



CYBER SAYS...

Follow these Top Security Recommendations

Cyber and fraud best practices for protecting yourself

Monitor Accounts and Credit

- Freeze your credit to prevent credit fraud:

Equifax 800-525-6285

Experian 888-397-3742

TransUnion 800-680-7289

- Monitor your accounts and credit score for suspicious activity; consider purchasing identity theft protection

Protect Your Accounts and Identity

- Create unique login identities and passwords (avoid using your email address)
- Enable two-factor authentication for Fidelity and other financial, email, phone and social media accounts
- Provide current email address and phone number so you can be contacted in real time in case of fraud
- Sign up for voice biometrics when offered
- Don't click on untrusted links or attachments in email or text
- Consider using a password vault/manager for lower risk accounts



Phishing still drives 90% of cybersecurity breaches.¹ If you're in doubt,

DON'T CLICK and DELETE!



There are now more than **15 billion stolen** account credentials available to cybercrime actors.²

Make yourself a difficult target for cyber criminals by not reusing passwords and avoiding weak, commonly used passwords, e.g., 123456.

Safeguard your Data, Mail and Online Shopping

- Backup your data to a secure cloud location
- Consider using trusted payment systems and never use debit cards for online purchases
- Protect your mail – sign up for USPS's free **Informed Delivery Service**

Secure your Devices

- Use a personal firewall and anti-virus software on your personal devices
- Use trusted devices for conducting sensitive transactions
- Avoid conducting sensitive transactions over public Wi-Fi
- Secure your mobile services, including cellphone and mobile provider account
- Update/patch your Internet of Things (IoT) devices - e.g., smart TVs



1. Graphus, Inc, January 2020

2. The Digital Shadows Photon Research team as seen on Forbes.com, July 2020