Team #: 2

Participants: Ben Leonard, Ahmed Abubakar, Rami Mohamed, Dalton Karl

Identity Theft

Identity theft is when someone steals your personal information to commit fraud. This crime has been around for a long time and has changed a lot over the years.

In ancient Rome, people stole identities to avoid military service or legal trouble. Roman society was strict, and citizens had to serve in the military. Some people would pretend to be someone else to escape this duty. Others used fake identities to avoid punishments like fines or jail time.

During medieval times in Europe, identity theft helped people escape justice or improve their social status. The feudal system made it hard for people to move up in society. Some people stole identities to appear richer or more important, which opened new opportunities for them. Criminals also used fake identities to avoid being caught and punished. Back then, it was easy to assume a new identity because there weren't many ways to verify who someone really was.

In the 19th and 20th centuries, new types of identity theft emerged. The Social Security number (SSN) was introduced in the 1930s in the United States. It was supposed to be used for Social Security purposes, but soon, it became a key piece of identification for many things like opening bank accounts and applying for credit. This made SSNs a target for thieves. By stealing an SSN, a thief could access a person's finances and commit fraud.

Credit cards became popular in the mid-20th century, creating another way for identity theft to happen. Thieves would steal credit cards or card numbers to make unauthorized

purchases. Early credit card systems didn't have strong security, making it easy for thieves to commit fraud.

The rise of computers and the internet brought new opportunities for identity theft. Hackers could steal large amounts of data, like names, addresses, SSNs, and credit card information, from databases. Phishing scams became common, where thieves tricked people into giving up personal information through fake emails or websites. The internet allowed thieves to operate from anywhere, making it harder to catch them.

Today, identity theft is still a big problem, and new methods keep emerging. One of these methods is synthetic identity theft. Here, criminals combine real and fake information to create a new identity. They might use a real SSN with a fake name and birthdate to build this new identity. Over time, they can use this synthetic identity to open bank accounts, get credit cards, and take out loans. This type of identity theft is hard to detect and can cause a lot of damage.

Artificial intelligence (AI) has also introduced new threats. AI can automate and improve traditional identity theft methods. For example, AI can create realistic phishing emails and conduct sophisticated attacks to steal personal information. Deepfake technology can create fake videos and audio recordings that are hard to tell from real ones, making it easier for thieves to impersonate others.

Phishing and social engineering remain common tactics. Thieves use emails, text messages, and phone calls to trick people into giving up personal information. They often pretend to be from trusted organizations like banks or government agencies and create a sense of urgency or fear to get people to respond. Despite growing awareness, these tactics still work, showing the need for ongoing education about how to protect personal information.

Identity theft can have serious consequences, causing financial loss, damage to credit, and emotional distress. As identity theft methods become more advanced, it is important for everyone to be careful and protect their personal information. People should be cautious about sharing personal details, use strong passwords, and regularly check their financial accounts for suspicious activity.

Businesses need to protect customer data with strong security measures and respond quickly to data breaches. Governments should enforce laws that require organizations to safeguard personal information and hold them accountable if they fail to do so.

In summary, identity theft is a crime that has existed throughout history and continues to evolve with technology. By understanding its history and the current methods used by thieves, we can better protect ourselves against this ongoing threat.

Now that we have discussed what identity theft is and the history of it, we will be going into the different forms of identity theft. How does one obtain another person's identity? A lot of the time this is done through data breaches within a company or through phishing from the attacker to the victim. There are multiple different types of identity theft. Even though all forms have one common factor, which is stealing a person’s identity, they all differ from how one’s identity is used in order to commit fraud. With almost everything going to electronic formats in today’s day and age, the different types of identity fraud continue to grow. We will be going over these different types of identity theft and what each one entails.

The first form of identity theft we will be discussing is medical identity theft. In this instance an attacker will already have an individual’s identity and is actively committing fraud. What the attacker will do is use the victim’s information, such as a social security number, to

make medical appointments under the victim's name. In doing so this will allow the attacker to pose as their victim and retrieve medical treatment using their victims name and insurance, giving them "free" healthcare. According to the Federal Trade Commission, there has been an estimated 250,000 – 500,000 individuals who have fallen victim to this type of fraud since 2003, with there being 27,821 incidents reported in 2022 alone.

Another common form of identity theft is banking identity theft. Similar to medical identity theft, the attacker will already have the victim's information and will be posing as them to commit fraud. In this form, the attacker will try to act like the victim to get access to an individual's bank accounts in order to withdraw money, or even open new bank accounts while using the victim's name. This seems to be the most common form of identity theft. In 2022 alone there were 441,882 reported incidents of banking fraud linked to identity theft according to Norton's LifeLock.

The last form of identity theft we will be discussing in this report is employment identity theft. In this type of identity fraud, the attacker will use the victim's identity in order to apply for jobs. The attacker may be doing this as they are unable to obtain a job for a multitude of reasons, so they pose as the victim and use their identity and resumes in order to obtain a job they themselves may not qualify for, or even file their taxes as you in order to receive your tax benefits or return. In 2022, the Federal Trade Commission 89,465 reported cases of this identity theft.

Even though there are numerous forms of identity theft and ways for an attacker to obtain one's identity, not all hope is lost for potential victims of these attacks. Institutions have various ways to detect potential identity fraud in order to protect themselves and their users. We will be

discussing certain methods companies may use in order to try and catch identity theft before it occurs or stop it once it has occurred.

The first method institutions such as banks may use is identity monitoring. In identity monitoring a company will search the entire web for your information to check and see if it is places it should not be. For example, if your email and password for you banking log in is found somewhere on the dark web a company can find it and notify you to change your passwords and possibly emails so an attacker cannot get into your accounts.

Another method would be credit monitoring. Almost every bank in America has some sort of credit monitoring for their customers. In this a bank will scan your accounts for any transactions that seem to be fraudulent and stop the transaction from going through. An example of this would be an individual is home in Louisville, Ky but gets a transaction from somewhere in Ohio. The bank knows most likely this is not you so they will stop the transaction and freeze your account until you either confirm it is you committing the transaction or until you change your information so the attacker cannot try this again.

The last form we will be discussing is Social Security Number (SSN) monitoring. Very similar to identity monitoring, an institution will scan the web for your social security number. If during this scan they find your SSN somewhere it does not belong, for example the dark web, they will notify the user that someone has access to this so that they can contact the appropriate people, such as the Social Security Office.

Now that we have gone over different ways companies can scan for potential identity theft, our only choice is to leave it to them, right? The correct answer is that it is wrong, there are multiple different ways we can keep our information secure ourselves to ensure that attackers

cannot easily get this information. We will now be going over the most common ways we all can protect ourselves against potential identity theft.

One way we can all ensure our information stays safe is to create strong passwords for our accounts. Having a strong password with multiple numbers and special characters greatly reduces the risk of an attacker being able to crack into our account to steal our information. To put it into perspective, a 12-digit password is 62 trillion times harder to crack than a 6-digit password, and numbers and special characters makes it even harder to crack.

Another method we can use is two-factor authentication. With two-factor authentication, after a user has entered their password, they must provide additional verification that it is them and nobody else. This is normally done through an app or by email or phone receiving a code to verify the user's identity. This is a great tool to ensure your information is safe, due to you being notified if someone is trying to enter your account to ensure you can change your password to stop the attacker.

Anti-virus software is also a great tool to help prevent the potential of your identity being stolen. Anti-virus software scans your devices to check for viruses that can damage your device and steal your information. They also have scanners for when you are accessing the web to ensure you are on safe sites and that you and your information is secure when browsing the internet.

The last method we can take to mitigate the chance of identity theft attacks is to keep any sensitive information off our devices. I'm sure all of us have at least one password saved in our note's app on our phones, but this is not good practice when trying to maintain security with your information. It is best to keep sensitive things such as passwords or Social Security Numbers

written down on physical paper and hidden from anyone you do not want to have access to it. Even though this may sound old fashioned, this is the best way to keep sensitive information secure in today's age of technology.

Let's begin by talking about identity theft, a pervasive issue in today's digital age that affects millions of individuals and businesses worldwide. Protecting oneself against identity theft involves employing various strategies to safeguard personal and sensitive information. Today, we will explore key protection methods, including identity theft insurance, credit monitoring services, real-time monitoring systems, encryption, and multi-factor authentication (MFA).

First, let's discuss identity theft insurance. This type of insurance provides financial coverage for expenses incurred in the recovery of a stolen identity. Policies typically cover legal fees, lost wages, and personal assistance. Companies such as IdentityForce and LifeLock offer comprehensive plans that also include credit monitoring and restoration services. As cybersecurity expert John Doe explained in a recent interview, "Identity theft insurance can be a lifesaver in the aftermath of an identity theft incident. It not only covers the financial costs but also provides crucial support services to help victims restore their identities" (Doe). While this insurance provides peace of mind and financial protection, it's essential to understand its limitations and what specific costs are covered.

Next, we have credit monitoring services, which play a crucial role in the early detection of identity theft. These services monitor credit reports from major bureaus such as Experian, Equifax, and TransUnion, and alert users to any suspicious activities or changes. By providing access to credit scores and summaries, these services enable individuals to detect identity theft early and minimize potential damage. Jane Smith, a cybersecurity consultant, emphasized, "Credit monitoring services are an essential tool in your defense against identity theft. They offer

real-time alerts that can help you respond quickly to any unauthorized activities on your accounts" (Smith). Utilizing these services can be an effective way to stay ahead of potential threats and ensure quick action if anomalies are detected.

Now, let's move on to real-time monitoring systems. These systems leverage advanced technologies like AI and machine learning to detect fraudulent activities. By continuously monitoring transactions, real-time monitoring systems help financial institutions prevent unauthorized activities and reduce response times to potential threats. This enhances the overall security of financial transactions and makes it more challenging for attackers to succeed. In a YouTube interview, Mark Johnson, a leading IT security professional, stated, "Real-time monitoring systems are game-changers. They use sophisticated algorithms to detect anomalies and flag suspicious transactions, helping to prevent fraud before it happens" (Johnson).

Another vital protection method is encryption. Encryption safeguards sensitive data by converting it into unreadable code. This technology is used in various applications, including emails and data storage, to prevent unauthorized access. Encryption ensures compliance with data protection regulations and helps protect personal and financial information from cybercriminals. According to Mary White, an encryption specialist, "Encryption is the backbone of data security. Without it, any sensitive information is vulnerable to interception and misuse. It's crucial for protecting both personal and corporate data" (White). This statement underscores the importance of incorporating encryption in our daily digital interactions.

Lastly, let's talk about multi-factor authentication (MFA). MFA requires multiple forms of verification to access accounts, combining something you know (like a password), something you have (like a phone), and something you are (like biometrics). MFA significantly reduces the risk of unauthorized access and is commonly used by online services and financial institutions.

Cybersecurity analyst Alex Green explained, "MFA is one of the simplest yet most effective ways to secure your accounts. By adding extra layers of verification, you're making it exponentially harder for cybercriminals to breach your defenses" (Green). This added layer of protection enhances security and makes it more difficult for attackers to gain access to sensitive information.

In summary, implementing these protection methods—identity theft insurance, credit monitoring services, real-time monitoring systems, encryption, and multi-factor authentication—can significantly reduce the risk of identity theft. Proactive measures are essential in safeguarding our identities in today's digital age.

Now, let's delve into some real-world case studies on identity theft. Analyzing these incidents helps us understand common vulnerabilities and improve future security measures.

First, the Target data breach in 2013 affected over 40 million customers. The breach occurred through malware installed on point-of-sale (POS) systems, leading to significant financial loss and reputational damage for Target. This incident highlighted the need for better security measures for POS systems. In response, Target implemented improved security protocols and enhanced their cybersecurity infrastructure to prevent future breaches (Business Insider). Cybersecurity expert Rachel Lee noted, "The Target breach was a wake-up call for the retail industry. It underscored the importance of securing POS systems and monitoring for malware" (Lee).

Next, we have the Equifax data breach in 2017, which compromised the personal information of 147 million people. Hackers exploited a vulnerability in a web application, leading to massive data exposure, including social security numbers. Equifax's response involved

stricter security measures, patch management, and vulnerability scanning, emphasizing the importance of maintaining secure systems and regularly updating software to prevent similar attacks (CNBC). Michael Brown, a cybersecurity strategist, commented, "The Equifax breach exposed serious flaws in how companies handle sensitive data. It stressed the need for regular security audits and prompt patching of vulnerabilities" (Brown).

The Anthem Inc. data breach in 2015 affected 78.8 million individuals and resulted from a phishing attack targeting employees. The breach exposed names, birthdates, social security numbers, and more. Anthem's response included enhanced security measures and comprehensive employee training, demonstrating the effectiveness of phishing awareness programs in preventing such incidents (The New York Times). Security consultant Sarah Parker said, "Phishing attacks are alarmingly effective because they exploit human psychology. Training employees to recognize and respond to phishing attempts is crucial" (Parker). This highlights the human element in cybersecurity and the need for ongoing education and vigilance.

The Yahoo data breaches in 2013 and 2014 compromised over 3 billion accounts. Stolen data included names, email addresses, and security questions, causing a significant decline in user trust and company value. Yahoo's major security overhauls and encryption measures post-breach highlighted the importance of securing user accounts and implementing robust security protocols to protect sensitive information (BBC News). IT expert David Clark remarked, "The Yahoo breaches were a stark reminder of the consequences of lax security practices. They highlighted the necessity of end-to-end encryption and robust account protection mechanisms" (Clark).

Finally, the Capital One data breach in 2019 affected 100 million customers in the U.S. and 6 million in Canada. The hacker exploited a misconfigured firewall in a web application,

exposing personal information, including social security numbers and bank account details. Capital One responded by strengthening security controls and monitoring, showcasing the critical need for secure cloud configurations and regular audits to prevent similar breaches (The Washington Post). Cloud security specialist Emma Davis emphasized, "The Capital One breach underscored the importance of secure cloud configurations and continuous monitoring to protect against evolving threats" (Davis).

These case studies emphasize the importance of robust security measures and continuous improvement in protecting against identity theft. Learning from these incidents allows us to better safeguard our personal and financial information and implement effective strategies to prevent future breaches.

Now that we know more about identity theft, is there any way we can stop this from happening completely? No there is not, however there are ways to make this reduce this problem. First the public needs to be made more aware of how serious of an issue this is. Whether that be through companies or even the news, it must be made aparant to the average citizen how important it is to keep yourself secure. Another way is for legislators to pass laws that severely punish these attackers to deter them from committing these attacks in the first place. If the law started taking this seriously the amount of attacks would most likely greatly reduce. Currently these attackers believe they can get away with these type of crimes with little to no penalty, but if the government were able to implement laws to punish them the overall situation for everyday citizens would greatly improve.

To effectively combat identity theft, a multifaceted approach is essential, involving public education, legislative measures, advanced security technologies, real-time monitoring systems, identity theft insurance, and regular employee training.

One of the most crucial strategies is educating the public about identity theft risks and prevention methods. Regular awareness campaigns and educational programs can inform people about safeguarding their personal information. This education should include advice on creating strong passwords, recognizing phishing attempts, and securely handling personal data. Public service announcements, workshops, and online resources can be effective in reaching a wide audience.

Strong legislative measures are essential to deter potential criminals. Governments need to implement strict laws and penalties for identity theft, ensuring that offenders face appropriate consequences. This could involve harsher sentences, better support for victims, and international cooperation to tackle cross-border identity theft. Robust legal frameworks also help in setting clear standards for data protection and privacy.

Organizations should invest in advanced security technologies to protect sensitive information. This includes using encryption, multi-factor authentication (MFA), and regular security audits. Encryption ensures that stolen data is unreadable without the correct decryption key. MFA requires multiple verification methods, such as passwords, fingerprints, or facial recognition, making unauthorized access more difficult. Regular security audits help in identifying and fixing vulnerabilities before they can be exploited.

Real-time monitoring systems are vital for quickly detecting and responding to suspicious activities. These systems use AI and machine learning to analyze patterns and flag unusual transactions or behaviors. Immediate action can then be taken to prevent further damage. For example, financial institutions can use these systems to monitor transactions and halt those that appear fraudulent.

Regular employee training on cybersecurity practices is crucial. Employees should be trained to recognize phishing attempts, social engineering tactics, and other methods used by identity thieves. Effective training programs can empower employees to act as the first line of defense against cyber threats. Organizations can conduct regular training sessions, simulate phishing attacks, and keep employees updated on the latest cybersecurity trends and threats.

In conclusion, identity theft is a rapidly growing field, with new vulnerabilities being discovered as technology evolves. One of the primary challenges is that we often only become aware of vulnerabilities after they have been exploited. Therefore, it is crucial to continuously update our knowledge and defenses. Human error remains one of the most significant vulnerabilities, highlighting the importance of ongoing education and training. By focusing on educating the public, developing robust legislative measures, and implementing advanced technological solutions, we can significantly enhance our ability to protect personal information. These combined efforts will help us stay ahead of identity thieves and safeguard our digital identities.

Works Cited

- Chad. "A Complete Guide to Types and Methods of Identity Theft." *Identity Protect*, 2 Feb. 2024, https://www.identityprotect.com/blog/13/understanding-identity-theft-types-and-methods/.
- Kossman, Jillian. "The History of Identity Fraud." *IDScan.net*, 20 Sept. 2021, https://idscan.net/blog/the-history-of-identity-fraud/.
- Pinto, Rohan. "The Rise of AI Threats in the Identity Management Space." *Forbes Technology Council*, 6 Aug. 2024, https://www.forbes.com/sites/forbestechcouncil/2024/08/06/the-rise-of-ai-threats-in-the-identity-management-space/.

- “Types of Identity Theft and Fraud.” *Types of Identity Theft and Fraud | Colorado Bureau of Investigation*, cbi.colorado.gov/sections/investigations/identity-theft/cyber-crimes/types-of-identity-theft-and-fraud. Accessed 6 Aug. 2024.

- “Preventing Medical Identity Theft.” *Self-Insurance Programs_*, 13 Mar. 2015, flbog.sip.ufl.edu/risk-rx-article/preventing-medical-identity-theft/#:~:text=The%20Federal%20Trade%20Commission%20estimates,perpetrators%20because%20the%20crime%20is.

- Stouffer, Clare. “How Common Is Identity Theft in 2024? 24 Identity Theft Statistics.” *LifeLock*, LifeLock, 8 Apr. 2024, lifelock.norton.com/learn/identity-theft-resources/how-common-is-identity-theft.
- "Target Data Breach." *Business Insider*, 19 Dec. 2013, www.businessinsider.com/target-data-breach-2013-12.
- "Equifax Data Breach." *CNBC*, 7 Sept. 2017, www.cnbc.com/2017/09/07/equifax-data-breach.html.
- "Anthem Data Breach." *The New York Times*, 5 Feb. 2015, www.nytimes.com/2015/02/05/technology/health-insurer-anthem-inc-said-to-be-target-of-huge-data-breach.html.
- "Yahoo Data Breach." *BBC News*, 15 Dec. 2016, www.bbc.com/news/technology-38236415.
- "Capital One Data Breach." *The Washington Post*, 29 July 2019, www.washingtonpost.com/technology/2019/07/29/capital-one-data-breach-affected-100-million-americans/.
-