Identity Theft As The Fastest Growing Cybercrime

In this emerging world of technology, there are many people who use it for good; from connecting with friends on social media, to those donating to online support groups. However, emerging from the same world you have those who use the internet as a means of stealing information such as photographs, credit card numbers, and other private information. Having this information stolen is just as bad as having your wallet stolen, or perhaps much worse. It can take place anywhere; at a store, a business, or even your home. A lot of times, it's a person you once knew who is behind all of it! This unethical behavior is known as identity theft.

Identity theft is the fastest growing cybercrime gaining a new victim nearly every two minutes. 1 of 15 Americans have experienced identity theft in some form. It can happen much faster than you think. One click on the wrong website is all it takes. Some sites will secretly download malware that can track your every keystroke and send the information to either an e-mail address or 3rd-party application. Other cybertheft tools have been developed to copy and send off your recent browsing history. These criminals scope out anything that may be beneficial to them such as uploaded pictures, credit card numbers, and recently used login tokens. You know those websites that say "Secured by.."? They use something called a token that acts as a one-time password. "Typically services using this method will issue access tokens that last anywhere from several hours to a couple weeks. When the service issues the access token, it also generates a refresh token that never expires and returns that in the response as well." OAuth personnel state. If somebody is tracking your browser history, they can see those token 'IDs' in the site-link, spoof your IP address, and log into your secured account. That takes less than one minute. There's no telling what they log into first. It's quite possible that you've checked your bank statements lately and those pages can contain some extremely delicate information. If you see your password listed as stars, (******), Firefox and Chrome have a fancy feature that lets you convert that to plain text. From there, it just gets worse, and once somebody has your social security number, it's all downhill from there.

Amy Krebs was always very careful when using a computer, until one day, somebody had gotten access to her online credit reports. Now, Amy is the new victim. She first realized that something was going on when she received a call from a major credit card company saying that somebody had attempted to obtain a credit card using her name, social security number, and address. At first she thought that that call was a scammer trying to get her information. But it turned out that somebody really had tried opening an account with her info. The company said they would send a new card out to her, but before the call had taken place, the criminal had changed the home address listed in her account and the card was sent to them instead. Amy wanted to make sure there were no extreme charges so she checked her credit reports. Upon logging in, she was greeted with her security questions, "What addresses have you lived at?" and "What addresses have you worked at?". She was unable to view one of her report websites as the criminal had already overwritten the information on file. Six months went by with very little action able to be taken from companies, bureaus, and herself. In this time, the criminal had tried opening approximately 50 credit card accounts using Amy's information. Amy would receive multiple calls a day from different banks stating that an attempt was made but the account was flagged so no action would be taken. This all took a turn when Amy searched down her statements and found a medical collection agency listed. She then turned to the

police, who started a case and tracked her down. With a warrant, the criminal was arrested but she would not plead guilty. From courtroom to courtroom she pleaded not guilty and it wasn't until the trial that she finally pleaded guilty, but because it was a non-violent felony charge, she was not placed in jail. She was instead sentenced to community service. After this ordeal, Amy wanted to share her story to help people so she started a blog called 'AKAJaneDoe'. Amy says, "Question when someone asks you for your SSN. I'm shocked by how often, when I ask, 'Do you really need that?' they say no... Wherever your information is held, where you file taxes, where you buy a car, go to school, get a job, they have your Social Security number." That's a good point. Don't give out any sensitive information or any information, for that matter, regarding your personal life.

In September of 2017, Equifax, one of the largest consumer credit report companies, revealed it had been hacked leaving 143 million American citizens vulnerable to identity theft. IT specialist Art Damiao encountered identity theft soon after when a hacker called him after breaking into his personal email, claiming that he had all of his information. Art wanted to test him so he asked what his social security number is. The hacker read it off in perfect sequence and Art hung up. The hacker soon called back to tell him that would no longer store his information or use it if Art were to send him $300 of bitcoin. The hacker was holding him up for ransom without touching him. All it took was his email account. Art always enabled Two-Factor Authentication, which sends alerts to your phone when a password change attempt is made. He received many notifications of this type during this encounter. Cybersecurity expert Serhat Atli took reporters on a tour of the dark web, showing them where criminals can make deals for bulk lists of US citizen names, date of birth, social security numbers, and credit card numbers, many for less than $50. "Damiao did not pay the bitcoin ransom. He doesn't know how his information leaked out, but says he did learn from the Equifax website that he is one of the millions of victims of that hack, which he says is certainly suspicious timing." says Anna Werner at CBS News.

Another popular form of capturing somebody's identity is through the form of ransomware. These hackers will call you claiming to be a Microsoft certified technician who has detected malware on your system. They will guide you in connecting their computer to yours in what is known as 'remote desktop connection'. Once they are connected to your computer, they can copy files over to your desktop and run a file which can lock you out of your computer. Often times, they will change your wallpaper to an almost-official looking Homeland Security warning stating that they have found illegally obtained software on your computer. They will ask your for any amount of money usually in the form of a gift card. Once your computer gets this kind of virus, it takes an entire hard drive wipe to get it back to running state. But during the time that your desktop if connected to theirs, they have all that time to copy your files, cookies, contact lists, anything on your computer.

So what can you do to prevent your identity from being stolen? Don't ever give out your personal information unless you completely trust the company or person you are communicating that information to. If at all possible, bring any confidential material to the physical place of business. If your phone is constantly flooded with calls about free hotel stays and computer malware, take action and place yourself of the Federal Trade Commission's official 'Do Not Call' Registry. Practice safe computing by installing firewall, anti-spyware, and anti-virus software on your computer such as Norton or BitDefender. In the real world, watch your bags and your pockets. You can never be too careful when it comes to saving yourself from fraud. Don't leave any documents in your vehicles.

If you think you have become a victim of identity theft, contact a credit reporting agency's fraud alert department and place a fraud alert on your credit report. This stop thieves from opening any accounts in your name. Most credit companies offer no-cost fraud protection where you won't be held responsible for charges made by thieves who steal your account info. Call your banks and ask them to close your accounts and open new ones with new PINs and passwords. Call the police and file a report so there is a case for the crime. Check your statements daily for any new activity. Contact the credit reporting agencies and ask to have the fraudulent activity removed from your reports. Be sure to remember to ask your creditors if you can reverse the fraudulent charges placed on your accounts. It would be crummy not to get back any of the money that you didn't spend. After that, it's up to the police to catch the criminal and hopefully teach them the error of their ways.

Identity theft can happen to anyone. From the soccer mom on Facebook to a SpaceX administrator, anybody can have their information stolen. It's rarely a matter of how secure your documents are, but rather the ethical decision-making of those around you. It's not hard to pick up a wallet. People will do anything to survive, even if it means ruining somebody else's life. There are, however, ways to prevent it. Utilizing anti-malware software and having guidelines for what you share with people can prevent identity theft. If something seems too good to be true, it usually is. So don't go entering your social security number into an advertisement that says you won $1,000 for clicking on a swinging monkey. That's a sure-fire way to end up in the same circle as Amy or Art. They didn't ask for it.