PRACTICAL PLANNING:

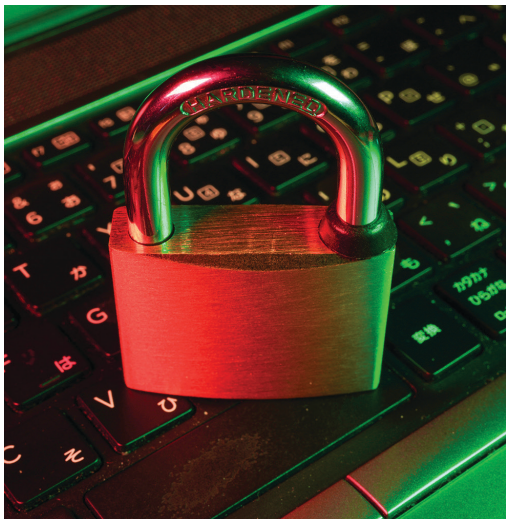
Four steps to lock down your data

by Glen Goland, JD, CFP®
Senior Wealth Advisor, Investment Advisor

There have been so many data breaches over the last few years that everyone reading this ought to assume that their name, social security number, and birthday is out there for sale on the internet somewhere. Below are four steps you can take to limit the damage a thief can do with this data.

1. Freeze your credit with the three major reporting agencies: *Transunion*, *Experian*, and *Equifax*.

This is the most important thing you can do to protect against thieves inflicting financial damage with your personal data. Click the above links to access each website and get started.



2. Opt in to the IRS offering for an *Identity Protection PIN (IP PIN)*.

The COVID pandemic brought with it an increase in fraudulently-filed tax returns; this simple step may save you some headaches down the line. As of this year, you don't have to be a victim of identity theft to opt in to this IRS program. If you volunteer for an IP PIN, the IRS will generate a unique PIN once you complete an identity verification process, which is then required each time you file tax returns. Visit ***https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin*** to learn more and get started.

3. Exercise caution with your email.

Remember that email is almost always going to be the first point of attack. Be VERY careful when reading email and opening attachments or clicking on links. Questions you should have in mind are:

- Do I know the person emailing me?
- Was I expecting this person to email me an attachment or include a link?
- Is there anything fishy about the email address of the person sending me an attachment?

DO NOT open attachments or click on links from people you do not know, and sound the alarms when an email instructs you to "update personal information" (change your password, update billing information, enter credit card numbers, etc.). When in doubt, use the hover rule to validate link URLs (hover your cursor over the link to view the full website address, but DON'T click on it). Trust your instinct if something does not feel right, and always think twice before opening an attachment or clicking on a link.

4. Use better passwords

Strongly consider a password management system such as LastPass, Bitwarden, and 1Password, all great options. These are low-cost, very easy to use, and a terrific safeguard against the risk of vulnerable passwords. The longer your password is, the more difficult it will be for someone to guess. Avoid common traps like using the same password across platforms, using the same phrase over time while switching out one character when updating, and using birthdays/pets/kids' names.

Our Chief Information Officer is constantly reminding our team to maintain what he calls, "healthy digital hygiene." We develop wholesome lifestyle habits in our lives; the same should be said for establishing healthy digital habits to protect the electronic information and assets that have been exposed on the internet. Along with using secure passwords, it is best practice to close any unused/stale online accounts, ensure your antivirus tools are active, regularly update your operating system and software, review the security/privacy settings on social media accounts, and use Multi Factor Authentication (MFA) whenever possible.

Our team will continue to provide cybersecurity updates and tips as appropriate.