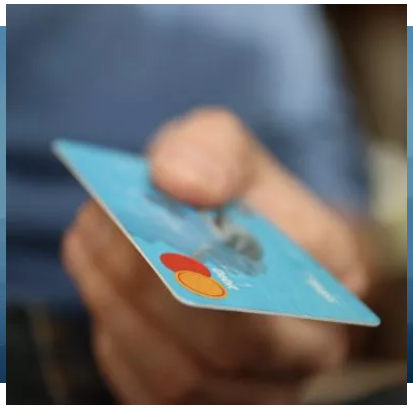

06.22.21 | INSIGHTS

Personal Digital Security

Becky Aardal – CERTIFIED FINANCIAL PLANNER™ | Chief Compliance Officer

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:

- **Keep all software up to date** – With your phones and computers you should be able to turn on automatic updates and that is the best way to ensure that updates are complete.
- **Use anti-virus protection** – Again, keep this up to date.
- **Use strong passwords** – Do not use the same password for multiple sites. Reset or change passwords once a year. Consider using a password manager.
- **Use two factor or multi factor authentication (if possible)** – 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.
- **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.
- **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.
- **Review and verbally confirm** all disbursement request details thoroughly before providing

Services

Financial Planning

Investment Management

Related Team Members

Jeff Schaefer

Becky Aardal

Lowell Hansen

Kirsten Hollander

Andrea Searle

Henry Schaefer

Dawn Johnson

© 2026 Schaefer Financial Management | 7700 E. Arapahoe Road, Suite 265 Centennial, CO 80112

your approval, especially when sending funds to another country. Never trust wire instructions received via e-mail without verbal confirmation.

- **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 and what sort of information they track and have access too. 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.
- **Backup data** regularly on both computers and phones.
- **Turn off** Bluetooth when it is not in use and do not use public Wi-Fi.
- **Review online** accounts and credit reports on a regular basis.
- **Cover** web cams or laptop cameras when not in use.
- **Complete** an annual review your own personal digital security.

WHAT TO DO IF YOU SUSPECT A BREACH

- Call your respective account branches that you believe have been hacked so they can watch for suspicious activity and collaborate with you on other steps to take.
- If you have further questions, call Schaefer Financial Management at 303-770-6700 and we can assist you with the necessary steps to take.

LEARN MORE

Visit these sites for more information and best practices:

- StaySafeOnline.org: Review the STOP. THINK. CONNECT™ cybersecurity educational campaign.
- OnGuardOnline.gov: Focused on online security for kids, it includes a blog on current cyber trends.
- FDIC Consumer Assistance & Information.
- FBI Scams and Safety provides additional tips.

READ FULL ARTICLE