Online Security:
Tips for Keeping Your Retirement Account Information Safe

Protect your data and personal information when online

Keep passwords private and complex: Never provide your account password or user name in an email, and do not share these with anyone. When creating new passwords, use a combination of letters, numbers and special characters—you should never use the same password for multiple accounts. Also, avoid saving passwords in your browser.

Manage privacy settings: Privacy settings offer you more control of your personal information online. It's best to set up privacy settings immediately upon set-up of new web browsers, online accounts and applications.

Watch your Wi-Fi: Avoid using public wireless networks and public computers for any confidential, sensitive or financial activity, including accessing your retirement plan. Make sure to also secure your wireless network at home with a password to prevent unauthorized individuals within proximity to hijack your wireless network.

Think before you sync: While syncing your data to the cloud offers convenience by allowing you to access it from multiple devices, information saved to the cloud may be more easily accessed by fraudsters. Consider storing your most sensitive financial and personal information in a more private and secure location.

Disable Bluetooth when not in use: While Bluetooth technology offers mobile convenience, it also creates vulnerabilities when it comes to personal information. Keep your Bluetooth connection off when not in use.

Update protection software: Use anti-virus software**,** anti-spyware, and a firewall to protect private information on all of your devices. Be sure to set your preferences to update these protections often.

Don't forget to sign out: Always sign out of all accounts, including your retirement account, when you leave them. After logging off, you should also close the browsing window used to access your account.

Turn off your computer: When you're finished using your computer or laptop, power it off. Leaving computer devices on and connected to the internet can leave the door open to potential data attacks.

A note about 2FA: Two-factor authentication is an enhanced security feature used to help verify user identity. Upon login, you are sent a one-time verification code. Even if a fraudster has your user ID and password, 2FA makes it much more difficult for them to access your accounts or personal information. Many service providers now require 2FA as an enhanced security protection.

Protect your computer and mobile device

Lock up your laptop: Don’t use your laptop’s automatic login feature. In the event that your laptop is lost or stolen, it makes it harder for anyone to gain access to your personal information.

Set your device to automatically lock: Enable tablets, smartphones, computers and other devices to lock after a short period of time.

Install operating system updates: Operating updates contain critical security patches that will protect your computer from recently discovered threats. It’s best to set your operating system to update automatically.

Safely dispose of data: Before you dispose of a computer, be sure to delete all the personal information it stores. Use a wipe utility program to overwrite the entire hard drive. When disposing of mobile devices, make sure to safely transfer your data to a new device before deleting information permanently.

Make old hard drives unreadable: Still have old hard drives at home? Make them unreadable before throwing them out. After you back up your data and transfer the files, you can shred the disk, magnetically clean the disk, or use software to wipe the disk clean.

Be Alert to Impersonators

Be “email alert”: Phishing is a technique use to fraudulently obtain private information. Typically the phisher sends an email that appears to come from a legitimate business. Prevent being scammed by never clicking on links within emails—even from "trusted" sources; type the URL instead. Also, do not open files or download programs from emails unless you trust the sender. If you’re ever unsure of an email you receive, contact the sender directly.

Prevent identity theft: Identity thieves use a victim’s name, credit card information and other identifying information to commit fraud and other crimes. To help avoid identity theft:

- Routinely monitor bank and credit card accounts for unauthorized transactions
- Review credit reports once a year and check for accounts that you have not opened
- Pay attention to billing cycles for late or out of order financial statements
- Protect your Social Security number
  - only share your number on a need-to-know basis, e.g. for employment or tax purposes
  - always ask if you can use a different kind of identification
- Be vigilant
  - before you share information, whether at a workplace, business, school, or doctor’s office, ask who will have access to your information, how it will be handled, and how it will be disposed of

Beware of pretexting: Pretexting happens when a person uses a false scenario to persuade a targeted victim to share personal information. Through prior research and access to critical information like a Social Security number, the schemer often establishes legitimacy to further the crime. Prevent pretexting by never sharing private financial information over the phone or internet. Also, do not use password backup questions that are publicly available—for example, your mother’s maiden name. Opt for lesser-known details.

While no security precautions are guaranteed to completely protect you from identity theft, using the above tips will help you thwart many types of fraudulent attempts. If you have any questions, please contact our Participant Service Center.