GRAGG FINANCIAL

Beyond the Traditional

IBM defines cybersecurity as “the practice of protecting critical systems and sensitive information from digital attacks.”

You may not be in the business of defending critical infrastructure from online threats. But fraud, identity theft, and online scams that target your finances pose significant challenges for everyone in today’s digital world.

Armed with knowledge, vigilance, and a healthy dose of caution, you can minimize risks and stay safe online.

Let’s start with SPAM

We’ve all received emails that are obviously fraudulent. Others, however, appear to be legit. Be careful.

The best advise with SPAM is to ignore the email. It may contain links that ask for personal information. The link could be malware, which might provide the spammer with access to sensitive files on your computer.

Another risk is ransomware, which blocks access to files unless you pay a ransom (usually in Bitcoin) by their deadline.

Avoid the unpleasant choice of paying the ransom or losing files. Back up your data on the cloud and/or an external hard drive.

SPAM is also becoming more prevalent via text or instant messaging. Have you ever received an unsolicited text from a major corporation? Maybe it appears to come from Amazon, FedEx, or a well-known corporation.

While some messages provide updates and estimated delivery times, others are generated by criminals, hoping you’ll respond by providing them with personal information.

Let me give you a quick example. “Answer Few Questions Get Paid (dollar emoji).” This was clearly an attempt to defraud unsuspecting recipients. Poor grammar added to its fraudulent tone.

Or, “USP-We are unable to deliver your package due to missing address information, please fill in you address promptly (includes a link).” Yes, UPS was spelled USP, and the link didn’t include UPS embedded within a random string of characters.

How might you sidestep a financial minefield? Don’t give out your email or post it publicly. Never reply since a response informs the spammer that your email or phone number is legitimate.

Think before you click on a link. Download filtering tools and anti-virus software, both for your computer and smartphone.

Social media

Have you received a brief instant message from a Facebook friend that’s worded in a way that doesn’t reflect your friend’s personality but happens to include a link? If so, their account was probably hacked. Confirm by contacting your friend through another platform.

Have you received a friend request from an established friend on Facebook?

In most cases, a criminal has impersonated your friend’s profile. Before accepting the friend request, talk to your friend and make sure it’s legitimate. Some folks have more than one profile on Facebook.

Also, be leery of accepting friend requests from strangers. You don’t know them. Why would they send you a friend request? Consider this: would you give your phone number or address to a total stranger if asked?

Becoming a ‘friend’ with a stranger offers them a peek at your private life.

While we’re discussing Facebook (or, for that matter, social media in general), be careful what you post.

It seems harmless to mention your anniversary, pet’s name, birthday celebration, first concert you attended, or your first job. But these can provide answers to security questions that will give a fraudster access to an account.

Simply put, ignore the public post that asks, “Date yourself. What’s the first concert you attended, or first car owned?”

Watch for online scams

Some scams impersonate official government websites such as Social Security or the [**https://www.irs.gov/newsroom/avoid-scams-know-the-facts-on-how-the-irs-contacts-taxpayers** IRS].

For starters, the IRS doesn’t send unsolicited emails and won’t discuss tax account information via email or use email to solicit sensitive financial and personal information from you. The IRS initiates contact with taxpayers via regular mail.

[**https://faq.ssa.gov/en-us/Topic/article/KA-10018** Social security scams] are also a growing problem. If there is an issue, Social Security will generally send you a letter. Callbacks occur only if you’ve requested one.

Scammers may offer to increase benefits, protect assets, or resolve identity theft, but often demand payment via retail gift cards, wire transfers, pre-paid debit cards, or cash.

That is a HUGE red flag! It screams fraud! The Social Security Administration won’t ask for something like a gift card, cash, or pre-paid debit card.

They may also threaten to have you arrested or take legal action if you ignore their overtures.

Just hang up the phone or ignore the email. That seems obvious, but fraudsters wouldn't be spending time fishing for cash if these scams didn't work.

Cryptocurrency scams

Scams involving, for example, Bitcoin have proliferated and scammers are looking for ways to cash in.

According to the FTC, no legitimate business is going to demand cryptocurrency in advance or payment in cryptocurrency only.

Are you being pitched a risk-free investment in crypto that guarantees big profits? If you send them money, expect to lose 100% of your investment.

Keep online dating and investment advice separate. If you meet someone on a dating site, and they want to show you how to invest in crypto or ask you to send them crypto, you're staring down the barrel of a scam.

End contact immediately. They are only interested in mining your savings, not romance.

Dodging identity theft

Consider freezing your credit. When you freeze your credit report, no one can request your report. No one (including you) can apply for a loan or obtain a credit card while your credit is frozen.

Collect your mail daily and review bank statements on a regular basis.

Install and keep anti-virus software updated. This not only applies to PCs. Apple products aren't immune from malware and viruses either.

Create unique and complex passwords for each account. A good password manager program can easily assist you.

But you may use the 'default option' if you use Google Chrome as your browser. Google will automatically supply you with a random string of characters, letters, and numbers and save the password for you.

It's generally considered to be a safe option and better than recycling a password that you've used numerous times (and one that might have been stolen and is available on the dark web).

While we are on the topic of browsers, keep them updated.

Updates not only incorporate fixes, new features, and efficiencies, but more importantly, they include the latest security updates.

Free plug-ins for your browser can also provide an added layer of safety by warning you that a website you've clicked on has been compromised by hackers.

Consider two-factor authentication. When you log into an account, a code will be sent to your phone or email that you must input before you can access the account.

Final thoughts

One can't be completely safe online. But if you are proactive and take the necessary precautions, you greatly reduce your odds of becoming a victim.

Many of the ideas we suggest may seem elementary. But in the moment we open that email, text, or answer the phone, our guard may be down. No one is immune from a momentary lapse of

judgment.

You've heard the adage, a penny saved is a penny earned. Well, a healthy amount of skepticism and caution online can pay huge dividends.

As always, thank you for the trust, confidence, and the opportunity to serve as your financial advisor.

Your Gragg Financial Team