Preempting Cybercrime

Cybercrime impacts more than one million victims ***per day*** with 69% of adults having experienced cybercrime in their lifetime according to Norton cybercrime report. Consider the technological advances already underway; vehicle-to-infrastructure communication, driverless vehicles, smart homes and appliances storing sensitive data, Apple Pay and Samsung Pay, medical analytics, personal drone usage and robotics. These revolutions undoubtedly will reshape our lives and provide tremendous value but will subject us to cyber vulnerabilities as well. Frontier advocates for our clients by using our Wealth PASS vault to transfer sensitive information, encrypting confidential documents sent by e-mail, and verbally verifying wire instructions while requiring a password. We also ensure our anti-virus software is up-to-date, monitor our firewall, and employ industry-leading IT firms to further secure your data and our network. As our world becomes more technology dependent, users must diligently protect their information because cybercrime will undoubtedly continue to rise. Below are six steps to help protect yourself.

1. Change your passwords frequently, make them complex and unique. Ensure that you have a unique password for all accounts, especially your e-mail. Make it at least eight characters long, include at least one number, one capital letter, and one lower case letter. Don't use personal information such as your date of birth for your passwords or login IDs. Change your passwords every six months and create passwords that are hard for fraudsters to guess. For accounts that ask questions to further verify your identity, select questions that aren't readily ascertainable. To store your passwords, there are password managers such as Dashlane 4 and Last Pass. If you write down your passwords, be sure to store securely. Consider adding a verbal password to your financial accounts for an extra layer of security. Opt for a free security token if available through your custodian to make every login even more secure. Select dual/multi-factor authentication if available which is a means of confirming your identity by at least two different methods, such as a password and text code to your prescribed number.

2. Destroy hard drives, remote wipe devices, encrypt devices, and delete data stored in the cloud. When discarding old devices, it is best to **physically destroy the hard drives** (i.e. smash with a hammer). Laptops, desktops, tablets, flash drives, SSDs/HDDs (storage devices), printers, scanners, copiers, and SIM cards all have hard drives that should be **encrypted** while in use and physically destroyed when discarding. Deleting and formatting do not actually erase the data – it makes files unavailable to access but data *can be* recovered. A secure wipe is the second-best option if unable to physically destroy the hard drive. Secure wipes completely overwrite your entire hard drive with blank data several times. When using **wireless** keyboards, mice, and **Bluetooth** connected devices, make sure the devices are **encrypted** and set up a strong pin. We recommend using **wired devices** when possible. Remember: **cell phones store data** and removing the SIM/SD card does not erase internal memory. Experts recommend encrypting your mobile data and then engaging in a factory reset. Consider tracking software to remote wipe, track, and lock lost/stolen devices. If you back up your data on your devices to the cloud, remote wipe **may not delete cloud data**. You may need to manage your device's storage by selecting delete. Applications that can locate, lock, and/or erase wireless devices are covered here: http://www.ctia.org/consumer-tips/how-to-deter-smartphone-thefts-and-protect-your-data.

3. Shred sensitive data, encrypt and password protect documents, and use Frontier's Wealth PASS vault. Be sensitive to mailings you receive and take the time to shred confidential documents. When engaging

in confidential communication online, ensure that you are encrypting and password protecting sensitive documents. **Frontier's Wealth PASS** is an online vault with two-factor authentication, advanced 256-bit encryption, and other protections. Clients use the vault to share information with advisors, store estate planning documents, tax returns, passports, driver's licenses, and deeds, as well as other items.

4. Never use public wi-fi, seek https in the web address when online, and be careful what you share. Most public wi-fi does not require authentication to establish a network connection (i.e. if no password is required to connect, password is not sophisticated, or almost never changed). Use a virtual private network to connect, if possible. If the web address has **"https"**, the "s" stands for secure and your information is encrypted. Pay attention as you move throughout the website to ensure https is not just on the initial page you pull up online. **Never** accept software updates including anti-virus "updates" when connected to a public wi-fi. If you must use a public computer, clear the browser's cache history and cookies before leaving. Your financial institutions will **never** ask for your user ID and password. Don't stay permanently signed in to accounts - log out so that you are less susceptible to attack. **Do not follow web links.** Forward suspicious e-mails to the appropriate authorities. To report IRS fraud: https://www.irs.gov/uac/scam-calls-and-emails-using-irs-as-bait-persist. To report other types of fraud: https://www.usa.gov/stop-scams-frauds#item-35157.

5. Install and maintain anti-virus and anti-spyware, activate your computer firewall, and set pins/passwords. **Schedule updates and patches** to your devices. All devices need to have up-to-date anti-virus and anti-spyware software. **Set pins and password**s on your devices as this is a first line of defense if your device (including your cell phone) is stolen. Configure devices to lock after five attempts. **Report stolen devices** to local law enforcement authorities and then register the stolen devices with your wireless provider (if applicable). This provides notice to all major wireless service providers of the theft and will allow for remote disabling of the device so that it cannot be activated on any wireless network without your permission. See link for how to stay safe online: https://www.consumer.ftc.gov/features/feature-0038-onguardonline.

6. Regularly review medical records, account statements, credit reports, and use credit cards for online payment. Medical identity theft is on the rise with over 90% of healthcare organizations having lost data to hackers at least once in the past two years according to the Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data. When medical data is breached, hackers have access to social security numbers, addresses, phone numbers, drug prescriptions, personal health records, credit history and credit reports. **Personal information can be changed** such as your blood type, allergies, and address. Regularly review your medical records and explanation of benefits. Reviewing financial accounts regularly can help catch suspicious activity. Frontier's Wealth PASS allows you to aggregate all accounts through one sign-in making account reviews easier to manage. Use credit cards instead of debit cards when shopping online. Enable text alerts from your credit card and other financial institutions to notify you of suspicious activity. Consider purchasing identity monitoring services from companies such as LifeLock, Inc. or IdentityForce™. You are entitled to a free annual credit report every twelve months. To order your free credit report, go to: https://www.annualcreditreport.com/index.action.

Jessica Cafferata, JD, CFP®

Senior Financial Planner