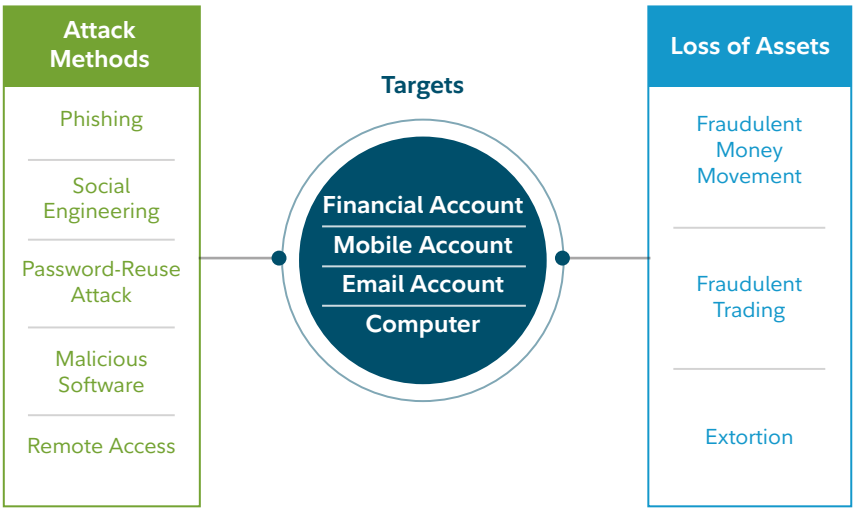
# Make Yourself a Difficult Target for Cybercriminals

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, (e.g., 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.
- Avoid using your name or email address as a login identifier and be sure to always enable multi-factor authentication. Don't reuse passwords and avoid weak, commonly used passwords like 123456.

**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.

Fidelity INVESTMENTS

- 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 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 case it's lost or stolen.

- Activate the passcode or lock functions for each device, set them to auto-lock, and enable remote lock and data wipe. Use the "find my phone" and face ID/touch ID features, if available. This is the simplest thing you can do to ensure security on your mobile 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).
- Backup your data to a secure cloud location.
- 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.
- Limit personal and company information you share on social media. Cybercriminals often use this information to impersonate an individual or group that their target knows, in an attempt to defraud them.

**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, consider doing so

While a credit freeze has long been used reactively in the event of identity theft, it's become a common proactive, preemptive step, as well.

**Equifax**
Equifax.com/personal/credit-report-services
800-685-1111

**Transunion**
TransUnion.com/credit-help
888-909-8872

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

**Learn More** Credit Freeze FAQs
https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs

## 8 Beware of impostors

Watch out for scams. Each year, cybercriminals use a variety of creative techniques to impersonate known entities—over email or social media, or by phone—to take control of financial accounts and defraud individuals.

- These criminals can easily fake incoming phone numbers on caller ID to appear they are calling from a trusted institution, such as your bank.
- Look out for emails or calls that suggest that immediate action is required to avoid dire consequences.
- Never give an unverified individual remote access to your computer after receiving a call, email, or pop-up message to do so.

## 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




870233.7.1