Centreville Bank

Transcript for Identity Theft Prevention From Centreville Bank

Introduction

The message you are about to see is true. The information provided is to protect the innocent. This is our country. The United States of America. Over 8 million of its citizens will be victims of identity theft this year... resulting in the loss of billions of dollars. That's when we go to work. Our job is to help you prevent identity theft. We carry a badge. Identity theft occurs when someone uses your personal information without your knowledge to commit fraud. While the terms may sound unfamiliar... Phishing, Pharming, Spyware, Dumpster Diving... they are actually techniques used by thieves... to put your identity... and your financial well-being at risk. And their attacks grow more frequent and sophisticated every year. Think of us as your Identity Theft Security Team... and we're here to help. We'll give you the facts about Identity Theft... what to watch for... and how to avoid being a victim. Take a few moments to learn about each of the Identity Theft Danger Zones... and the simple steps you can take to avoid being a victim.

Email

Sending and receiving email is as common today as using a home telephone. Some emails arrive disguised as official notices. They might claim to represent your financial institution... a credit card company... or maybe another source. You never know. It's a scam called phishing. And that's just what the crooks are doing. Fishing for your personal information. The best defense is to learn how these scams work... and how to protect yourself, along with your good name. The first step is to learn how to spot phishing... and other email scams. Always keep in mind that... Any email requesting personal information... or asking to verify an account... is usually a scam... even if it looks authentic. The message will often threaten a dire consequence... if you don't respond immediately... such as closing your account. And the email may instruct you to click on a link... or call a phone number to update your account... or even claim a prize. These are clear signs that someone is "Phishing" for your information. By following these simple steps... you can protect yourself from most email scams. Never respond to any email asking for confidential information. Even if it appears urgent. Chances are it is a fraudulent email. Never click on a link from an email. Instead, type the known website address into your browser. Do not call any phone numbers provided in a suspicious email. It could be a fake phone number. And finally... always use anti-virus and anti-spyware software on your computer... and keep them up-to-date. Remember, email is not a secure form of communication. So feel free to use your email... but don't use it to send or receive confidential information. And if you follow the four basic steps listed... you can protect yourself from most phishing and other emailscams.

Internet

This is the World Wide Web. It's a big place out there... with over 10 billlion Websites. People use it every day to keep in touch with friends... find information and do business. You can find just about anything... including crime. Malware, spyware... trojans, viruses... keystroke loggers. These are the tools used by criminals... and if you're not careful, they can steal your identity. There's one thing you need to know. That's how to use the Web safely. Learning how to practice safe surfing is easy. Follow these steps to protect your computer from the majority of Internet crime. Make sure you have anti-virus... and anti-spyware software installed on your computer. Keep them updated... and run a full system scan at least weekly. Keep your computer operating system up-to-date... and your firewall turned on. Use strong passwords for secure sites. These should include eight or more characters with random numbers... and change passwords every six months. If you download anything from the Internet such as music... movies, or pictures... make sure you do so only from trusted Websites. Downloads can be infected with spyware attached to the file. Watch for signs of spyware... this includes frequent pop up ads... unexpected icons on your desktop... random error messages... or sluggish computer performance are all signs of infection. Run a full system anti-virus and anti-spyware scan... to safely remove. Be careful when using public computers... to perform any type of personal transactions. Just logging into a Website... may give away passwords and other private information... if spyware has been installed on that computer. Following these steps will help protect you from identity theft on the internet.

Telephone

People use telephones every day... at home, at work... or anywhere from their mobile phone. But there's something many people don't know. Your telephone is one of the most often used sources for criminal activity. Here's how it works. Your phone rings. The caller claims to be from your financial institution... or any other source. They begin asking questions about you and your account. This could be a telephone scam called vishing. Someone is attempting to steal your identity. And it happens to millions of Americans every year. Follow these steps to protect yourself... from most types of Identity Theft telephone scams. Never offer personal or account information over the phone... without verifying the caller's identity. If you are uncertain of the identity of a caller... hang up and initiate the call yourself... using a known phone number. Do not call any phone number received in a voice message... or email asking for personal information. It could lead you to a phony answering system. As a general guideline... be highly suspicious anytime you are requested to provide personal information... over the phone.

Payments

It was 4:30 on a Saturday afternoon... the weather outside was clear and mild. My partner and I were responding to a 459ID... another case of stolen identity. When we arrived at the scene, the evidence was everywhere. The home had no paper shredder... A checkbook was laying open on the table. And there was a credit card statement in the trash. This victim was careless with their personal information. You know what gets me? This crime could have been prevented. Don't make it easy for criminals to steal your identity. Here are some common sense tips... to avoid being a victim of payment fraud. Balance your checkbook... and verify all account and credit card statements... as soon as they arrive. Keep all checks, credit and debit cards in a safe place. Don't leave outgoing checks or paid bills in your mailbox. And report lost or stolen items immediately. Don't write PIN numbers on your credit or debit cards... or leave them in your wallet for a thief to find. Use a paper shredder to securely dispose of any documents... containing personal information. Make online purchases only from trusted sites. If you have questions about a company... you can check them out with the Better Business Bureau. Consider paying all your bills electronically... with online bill pay service. This method is more secure than mailing paper checks. Reducing your risk of identity theft... starts with protecting your personal information. Always be diligent about protecting your identity.

Home

The information you are about to receive is true. This is the neighborhood. It could be anywhere in the country... it might even be your own. It's a friendly place with helpful neighbors... kids playing together... there might even be an annual picnic or block party... you never know. But not everyone in this neighborhood is helpful. Someone could be out there... trying to steal your good name... and your identity. And they're doing it by going through your trash... and your mailbox. If you don't protect your personal information around the home... you're headed for the Danger Zone. I've seen it too many times. I carry a badge. Follow these steps to protect against identity theft in your home. Invest in a personal shredder. This is your first line of defense. Shred checking and credit card statements... cancelled checks... pre-approved credit card offers... or anything with your personal information on it before disposal. Place garbage out on the morning of pickup... rather than the night before. This gives dumpster divers less opportunity to go through your trash. Install a mailbox with a locking mechanism... or pick up your mail immediately after it is delivered each day. Change that old habit of placing mail in your mailbox... for the carrier to pick up. Always place out-going mail in an official, secure mailbox. It's good practice to store your mail... bank statements... and other papers someplace where they are out of sight... and out of reach of anyone... who might be in your home. By following these steps... You are on the right track to protecting your identity. Learning about all the identity theft danger zones... and the simple steps you can take to avoid being a victim... is the best way to protect your good name.