

Keep Your Retirement Account Secure from Online Threats

In today's digital age, safeguarding your retirement account from cyber threats is more crucial than ever. As we increasingly rely on online platforms to manage our finances, the risks of cyberattacks and identity theft grow.

Protecting your retirement account requires a combination of vigilance, best practices, and advanced security measures. By following these essential steps, you can reduce your risk of cyber threats for a more secure financial future.

BEST PRACTICES TO SAFEGUARD YOUR RETIREMENT ACCOUNT

- ❑ **Register, set up, and routinely monitor your online account.** Create unique login credentials to access your account online, and regularly review your account activity to detect any unauthorized changes.
- ❑ **Use a strong and unique password.** Choose passwords that include a mix of uppercase and lowercase letters, numbers, and special characters. Ensure that it is significantly different from previous passwords and is not used for multiple websites. Avoid using easily guessable information like birthdays or common words. Change your password regularly—ideally every 120 days—to reduce the risk of unauthorized access.
- ❑ **Enable multi-factor authentication (MFA).** Whenever possible, enable MFA for an additional layer of security. This typically requires entering a one-time code sent to your phone or email in addition to your password.



Learn how Ascensus protects your information and what actions you can take to stay secure online. Visit ascensus.com/security.

- ❑ **Keep your contact information up to date.** Regularly update your contact details to ensure timely communication if there is an issue with your account.
- ❑ **Secure your private information.** Store your Social Security card, other identification cards, checks, and account statements in a safe and secure location.
- ❑ **Close unused accounts.** Close any accounts you no longer use to minimize your vulnerability to cyber threats.
- ❑ **Avoid public Wi-Fi networks.** Free Wi-Fi at airports, hotels, or coffee shops may be convenient, but it also tends to be unsecured. Use a secure home or mobile network to access sensitive information instead.
- ❑ **Beware of phishing scams.** Phishing messages aim to trick you into sharing personal information, such as passwords or account numbers. Never click links or open attachments that look suspicious and think carefully about any requests to disclose personal or account details.

Guarding your retirement account from cyber threats is an ongoing process that requires diligence and proactive measures. By implementing these best practices, you can protect your savings for a more secure financial future and have peace of mind.



For more guidance from the Department of Labor, read [Online Security Tips at DOL.gov](#).

Learn more

Tap into more resources that can help you prepare for a better future. Visit [Retirement Saving Resources](#).

 ascensus.com

This material has been prepared for general education and informational purposes only. It is not intended to provide legal, tax, or investment advice. Please consult your independent legal counsel and/or professional tax advisor regarding any legal or tax issues raised in this communication.

Ascensus, LLC provides administrative and recordkeeping services. It is not a broker-dealer or an investment advisor and does not provide tax, legal, or accounting services. Ascensus® and the Ascensus logo are registered trademarks of Ascensus, LLC. Copyright ©2025 Ascensus, LLC. All Rights Reserved. 1780450-RET-1780451 (02/2025)