilizing public networks or virtual private networks attackers can conceal information about themselves such as their whole identity, where they are living, and who else may be involved in the operations. Some identity thieves or groups that steal information may reside in other countries as well, further complicating the act of finding and catching them. When they are not stopped, they may continue committing identity theft and affecting the lives of those whose information they steal.

With identity theft being hard to recognize at times and due to its predatory nature, millions of individuals fall victim to it each year. In studying identity theft and understanding how it is performed, what information is targeted, and how to protect against it, individuals can better protect themselves and those they know while using internet functions. In reporting identity theft individuals can begin the process of restoring their life and reputability (O’Shea, 2023).

**Conclusion**

In review of identity theft in information technology, there are several points to remember and consider. It is important for all to understand not only how identity theft is performed in general, but also how it is specifically performed through digital means. With the vast majority of the world’s population utilizing digital devices and the internet in some form, more and more people are at risk of identity theft as they communicate and interact with others online. Through education and learning individuals can gain a greater understanding of identity theft through digital environments and know what they can do to both protect against it and recognize effects if it has already occurred. Users in both personal and professional environments should learn about identity theft to protect themselves and those around them through securing their personal information.

**Resources**

Facts + Statistics: Identity theft and cybercrime | III. (n.d.). https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime

Hayes, M. (2020, September 29). The Many Different Forms of Identity Theft. *Experian*. https://www.experian.com/blogs/ask-experian/20-types-of-identity-theft-and-fraud/

Henson, S. (2017, September 1). What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself? *Experian*. https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/

Identity Theft Resource Center. (2023, January 31). Annual Data Breach Report - ITRC. *ITRC*. https://www.idtheftcenter.org/publication/2022-data-breach-report/

Masjedi, Y. (2022, September 20). The 13 Latest Types of Identity Theft in 2022. *Identity Guard*. https://www.identityguard.com/news/types-of-identity-theft

Nead, N. (2021, July 30). How To Prevent a Data Breach in Your Company. *Forbes*. <https://www.forbes.com/sites/forbesbusinesscouncil/2021/07/30/how-to-prevent-a-data-breach-in-your-company/?sh=4c83152f18da>

O’Shea, B. (2023, February 7). Identity Theft: What It Is, How to Prevent It, Warning Signs and Tips. *Nerdwallet*. https://www.nerdwallet.com/article/finance/how-to-prevent-identity-theft##thenwhat

Ramsey Solutions. (2023, Feb 2). How to Prevent Identity Theft. *Ramseysolutions*. https://www.ramseysolutions.com/insurance/protect-yourself-from-identity-theft

Ravichandran, H. (2023, January 6). How Does Identity Theft Happen? (And How to Avoid It). *Aura*. https://www.aura.com/learn/how-does-identity-theft-happen

What is Online Identity Theft? How to. (n.d.). © Copyright 2004 - 2023 Webroot Inc. All Rights Reserved. https://www.webroot.com/us/en/resources/tips-articles/malware-identity-theft