**Waterworth Wealth Advisors, LLC**

1225 South Main Street, Suite 103, Grapevine TX 76051
817.410.9000 | waterworthwa.com

# Technology Security and Identity Theft Prevention Checklist

## Protect Usernames, Passwords and PINs

- ✓ Keep your usernames, passwords and PINs private - don't store them on your hard drive unless you use an encrypted database such as an online password manager. If you have a password book, make sure it’s in a secured location.

- ✓ Use an online password manager like LastPass to add extra security to your online accounts. LastPass auto fills your usernames and passwords for you and creates secure passwords for your online accounts.

- ✓ Create tough-to-crack passwords and PINs, using a minimum of 8 letters and numbers and, if possible, special symbols. It’s best if these passwords do not resemble any pet names or real words. If you have a password manager, it will create and store very strong passwords for you.

- ✓ Change your passwords often, and avoid using the same password for multiple accounts.

## Safeguard Your Computer

- ✓ Install an up-to-date anti-virus, anti-spyware package such as Kaspersky or Malwarebytes to prevent against malware and malicious individuals (read: hackers) from spying on your online activity or accessing any files or documents saved to your computer.

- ✓ Check to make sure that the firewall software on your computer system is working. You can confirm this by going into Windows Defender for PC users, or for Mac users this is accessed through Security and the Firewall tab. The software will show the status and you can see if it is working.

- ✓ Install AdBlock and anti-tracker software on your browser to make sure that no invasive ads are tracking your browsing history and recording your data. For blocking ads, AdBlock and AdBlock Plus get the job done. For preventing tracking software, use a program like Privacy Badger to block potential trackers.

- ✓ Configure security settings to receive automatic updates for your anti-virus, anti-spam, and spyware detection programs. This setting should be automatic but you can change it within the software for these programs by opening up the program and reviewing the update and alert settings.

- ✓ Use a Virtual Private Network (VPN) to be protected while on public networks and prevent cyber criminals from intercepting what you do online.

Securities offered through Kestra Investment Services, LLC (Kestra IS), member FINRA/SIPC. Investment advisory services offered through Kestra Advisory Services, LLC (Kestra AS), an affiliate of Kestra IS. Waterworth Wealth Advisors LLC is not affiliated with Kestra IS or Kestra AS.

✓ Before disposing of a computer or smart phone, delete personal information and completely erase everything on the device. Once the data is wiped, they can be recycled at Best Buy or sold through Ebay or other online marketplaces. However, be warned that the best way to ensure your data is wiped from the device is to have it destroyed or destroy it yourself by drilling a hole through it, etc.

## Be Smart When Accessing Your Bank and Investment Accounts Online

✓ Use your own computer or mobile device with a secure connection rather than a public or shared computer or mobile device. For more information on using a secure internet connection, see our post titled.

✓ Confirm that you have a secure web connection throughout your session by looking for a web site address that starts with "http**s**://" instead of "http://'' and a secure symbol such as the closed padlock key on your status bar.

✓ When you are finished accessing an online account, be sure to log out completely and close your browser.

## Mobile Devices

✓ Your phone is vulnerable to viruses and malware, be default there is no safeguard on your phone by so install anti-virus software on your phone.

✓ Don't use public Wi-Fi networks without a VPN because the activity and data on your phone can be collected and viewed by hackers on the unsecured network.

✓ Mobile devices are easy to steal, avoid keeping any private information on them such as your passwords and Social Security Number.

✓ Download an anti-theft app to lock your phone down or wipe its data if it gets stolen. For Apple products you can use the Find my Phone feature, but that is not as secure as other providers like the Kaspersky phone bundle, which includes anti-virus and anti-theft software.

✓ Make sure that your device is password protected, a four or six digit pin is somewhat secure while an actual password will be more secure. Fingerprint log in is the most secure way of accessing your phone.

## Use Wireless Connections Wisely

✓ Check to make sure your device has firewall software. A firewall is software or hardware that blocks bad traffic from breaching your computer when using the internet and keeps your computer protected. Windows and Apple computers have firewall software by default. You can also use 3rd party firewalls, like Kaspersky and Norton Security. Confirm the firewall is working by going into system settings and finding Security. There you should find the firewall program and you can check its status to see if it is working.

Securities offered through Kestra Investment Services, LLC (Kestra IS), member FINRA/SIPC. Investment advisory services offered through Kestra Advisory Services, LLC (Kestra AS), an affiliate of Kestra IS. Waterworth Wealth Advisors LLC is not affiliated with Kestra IS or Kestra AS.

- ✓ Check your wireless network. If the router uses the obsolete Wired Equivalent Privacy (WEP) protocol for security, throw it out and buy a new model that employs at least WPA2. You can check by clicking the router on your networks and checking in its properties.

- ✓ Shut off wireless connectivity or remove the wireless network card if you leave your computer unattended.

- ✓ When accessing a hot-spot or using an unencrypted wireless connection, disable sharing on your connected devices so no-one can break into your device. To do this, access your network settings and go into the sharing section where you will be able to adjust what is shared over a network.

- ✓ Use encryption software to secure your wireless connection at home and use it whenever emailing confidential information such as financial documents. Any emails that you wish to keep confidential and secure, use a VPN to protect and encrypt your connections.

## Email and Social Sites

- ✓ Never respond to email correspondence appearing to be from a legitimate investment provider, Credit Card Company or the IRS by clicking on a link and entering a password, these are from imposters. Legitimate requests for sensitive information won't arrive this way.

- ✓ Don't get pulled into websites that look fake, or get phished by giving your personal and private information on an illegitimate website.

- ✓ Never click any links that are sent from illegitimate phishing email sources. Open a fresh web browser session and go to the official site from a source like Google or a link from a reliable source.

- ✓ Never respond to an email that asks you to reveal personal information, such as account numbers, your Social Security number, passwords or PINs. Limit the amount of personal information you share online, including your date of birth.

- ✓ Never give any personal information to someone who sends you a message through a social-media site.

- ✓ Keep your Social Security number private, and avoid using it as a username, password, or PIN. Never carry your Social Security card or put your number on your checks (unless for tax purposes which should be sent via certified mail). Disclose it only when absolutely necessary, using other types of ID whenever possible

## Keep an Eye on Your Finances

- ✓ Always read your monthly account statements, and alert your brokerage firm or other financial institutions if you see a transaction you did not authorize or if your statement doesn't arrive.

Securities offered through Kestra Investment Services, LLC (Kestra IS), member FINRA/SIPC. Investment advisory services offered through Kestra Advisory Services, LLC (Kestra AS), an affiliate of Kestra IS. Waterworth Wealth Advisors LLC is not affiliated with Kestra IS or Kestra AS.

✓ Check your credit report, if you have dependents, it is wise to also check their credit reports.

✓ Store financial records in a safe place, and shred documents containing sensitive information. Waterworth Wealth Advisors has a secured shredder box in the office and clients are welcome to use it.

✓ Store extra blank checks in a locked space and take sensitive out-going mail with private information to the post office directly.

✓ Minimize your exposure by carrying only the minimum items in your purse or wallet. Make a photocopy of your credit cards, front and back, and list the phone numbers to call if the cards are lost or stolen.

✓ Get fraud alert. Most credit card companies offer fraud protection, some are free and others cost a small fee. These programs alert you if there is suspicious activity on your account.

## Recommended Links

- **VPN Software**
  - Tunnelbear: https://www.tunnelbear.com
  - VPN Unlimited: https://www.vpnunlimitedapp.com

- **Anti-Virus Software**
  - Kaspersky Anti-Virus: https://usa.kaspersky.com/
  - Malwarebytes: https://www.malwarebytes.com/
  - Norton Security: https://us.norton.com/norton-security-antivirus

- **Anti-Tracking Software**
  - AdBlock: https://getadblock.com/
  - Privacy Badger: https://www.eff.org/privacybadger

The web site links referenced are being provided strictly as a courtesy. Neither us, nor Kestra IS or Kestra AS are liable for any direct or indirect technical or system issues or any consequences arising out of your access to or your use of the links provided.