# Identity Theft

Teaundra Thompson

Charleston Southern University

CSCI 405: Principles of Cybersecurity

Professor Hill

October 21st, 2025

## Abstract

This paper details the methods and forms of identity theft and the effects it has on victims. There are also recommendations for preventing identity theft. Identity theft is a life-altering crime and it can potentially cause serious legal trouble for victims. Individuals’ personally identifiable information is stored in countless places which increases the risk of becoming a victim of identity theft due to the chance of a data breach. One of the leading forms of identity theft is credit card fraud. Such a form of identity theft can place victims in financial jeopardy and cause tremendous stress on a victim. Not only do adults have to be concerned about identity theft, so do children. Children are the leading victims in identity theft due to the value of their social security numbers. It is important for everyone to adopt good cyber safety habits and ensure all sensitive documents are stored in a secure safe place.

*Keywords:* Identity theft, credit card fraud, phishing, scams, personal information

## Modern Identity Theft

Identity theft is the act of obtaining an individual’s personally identifiable information illegally to impersonate said individual, and to receive goods and services under the stolen identity (Glotfelty, 2023). Identity theft is not a recent phenomenon as it has been reported ever since the 1980s (Cassim, 2015). Identity thieves relied on traditional identity theft methods such as lockpicking and stealing mail to accomplish their nefarious goals. Traditional methods of identity theft also include stealing wallets, bags, dumpster diving, and burglary (Angelopoulou, 2007). Digital methods involve phishing, pharming, malware, web-spoofing, card skimming, and social engineering (Angelopoulou, 2007; *Credit Card and Debit Card Fraud*, 2024). The time from the 1980s to now has allowed for countless new identity theft methods considering the rapid growth of technology. Due to the growing practice of storing personally identifiable information in digital systems, digital identity theft has become increasingly common. While there is no “one cure-all” for identity theft, having good cybersecurity and personal security practices can greatly decrease the risk of becoming an identity theft victim.

## Physical Identity Theft

The simplest and most easily executable form of identity theft is physical theft. Theft of personal information sources can wreak havoc on a company or individual. An example of physical theft is an incident that occurred in May 2005, when a laptop containing personally identifiable information on 80,000 employees was stolen from the Department of Justice (Hedayati, 2012). Dumpster diving also provides personally identifiable information to thieves because they can find financial documents or bank statements that have been discarded. Mail theft is another form of identity theft that is easy to execute. Thieves can easily obtain mail from a mailbox because it lacks security and people typically do not monitor their mailboxes closely. Unlike theft of a tangible personal belonging, theft of mail or documents in the garbage can easily go by undetected and can cause as much damage as the theft of a purse or wallet. With the growing use of technology, financial receipts and sensitive documents are not as prevalent in garbage or mailboxes. Majority of such documents are stored digitally which prodded bad actors to start pivoting to digital identity theft as more information can be stolen in that matter. Due to this factor, there are few statistics specifically on physical identity theft.

## Card Identity Theft

The most usual form of identity theft is through digital means. For the remainder of this paper, I will refer to digital identity theft simply as “identity theft” due to its prevalence. There were 1,353,175 reports of identity theft in 2024 which made up over 17% of the total reports made to the Federal Trade commission (Federal Trade Commission, 2025). The most reported form of identity theft was credit card fraud, with 449,032 reports. Credit card fraud can be accomplished by physical theft of the card, stealing card information online, or by card skimming (*Credit Card and Debit Card Fraud*, 2024). Credit card skimming involves installing or placing devices inside ATMs, point-of-sale terminals, or fuel pumps to capture card data and PINs (*Skimming*, n.d.). This form of theft costs financial institutions and consumers over $1 billion annually. Fuel pump skimmers are typically attached to internal wiring and are not visible. They store data to be downloaded or accessed wirelessly at a later time. To prevent becoming a victim of fuel pump skimming use “tap to pay” or pay inside. ATM and point-of-sale (POS) skimming involves the same discrete device as fuel pump skimming, but some of the skimmer devices can be placed over the card reader or be placed amongst exposed cables. There can also be pinhole cameras on or around the machine to record PIN entries. Keylogger keypad overlays are another device that is used for skimming on these machines. It only requires a few seconds to install a skimming device which can be accomplished undetected by creating distractions. Skimming devices on ATMs and POSs can store data to be transferred later and some can even transmit the data wirelessly in real time. EBT cards are also an enthralling target for skimmers because they lack microchips which secure payments. The lack of micro-chips allows for bad actors to steal the card information and “cash out” EBT cash benefits. To mitigate these skimming methods be sure to examine card readers and machines before making a purchase. Also be sure to routinely monitor your accounts and balances to verify there are no fraudulent transactions. Card fraud is a milder form of identity theft since personally identifiable information is not being used to open accounts or get loans. Regardless, it still creates a threat to one's livelihood.

## **Digital Identity Theft**

Our industrialized digital world opens many doors and developments for new methods and forms of identity theft. Phishing is a method that is heavily prevalent with an estimated 3.4 billion phishes sent daily (Griffiths, 2025). Phishing typically uses spoofing within the email or within hyperlinks to manipulate people into thinking the emails are legitimate (*Spoofing and Phishing*, n.d.). Upon interacting with a phish, users are then sent to a spoofed website that is either a credential harvester or is asking the user to provide personally identifiable information. In 2021, over 300,000 people globally fell victim to phishing attacks running up a loss of 44.2 million dollars (Griffiths, 2025). Phishing has several variations: smishing which utilizes text messages, vishing which involves phone calls, and pharming which involves placing malware on a machine to create unwanted website redirects. Vishing has rapidly increased due to American companies outsourcing call centers (Cassim, 2015). One country that is commonly used for call center outsourcing is India. As a result, Indian outsourcing firms are gaining increasing access to Americans' sensitive data and that creates potential for identity theft though data breaches. Pharming is another variation that bypasses the need for a target to click a link or interact with an email (*What Is Pharming?*, 2021). Malware such as Trojans and keyloggers can be used to execute pharming attacks. They can infect the machine's network, manipulate DNS settings, and modify host files to automatically redirect the target to spoofed websites to steal personal info. An example of a pharming attack is the DNS Changer Malware. It modified DNS settings on machines and redirected users to malicious servers allowing bad actors to intercept sensitive information and commit identity theft. The sensitive information that is derived from identity theft is used to not only commit theft and fraud, but also to facilitate other crimes such as illegal immigration, terrorism and espionage (Cassim, 2015). Identity theft also facilitates criminal identity theft, which is the act of posing as another person to evade arrest and criminal sanctions. Identity theft can also result in medical identity theft, allowing someone to obtain medical services under the guise of being another person. Theft of an identity can take a major toll on an individual as it can take years for them to clear their name.

## Child Identity theft

Identity theft is usually never discovered immediately. It could take months or years for someone to realize their identity has been stolen. This is especially true for victims who are children. Children are an eye-catching target for bad actors (Power, 2020). The reason being that a child’s identity is a blank slate, and their social security number (SSN) can be stolen and paired with any name and birth date to create a new identity. Child identity theft has a low chance of being discovered because a child will not be using their SSN until they come of age and a parent does not typically monitor their child’s identity. The main thing that bad actors want from children is their SSN. A lack of history attached to an SSN makes it effortless to attach it to a new identity and aid in criminal activities. Not only do bad actors prey on children’s identities, so do their own parents. Based on statistics from 2017, over one million children were victims of identity theft and sixty percent of those children knew the perpetrator, their parent(s) (Betz-Hamilton, 2020). When parents steal their children’s identity they use them for fraudulent financial purposes, such as opening credits card, getting loans, and even getting mortgages. Notably, children’s SSNs are fifty-one times higher to be stolen than adults, highlighting just how valuable a child’s identity is (Power, 2020). The youngest known victim of identity theft was a five-month-old infant, and the largest resulting fraud was $725,000 committed against a 16-year-old. Identity theft can be detrimental to a child’s future. Being a victim of identity theft as a child can prevent young adults from going to college, getting their first car, or apartment. Parents should take steps to instruct their child about cyber safety to prevent them from sharing personally identifiable information online, which could lead to identity theft. Parents should also keep children's sensitive documents in a safe place and only give them to their children once they are of age.

## Remediation and Mitigation

Currently the US government does not have a set of comprehensive laws protecting citizens' identity, but states such as California and South Carolina have laws that protect citizens' identities and prosecutes identity thieves (*2007-2008 Bill 453: Financial Identity Fraud and Identity Theft Protection Act - South Carolina Legislature Online*, 2008; Cassim, 2015). Both California and South Carolina require businesses and any public entity to notify consumers of data breaches. Furthermore, South Carolina requires credit bureaus to allow consumers to request a credit freeze if they suspect they are a victim of identity theft. Overall, what the federal government lacks in identity protection laws, states make up for it. Identity theft is not one hundred percent preventable, but individuals can take proactive measures to prevent becoming a victim. Shred documents before throwing them in the trash prevents thieves from stealing information by dumpster diving (Hedayati, 2012). Regularly checking credit reports and reviewing financial statements can bring attention to any fraudulent activity and prevent further damage to one's credit. Ensure that all devices are secure and computers have antivirus software and firewalls enabled. Never interact with suspicious or unwarranted emails and ensure all websites visited are secure and they have an up-to-date privacy policy. Create and use strong passwords, and do not reuse the same password. It is nearly impossible to remember every single password that one may create, so utilize a secure password manager application to assist with retrieving passwords. Finally, keep social media accounts private and do not post personal information such as addresses.

## Conclusion

Just like any crime, identity theft is not one hundred percent preventable, but bringing awareness to it and promoting cyber safety habits can greatly reduce the chances of someone becoming a victim. With the ever-growing presence of technology in daily life, it is important to only provide personal information if necessary. Having personal information in the least number of places as possible greatly decreases the risk of becoming a victim. Protecting your information and children's information is crucial to attempting to prevent identity theft. Promoting cyber safety habits in the community and within households can help people to better recognize scams and potentially prevent them from becoming victims.

## References

*2007-2008 Bill 453: Financial Identity Fraud and Identity Theft Protection Act—South Carolina Legislature Online*. (2008). https://www.scstatehouse.gov/sess117_2007-2008/bills/453.htm

Angelopoulou, O. (2007). ID Theft: A computer forensics' investigation framework. *Australian Digital Forensics Conference*. https://doi.org/10.4225/75/57ad41987ff2b

Betz-Hamilton, A. (2020). A Phenomenological Study on Parental Perpetrators of Child Identity Theft. *Journal of Financial Counseling and Planning*, *31*(2), 219–228.

Cassim, F. (2015). Protecting Personal Information in the Era of Identity Theft: Just how Safe is our Personal Information from Identity Thieves? *Potchefstroom Electronic Law Journal*, *18*(2), 68–110. https://doi.org/10.4314/pelj.v18i2.02

*Credit Card and Debit Card Fraud*. (2024). OCC.Gov. https://www.occ.gov/topics/consumers-and-communities/consumer-protection/fraud-resources/credit-card-and-debit-card-fraud.html

Federal Trade Commission. (2025). *Consumer Sentinel Network Data Book 2024*.

Glotfelty, C. V. (2023). *Identity theft and businesses | Research Starters | EBSCO Research*. EBSCO. https://www.ebsco.com

Griffiths, C. (2025, June). *The Latest Phishing Statistics (updated June 2025) | AAG IT Support*. https://aag-it.com/the-latest-phishing-statistics/

Hedayati, A. (2012). *An analysis of identity theft: Motives, related frauds, techniques and prevention*.

Power, R. (2020). *CHILD IDENTITY THEFT New Evidence Indicates Identity Thieves are Targeting Children for Unused Social Security Numbers*. https://eriskhub.com/files/articles/article229.pdf

*Skimming*. (n.d.). [Page]. Federal Bureau of Investigation. Retrieved October 17, 2025, from https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/skimming

*What Is Pharming? - Definition, Examples & More | Proofpoint US*. (2021, July 29). Proofpoint. https://www.proofpoint.com/us/threat-reference/pharming