# 6 keys
## to protecting yourself online

As cyber fraud continues to evolve, it is more critical than ever to take measures to protect your identity and mitigate potential security risks. Here are six areas in which you can take action to better protect **your identity, your accounts,** and **your technology.**

# 1. Manage your devices

- Install the most up-to-date antivirus and anti-spyware programs on all devices, and update these software programs as they become available. Run these programs regularly to provide maximum protection for your device.
- Access sensitive data only through a secure location or device; never access confidential personal data via a public computer, such as in a hotel or cybercafé.
- If you have children, set up a separate computer they can use for games and other online activities.

## 2. Protect all passwords

- Regularly reset your passwords, including those for your email accounts. Avoid using common passwords across a range of financial relationships.
- Use a unique username for financial accounts you access online. Never use your Social Security number in any part of your login activity.


## 3. Surf the Web safely

- Do not connect to the Internet via unsecured or unknown wireless networks, such as those in public locations like hotels or cybercafés. These networks may lack virus protection and are highly susceptible to attacks, so should never be used to access confidential personal data.


## 4. Protect information on social networks

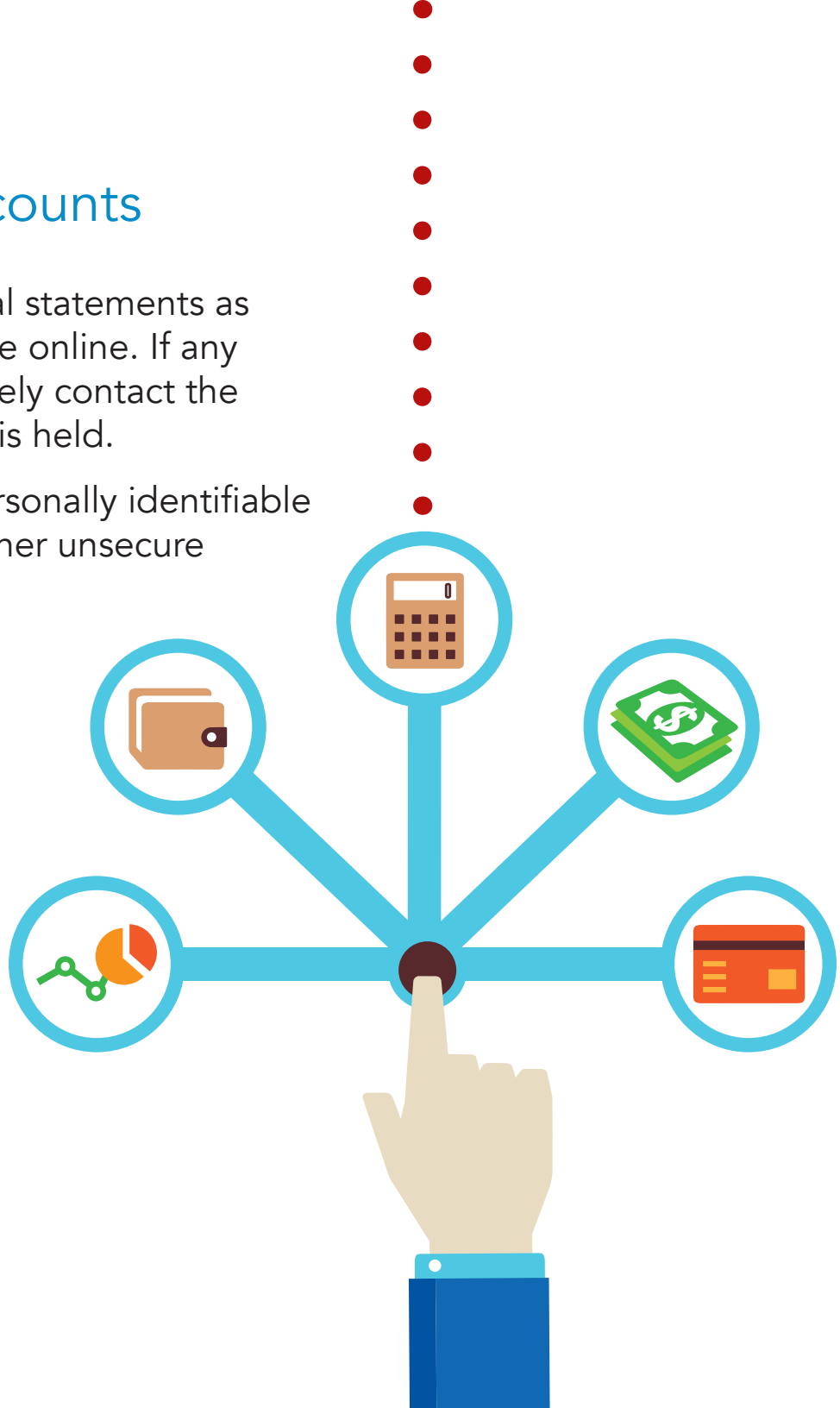
- Limit the amount of personal information you post on social networking sites. Never post your Social Security number (even the last four digits). Consider keeping your birth date, home address, and home phone number confidential.
- Consider whether you want to post information about births, children's birthdays, or the loss of loved ones. Sharing too much information can make you more susceptible to fraudsters and allow them to quickly pass a variety of challenges related to the authentication of your personal information. Never underestimate the public sources individuals will use to learn critical facts about people.

## 5. Protect your email accounts

- Delete any emails that include detailed financial information beyond the time it's needed. In addition, continuously assess whether you even need to store any personal and financial information in an email account.
- Use secure data storage programs—such as cloud storage and/or online vaults—to archive critical data and documents.
- Review unsolicited emails carefully. Never click links in unsolicited emails or in pop-up ads, especially those that warn that your computer is infected with a virus and request that you take immediate action.
- Establish separate email accounts for personal correspondence and financial transactions.

## 6. Safeguard your financial accounts

- Review all your credit card and financial statements as soon as they arrive or become available online. If any transaction looks suspicious, immediately contact the financial institution where the account is held.
- Never send account information or personally identifiable information over email, chat, or any other unsecure channel.
- Be suspicious of any unsolicited email requesting personal information. Further, never respond to an email requesting information by clicking a link within the email. Instead, type the website's URL into the browser yourself.




Approved for use in Advisor and 401(k) markets. Firm review may apply.

Fidelity Brokerage Services LLC, Member NYSE, SIPC, 900 Salem Street, Smithfield, RI 02917



684151.8.1