

Staying Safe in an Online World

Wealth Management Insights | July 2016

In the early days of the internet, protecting your personal and financial information was relatively straightforward: Keep your passwords to yourself, log out of any online accounts and disregard email from strangers promising a fortune in exchange for your banking information. As smartphones and other mobile devices have increased in popularity, so has the amount of personal information people share – making the instances of cybercrime much more commonplace today. This month’s Wealth Management Insights looks at the steps you can take now to increase your personal cyber security.

.....
For more tips on protecting yourself from cybercrime, check out **Digest’s Winter 2015** interview with FBI special agent Jeff Lanza at bairddigest.com.
.....

What you should know:

1. Simple passwords have gotten too easy to crack.

- “P@ssword” is not fooling anybody. A strong password will have at least 12 characters, be hard to guess and include numbers and special characters. Avoid using words or names as passwords, as they leave the user susceptible to “dictionary attacks.”
- Use a different password for each online website. This will help keep a criminal who has accessed one of your accounts from logging into all of your accounts.
- If remembering and regularly changing your passwords seem too difficult, consider using a

password manager, which can remember (and fill in!) your credentials for you.

2. Your online behavior can be the best defense.

- Update your operating system and any applications as soon as they become available – they often contain the most current defenses against malware and other security threats.
- Be skeptical of “phishing” emails asking you to enter personal information or to click on an unfamiliar link – even if it comes from people or institutions you trust. If you have doubts, verify offline before proceeding. ▶

- Make sure your computer is protected by antivirus software, and investigate how to maximize the security options provided by your operating system and internet provider.

3. Your mobile phone or tablet has its own unique vulnerabilities.

- Set your phone to lock after a short idle time – and require a password to unlock it. That can help prevent anyone who takes possession of your phone from accessing the information and contacts stored on your device.
- Use care when deciding to download an app. Is the app created by a reputable company? Is it well-reviewed, and by several users? Be wary if an app you download requests permission to access other, unrelated information like your photos or contacts.

- The portability of these devices increases the risk. Don't store anything on a smartphone or tablet that you wouldn't want made public, and back it up regularly.

What you should do now:

The ease and convenience of making online and mobile purchases come with a cost – an increased vulnerability to having your personal and financial information hacked by cybercriminals. Your best defense against these types of attacks is to stay alert and limit your exposure to fraud. Your Baird Financial Advisor can provide additional advice on how to keep your financial information safe online. ■