



Your cybersecurity

By Diane

I recently read an article about “keeping yourself cyber safe.” Some days it feels like every other article I read is about someone scamming another person. Spam continues to bombard us. Cybercriminals have gotten very creative in the way they obtain information, and cyber fraud is rising. Listed below are some tips to help keep your data safe:

1. **Social media** – Not only do social platforms track your activity, but criminals use this information to create fake profiles that make it look like you. Keep an eye on the personal information you share. Those posts where you see “what was your very first concert” – those are security questions for many logins. What one interprets as a fun trivia question is just an attempt to gain access to a secure website.
2. **Layered approach** – Keep control in your hands. Make sure you are using features that help protect your data. Examples of these include: logging into financial sites only from your home computer, using a separate email for online interactions (I have a 25-year-old Hotmail account for this purpose only), using a credit card instead of a debit card for additional liability protection, using dual-factor (face recognition, PINs, etc.) and secure portals. The more layers you can use, the more protection you can add.
3. **Secure the house account** – Spending all this time at home has made us more connected to the fast-paced life of the internet, whether it is shopping, streaming, or Zooming. Don’t allow hackers the opportunity to invade your home bubble through Bluetooth and Wi-Fi. Instead, secure your home network with a strong password and encrypt it with a firewall.
4. **“Free Wi-Fi”** – Otherwise known as an unencrypted network with unrestricted access to ANY unsecured device. This should scare anyone. Resist doing anything personal (especially financial) until you can get to a secured network or use a VPN.
5. **“Kids these days”** – I won’t lie, my kids can do something on their phone in the blink of an eye. Sometimes it is done so fast the final word hasn’t even exited my mouth. Their lives are so intertwined with technology, much more than I desire some days. So taking the time to teach, educate, monitor, and restrict their online presence is more important than ever.

Technology continues to make our lives easier, but its increased presence makes us more susceptible to fraud and cybercrimes. Taking security measures to protect your personal information is just the first step. Being aware and making good decisions is the next.

Our custodian has also shared some best practices in the past. Find these [here](#).

Clicking on the links above may result in you leaving the Pittenger & Anderson, Inc. website. The opinions and ideas expressed on these external websites are those of third-party vendors and Pittenger & Anderson, Inc. has not approved or endorsed any of this third-party content. For the full Terms & Conditions of using the Pittenger & Anderson, Inc. website, [click on this link](#).

Pittenger & Anderson, Inc. does not provide tax, legal, or accounting advice. This material has been prepared for informational purposes only, and is not intended to provide, and should not be relied on for, tax, legal, or

accounting advice. You should consult your own tax, legal, and accounting advisors before engaging in any transaction. Additionally, the information presented here is not intended to be a recommendation to buy or sell any specific security. To learn more about our firm and investment approach, check out our [Form ADV](#).

To view this article and others like it online, visit the P&A blog at <https://pittand.com/blog/>.