GW&K INVESTMENT MANAGEMENT

PRIVATE WEALTH MANAGEMENT

JANUARY 2023

QUICK TIPS FOR SAFEGUARDING YOUR PERSONAL DATA

The digital world allows us to control our lives with a few clicks of a mouse or the touch of a screen — but also increases the risk of fraud. Cybercriminals can crack shorter passwords in a few seconds or send sophisticated "phishing" emails designed to entice you to take an action that could compromise your accounts. Here are a few best practices we employ at GW&K that will help you to reduce your risk in the digital world.

PASSWORDS

- Create passwords that are complex, unique, and include numbers, letters, and special characters (e.g., !, $, %,*). Longer is better, so passphrases are good options. Passphrases are combinations of words that are meaningful to you and easier to remember — for example, jazz1oceansteak!, puppy54Bostonmountain*.
- Avoid using names, significant dates, Social Security numbers, phone numbers, or other options that could be easily guessed, such as "password123".
- Do not share passwords or use the same password for different logins.
- Never save passwords to an internet browser when using a public device.

PHONE & EMAIL SCAMS

- Do not provide, validate, or confirm personal or financial information, such as credit card or Social Security numbers, to individuals you don't know — especially over the phone. Be suspicious of anything that the caller or email sender says is "urgent." If you receive a call from your bank, you can always hang up and call them back on a number you know to be legitimate.
- Carefully examine any email you receive that asks you to take an action. Doublecheck the sender's e-mail address and review the content of the message for any irregularities in spelling, diction, punctuation, or format, which can be signs of fraud.

QUICK TIPS FOR SAFEGUARDING YOUR PERSONAL DATA

- Be extremely suspicious of any email or text message asking you to login to or enter your password for a site.
- Avoid clicking on links in emails altogether, especially for logging into a personal account at a financial institution. Instead, navigate to the website in your internet browser, and safely login there.
- Do not open, download, or click on unsolicited or unexpected email attachments.
- Activate your email's spam filters to help filter out suspicious and unsolicited emails.
- Conduct independent research on charities, travel, or business and investment opportunities you hear of from unsolicited calls or emails.

PERSONAL SECURITY MEASURES

- Be thoughtful about personal information you share online — including on social media sites. For example, be cautious about announcing vacation plans if that means your primary residence will be empty.
- Set a reminder to change passwords regularly – a good New Year's resolution!
- Use face and voice recognition to unlock personal devices or access websites when possible.
- Protect and lock devices that store passwords, credit cards, and personal information.
- Check regularly for system updates that may improve security on your personal devices.
- Secure home internet networks with a password.
- Be cautious when joining public Wi-Fi networks.
- Educate and assist children and elderly family members with cybersecurity best practices.
- Where possible, set-up two-factor authentication, which requires a second identity check in addition to your password to access a website or device, such as a one-time code sent via text message.
- Review your bank and credit card ledgers frequently and promptly report any unfamiliar activity to your financial institution.

Please reach out to your GW&K representative if you have any questions.