
Cybercrime and Society: Identity Theft

In the 21st century cybercrime has become one of the biggest forms of crime in the world. It's a cowardly act of crime which can be performed from across the world. It is estimated that cybercrime could cost companies worldwide over 5.2 trillion dollars over the next five years. However this is an estimated number as finding exact dollar amounts in cybercrime is very difficult because a lot of thefts aren't reported. One of the largest forms of theft in cybercrime comes in the form of identity theft, which "use of an individual's personally identifying information by someone else (often a stranger) without that individual's permission or knowledge. This form of impersonation is often used to commit fraud, generally resulting in financial harm to the individual and financial gain to the impersonator."

Identity theft is usually targeted towards a specific individual. Criminals will usually target someone and try to gain any type of public information from online and social media accounts such as a person's phone number or address, and if possibly an confidential information, such as a person's Social Security number, credit card numbers which can help the perpetrator take your identity more easily. Criminals have a lot of interest in social security cards, because social security numbers aren't updated, criminals can wait years to use it to steal someone's info. By acquiring access to that information, an identity thief can impersonate someone else to commit fraud. Most forms of identity theft are revolve around financial gains, some will gain access to personal accounts and then use that to gain a ransom from you in exchange for it back. In 2017, 7 million people experienced some form of identity theft according to a survey by Harris Poll in 2018, and happens regularly, every 2 seconds a person was victimized somewhere in the world.

Stealing peoples personal information has made has made huge strides since the start of the millennia. The older and simpler way of stealing information by criminals included techniques such as stealing mail, dumpster diving for information, eavesdropping on conversations which is referred to as shoulder surfing by some people, or just theft by unlawful taking. People even went as far as taking information from deceased individuals by collecting information tombstones. With the huge strides in technology in the past 20 years, more and more people are relying on phones and computers to do everyday tasks, cyber =crime criminals have grown with it. Instead of dumpster diving for or eavesdropping on people for information, criminals can simply take someone's personal data without leaving their house.

Criminals have gotten very clever now using techniques such as skimmers which are essentially copy machines that are placed on ATM card readers which collect all of your card information when using the ATM. Other methods include spam which can be in the form of a banking

Need help with the assignment?

Our professionals are ready to assist with any writing!

GET HELP

website or shopping website which usually asks you to update information and collects your data that way. Personal computers are also a big target for cyber criminals which can access all of your files and personal info without authorization. Much of these can be avoided if you are just smart about your information. Cyber Criminals mostly depend on people being ignorant to these types of techniques and much of these can be avoided if you just look for them. Skimmers are often a replica of the card slot itself that fits over the card reader and can be popped on and off. So the next time you use a ATM just give a small tug on the plastic part of the reader, skimmers can be easily found and removed if you know what you're looking for.

By being safe and cautious about these forms of theft can save you a ton of time in the end. In 2017 it was estimated that 140 million hours were spent of identity theft victims trying to regain and fix their information. Identity theft was ranked the number 1 consumer complaint in 2014 for the 15th year in a row. This is due to the hundreds of thousands of data breaches to large corporations each year. Criminals will steal hundreds of people's information from the corporations' data base. Large corporations tend to not share this info with the public and their consumers because it makes them look weak and shows that they can't protect their customers' info. It cost roughly 4 million dollars for each data breach that occurs. This is from either rein-busting customers or trying to upgrade the software to help better protect from it happening again.

Need help with the assignment?

Our professionals are ready to assist with any writing!

[GET HELP](#)