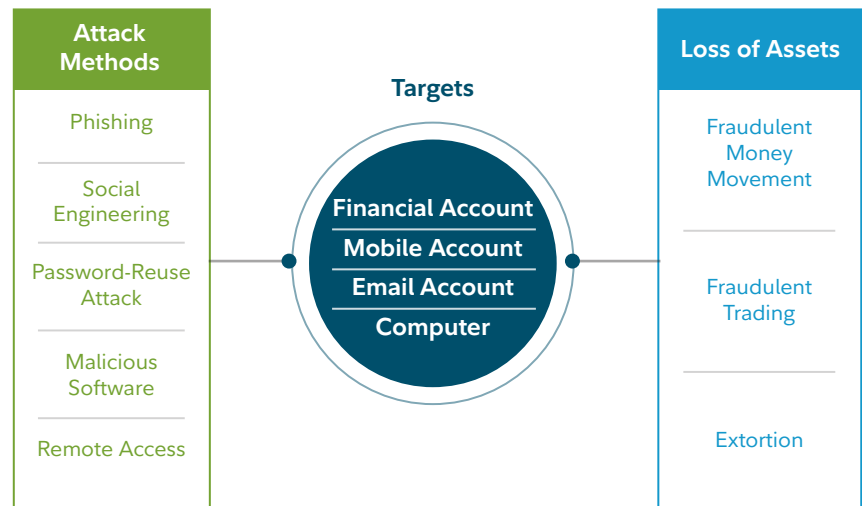


Make Yourself a Difficult Target for Cybercriminals

Cybercriminals may be targeting your wealth. Fidelity's Cyber Fraud Investigations Team recommends you reduce your risk by considering the following actions. Consult your financial representative if you are unsure how to accomplish these tasks.



Follow these steps, in order, to regain control of your digital life.

1 Use a password manager to keep track of your passwords

- Don't save passwords in your web-browser, (i.e., Chrome, Safari, Firefox, Microsoft Edge) as they are susceptible to malware attacks.
- If you aren't using a password manager, a sheet of paper, kept in a secure place, is better than reusing or choosing weak passwords, or keeping them in an electronic document or spreadsheet on your computer.

Learn More

How to choose and utilize a password manager:
<https://www.cnet.com/how-to/best-password-manager/>

2 Protect your financial accounts

Log in to your financial provider's website

- If you haven't registered for log-in credentials, do so now. If you don't intend to use them, ask your financial provider to put a block on them.
- If your username is like your name, email address, or usernames you have chosen for other sites, create a new one that is unique to your financial provider.
- If your password is like one that you have used at another site, create a new one that is unique to your financial provider.
- If you are not already using multifactor log-in authentication, like the Symantec VIP Access App at Fidelity, enroll now.

- If your provider offers voice biometrics, like Fidelity's MyVoice, that detect and verify your voice on a phone call, and you are not already enrolled, do so now.
- If you are not already leveraging security alerts to warn you of suspicious behavior or changes to your account, activate them now.

Learn More

How to enroll in Symantec VIP Protection, Fidelity MyVoice, and Security Alerts at Fidelity: <https://www.fidelity.com/security/overview>

3 Protect your mobile device/accounts

Log in to your mobile provider's web portal (ex: att.com, verizon.com, etc.)

- If your username is like your name, email address, or usernames you have chosen for other sites, create a new one that is unique to your mobile provider.
- If your password is like one that you have used at another site, create a new one that is unique to your mobile provider.
- If you are not already using multifactor authentication for extra log-in protection, enroll now.
- If you are not already using a pin or pass-phrase to prevent criminals from porting your phone to a new carrier or swapping their SIM card for yours, create one now.

Secure your mobile device in the event it is lost or stolen

- Activate a PIN or lock function for your mobile device. Using a PIN is the simplest and most important thing you can do to ensure security on your mobile device, especially if it's lost or stolen. Set the device to auto-lock. You could also enable fingerprint-based protection if it's available on your device.

Install anti-virus software on your mobile device and activate automatic updates to ensure the devices remain protected.

Before trading in an old device, erase any personal information it may contain by resetting it to its factory settings.

Learn More

Most mobile providers—Verizon, AT&T, etc.—offer two-factor log-in authentication as a security option. A web search of your mobile provider plus "two-factor authentication" or "account security" will lead you to instructions.

4 Protect your email accounts

Log in to your email provider's web portal

- If your password is like one that you have used at another site, create a new one that is unique to your email provider.
- If you are not already using multi-factor authentication for extra log-in protection, enroll now.

- If you are not already leveraging security alerts to warn you of suspicious behavior or changes to your account, activate them now.

If you access your email account via an application like Outlook or Mail, and if you just updated your password via your provider's web portal, go to those applications and update your password.

Learn More

Most email providers—Google, Microsoft, Yahoo, etc.—offer two-factor login authentication as a security option. A web search of your email provider plus "two-factor authentication" or "account security" will lead you to instructions.

5 Protect your computer, tablet, and mobile device from malicious software

- Keep your operating system up to date (auto-update is recommended for most individuals).
- Use anti-virus software and keep both the software and virus definitions up to date (auto-update is recommended for most individuals).

6 Secure access to your social media accounts

Log into your social media accounts

- If your password is like one that you have used at another site, create a new one that is unique to your email provider.
- If you are not already using multi-factor authentication for extra log-in protection, enroll now.

Learn More

Most Social Media platforms—Facebook, Instagram, Twitter, etc.—offer two-factor login authentication as a security option. A web search of your social media platform plus “two-factor authentication” or “account security” will lead you to instructions.

7 If you haven't already frozen your credit, considering doing so

Equifax

[Equifax.com/personal/credit-report-services](https://www.equifax.com/personal/credit-report-services)

800-685-1111

Transunion

[TransUnion.com/credit-help](https://www.transunion.com/credit-help)

888-909-8872

Experian

[Experian.com/help](https://www.experian.com/help)

888-EXPERIAN (888-397-3742)

Learn More

Credit Freeze FAQs

<https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs>

Act quickly if you think you have been compromised

If you think your financial account has been compromised

- Contact your financial representative immediately
- Change your password from a different device than the one from which you typically log in
- Ensure that old or lost devices are no longer considered “trusted”

If you think your mobile account may have been compromised

- Change the password for your provider’s online portal
- Contact your provider immediately
- Ensure that old or lost devices are no longer considered “trusted”

If you think your email account may have been compromised

- Log in to your account from a new device
- Create a new password
- Check your email settings for any rules or filters that may have been created to forward or move incoming messages

- Ensure that old or lost devices are no longer considered “trusted”
- Contact your provider immediately

If you think your computer may be infected with malicious software

- Stop using it
- Disconnect it from the internet or shut it down all together
- Seek professional assistance

If you think you are the victim of identity theft

- Put a fraud alert on your credit reports
- Contact any institution directly affected
- File a police report
- Contact the Social Security Administration and the Internal Revenue Service if you believe your Social Security Number has been compromised
- **Social Security Administration:** 800-772-1213
- **Internal Revenue Service:** 800-829-0433



The information contained herein is as of the date of its publication, is subject to change, and is general in nature. Such information is provided for informational purposes only and should not be considered legal, tax, or compliance advice. Fidelity does not provide financial or investment advice. Fidelity cannot guarantee that such information is accurate, complete, or timely. Federal and state laws and regulations are complex and are subject to change. Laws of a specific state or laws that may be applicable to a particular situation may affect the applicability, accuracy, or completeness of this information. This information is not individualized, is not intended to serve as the primary or sole basis for your decisions, as there may be other factors you should consider, and may not be inclusive of everything that a firm should consider in this type of planning decision. Some of the concepts may not be applicable to all firms. Always consult an attorney, tax professional, or compliance representative regarding your specific legal, tax, or regulatory situation.

Information provided in this document is for informational and educational purposes only. To the extent any investment information in this material is deemed to be a recommendation, it is not meant to be impartial investment advice or advice in a fiduciary capacity and is not intended to be used as a primary basis for you or your client's investment decisions. Fidelity and its representatives may have a conflict of interest in the products or services mentioned in this material because they have a financial interest in, and receive compensation, directly or indirectly, in connection with the management, distribution, and/or servicing of these products or services, including Fidelity funds, certain third-party funds and products, and certain investment services.

The content provided and maintained by any third-party website is not owned or controlled by Fidelity. Fidelity takes no responsibility whatsoever nor in any way endorses any such content.

Third-party marks are the property of their respective owners; all other marks are the property of FMR LLC. Third parties referenced herein are independent companies and are not affiliated with Fidelity Investments. Listing them does not suggest a recommendation or endorsement by Fidelity Investments.

Fidelity InstitutionalSM provides investment products through Fidelity Distributors Company LLC; clearing, custody, or other brokerage services through National Financial Services LLC or Fidelity Brokerage Services LLC (Members NYSE, SIPC); and institutional advisory services through Fidelity Institutional Wealth Adviser LLC.

Personal and workplace investment products are provided by Fidelity Brokerage Services LLC, Member NYSE, SIPC.

Institutional asset management is provided by FIAM LLC and Fidelity Institutional Asset Management Trust Company.

© 2021 FMR LLC. All rights reserved.

870233.4.0

1.9893541.102

0421