FRONTIER
Powered by HIGHTOWER

PREEMPTING CYBERCRIME

Cybercrime impacts more than one million victims per day with 69% of adults having experienced this violation in their lifetime according to the 2021 Norton™ Cyber Safety Insights Report cybercrime report. As tremendous technological advancements continue to shape our world such as vehicle-to-infrastructure communication, driverless vehicles, smart homes and appliances, Apple Pay, medical analytics, personal drone usage and robotics, our exposure to cyber vulnerabilities remain widespread. With our increasing dependence upon technology, we must diligently protect our information.

Frontier's Wealth PASS vault offers clients an added layer of protection. Wealth PASS is an online vault with two-factor authentication, advanced 256-bit encryption, and other protections. This solution safeguards sensitive information by encrypting confidential documents sent by e-mail and verbally verifying wire instructions while requiring a password. 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. We are vigilante in ensuring that our anti-virus software is up-to-date, monitoring our firewalls, and employing industry-leading IT firms to secure your data and our network.

Below are five steps you can take to proactively protect yourself from cybercrimes:

1. **Keep Them Guessing:** Change your passwords frequently, make them complex and unique:

- Ensure that you have a unique password that's not based on personal information for all accounts, especially your e-mail that includes at least eight characters, one number, one capital letter, and one lower case letter.
- If accounts ask you to select questions to further verify your identity, choose options with answers that aren't readily ascertainable.
- Change passwords every six months.

This can be a lot of information to track, but there are several online password managers that can help such as Dashlane 4 and Last Pass. If you write down your passwords, be sure to store them securely. Consider adding a verbal password to your financial accounts for an extra layer of protection and opt for a free security token, if available, through your custodian to make every login more secure. Implementing a dual/multi-factor authentication, a means of confirming your identity by at least two different methods, such as a password and text code to your prescribed number is also good practice.

2. **Wipe the Slate Clean:** Destroy hard drives, remote wipe devices, encrypt devices, and delete data stored in the cloud.

Laptops, desktops, tablets, flash drives, SSDs/HDDs (storage devices), printers, scanners, copiers, and SIM cards all have

FRONTIER
Powered by HIGHTOWER

hard drives that should be encrypted while in use. When discarding old devices, it is recommended to physically destroy the hard drives. It's not enough to delete and reformat data – such actions only make files unavailable to access, but data can be recovered. Smashing hard drives with a hammer is encouraged! 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 they are encrypted and set-up a strong pin. Consider implementing tracking software to remote wipe, track, and lock lost/stolen devices, but note that if your devices are backed up on the cloud, this step alone may not successfully delete your data. You may need to manage your device's storage by selecting the "delete" option.

Applications that can locate, lock, and/or erase wireless devices are covered here: https://www.ctia.org/consumer-resources/protecting-your-data

3. **Prioritize Privacy.** Never use public Wi-Fi, seek secure web browsers as indicated by HTTPS and use caution when sharing your information online.

Private networks offer the most security as most public Wi-Fis do not require authentication to establish a network connection. The "S" in "HTTPS" indicates a secure connection, meaning that websites that begin with this acronym encrypts your information. Take notice to ensure that the "https" remains in place as you browse beyond a site's landing page and never accept software updates including anti-virus "updates" when connected to public Wi-Fi. If you must use a public computer, clear the browser's cache history and cookies upon completing your session, taking care to log out of any website you've logged into. Do not follow unverified web links.

Forward any suspicious e-mails to the appropriate authorities. To report IRS fraud: https://www.irs.gov/newsroom/dont-fall-for-scam-calls-and-emails-impersonating-irs To report other types of fraud: https://www.usa.gov/stop-scams-frauds#item-35157.

4. **Leverage Secure Solutions.** Install and maintain anti-virus and anti-spyware, activate your computer firewall, and set pins/passwords:

- Schedule updates and patches to your devices, ensuring that all devices anti-virus and anti-spyware software are up-to-date.
- Set pins and passwords on your devices as the first line of defense in the event that they are stolen.
- Configure devices to lock after five attempts.
- Report stolen devices to local law enforcement authorities and register them with your wireless provider, if applicable This provides notice to all major wireless service providers of the theft, allowing for remote disabling of the device to prevent it from being activated on any wireless network without your permission.

Learn more about staying safe online with the following resource: https://www.consumer.ftc.gov/features/feature-0038-onguardonline

FRONTIER
Powered by HIGHTOWER

5. Best Practices. Regularly review medical records, account statements, credit re ports 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 making it possible to change your personal information including blood type, allergies, and addresses. It's important to regularly review your medical records and explanation of benefits as well as your financial accounts to catch any suspicious activity. Solutions such as Frontier's Wealth PASS simplifies this process, allowing you to aggregate and monitor all accounts through one sign-in.

Follow these best practices for added security:

- 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; order your free credit report by visiting: https://www.annualcreditreport.com/index.action

THE FRONTIER PLANNING TEAM
(800) 553-8034

WWW.FRONTIERINVEST.COM