

## Safeguarding Your Financial Information: An Identity Theft Prevention Checklist

Reports of lost laptops or security breaches at financial institutions can spark fears about identity theft. But these aren't the only ways identity theft can happen. Use this checklist to safeguard your sensitive information and help keep identity thieves at bay:

### Protect Usernames, Passwords and PINs

- Keep your usernames, passwords and PINs private—and don't store them on your hard drive.

---

- Create tough-to-crack passwords and PINs, using a minimum of 8 letters and numbers and, if possible, special symbols.

---

- Change your passwords often, and avoid using the same password for multiple accounts.

---

### Safeguard Your Computer

- Install a personal firewall and an up-to-date security software package.

---

- Configure your security settings to receive automatic updates for your anti-virus, anti-spam, and spyware detection programs.

---



- If authorized, use a Virtual Private Network (VPN) which offers protections that standard networks do not.

---

### Be Smart When Accessing Your Brokerage Account Online

- Use your own computer rather than a public or shared computer.

---

- Confirm that you have a secure Web connection throughout your session by looking for:
  - > A website address starting with "https://" instead of "http://" and
  - > A secure symbol such as a closed padlock  or key  on your status bar.

---

- When you're done, be sure to log out completely and close your browser.

---

### Use Wireless Connections Wisely

- Use encryption software to secure your wireless connection at home.

---

- Shut off wireless connectivity or remove the wireless network card if you leave your computer unattended.

- 
- When visiting a hot-spot or using an unencrypted wireless connection, disable wireless ad hoc mode to prevent unknown or rogue connections, and disable file and printer sharing capabilities when visiting hotspots.
- 

## Avoid Inviting Trouble

- Never respond to an email that asks you to reveal personal information, such as account numbers, your Social Security number, or passwords or PINs.
  - Keep your Social Security number private, and avoid using it as a username, password, or PIN.
  - Use care when downloading files from Internet sites or clicking links in pop-up ads.
- 

## Keep an Eye on Your Finances

- Always read your monthly account statements, and alert your brokerage firm or other financial institutions if you see a transaction you didn't authorize or if your statement doesn't arrive.
  - Check your credit report using [AnnualCreditReport.com](https://www.annualcreditreport.com).
  - Store financial records in a safe place, and shred—never simply toss out—documents containing sensitive information.
- 

Your brokerage firm or other financial institution should always be your first call if you suspect your account has been compromised or your identity has been stolen. For more information and resources on preventing identity theft, visit the Federal Trade Commission's [Identity Theft website](#).