Key Private Bank

Eight steps to protect your passwords and digital assets

by Nancy L. Anderson, CFP,® Regional Planning Strategist

While the digital world gives access to data in an instant, along with technological progress comes the need for strong layers of protection. Unfortunately, the digital world is increasingly becoming more dangerous for high-net-worth individuals and families. According to the 2018 Identity Fraud Study from Javelin Research, victims of fraud increased by 1.3 million, representing a $16.8 billion loss for U.S. consumers. Account takeover (ATO) also tripled, reaching a four-year high. Total ATO losses reached $5.1 billion, a 120% increase year-over-year.[1]

With your personal financial information, you have a lot at stake. In a digital world, you store and share information online regularly, so taking steps to ensure privacy and security is vital.

Here are eight tips to protect your personal data online

1. Create strong passwords

Why	A strong password is your first line of defense in protecting your data. Cybercriminals could crack an easy password and, if used for multiple accounts, could access your accounts quickly. An overly simple password is one of the weak links in a data breach according to Pew Research[2]. **Top 5 Most Common Passwords (avoid these)[3]:** 1. 123456 2. 123456789 3. qwerty 4. password 5. 111111 Use a mix of 16 characters that include capitals and lower case, numbers, and symbols that aren't easy figure out.
How	Create them on your own or use a password generation app.
Do it yourself	If you create passwords on your own, you can use a memory trick to remember them. Here is an example: This complex password, **"tgF51*JoBC"** is derived from the first letter of each of these words (with a number such as an age and a random symbol thrown in.): **the grey Fox 51 (asterisk) Jumps over the Brown Cow becomes tgF51*JoBC**
Use technology	Password security websites include features that can randomly generate complex passwords for you. This way you can automatically create long unique passwords for each account you own/use.

2. Organize your passwords to easily remember them

Why

Creating a strong password is one thing, remembering it is another. Create a system to store your passwords and use it regularly.

How

Use a password system to remember your logins and passwords.

Paper password system

Store in a locked drawer, home safe, or other secure location. Share the location and how to access with spouse, partner, and/or trusted family member.

Advantages:

- No cost
- Stored in one place
- Unlimited number of user names and passwords can be stored
- For lower tech individuals, this option is very simple

Disadvantages:

- Not always accessible
- Can't share with others easily
- Could be lost or stolen

Digital password management systems – online and mobile

A password management system works like this: they store the URLs, user names, and passwords for all the sites you use. You sign in using one master password to their encrypted site and/or using your fingerprint on your mobile device.

You can copy and paste complex passwords or use the auto-fill password from within the password manager service, preventing you from having to type in the complex password yourself. This way you can use unique passwords with many characters without having to memorize or even type them in.

Some advanced features to look for

Share passwords with other users such as your spouse, partner, adult children, and successor trustees. Look for an application that allows you to share individual passwords (not all of them at once) with others.

Look for a provision for "digital legacy" so your executor or trustee can access your information in the event of your death.

Advantages:

- Access your user names and passwords from anywhere on your multiple devices.
- Auto-fill feature so longer and complex passwords don't trigger a lock out due to missed characters.
- They are free or inexpensive
- Many of the password security systems have a free version to try out, and the full-service versions are under $60 per year.

Cons:

- Time to set up. To use it properly, you will need to enter your user names and passwords with the URLs into the system.
- Need to remember your master user name and password.
- Cost to administer. There are free versions, but the paid versions are more robust.

3. Change your passwords every 90 days

Why	You may not be aware that your data is compromised. Be vigilant and change your passwords on a regular basis.
How	Set a reminder on your phone or mark on your calendar to make the change. Replace weak passwords with strong ones, especially on your email accounts and financial accounts. Eliminate duplicate passwords and replace them with unique complex passwords with letters, numbers, and symbols. If you have a paper-based system, once you update your passwords and record the changes, make a copy and store in a second location such as a safety deposit box.

4. Disable auto-fill on your computer

Why	This will prevent your personal data from being unintentionally saved or used in your browser. If a cybercriminal gained access to your computer, they could find your usernames and passwords through auto-fill.
How	Your browser such as Chrome, Explorer, Firefox, or Safari will have directions in its privacy and security sections on how to turn off “auto-fill” and clear the existing data.

5. Avoid saving your credit card information online

Why	When shopping online or booking travel, you may be asked to create an online profile for “easier checkout.” While the checkout may be faster for you, having your credit card information stored on multiple hotel, airline, and shopping websites makes you vulnerable to fraud.
How	Take the time to enter your credit card data each time you use a site, especially for sites you don’t use very often. Review your credit card transactions each month to ensure they are valid. When shopping or booking travel online, be sure to always use a credit card and not a debit card. Using credit cards can deter fraudsters from accessing your checking account directly and often include fraud prevention monitoring and features.

 **6. Use a separate device for "at risk" activities**	
Why	Website browsing and social media sites can be targets for hackers. Cybercriminals create links that look like ads that are malware or viruses.
How	Use a specific device such as your desktop computer for banking and financial transactions that you'd like to keep private. Have your family use designated devices such as a specific laptop, mobile phone, or an iPad for social media and general internet browsing activity.

 **7. Keep a list of digital assets and close old accounts**	
Why	Organize online security – close accounts you no longer use. With email, financial accounts, shopping, and social media sites, consumers can have upwards of 50 separate logins. Consumer Reports recommends getting rid of accounts you no longer care about. When you delete accounts you no longer use, there is less data that could be misused.
How	Simply make a list of the sites you use regularly or record every site you use in your online password management system. To this list, also add hardware such as desktop and laptop computers, iPads, and smart phones. Note where you store certain important information, such as your tax returns. Shut down sites you remember, but no longer use. Then use the Consumer Reports guide[4] to finding old online accounts. Search for your name and email addresses in your favorite search engine such as Google and then others such as Bing. Look through your saved emails for accounts you signed up for in the past. Review your saved logins in your privacy settings and delete ones you no longer use.

Eight steps to protect your passwords and digital assets

8. Incorporate your digital assets into your estate plan	
Why	If you are incapacitated or pass away, your loved ones may want or need access to your online accounts. For example, without knowing the password to your computer, your spouse can't open it to access needed files, such as tax returns and online bill pay. Without knowing your passwords to social media, they can't shut them down or provide notices to your online community.
How	Review your estate plan with your attorney to discuss adding digital assets. This way, you've planned ahead and designated someone to handle your digital assets when you are gone. At a minimum, inform your spouse and/or trusted family members where your digital assets list and password information are stored.

The world has changed. The good news is that simply taking a few steps toward digital protection can make a big difference in preventing identity theft and fraud.

About the Author

As a Regional Planning Strategist for Key Private Bank, Nancy proactively advises clients on the development of a personalized, comprehensive financial plan that creates a financial roadmap so they can make more informed, confident decisions.

Nancy is a highly experienced professional who works closely with the relationship team to understand a client's personal situation and goals to develop an integrated, customized set of strategies to help them reach their objectives. She is also well-versed in sophisticated planning strategies to help clients address complex issues. Nancy is a member of Key Private Bank's Wealth Institute, which provides commentary and advice on current topics and issues that impact our clients' wealth management planning.

Prior to joining Key, Nancy served as director of financial advisory firm, Financial Finesse, providing retirement planning and tax advice for executives of Fortune 500 companies. She has provided guidance and advice to high net worth clients since 2001.

A nationally recognized expert in retirement planning, Nancy has penned a popular personal finance column on Forbes.com since 2012. She also serves on the board of the Utah Financial Planning Association.

For more information about how to prevent identity theft, contact your Key Private Bank advisor.

Key Private Bank

Key Private Bank

[1] Pascual, Al; Marchini, Kyle, Miller, Sarah. "2018 Identity Fraud: Fraud Enters a New Era of Complexity". Javelin Research. Published: February 6, 2018. Accessed: October 31, 2019. https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity

[2] Smith, Aaron. "Americans and Cybersecurity" [Web Post]. Pew Research Center. Published: January 26, 2017. Accessed: October 31, 2019. https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/

[3] Picheta, Rob. "How hackable is your password?" CNN Business. Published: April 23, 2019. Accessed: October 31, 2019. https://www.cnn.com/2019/04/22/uk/most-common-passwords-scli-gbr-intl/index.html

[4] Germain, Thomas. "Privacy Fix: How to Find Old Online Accounts". Consumer Reports. Published: April 10, 2019. Accessed: October 31, 2019. https://www.consumerreports.org/digital-security/how-to-find-old-online-accounts/