ProVest Wealth Advisors

Financial Security, from Fraud

223 E. Blackstock Road
Spartanburg, SC 29301

p. 864 582 7766
1-800-277-0025

asknoel@theprovestperspective.com
www.TheProvestPerspective.com
www.ProVestWealth.com

Table of Contents

223 E. Blackstock Road
Spartanburg, SC 29301

p. 864 582 7766
1-800-277-0025

asknoel@theprovestperspective.com
www.TheProvestPerspective.com
www.ProVestWealth.com

Introduction

What does financial security mean to you? It could mean the peace of mind you feel when you aren't worried about your income being enough to cover your expenses. It also could mean that you have enough money saved to cover emergencies and your future financial goals. This report discusses a different aspect of financial security. That is, how it relates to keeping your finances secure from identity theft and scams. Since the pandemic started, identity theft and scams are more common than ever before. That is because so many thieves are scammers are taking advantage of people's vulnerability due to corona virus fears. This report addresses the ways that thieves and scammers get your information as well as how to protect yourself, so you can have a new kind of Financial Security

Identity theft

Many things have changed over the last couple of decades; some things for the better, others for the worse. Credit and debit cards have made it easier to pay for your purchases, but they've also made it easier for hackers and con artists to get the information they need to steal your identity. This is especially true when paying for goods and services over the internet.

The scariest thing is that most people don't know they're a target until it's too late.

Fortunately, there are steps you can take to protect your identity. The first step is to recognize the most important tools you have to combat identity theft which is awareness and knowledge**.** Identity thieves target many different types of people, but the older you get, and the closer you are to retirement, the higher up their list you go. Why? Because older adults frequently have access to cash they've been saving up for their entire lives. Many older adults also have great credit that they've been building up over a long period of time. Additionally, some people value their independence so much they are hesitant to report that their finances or identity have been compromised, fearing their relatives will think they can't handle things on their own.

Here are some steps you can take to help prevent this:

- Do not publish the date of birth and death in obituaries. Dishonest people can use that information to obtain a death certificate, which usually includes the social security number for the deceased individual.
- Don't make impulsive decisions based on fear. If you receive an email or phone call stating that it's from your bank or the government, and that you're in trouble, look into it before providing the sender with any personal information. Typically, the government will not contact you by email or phone. They will contact you by mail. Your bank will never ask you to provide information through email either. If you're concerned about the credibility of a call or email from your bank, contact the nearest branch and ask them.
- If someone contacts you saying they're a relative in trouble and need your help, ask them something that only your relative would know. Or ask a trick question that reveals they're lying, such as "How's your dog Scruffy? Did he get better?" when you know that relative doesn't have a dog. If they say "Oh he's doing much better," then you know they're a fraud and you should immediately hang up.
- Keep all personal documents in a safe place. Don't carry them around with you, especially not your Social Security card.
- Don't open emails from senders you don't recognize. These can be disguised as special offers for things such as "weight loss," miracle cures for different ailments, or products at unbelievably low prices. Scammers keep coming up with new subjects to hook you.

Phishing

Imagine this scenario. You get an email that appears to be from your bank. You open it and read a message riddled with misspelled words that direct you to "click the link below." You click on the link, and are taken to a page that looks almost exactly like the website you're used to visiting … almost.

You've been phished.

Hopefully, this scenario has never happened to you. Or if it has, you recognized the warning signs and knew to stay away. Unfortunately, many people *don't* recognize those warning signs, and fall prey to a particularly insidious form of Internet fraud called phishing.

Phishing is defined as *"the creation of email messages and Web pages that are replicas of existing, legitimate sites and businesses. These Web sites and emails are used to trick users into submitting personal, financial, or password data. These emails often ask for information such as credit card numbers, bank account information, Social Security numbers, and passwords that will be used to commit fraud."*[1] Phishing is a play on the word "fishing,", with regular people as the prey, and fake emails/web sites as the bait.

The following is a breakdown of the areas crooks like to target:

- Retail/Service – 29.37%
- Payment Services – 25.13%
- Email – 12.39%
- Social Networking – 6.43%
- Other – 26.68%

People who fall for these scams are often duped into giving out sensitive information, like their Social Security numbers, account passwords, credit card numbers, or even bank PIN numbers. Or, they may be directed to sites that proceed to install malicious software onto their computer or mobile device. Either way, phishing poses a major threat to your finances, your identity, or your data.

Thankfully, phishing is easy to avoid if you follow a few common-sense rules.

1) Legitimate banks, retailers, and social media sites should *never* ask for your personal information via email. If you receive a message from someone asking for this info, assume it's a scam.
2) Furthermore, as a general rule of thumb, do not reply to *any* message, electronic or otherwise, that requests your personal information.
3) Never use links in an email to connect to a website. Open a new browser window and type the site address in directly.
4) Always double-check the URL of any site you intend to visit. Some thieves set up sites with URLs that look very similar to a legitimate site. For example, "amzon.com" instead of "amazon," or "facebok.com" instead of "facebook." You get the idea.
5) When doing business online, look at each website's address. Secure websites should have a small symbol of a lock next to their URL, or the letters *https* (instead of merely http) at the beginning of the address. Both the lock and the letter "s" indicate that the site has been verified as secure.

Also, learn to recognize what common phishing messages look like. There are often a few telltale signs like……

> *Dear **Costumer**,*
>
> *We have **recieved** (misspelling) notice that your identity is not secure! This could put your account in danger. To register for a higher **lvel** of security, simply:*
>
> 1. ***Click the link below to open a secure portal to our site***
> 2. *Confirm **your** (incorrect use of word) the owner of the account by answering a few simple questions*
>
> *If you do not comply with these instructions in 7 days **we have no choice but to permanently delete your account.***
>
> *Sincerely,*
>
> ***Your Bank, Privacy Division***

The warning signs aren't hard to spot. Look for misspelled words (costumer, recieved, lvel, etc.), links to click on ("Click the link below"), threats ("If you do not comply"), and references to a well-known business or organization.

Other Scams

Phishing Scams – I talked about this in the last segment, but one twist on this scam during the holidays is for individuals posing as shipping companies or online retailers, asking for personal information to resolve a shipping error. Their goal is to get personal information from people who are worried their online purchases won't ship in time. Another one is individuals asking for charitable donations posing as a legitimate organization, hoping to cash in on your holiday generosity. These can be avoided in similar ways from the ones mentioned in previously.…

- Don't click links in email messages.
- Type addresses directly into your browser or use your personal bookmarks.
- Check the site's security certificate before you enter personal or financial information into a website.
- Don't enter personal or financial information into pop-up windows.
- Keep your computer software current with the latest security updates.

Text Message Scams – Also called "smishing," or SMS phishing, works very similarly to regular phishing. Scammers send out texts asking, for example, for your PIN to reactivate your debit card or to cancel some trial of a service to avoid charges. It may be time to discuss these types of scams with any children you may have at home.

To avoid this type of scam, in addition to the tips on avoiding phishing scams, don't respond to any texts from numbers you don't recognize, & alert your wireless provider to any suspicious texts.

Gift Card Scams – With this scam thieves will go into retailers and find gift cards that are yet to be purchased. They write down the numbers to the gift cards and track them electronically until they are purchased. Once activated upon purchase, the scammer will drain the funds leaving the gift card empty for its rightful owner. To avoid this scam, avoid purchasing gift cards that have either damaged or no packaging. If you feel uncomfortable buying a gift card you find in a store, you can always ask the staff if they have any in the back that haven't been accessible to the public. Also, to further protect yourself, avoid buying gift cards from third party vendors you aren't familiar with.

Fake Coupons – With everyone trying to save a little money on shopping, coupons can be a handy resource, & there are scammers who set up websites that provide fake coupons in order to steal personal information. Be wary of websites offering coupons or discounts to third parties in exchange for personal information.

Counterfeit Gifts – Just as everyone is trying to save money with coupons, people are also on the hunt for deep discounts. Another scam to avoid is the sale of counterfeit goods. If this year's newest smartphone or gadget is being sold for a price that seems too good to be true, it probably is! To avoid this type of scam, do your research on how to identify authentic goods, or purchase these items directly from the manufacturers.

ProVest Wealth Advisors / 223 East Blackstock Rd Spartanburg, SC 29301 / 800-277-0025 or 864-582-7766