Online Identity Theft: Types And Methods For Committing

What is Online Identity Theft?

Everyone is unique. We all have our own set of traits, DNA, and fingerprints. Each individual possesses their own unique characteristics, interests, and talents to make up a unique identity. Our identity combines all of these things into us. When that identity is taken from us, or stolen, we lose who we are. Though we don't lose the sense of who we are to ourselves, we lose it to others. Bad actors masquerade around claiming to be us, behaving and committing actions as one individual under the disguise and at the expense of another.

Online Identity Theft is the use of someone else's identity for personal gain. The perpetrator "steals" a victim's identity and engages in various activities under the victim's name and credentials such as addresses, Social Security Number, account usernames and passwords, bank account information, and credit card numbers (Webroot). The victim's information may also be sold to various "bidders," seeking to obtain identities for nefarious reasons. According to the Consumer Sentinel Network of the Federal Trade Commission (FTC), approximately 3 million reports of identity theft and fraud were filed in 2018. 444,602 complaints were classified as identity theft, compromising almost 15% of the total reports (Insurance Information Institute). The identity thief looks to benefit themselves in their own interest and personal gain at the expense of innocent and unsuspecting people. The online security of hundreds of thousands of victims has been compromised and many have had their finances exploited and their reputation ruined as a result of such a heinous and serious crime.

Types of Online Identity Theft

There are various types of identity theft and the methods for how it is committed by perpetrators. In 2018, the top five types of identity theft fraud included 1) Credit card fraud in which new accounts were opened in victims' names, 2) Miscellaneous identity theft (i.e. online shopping, online accounts, insurance, etc.), 3) Tax fraud, 4) Mobile telephone with new accounts being opened, and 5) Credit card fraud in which victims' existing accounts were being used. The most prevalent type was credit card fraud with new accounts being opened. 130,928 reports were filed for this type, making up 40.5% of the "total top five" (Insurance Information Institute).

Simply put, any form of identity theft that has been committed using online methods can be classified as online identity theft. A perpetrator may commit Criminal Identity Theft, impersonating another individual to avoid police arrest and conceal criminal records. Financial Identity Theft involves using a stolen identity for financial gain, such as opening credit cards in the victim's name and making online purchases using stolen payment information. Medical Identity Theft occurs when one seeks health benefits using another's identity (Pixel Privacy). The types listed above are examples that may involve stealing one's identity through some method(s) carried out online.

Various forms of identity theft may be committed without the use of technology and the Internet. It may occur in the real world and the perpetrator may engage in Internet activities using stolen identities. The same goes for the theft occurring online and exploiting the identity through real-

world activities. Thus, various forms of identity theft may be committed for fraudulent actions and personal gain interchangeably both in the digital and non-digital world.

Methods for Committing Online Identity Theft

There are various means for committing online identity theft. Phishing involves attempting to acquire one's sensitive information through some form of digital communication. Sensitive information that could be phished includes the victim's name, usernames, passwords, payment information, address, and other contact information. The most common execution of phishing is sending out "spam" or "scam" emails with the goal of victims clicking on links, frequently disguised as promotions or rewards, and being prompted to enter their information to "claim their prize." Another objective is to have the victim download malicious files within the email containing malware that will infect the victim's computer, gaining the thief access to files and information stored on that particular device.

Pharming involves a hacker redirecting a legitimate website's traffic to a fake website. The hacker gains access to the website's server and installs a redirect address to the fake site. Visitors are now redirected to the hacker's fake site and enter their information to access accounts and complete purchases, making their information available to the hacker. The pharming method is similar to phishing as the victim is "tricked" into providing their sensitive information. However, the victim does not click on a suspicious email, but rather enters a web address they may have visited several times and had no reason to believe that the website's security had been compromised at the hands of a hacker.

Another method may involve a perpetrator creating a fake online profile to interact with people through email and social media. One instance could be that a perpetrator claims to be an employee of an organization with seemingly authentic credentials and requests the victim to "confirm their account" with their information. The thief may also impersonate a real individual or even use a stolen online profile to capture yet another online identity. Scammers may also create fake online dating profiles and start an "online relationship" with their victim. They may gain the victim's trust and the scammer may ask for gifts and financial transactions. They may also get to know their victim's intimate details which can be used if the perpetrator wishes to impersonate their victim in the future. Furthermore, the perpetrator may exploit other intimate information, such as revealing pictures, which can be used to blackmail the victim to send bank account information, credit card numbers, and effectively their entire identity. Also under the cover of an impersonation or fake identity, a thief may convince someone of an issue with their device or Internet and request remote access to "fix the problem," resulting in personal and financial details being disclosed to the perpetrator.

Who is at Risk?

Essentially, anyone's identity can be stolen. It can happen to completely unaware and unsecured people on the Internet as well as those who take necessary online precautions. People may be specifically targeted or chosen at random. Everyone has this common, preconceived notion that "it's not going to happen to me" and often retain this idea when they hear stories or learn that someone close to them has fallen victim to such a serious offense. Online identity theft is one of those things people hear about on the evening news and falsely assume 'well, it surely can't happen to me!'

Those who are the least informed about the dangers of online identity theft are perhaps most at risk for becoming victims, along with those not as familiar with technology and the Internet. A common group like this includes elders, who may not be as familiar with the Internet and technology as much as younger generations. In fact, most elders may only use the Internet for email and to “like” their grandchildren’s pictures on Facebook. However, simply owning an email account is enough for them to fall victim to online identity theft, specifically phishing, and may unsuspectingly click on a scam email targeting elders (i.e. “You could be getting more from your retirement, Alice! Click here to claim your benefits!”).

Another group is children. Even though today’s youth are growing up with the Internet and spending more time online than previous generations, they are another vulnerable group at risk for identity theft. Unless parental controls and supervision are utilized to manage a child’s Internet activity, young ones may be tricked into providing details such as name, home address, and contact information if they visit dangerous websites or click on malicious links (Johansen). Many kids enjoy playing online games, including ones downloaded from the app store. A child may download a fake app resembling an authentic game and could enter their parents’ credit card information to complete in-game purchases, ultimately handing over their details to the thief.

Possible Solutions and Prevention of Online Identity Theft

There are several actions to be taken upon discovery that one’s identity has been compromised or stolen. If the theft is caught early enough, one may immediately change passwords and security questions to try to regain complete control over all online accounts. The victim should check and close bank accounts and credit cards. If new accounts or cards have been activated without one’s knowledge, immediately report and close them. It is important to contact the Social Security Administration (SSN) and Department of Motor Vehicles (driver’s license) as well as filing a report with law enforcement, before serious offenses are committed by the thief in the victim’s name (Stay Safe Online).

Though there is never a sure-fire way to completely prevent online identity theft, there are considerable ways for one to prevent their identity from being stolen in cyber world. An individual may install anti-virus and anti-malware software to protect from hackers infecting their devices and to recognize if any malicious files are present. Installing the latest software updates can patch device vulnerabilities that could be exploited by hackers. When using email, people can be aware of phishing and recognizing malicious emails that may harm devices and collect information. A person may also update their password to stronger and more unique “passphrases” for each account and store them in a safe place (Internet Safety 101).

Another way to prevent online identity theft is to not go online in the first place. However, the vast majority of people have most likely already been online and own several accounts with extended history on the Internet, so this option is not available for most people. Some people in the world have definitely never been online, so at least they are safe from identity theft in the online world.

Precautions may also be taken offline. People should protect their devices (i.e. computer, smartphone, tablet), credit cards, and documents containing sensitive information. Caution should be utilized when receiving suspicious (scam) phone calls just as it would be taken with

phishing and scam emails. Bank accounts and statements should be checked frequently and suspicious purchases reported immediately.

Conclusion

One can never be too careful in the two worlds that exist today, the real world and the cyber world. Of course, countless precautions do not ensure complete, guaranteed safety on the Internet. Individuals engaging in online activity should hold constant vigilance and avoid suspicious strangers, bizarre messages, and shady websites. We may possess one, unique identity in both worlds, but there are countless villains masquerading around with fake and even multiple stolen identities looking to exploit the innocent and unsuspecting people of the Internet.