

## Personal Digital Security

We live in a world where much of our lives, whether it be personal or professional, resides online. We make purchases, do our banking, share parts of our personal lives and plan social events through the digital world. While we increasingly rely more and more on the internet and other digital networks, we need to assess the risks that come along with the conveniences.

A lot of the information that we put into the internet automatically opens us for the possibility of an online attack. These hackers may be tracking small things from the items you purchase to ultimately trying to steal your identity. We need to be diligent in our attempt to prevent these attacks. This year, some of our clients have personally experienced the filing of false unemployment claims and then perhaps the filing of a fraudulent income tax return.

Here is a quick list of items that you can easily review to help fortify your digital security:

1. Keep all software up to date – phones to computers – you should be able to turn on automatic updates and that is the best way to ensure that updates are done
2. Use anti-virus protection - again keep this up to date
3. Use strong passwords – do not use the same password for multiple sites. Reset or change passwords once a year. Consider using a password manager
4. If possible, use two factor or multi factor authentication – more and more websites are offering this, sometimes it can be a text to your cell phone, answering specific questions or an additional password. Despite the hassle of answering security questions the added security and peace of mind is worth it.
5. Learn about phishing scams – be suspicious of emails phone calls and flyers. Bottom line, don't open emails from people you don't know. Hover over the top of the name of the sender or link to determine where the email is actually coming from. Looking at the grammar can sometimes be an easy red flag.
6. Limit the amount of information that you put into the internet i.e. name, address, phone – be cautious about social media and review your privacy settings
7. Keep mobile devices secure – create a password, do not make it the same other passwords especially a bank or credit card password. Know what kind of apps you are installing. Consider loading a find my device app on the phone in case it gets lost. Use touch ID or facial ID. Consider turning off your location data or at the very least monitoring which apps allow it
8. Backup data regularly on both computers and phones
9. Don't use public Wi-Fi
10. Review online accounts and credit reports on a regular basis
11. Cover web cams when not in use
12. Complete an annual review your own personal digital security

What to do if you expect a breach

- Call your respective account branches from a number that you trust directly from their website.

If you have further questions on steps to take, call Schaefer Financial Management at 303-770-6700 and we can assist you with the necessary steps to take