Security Spotlight

An Informational Guide for Securitas USA Clients and Employees

September 2015 | Securitas Security Services, USA, Inc. | Number 138

Identity Theft: The Digital Doppelganger

"But he that fliches from me my good name/Robs me of that which not enriches him/And makes me poor indeed." (Shakespeare, Othello, Act iii, Sc.3.)

We live in a modern digital world where there exists a growing and unknown threat from cyber thieves. As we approach the end of the summer and begin to prepare for the holiday season, we must realize that we all are at risk of identity theft. In the era of quick internet searches one can find out a treasure trove of information on people with nothing more than a name and maybe an address. Understanding and awareness is what can mean the difference between proactively stopping a crime in its tracks or working reactively for months, if not years, to repair the damage.

What Is Identity Theft?

The United States government defines identity theft as, one who steals your personal information and uses it without your permission for some form of gain (Federal Trade Commission). There are a myriad of methods that these thieves employ to gain your personal information and data. From the relatively low tech 'shoulder serf' where an individual watches from behind or within eye sight of a machine, as you enter numerical information, such as an ATM pin or zip code at a gas station pump, to the more advanced 'fishing' emails. In this a thief sends an official looking email stating that you have been selected or promised some financial benefit, but before you can continue you must supply validating information. The unsuspecting individual responds with their personal information, which the spammer utilizes to begin the process of identity theft. This can lead the criminal to take out a loan or credit card in your name, without you being aware, because they have all your pertinent data. The victim of the crime might not discover what has happened for some time because these thieves usually have the bill sent to another address. It then masks the crime and allows them a "get-away" in the digital domain. This can cause immediate repercussions for you in terms of negatively impacting your credit score, calls from debt collectors about the debts taken out in your name, collection notices, bank accounts missing money, false charges on your credit card, and banks declining transactions associated with your accounts.

Secure Your Information

One of the simplest ways you can protect yourself is to be aware of what financial information is used and shared. Be extremely careful with whom you provide your personal information to, whether it is over the phone, through email, or a website. If you are the one who has initiated the contact than most times you will be protected. It is when you are contacted through any means with someone requesting information. If you are ever in doubt do NOT provide it. If it is a phone call tell

them you will call them back, but do NOT use the number they provide. You can search your paper statements or go online to find the phone numbers or contact information of any organization to verify. Customer service representatives will be able to tell you if they have tried to contact you regarding a request for information. If you are unsure you can contact the Better Business Bureau to verify any business, brand, or charity for its legitimacy. Before you discard such items as cell phones, tablets, or personal computers, make sure you factory reset the systems or wipe the digital information from them. If you are submitting information online look for the 'lock' icon in the internet browser at the top. Also, look for sites that have web addresses that begin with 'https' in the browser. The 's' stands for secure. If it is not present then whatever information is sent is not protected. Never leave your passwords on a sheet of paper that can be easily found in your desk at work or other less secure places. Finally, be careful what information is posted to social networking apps, because tech savvy individuals can piece together your personal information with your indirect help.

How To Protect Yourself

The best defense is a great offense, as the saying goes. This is definitely true when dealing with identity theft. Like the Securitas value of Vigilance, one must actively protect personal information from would be thieves. The US Department of Justice states that you should utilize a 'need to know' attitude when it comes to your personal information. First and foremost do not share your social security number unless absolutely necessary. Next, when you receive your monthly statements from financial institutions carefully review them for any possible errors or mistakes. Shred all personal papers and records before you throw them in the trash, once you discard something you lose control over it. Do not employ one password for multiple sites, rather vary your passwords for an added layer of protection. Obtain a copy of your credit report, one from each of the three main credit reporting agencies. You have the legal right to a free report once a year. Carefully review all the information and if there are any unauthorized or incorrect pieces of information immediately dispute it with the credit agency. Also, as a further optional method, you can subscribe to a credit monitoring company who will notify you immediately if there are any associated changes with your credit score. Finally, if you are going to be away from home for an extended period of time and a friend or neighbor can't collect your mail, you can go online and submit a mail hold to the US Postal Service until you return. This way you will ensure that no one is rummaging through your mail box while you are away.

What if Your Identity Is Compromised?

If the worst case scenario does occur and you have become a victim of identity theft there are several actions that you can immediately take to begin the process of protecting yourself. It will be time consuming and in some cases money out of your own pocket, but it is necessary to correct and protect yourself. You should do all of the following:

· Call one of the three major credit reporting agencies and have them place a fraud alert on your credit report. By law they must notify the other two agencies to do the same. An initial fraud alert is good for 90 days, but you can get an extended fraud alert for up to 7 years, with law enforcement documentation.

· Order all three credit reports to review all associated information with your credit. If there are errors notify the respective agency. Note: credit reports and scores do vary slightly between the three major credit reporting agencies, hence why you should order all three.

· File an Identity Theft Report through the Federal Trade Commission. This will allow you to get fraudulent information removed from your credit report and stop any debt collections associated with those illegal accounts.

· Take your Identity Theft Report and file that with the local FBI or US Secret Service field office. Obtain a copy of the completed report for your records. The federal law enforcement agency will open a file and begin an investigation into the crime.

· Contact the Social Security Administration if you suspect that your Social Security number has been compromised or used in the identity theft.

· Contact all your financial institutions to check to make sure your accounts have not been compromised and for them to track any and all future transactions associated with those accounts.

· If you suspect that a thief has submitted a change of address form with the US Post Office contact the US Postal Inspection Service.

· Finally, contact the Internal Revenue Service if you believe that the identity theft was associated with a tax filing. Unfortunately, this has become a recent and growing crime with the ease of digital submission of tax returns.

Contact Information

Better Business Bureau – www.bbb.org
Federal Trade Commission – www.identitytheft.gov
Internal Revenue Service – www.irs.gov/Individuals/Identity-Protection
Social Security Administration – www.socialsecurity.gov
United States Postal Service – www.postalinspectors.uspis.gov