

Beyond The Numbers: Four Tips For Protecting Your Family's Digital Legacy

By: Director, Jimmy Trimble, CFP® and VP of Technology, John Dolan

In an era where our lives are increasingly digitized, the importance of personal security and privacy cannot be understated. For the affluent, this is not merely about safeguarding wealth but about protecting a legacy. As Warren Buffett wisely noted, "It takes 20 years to build a reputation and five minutes to ruin it." This is particularly true in the digital realm, where a single lapse can have long-term consequences.

The Imperative of Digital Vigilance

The digital age, while offering unmatched convenience and connectivity, also presents complex challenges in protecting personal data against sophisticated cyber threats. "The more you know, the less you need to say," Jim Rohn reminds us, highlighting the power of discretion in our digital engagements. In addition to discretion, proactive measures—such as using strong, unique passwords, enabling two-factor authentication, and ensuring your software is updated—are foundational to digital privacy.



Four Actionable Steps for Enhanced Security

1. **Secure Wi-Fi Use:** Always verify public Wi-Fi networks and consider using a VPN, or virtual private network, to ensure a secure connection. Another option is to use the personal hotspot available on your cell phone. If you use your phone's hotspot, make sure a Wi-Fi password is required to connect and don't share it with others. To learn more, check out this link to a [ZDNET article](#) on this and related topics.
2. **Robust Account Protection:** According to [Verizon's 2023 Data Breach Investigation Report](#), compromised passwords are the cause of 83% of hacking-related system breaches. Your best defense against a password breach is using multi-factor authentication (MFA) alongside a password

vault. The password vault will generate and store unique passwords so that if one password is compromised the rest are still secure. If you must generate your own password, ensure it is at least 14 characters and does not include any personal information like your name, email address, birth date, or where you live.

MFA compliments your password by providing a roadblock when your credentials have been compromised. If your password is hacked, cybercriminals cannot access your account with that information alone. They will need to provide additional information, or you will receive a text message or email to verify that you are trying to access your account. You can read more about MFA [here](#) in an article by the Cybersecurity & Infrastructure Security Agency.

3. **Regular Updates:** Keep your devices and software updated to protect against malware and ransomware. An update could patch security weaknesses that were in a previous version. It could also help protect your personally identifiable information that is on your devices. You can also prevent passing a virus to your family and friends by making sure your software and systems are always updated. The FTC's consumer division produced [this article with more helpful tips](#) along these lines.
4. **Mindful Online Behavior:** Be cautious about clicking on unknown links and be discerning about the information you share online. Here is an [article on online safety basics](#) that goes into more depth on this topic. Phishing emails are becoming increasingly prevalent. This is where cybercriminals send communications that look legitimate, but in fact, it has dangerous links or information to try and gain access to your sensitive data. Here at HB, our VP of Technology created the FLOW acrostic to help identify phishing communications. Phishing emails will often try to utilize your curiosity alongside a sense of urgency to get you to open something dangerous. See how FLOW can help you avoid this mistake:
 - **From**
 - Who is the email from?
 - Ensure names and addresses are spelled correctly.
 - Is this type of email/attachment you would expect from the sender?
 - **Links**
 - Hover your mouse over any links before clicking – do they make sense?
 - Is the domain logical?

- Legitimate domains can be used maliciously (e.g., booking.com, YouTube.com).
- Look for misspelled domains (i.e., Homirchberg.com).
- **Observe**
 - Look at the content of the message, does it make sense? Does it make sense that it would be sent to you?
 - Review spelling, grammar, header, footer, and content of the message for inconsistencies.
- **What**
 - What exactly is the attachment?
 - Never click to find out ‘What it is’ – verify with the sender if not sure.

After using the list above, if you are still in doubt, do not open or click on anything in the email. Give the sender a call or send a text message to ensure you should open the message.

The Ripple Effect of Responsible Digital Citizenship

By adopting these measures, individuals not only protect themselves but also contribute to a safer digital ecosystem. This collective vigilance can set a standard that encourages our families and loved ones to follow suit and help foster an environment where privacy and security are paramount.

Conclusion

In our journey through the digital age, safeguarding our legacy and helping future generations do the same becomes increasingly important. As we embrace the tools and practices that shield us from digital risks, we lay the foundation for a legacy that is a testament to our commitment to safety, privacy, and the well-being of future generations.

At HB, our commitment to you and your family extends beyond the financial realm. Our team is here to help you and to continue serving you “Beyond the Numbers,” as we explore more ways to enrich your life experience.

To learn more or get help with your life experiences, please call 404.264.1400 or email us at info@homrichberg.com.

Important Disclosures

This article may not be copied, reproduced, or distributed without Homrich Berg's prior written consent.

All information is as of date above unless otherwise disclosed. The information is provided for informational purposes only and should not be considered a recommendation to purchase or sell any financial instrument, product or service sponsored by Homrich Berg or its affiliates or agents. The information does not represent legal, tax, accounting, or investment advice; recipients should consult their respective advisors regarding such matters. This material may not be suitable for all investors. Neither Homrich Berg, nor any affiliates, make any representation or warranty as to the accuracy or merit of this analysis for individual use. Information contained herein has been obtained from sources believed to be reliable but are not guaranteed. Investors are advised to consult with their investment professional about their specific financial needs and goals before making any investment decision.

©2024 Homrich Berg.