Security SpotLight

Securitas Security Services, USA, Inc.

November 2017

Number 164

An Informational Guide for Security Clients

Secure Your Information

A simple way to protect yourself is by being aware of what personal information is being used and shared. Be extremely careful to whom you provide personal information, whether over the phone, through email, or on a website. If you are the one who has initiated the contact, then most times you will be protected. Be alert when you are contacted by someone requesting information. If in doubt, do NOT provide it. If you receive a phone call, offer to call them back, but do NOT use the number they provide. Use the number from a paper statement or search online to verify the contact information of any organization. Customer service representatives will be able to tell you if they have tried to contact you with a request for information.

Integrity / Vigilance
Helpfulness

Identity Theft

We live in a digital world where a growing threat from cyber thieves exists. In preparing for the holiday season, we should acknowledge our vulnerability to identity theft, as evidenced by the numerous data breaches making headlines. Understanding and awareness can mean the difference between proactively preventing a crime or reactively spending months, if not years, repairing the damage.

What Is Identity Theft?

The United States government defines identity theft as personal information that is stolen and used without permission for some form of gain (Federal Trade Commission). There are a myriad of methods thieves employ to gain access to your personal information and data. Criminals can take out a loan or credit card in your name, without you being aware, using stolen personal data. Immediate repercussions can include a decline in your credit score, calls from debt collectors, collection notices, money missing from bank accounts, false charges on your credit card and transactions declined for accounts associated with your name.

Protect Yourself

The best defense is to be proactive. Like the Securitas value of Vigilance, one must actively protect personal information from would-be thieves. The U.S. Department of Justice recommends employing 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, carefully review monthly statements for any possible errors or mistakes. Shred all personal papers and records before throwing them away. Do not use the same password for multiple sites; 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. You can also subscribe to a credit monitoring

SpotLight

Securitas Security Services, USA, Inc.

Secure Your Inforamtion (continued)

The Better Business Bureau can verify the legitimacy of any business, brand, or charity.

Before discarding cell phones, tablets, or personal computers, erase all information and reset the systems to the original factory settings. Only submit information online when the 'lock' icon is in the browser address bar. Also, look for sites with web addresses beginning with 'https.' The 's' stands for secure. If it is not present, transmitted information is not protected. Never leave your passwords on a sheet of paper that can be easily found. Finally, be careful about sharing information on social media sites. Tech savvy individuals can piece together your personal information with your indirect help.

Additional Resources

Better Business Bureau
www.bbb.org

Federal Trade Commission
www.identitytheft.gov

Internal Revenue Service
www.irs.gov/Individuals/Identity-Protection

Social Security Administration
https://www.ssa.gov/

service that will provide immediate notification of 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, request a mail hold through the U.S. Postal Service until you return. This will help prevent anyone from rummaging through your mailbox while you are away.

What If Your Identity Is Compromised?

If you become a victim of identity theft, there are several immediate actions that will help mitigate the damage. The process is time-consuming, and some steps have a monetary cost, but it is necessary to salvage the situation and protect yourself. If your identity is compromised, do all of the following:

- Call one of the three major credit reporting agencies and 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 can be extended for up to seven years, with law enforcement documentation.
- Order all three credit reports and review all information associated with your credit. Notify the respective agency of errors. Note: credit reports and scores vary slightly between the three major credit reporting agencies, hence the need to 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 illegal accounts.
- File your Identity Theft Report with the local FBI or U.S. 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 verify that 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 U.S. Post Office contact the U.S. Postal Inspection Service.
- Finally, contact the Internal Revenue Service if you believe that the identity theft was associated with a tax filing. The ease of submitting a digital tax return has made this a growing crime.

Integrity / Vigilance
Helpfulness

For more information on this and other security related topics, visit the Securitas Safety Awareness Knowledge Center at
http://www.securitasinc.com/en/knowledge-center/security-and-safety-awareness-tips