

Your security is our priority

Let's work together to keep your account safe.

Financial accounts are tempting targets for fraudsters but there are ways to make your accounts more secure. A strong password, strong authentication questions, and multi-factor authentication can be key to securing your future.

Here are other ways you can protect your personal information:

- **If you haven't created an account yet, visit principal.com/welcome to help us verify your identity** and make sure you're the only one who can log in to and establish your account.
- **Choose a strong username and password.** Use a mix of letters, numbers, and special characters, and avoid common words or phrases. Go one step further by using a long, complex passphrase.
- **Avoid reusing passwords—and don't share them.** Make your passwords unique for each account. If you need to write it down to remember it, store it in a secure location.
- **Once you've created an account, future logins can be easier with a passkey.** Set one up—you can choose facial recognition, a fingerprint, or a PIN for safe, quick logins.
- **Log in to your account periodically.** Keep your information current, plus stay up to date on any plan changes.
- **Use current anti-virus protection software** on your devices.
- **Review account correspondence frequently** (within 48 hours) including transaction confirmations and notices.

We have your back.

We invest in safeguards to protect access to your personal information and retirement savings.

- Multi-factor authentication
- Behavioral biometrics
- Phone analysis and authentication technology
- Automated Clearing House (ACH) account verification
- Automated red flags for disbursements
- Real-time participant transaction updates

It's simple: Principal® will reimburse participants' employer-sponsored retirement accounts for losses from unauthorized activity occurring through no fault of their own.¹ Learn more at principal.com/customer-protection-guarantee

How do I qualify for the Customer Protection Guarantee?

Register your account online at principal.com/welcome and keep your contact information up to date, especially your mobile number and email address to ensure we can contact you in case of suspected unauthorized activity.



Trouble logging in? Visit principal.com/LoginHelp or call Principal at 800-986-3343.

How does social media impact my security?

The internet is a public resource. What you post on social media could someday become public. Nothing deleted from the internet is ever truly removed. Take steps to stay vigilant and minimize potential exposure to fraudsters.

Limit personal information.

Don't post information that would make you vulnerable, such as your address or information about your schedule or routine, including vacation plans. Make sure you're comfortable with the information your connections post about you.

Verify who your connections are.

The internet makes it easy for people to misrepresent their identities and potentially post misleading information. If you interact with people you don't personally know, be cautious about the amount of information you share with them.

Review your privacy settings.

The default settings for some sites may allow anyone to see your profile. Be sure to review your privacy settings regularly to make sure your choices are still appropriate.

Protect your identity.

Be aware of surveys or quizzes that ask for personal information that could lead to an answer for one of your security questions. For example, "Does anyone remember their first-grade teacher's name?" Since this is a common security question, your answer could be collected for use on your account at a later point.

Access your social media safely.

Social media applications from open internet hotspots provided at hotels, restaurants, and airports may compromise your personal information. Be sure to use a virtual private network (VPN) to encrypt your web traffic. Don't connect to networks you're not familiar with or can't verify their authenticity.

¹ The Customer Protection Guarantee applies to employer-sponsored retirement plans record kept by Principal® including defined benefit, defined contribution, employee stock ownership plans, retirement accounts with pension payments made through Principal® Custody Solutions, and nonqualified deferred compensation plans with distributions made through Principal. It's effective for unauthorized activity that occurs after participants have registered their account online, provided their contact information, and kept it up to date in the event of changes. Guarantee details are current and are subject to change. Exclusions to the policy may apply. <https://www.principal.com/customer-protection-guarantee>.

The subject matter in this communication is educational only and provided with the understanding that Principal® is not rendering legal, account, investment or tax advice. You should consult with appropriate counsel, financial professionals, and other advisors on all matters pertaining to legal, tax, investment or accounting obligations and requirements.

Insurance products and plan administrative services provided through Principal Life Insurance Company®, a member of the Principal Financial Group®, Des Moines, Iowa 50392.

Principal®, Principal Financial Group®, and Principal and the logomark design are registered trademarks of Principal Financial Services, Inc., a Principal Financial Group company, in the United States and are trademarks and service marks of Principal Financial Services, Inc., in various countries around the world.