Secure your digital life: Cybersecurity tips from Fidelity

Cybercriminals may be targeting your wealth. Consider six steps to help raise your awareness of potential threats, reduce your risk, and secure your digital life.

1 Stay alert

Be aware that cybercriminals can easily fake incoming phone numbers on caller ID to make it appear that they are calling from a trusted institution, such as your bank.

1. Be suspicious of unsolicited emails or calls that ask you to take action, especially if they suggest that immediate action is required to avoid dire consequences.
2. Cybercriminals often ask for login credentials and personally identifiable information. They may also ask you to read back one-time security codes. Never share this information with an unverified inbound caller.
3. Never give an unverified individual remote access to your computer after receiving a call, email, or pop-up request to do so.
4. Set up security alerts to monitor your accounts and notify you of any suspicious activity.

Learn more How to stay vigilant around fraud: https://www.fidelity.com/security/prevent-fraud-identity-theft

2 Secure your credentials

- Consider using a password manager, as they can make it easy to use distinct, strong credentials for your financial and other personal accounts.
- If you aren't using a password manager, consider using a sheet of paper kept in a secure place. This approach is better than using weak or reused passwords, or keeping passwords in an electronic document on your computer.
- Don't save passwords in your web browser, as they are susceptible to malware attacks.
- Avoid using easily guessed credentials such as an ID that resembles your name or email address, or a simple, easy-to-remember password such as "123456" or "Password."
- Be sure to always enable multi-factor authentication to enhance your security. If your provider offers fingerprint or face ID, consider enabling those features.
- Consider using a PIN or passphrase for your mobile account to prevent criminals from porting your phone to a new carrier or swapping their SIM card for yours.

Learn more How to choose and utilize a password manager: https://www.cnet.com/how-to/best-password-manager/
How to enhance your security at Fidelity with multi-factor authentication, Fidelity MyVoice biometrics, and security alerts: https://www.fidelity.com/security/overview

Fidelity INVESTMENTS

3 Secure your devices

- Keep your operating systems up-to-date to quickly patch new vulnerabilities as they're discovered. Auto-update is recommended for most individuals.
- Use antivirus software and keep both the software and virus definitions up-to-date on all devices. Auto-update is again a best practice for most people.
- Backup your data to a secure cloud location.
- For mobile devices, consider the following steps:
  - In case devices are lost or stolen, activate security features such as passcodes, lock/auto-lock functions, remote lock/data wipe, "find my phone," and face/touch ID.
  - Before trading in an old device, erase any personal information it may contain by resetting the device to its factory settings.

Learn more How to select a data-backup solution: https://www.cnet.com/tech/services-and-software/backup-your-data-to-the-cloud-a-complete-guide/

4 Secure your network

- Secure your home WiFi network with a strong password, and monitor the devices that connect to it (some service providers offer tools and alerts for this).
- Consider using a Virtual Private Network (VPN). VPNs encrypt your internet connection and mask your public IP address, providing a layer of privacy and security.
- Exercise caution when connecting to the internet via unsecured or unknown wireless networks, such as those in public locations like hotels or coffee shops. These networks may lack virus protection, are highly susceptible to attacks, and should never be used to access confidential personal data directly without the protection of a secure VPN connection.

Learn more How to use a VPN: https://www.cnet.com/tech/services-and-software/how-to-use-a-vpn/

5 Secure your reputation

- While credit freezes have long been used reactively in response to suspected identity theft, it's become a common proactive step as well. If you haven't already frozen your credit, consider doing so across the three major credit bureaus:

Equifax
Equifax.com/personal/credit-report-services
(888-378-4329)

TransUnion
TransUnion.com/credit-help
(833-806-1627)

Experian
Experian.com/help
(888-397-3742)

- Limit the personal and work-related information you share on social media. Cybercriminals can use this information to impersonate people or groups you know, in attempts to defraud you. Or, they may use this information to impersonate you to another target.

Learn more How to use credit freezes and fraud alerts: https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs

6 Act quickly if compromised

If you suspect an account has been compromised:

1. Contact and inform the provider immediately
2. Change your password from a device you don't normally use for that account
3. Select "log out of all devices"

If you suspect a device has been compromised/infected with malware:

1. Stop using the device
2. Disconnect it from internet or shut it down
3. Seek professional assistance

If you suspect you are a victim of identity theft:

1. Put a fraud alert on your credit reports
2. Contact any impacted institution directly
3. File a police report

If you believe your Social Security number has been compromised

1. Contact the Social Security Administration: (800-772-1213)
2. Contact the Internal Revenue Service: (800-829-0433)

870233.14.0

1.9893541.105