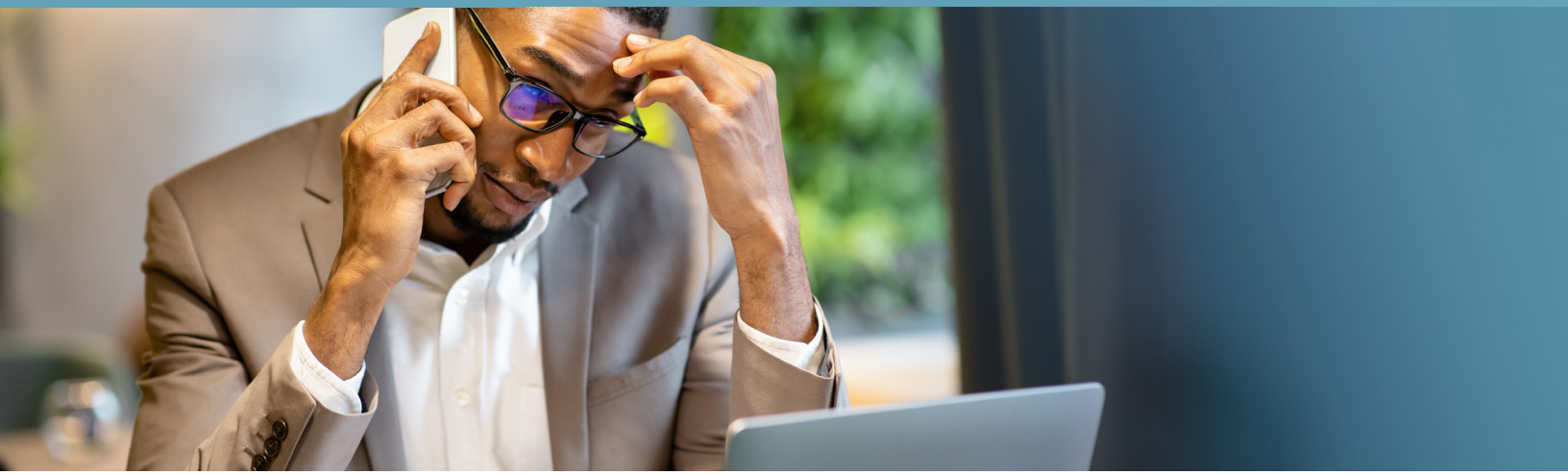
Protecting your retirement account and identity against cybercrime

hooker & holcombe



Identity thieves and other criminals are increasingly targeting retirement accounts instead of more traditional targets such as credit cards. Because of this trend, it's more important than ever to make sure that your account and personal data are secure.

Many security measures have been implemented to help safeguard your retirement account. You can also help by taking simple steps to protect yourself online and to minimize the damage to your retirement account if you become a victim of identity theft.

Tips for staying safe online

Online security doesn't have to be overwhelming. Following the preventative steps below can go a long way toward safeguarding your personal information, protecting you from identify theft, and keeping your accounts secure.

Follow general best practices

- Be suspicious of unexpected or unsolicited phone calls, emails, and texts asking you to send money or disclose personal information.
- If you receive a suspicious call about your retirement account, do not accept it. Instead, hang up and call back using a known contact number.
- Be cautious when sharing sensitive information and conducting personal or confidential business via email, since it can be compromised and used to facilitate identity theft.
- Be careful what you share on social media. Identity thieves routinely search social media for dates of birth, locations of birth, maiden names, vacation details, phone numbers, and other information.
- Check your email and account statements regularly for suspicious activity.
- Do not speak or type confidential information into a laptop or mobile device in public areas where someone could eavesdrop or see over your shoulder.

Be sure you're on a secure website

- Check the URL to see if it's a secure connection. Secure sites begin with "https" rather than "http."
- Log out completely to terminate the session when you've finished accessing your retirement plan or other financial accounts online.

Keep your technology up to date

- Keep your web browser and operating system up to date, and use auto-update when possible. Old software and operating systems can be susceptible to attack.
- Install antivirus and antispyware software on all computers and mobile devices, and update and scan for viruses regularly. If you or your family members use multiple devices in your home, consider isolating a device for your banking activity only.
- Enable the security settings on your web browser and other applications.

- Do not use free or found USB thumb drives—they could be infected with viruses or malware.
- Turn off Bluetooth when it's not needed so that hackers cannot access your devices via Bluetooth connections.
- Safely and securely dispose of old hardware that could contain personal information.

Be cautious with public networks

- Avoid using public computers. If you must use one, go to the browser settings and clear the browser history (cache) and cookies when you're finished.
- Only use wireless networks you trust or that are protected with a secure password.
- Do not log in to your retirement plan or conduct other financial activities when using public Wi-Fi.
- Do not accept software updates if you are connected to public Wi-Fi.

Be strategic with your login credentials

- Do not use personal information such as your birthday as part of your Login ID.
- Create a unique password for each financial institution you do business with and change it every six months.
- Use longer passwords when possible. Longer passwords are one of the most effective ways to protect against unauthorized account access.
- Consider using a password manager to create, manage, and store passwords that are unique and secure.
- Do not share your passwords.
- Avoid storing passwords on your hard drive or using "remember me" features in browsers or applications.
- Avoid storing user names, passwords, or other sensitive data in your email.
- Use secondary authentication methods, such as two-factor authentication (2FA) and image-based authentication, when they are available.

Beware of phishing

- Do not click on links or attachments in emails and text messages if they seem suspicious or were sent from someone you do not know.
- Hover over questionable links to reveal the site's full URL and see where the link really goes. Do not click on links that do not match the sender or what you would expect to see.
- Be suspicious of emails that have grayed-out Cc: and To: lines—they may have been sent to a mass distribution list.
- Check the sender's domain name in the email address to see if it matches what you would expect.
- Activate the spam filters in your email settings. This will help prevent unsolicited emails from coming to your inbox.

Steps to take when your personal data has been compromised

If your personal data is compromised, whether as part of a larger cyberattack or through an individual cybercrime, time is of the essence. You'll need to take immediate action to minimize the effects. Use the guidance below as a starting point through the first month and beyond.

Within the first 24–48 hours:

1. **Call your financial institution(s).** When they're aware, they can monitor your accounts.
2. **Call your employer, retirement plan provider, and recordkeeper.** Do this even if the breach did not involve your retirement account. When these parties are aware that your identity has been compromised, they can monitor your retirement account for unusual activity, such as large distribution requests.
3. **Call the Social Security Administration hotline.** Call 1-800-269-0271 (TTY 1-866-501-2101) if you suspect your Social Security number has been compromised.
4. **Contact the Federal Trade Commission.** Call 1-877-ID-THEFT (TTY 1-866-653-4261) or visit **www.ftc.gov.**
5. **Visit the IRS website.** Go to **www.irs.gov/newsroom/taxpayer-guide-to-identity-theft** for tips and educational resources.
6. **Close any unauthorized accounts.**
7. **Clean your computer.** Run reputable antivirus/antimalware/antispyware software.

8. **Change your passwords.** Do this once you've ensured your computer is clean—and remember to make each password unique, long, and strong.

Within the first week:

1. **Follow the legitimate directions provided by affected companies and organizations you do business with.** If the business offers credit protection services, sign up.

2. **Report the crime to your local police.** Do this even if the incident crosses several jurisdictions.

3. **Report your stolen money and/or identity to one of the three main credit bureaus.**
   Equifax: 1-800-525-6285; Experian: 1-888-397-3742; TransUnion: 1-800-680-7289.

4. **Put a freeze on your credit report.** Do this with each of the three main credit bureaus, using the numbers listed above or by visiting;
   www.equifaxsecurity2017.com
   www.experian.com/freeze/center.html
   www.transunion.com/credit-freeze.

Within the first month and beyond:

1. **Review all new statements as soon as they arrive.** Report any suspicious transactions to the business where they occurred.

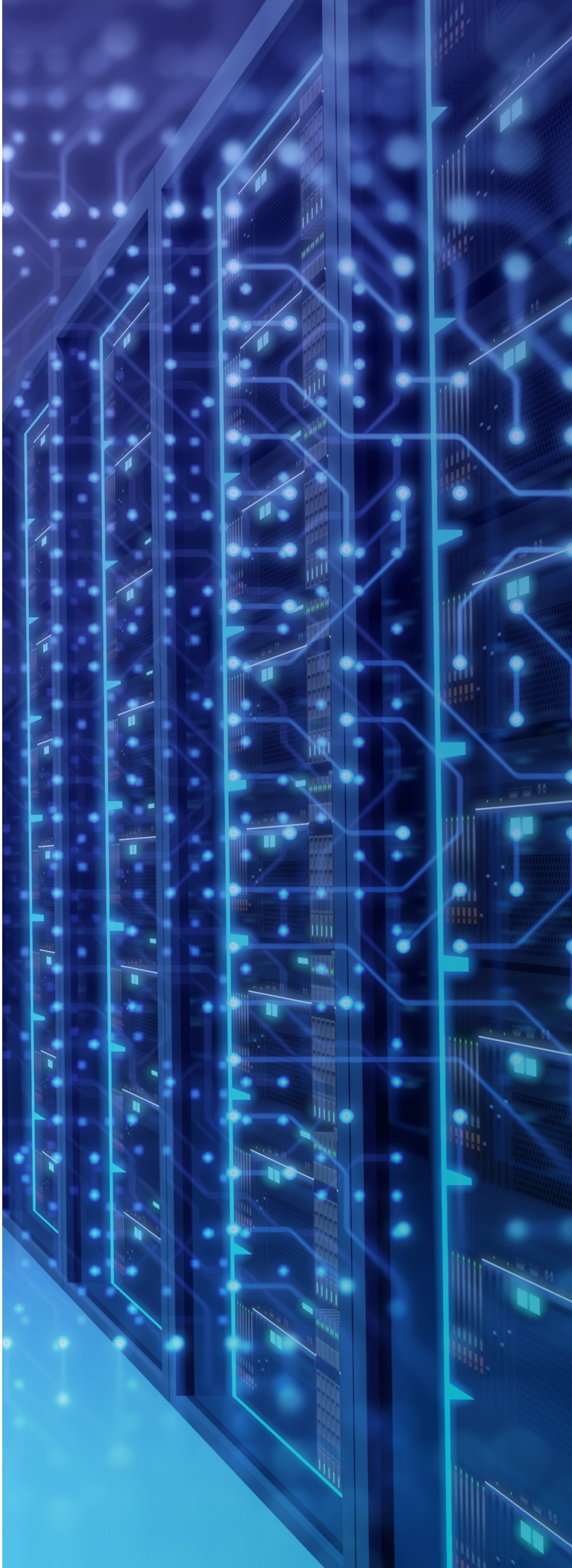
2. **Notify friends, family, and other relevant parties.** Tell them to beware of emails that may have been sent from your account.

3. **Speak with your financial advisor, if you work with one.** Together, you can take preventive measures to enhance identity verification.

4. **Create an online Social Security account.** If you're a victim of Social Security fraud, an online account will allow you to easily review your statement.

5. **Request a credit report every six months to check for unauthorized activity.** This will not affect your credit score.

For the next year, be diligent and take precautions to avoid further security incidents.



Glossary

Domain name
In an email address, this is the information that comes after the @ symbol—for example, "name.com" in "jane.doe@name.com."

Identity theft
Someone using your personal information to open fraudulent accounts, file fake tax returns, or do other criminal things in your name.

Image-based authentication
An authentication method where you are asked to recognize images from predefined categories.

Malware
Software that is intended to damage or disable computers and computer systems.

Password manager
An encrypted online or cloud-based program that generates, retrieves, and keeps track of passwords across many different accounts. Password managers can also store and protect information such as PINs, credit card numbers, and answers to security questions.

Phishing
An attempt to steal personal information, such as passwords or credit card numbers, by sending fraudulent emails or text messages that appear to be from a trusted source. Phishing attempts are usually urgent-sounding, legitimate-looking messages that ask you to disclose personal information or click on a questionable link.

Spam filter
A program that detects unsolicited and unwanted emails and prevents them from reaching your email inbox, usually sending them to a spam folder instead.

Two-factor authentication (2FA)
A method of confirming your identity using a second step to verify who you are. For example, the first step might be to enter your username and password, and the second step might be to enter a randomly generated number sent to you via email, text, phone call, or token.

URL
The web address that displays for a website in your browser's address bar.

Learn more

Visit these sites for more information and best practices:

- **StaySafeOnline.org:** Review the STOP. THINK. CONNECT.™ cybersecurity educational campaign.
- **OnGuardOnline.gov:** Focused on online security for kids. It includes a blog on current cyber trends.
- **FDIC Consumer Assistance & Information: www.fdic.gov/consumers/assistance/index.html**
- **FBI Scams and Safety: www.fbi.gov/scams-and-safety**