The Identity Theft
First Aid Kit

Safety Tips, Prescriptions and Resources for helping you keep your identity safe

Contents

Click to jump to a specific topic

Introduction

VanderLugt ▪ Mulder ▪ DeVries ▪ Elders
Certified Public Accountants

I was surprised by the first occurrence. Then, I learned that the IRS was receiving fraudulent tax returns across the country and that there seemed to be common type of a victim - ***doctors across the country were experiencing identity theft***. Shortly after April 15th, I set out to write and produce this simple e-booklet from the compiled information that we were gathering on the subject. The purpose of producing this resource is to answer three main questions received from clients:

1. What should I be doing to protect myself from Identity Theft?
2. What do I need to do if it happens to me?
3. Is there software that I could use to help protect my identity?

This free ebook is meant to be a quick resource for you. The third-party products referenced in this ebook are for your information only and are not meant to be an endorsement of the products. At this stage of our research, I was simply looking for some of the top resources. If you have questions regarding any of this information, please feel free to contact me at www.vmde.com.

Michael L. DeVries CFP®, CHBC, EA
(616) 949-9030 x12

Safety Tips

Protect your Social Security card and numbers. Do not carry your Social Security card or any documents that include your Social Security number in a wallet that can be misplaced or within a purse that can be stolen. Do not provide your social security number over the phone, through the mail or on the internet unless you have initiated the contact or you know with whom you are dealing.

Secure e-mails using an encryption process. If you need to attach a document to an e-mail that contains your social security number, use an encryption process to secure the document that you are sending. We offer such a process when sending documents to us. So, be sure to ask us about this before sending us documents via e-mail.

Opt out of pre-approved credit cards. Many times identity theft is committed simply by filling out the pre-approved credit card applications individuals receive via the mail. In order to limit this risk, you can call 1-888-5-OPTOUT (1-888-567-8688) to have your name removed from direct marketing lists.

Safety Tips

Protect your computer. Use firewalls and anti-spam/virus software on your computers and home network. Be sure to keep your software current by updating security patches, and changing your passwords occasionally. If you ever receive an e-mail or pop-up message that asks for person or financial information, you should not reply or click on the link in the message. If you feel that you have received a fraudulent e-mail or a suspicious file, you may forward these emails (without opening the attachment) to the Federal Trade Commission at www.ftc.gov.

Create strong passwords. Make sure to use passwords on credit card, bank, and telephone accounts that are not easily determinable or available. Avoid using information that can be easily associated with you such as your birthday, your mother's maiden name, your spouse's name, your children's name and/or the last four digits of your telephone number. Also, make sure to avoid using the same password for all accounts.

Click and Shop with Caution. Don't click on links contained in emails or social network sites that appear to be from friends or Aunt Gertrude, but the content just doesn't look like something they would send. And while shopping on-line can be a great experience, be sure to evaluate the site with which you use your credit card.

Safety Tips

Safeguard your financial and personal information. Safely store your financial and personal information under lock and key. Safeguarding your information is very important for every individual, especially when storing such information on a computer, mobile device or even using "cloud based" applications.

Guard your mail from theft. When away from home, have the U.S. Postal Service hold your personal mail.

Guard trash from theft. Make sure to tear or shred receipts, insurance information, credit applications, doctor's bills, checks and bank statements, old credit cards, and any credit offers you my receive in the mail, as well as any other source of personal information.

Protect wallet and other valuables. Always be aware of what is in your wallet. Individuals should only carry identification information and credit and debit cards that they regularly use in their wallet. Keep track of all credit cards and keep the 24-hour emergency telephone numbers of all credit cards you possess in your cell phone's address book. That way, if credit cards are ever stolen, you can quickly call the issuing credit card company and put a block on all potential unauthorized transactions. Most debit cards do not have fraud protection insurance, so when using them be aware of the risks involved and try to minimize those risks by checking your balance often and/or note where you had used your card.

Safety Tips

Use of unsecured Wi-Fi. While it may be convenient to get online at a local café, avoid the processing of bank transactions or looking up your account activity when you are online at an establishment that offers unsecured connections. Also, be sure to secure your home Wi-Fi network. Criminals have become increasingly adept at intercepting unsecured Wi-Fi communications.

Check your personal credit information (credit report). The Fair Credit Reporting Act (FCRA) requires each of the nationwide consumer reporting companies – Equifax, Experian, and TransUnion – to provide you with a free copy of your credit report, at your request, once every 12 months. The Federal Trade Commission's Web site provides instructions on how to access free credit reports or you can also find this information by typing key words such as "free credit report" into an Internet search engine. The credit rating agencies Web sites also provide information on accessing your credit ratings.

Prescription

If you feel that you are a victim of identity theft, you should take immediate steps to minimize the risk of damage to your identity:

- **Place an Initial Fraud Alert**
- **Order your credit reports**
- **Call the Federal Trade Commission (FTC) to report the crime**
- **Contact the IRS, Social Security Administration, and your local taxing authorities**

Place an Initial Fraud Alert

Three national credit reporting agencies keep records of your credit history. If someone has misused your personal or financial information, call one of these agencies and ask for an initial fraud alert on your credit report.

A fraud alert is free and will stay on your credit report for 90 days. You may renew your alert every 90 days. The agency that you call must tell the other agency's about your alert. Make sure that the credit reporting agency has your current contact information so they can stay in touch with you.

EQUIFAX
1-800-525-6285

Experian
A world of insight
1-888-397-3742

TransUnion
1-800-680-7289

Prescription

Order your credit reports

Once you have ordered your credit reports from the 3 agencies, review the reports for any unauthorized charges or accounts. Contact any related businesses if your accounts have been compromised. Make sure to record dates that you made any calls and/or sent letters to businesses. This information can be used when filing a police report or reporting to the Federal Trade Commission.

Contact the Federal Trade Commission (FTC) to report the crime

The FTC is available online at www.ftc.gov or by telephone at 1-877-ID THEFT (877-438-4338). The FTC works with individuals who believe that they have been victims of identity theft. They provide valuable materials as well as support to help contact enforcement agencies and credit reporting agencies to minimize damages.

Prescription

Other Agency's that are helpful for identity theft victims are:

Internal Revenue Service (1-800-908-4490) can help those who suspect that someone may have used improper identification information and caused tax violations. Information on reporting tax fraud to the IRS and additional steps to take are available online. You will need to complete Form 14039 and mail it with any other documentation to the IRS.

Michigan Treasury may be notified via email, by calling 517-636-4486, or by mail at: Identify Theft Unit, Income Tax Division, P.O. Box 30477, Lansing, MI 48909. Include taxpayer's name, address, last four digits of the Social Security Number, and brief description of the situation.

Social Security Administration (1-800-269-0271) can be contacted if a victim believes that his or her Social Security number has been used fraudulently.

The local FBI and/or U.S. Secret Service agencies can help victims report and investigate different types of identity theft.

Resources

Click on the Company Logo to go to their website

Password Management

I recently heard that you should think about your passwords like underwear – change them often. As funny as this may sound, it is true that regularly changing passwords would be a good practice. However, I really can't stomach the thought of having to change and manage all the passwords that I have for various online services.

As the number of passwords I need to remember continues to increase, finding a resource that assists me in managing them will be important to maintain my sanity. Password management software will also assist you in establishing a good password.

The hyper-linked resources listed to the right are password management systems that I have found and will be investigating for my personal use. This is not an endorsement, rather simply a resource for your information.

LastPass ****

1Password

PasswordBox

dashlane

Resources

Click on the Company Logo to go to their website

Identity Theft Protection

Many steps can be taken to protect your identity for free – go back and refer to the Tips Section of this Identity Theft First Aid Kit.

The key in all the tips offered is that you have to do them. Good intentions will not work. Following through and taking the necessary steps is something that some people just don't do very well. If you are one of those people, then check out the hyper-linked services to your right.

This is not an endorsement of these products, rather simply a resource for your information.

LifeLock
Relentlessly Protecting Your Identity™

IdentityForce.™

IDENTITY GUARD.

TrustedID®
You're in control

Resources

Click on the Company Logo to go to their website

Antivirus Programs

Antivirus software is used to safeguard your computer from malicious virus software that seeks to obtain information stored in your computer.

Even if you use programs, like the ones hyper-linked to the right, you should always use common sense when surfing the web. Avoid websites with suspicious pop-up ads and be careful not to click on links that appear in strange emails that were sent from your friends or appear on social media sites.

Cybercrime continues to increase and it's fueled by common mistakes people make when connected to the Internet.

This is not an endorsement of these products, rather simply a resource for your information.

McAfee An Intel Company

WEBROOT

Norton by Symantec

PANDA SECURITY

Resources

Click on the Company Logo to go to their website

File Sharing

Cloud based file storage and sharing software allow you the ability to sync your files between various devices – phones, PC's and Mac computers.

When choosing a service, be sure to find one that offers secure file sharing.

This is not an endorsement of these products, rather simply a resource for your information.

CITRIX ShareFile

HIGHTAIL

box

EGNYTE