


THE MONEY COACHES

Nothing can bring a real sense of security into the home except true love.
Dr. Graham

IDENTITY THEFT: HOW TO AVOID IT

Criminals will use many different means to attempt to obtain your personal information. Here are a couple to watch out for.

In an age where more financial transactions are done electronically than ever, identity theft is a very real problem. If you have had your identity stolen, you understand how trying it can be, but if you haven't, you may have no idea how at risk you may be or what you can do to lessen your vulnerability to it.
According to the Federal Trade Commission, they estimate that 9 million Americans yearly experience identity theft in some form. This is a real issue and it is not going away, so the best thing you can do is take steps to protect yourself from it.
What does that look like? That's what we are going to be talking about this month. Here are some of the primary ways to help protect yourself from identity theft.

Watch out for phishing scams.

Many times we are our own worst enemy when it comes to identity theft. Those trying to scam us out of our personal information are able to do so by preying upon ignorance, or simply rash action.
Here is an example: I once received an email that purported to be from Comcast informing me that my service was about to be disconnected due to non-payment and that to avoid interruption I should make a payment immediately. It seemed very official, had a random dollar amount owed, and had all the logos and images to indicate it was completely legitimate. The problem was, I don't have any service with Comcast. This was a scam.

The purpose of this email was to catch someone who *does* have Comcast service and might think that they are behind on their bill. This email could've caused them to hurriedly click the link and provide their login and password, thereby handing the person on the other end access to their account and personal information. These kinds of scams are common, and their entire purpose is getting you to provide login or credit card information. As a general rule, you should never click a link sent in an email which is asking for a password. If you make online payments with any business, go directly to their website rather than clicking a link from your email. Most of these types of scams prey on inattentiveness, so be aware of what you are doing before you sign in.

Phone scams are another common tactic to get your information.

One of the ways that is becoming common to attempt to get your personal information or money is by contact you over the phone. Scammers will do this in a multitude of ways, but it is typically done by impersonating someone from a legitimate business. For example, the IRS is the source of a constant supply of scam phone calls. In fact, more than $23 million has been paid since 2013 to scammers pretending to be the IRS.
How do they do it? They use a couple methods. First, they'll make unsolicited phone calls, often impersonating an IRS official and providing bogus credentials as a means of making themselves appear legitimate. They'll often attempt to intimidate and bully you into making a payment, sometimes even threatening with arrest if payment is not made. What can be even more confusing is that they are able to spoof caller ID, enabling them to make their call appear to be from the IRS.

This is not limited to the IRS, but can be from any company you may deal with. Their methods will be similar and their goal will be to get you to give over personal information or money. The best method, as with the emails, is to let the person know you will hang up and call back using the official number for the company requesting payment. Doing this lets you make sure that if you pay anything, it is going where it should.

Identity thieves also target your trash.

One thing you have to watch out for are those who use "dumpster diving" as a means to get to your personal information. Discarded mail, receipts, credit offers, or any other personal information that you throw away can find itself in the hands of a person who digs through it to get your stuff.
This is a primary reason to get yourself a paper shredder and use it liberally. Additionally, don't let your mail pile up on vacation, put it on hold so you don't become an appealing target to have it stolen and used in the same way.

Overly simplistic passwords can cost you.

No one likes having to remember a tough password, especially if they are required to be changed often. However, when you use weak passwords or passwords that are too easy to crack, like your birth date, address, or even "password," you put yourself at risk of identity theft.
If there is a data breach within a company you do business with, it is important to change your password, as it may be compromised through that breach. Don't let convenience come back to bite you!

Monitoring Your Credit Report

Sometimes even if you try to do everything the right way and are cautious, you can still end up getting your identity stolen. Companies that have your information can be hacked, or be careless with their own paper records, and just like that your information is compromised.

That is why it is very important to keep an eye on your credit report and check it regularly. Your credit report shows accounts in your name and will indicate any that have been opened. This gives you a chance to identify anything out of the ordinary and limit the damage done to you.

How do you go about getting your credit report? It isn't all that complicated. You'll need to get your report from each of the three credit bureaus, because sometimes the information they have available can differ depending on which one credit holders report to. The three credit bureaus are Equifax, Experian, and TransUnion.

You can request your credit report free from them each year, and while you won't get your credit score without paying a fee, you'll get the information you need to help identify possible fraud and deal with it.

We recommend getting information directly from the three bureaus rather than sites like Credit Karma or Free Credit Report, because many third party sites attempt to charge you for a credit report which you can get for free. What's worse, many will rope you into subscription services that can be a headache to shut off if you are not cautious.

Because you are able to get your credit report free each year directly through the Annual Credit Report website, there is little reason to go elsewhere.

Credit Bureau Information

Equifax
(888)766-0008
www.equifax.com

Experian
(888)397-3742
www.experian.com

TransUnion
(800)916-8800
www.transunion.com

Another great resource for information about your credit reports is the FTC page, which answers several frequently asked questions and has a video which explains how to get your free annual report. You can access that page here:

Federal Trade Commission Website

If you find issues with your credit report or are unsure how you should proceed once you have your information in front of you, you can contact us through The Money Coaches website or via phone or email. Additionally, if you have an other questions related to identity theft, how to protect yourself, or what to do if you think you've already fallen victim to it, don't hesitate to reach out to us. We can help point you in the right direction.

Lincoln Financial Group Corner

Putting a security freeze on your credit

A security freeze works by the consumer requesting the freeze with each of the credit bureaus. Once the freeze is in place, potential creditors are unable to access both your credit report and score unless you "unlock" your file – using a PIN number established when the freeze was initiated. This prevents would-be identity thieves from establishing new credit in your name. The consumer can still check their credit report and score at any time because the consumer places the freeze; this measure does not impact your credit score.

Current creditors are exempt from the freeze, along with law enforcement and other governmental agencies. And, if an account in collections exists, debt collectors are allowed to access your file as part of the collections process.

State laws control security freeze rights. Therefore, fees for establishing a security freeze vary by state and tend to range from $3-$20, with $10 being average. A fee is assessed for the initial freeze and, depending upon the state, may also be assessed for lifting the freeze, replacing the freeze or eliminating the freeze altogether. In cases of identity theft, most states do not charge any fees to enact a freeze and also may provide this for free to the elderly or minors.

Other options exist for limiting access to credit. A fraud alert is one example, however, it is only a temporary measure that lasts for 90 days. An extended fraud alert is also available to victims of identity theft; however, this also expires in time. A security freeze is a permanent measure until the consumer chooses to lift the freeze.

For more, check us out at www.themoneycoaches.com!

THE MONEY COACHES

Rich Keller
Cell: (765) 592-0027
rich@themoneycoaches.com

Kathy Keller
(765) 592-0285
kathy@themoneycoaches.com

Chris Blystone
(765) 731-1107
chris@themoneycoaches.com