In this issue:

Welcome to our October Savvy Cybersecurity newsletter. Read on to learn about all the happenings in the cybersecurity world this month, such as:

- The puppy scam to avoid
- How Covid-19 has affected identity theft numbers
- Two scams targeted at financial professionals and their clients
- And more

Home Title Fraud: How to Protect Yourself

Earlier this month, I received a question from a Savvy Cybersecurity member. A prospect that the advisor was trying to win reached out and mentioned seeing commercials about home title insurance; he was wondering if such a product was necessary to protect against home title fraud.

Home title fraud occurs when a scammer obtains your home property title and transfers the ownership into their name. In some cases, the scammer creates fraudulent home title documents and tries to pass them off as legitimate. In more advanced cases, the scammer will commit identity theft first and then do a home title transfer.

What happens when your home title is stolen? The fraudster can use your home equity to secure other loans in your name. In extreme cases, the thief can also try to sell your home using the documents. Often this type of fraud can go unnoticed until the true homeowner begins receiving foreclosure notices, seemingly out of nowhere.

While this type of fraud can be devastating, it is still fairly rare compared to other threats. In general, scammers go after older homeowners or people that own more than one home. Older homeowners tend to have more equity, while owners of multiple properties may not pay as close attention to their second home.

Scammers often use phishing emails to gather enough information to execute the fraud. In some cases, they will impersonate real estate agents and send emails to homeowners asking to verify the information. Be sure to always confirm by calling the real estate agent if you receive an email asking for details on your home.

How can you protect yourself?

What can you do to ensure that your home stays safe against this threat? The advisor's prospect asked about services such as LifeLock that provide home title insurance. In most cases, those services do little to protect you from home title fraud. In fact, such a service can be a scam itself.

Instead, you can take steps yourself to protect your home from this type of scam.

1. **Freeze your credit:** Setting up a credit freeze at the big three credit bureaus (Experian, Equifax, and TransUnion) is your first big step in protecting your home title from fraud. A credit freeze locks your credit file with a special PIN. Anytime you apply for a new line of credit, you need to provide the PIN before the credit can be approved.

   A credit freeze will make it difficult for the scammer to take out new credit using your home equity. Setting up a credit freeze is free in all 50 states and easy to do. You can apply online (or over the phone) with all of the credit bureaus. If you do need a new, legitimate line of credit—you simply lift the freeze with your PIN 24-48 hours prior to applying.

2. **Regularly check your property deed:** Another way to protect yourself is to regularly check your property deed status with your county. This will ensure that if someone has stolen your home title, you will catch the fraud early. You can call your county to see how you can check your deed details. You may also want to check your county tax records yearly to confirm that you are listed as the owner.

3. **Monitor your utility bills:** One sign that something might be wrong with your home title is if your regular bills stop arriving in your name to your address. Make sure you are regularly receiving utility, tax, and mortgage bills properly addressed to you.

What to do if you think you are a victim?

If you think your home title has been stolen, you will want to take action right away. First, contact your county recorder and alert them to the fraud. You may need to provide documents such as a mortgage bill and a copy of your deed. You should also reach out to your bank if you think any money is in motion.

File a police report so you have a paper trail of the fraud. You should also file a report with the Federal Trade Commission. You may need this documentation if you need to get a lawyer involved in the case. If you do need a lawyer, reach out to one that specializes in real estate fraud or title fraud.

Home title fraud prevention is much easier than dealing with a stolen home title. Be sure to take the steps above to avoid becoming a victim.

Cybersecurity shorts

The latest scam—puppies! The pandemic has caused an uptick in pet adoptions around the country, but now scammers are capitalizing on the trend. The scam begins with an ad for a chance to adopt a popular dog breed. The prospective dog owner sends money for the dog but then discovers the dog is not available to adopt. Experts advise that you video chat with the seller and the dog to ensure the dog exists. You should also only use reputable breeders or adoption agencies when looking for a furry friend.

Fake FINRA website attempts to trick financial professionals. The fake domain adds an extra n to FINRA—finnra.org. The imposter website looks very similar to the real FINRA website, causing confusion and security issues. More so, those behind the fake website are sending phishing emails with the fake domain to unsuspecting victims. If you receive any communication appearing to come from FINRA, be sure to take a close look at the domain before clicking or taking any action.

FINRA warns of fraudsters creating imposter websites for registered reps. Multiple broker-dealers have alerted the agency that fake websites appearing to be legitimate sites for registered reps have popped up in recent weeks. Scammers could use these fake websites to send phishing emails to clients and prospects. Be sure to monitor domains that use any combination of your name to look for imposters.

Have you conducted a Financial Sector Cybersecurity Framework Profile Assessment? This profile was created by the Financial Services Sector Coordinating Council (FSSCC) to help financial sector workers comply with cybersecurity regulations and standards. Assessing your own business can help prevent cybersecurity incidents from occurring. Follow the framework from Security Boulevard to complete your assessment.

Consumers have lost more than $100 million in coronavirus-related scams this year and more fraud may be on the way. One of the best ways to protect yourself from wide-spread identity theft is to freeze your credit if you have not done so already. A credit freeze will lock your credit report with a special PIN. To access your report or apply for a new line of credit, the PIN must be provided. Freezing your credit is free in all 50 states and can be done online or over the phone.

Microsoft launches new campaign to fight disinformation with two new technologies. The first, Microsoft Video Authenticator, will help detect manipulated videos or images. New AI technology can create realistic but fraudulent videos. This new technology from Microsoft will provide a percentage chance that the video or image was manipulated from its original version. The second technology will help readers determine if written content is authentic. You can learn more about the campaigns here.

Is TikTok a national security issue? Experts say"No," but we should be careful about how we share data. For example, if you only scroll through TikTok to watch videos, you may not want to grant access to your camera and microphone. This goes for other apps as well. It is important to review privacy and security practices for any new app you download. You can read more about protecting your data here.

Scam alert! Text messages alerting that you have an unclaimed package are fraudulent. The Better Business Bureau is reporting an uptick in these messages that ask you to click a link and provide credit card information. If you receive a text message like this, do not click but instead delete it.

One in 10 U.S. adults have experienced identity theft since the onset of the Covid-19 pandemic says a new survey by TransUnion. And 80% are concerned their identity will be stolen in the future. Respondents are also concerned about government agency fraud as unemployment scams continue to rise.

Only one-third of Americans have checked their credit report this year—a drop from last year. All Americans are entitled to a free credit report from each of the big credit reports per year. Checking your credit report regularly can help spot fraud early on. You can request your free credit report here.

Software updates

Microsoft: Microsoft released over 100 security fixes this month affecting Windows operating system, Internet Explorer, Edge, and other programs. Some flaws designated as critical could take over computers or networks with little or no action by users. Your devices should prompt you to update automatically but you can read more about the updates here.

WordPress: If you use WordPress to host your website or blog, update it now. Hackers are currently exploiting a vulnerability that allows them to run malicious scripts on the site and take over the network. A security patch has been released. Be sure you are running version 6.9 to be protected. You can learn more here.