Cybersecurity & Protecting Yourself

From Fraud and Online Threats

STRATEGIC RETIREMENT PARTNERS

Staying connected online makes life easier, but it also creates new opportunities for scammers. With rapid advances in artificial intelligence (AI), it's getting harder to tell what's real and what's fake, even for savvy users. Retirement accounts hold significant savings and sensitive personal information and have become a favorite target for fraudsters. The good news: a few smart habits can go a long way toward protecting your future.

Protecting Your Retirement Accounts

Retirement accounts often hold many years of savings, and have become prime targets for fraudsters. These accounts contain highly sensitive personal information, such as Social Security numbers, birthdates, salary details and beneficiary data, increasing their appeal to criminals. Retirement accounts are also not commonly checked regularly, and fraudulent activity can go unnoticed, and older generations are frequently targeted. It's important to know how to protect your account and to help parents or grandparents stay aware of threats. If you have accounts with multiple providers, be mindful that risks can come from several directions.

Common Threats to Watch For

Phishing emails or texts	Messages may look legitimate but attempt to steal your login information or personal data
Social engineering scams	Fraudsters impersonate trusted institutions, like your employer, your plan recordkeeper or the Internal Revenue Service (IRS)
Account takeover attempts	Attempts to reset your password or access your retirement account
Malware and ransomware	Harmful software that locks or steals information from your device
Scams targetting seniors and older participants	Targeting older generations who may not be able to identify advanced scams

Know Your Providers

Retirement plans involve several different service providers working behind the scenes. It's helpful to know who these providers are, such as the plan's recordkeeper (where your account is held), the payroll provider (who issues your pay stubs), and the plan's advisor (who supports education).

Understanding who the legitimate providers are makes it easier to spot suspicious contacts from anyone who shouldn't have access to your information. If you're not familiar with who your plan's service providers are, reach out to your Human Resources (HR) department.

Did You Know?

The Department of Labor (DOL) is also mindful of scams against retirement accounts and, originally issued guidance to help protect retirement assets in 2021.[i] This guidance was later updated in 2024.[ii] The DOL guidance includes online security tips for retirement plan participants.

Strengthen Login Security

- Use strong passwords. We are all guilty of using the same basic password we chose ages ago. Unfortunately, this can make it easier for thieves to access your accounts. Challenge yourself to choose a new, unique password on all financial accounts!
- Turn on multi-factor authentication (MFA) whenever available.
- Never share login credentials with anyone.

Update Your Contact Info

Keep your phone number, email and mailing address current so you receive important alerts.

Enable Account Alerts

Turn on notifications for withdrawals, logins or profile changes.

Safe Online and Device Practices

- Keep your software and apps updated to protect against security vulnerabilities.
- Use secure Wi-Fi networks and avoid logging in to financial accounts on public Wi-Fi.
- Install reputable antivirus or security software on your device.
- Log out of your accounts when finished, especially on shared computers.

Suspicious Activity

Pay attention to suspicious activity. If something appears off, pause and review carefully.

Be Mindful Of:

- Unexpected emails asking you to "verify your account"
- Messages with spelling errors, urgent warnings or unfamiliar links
- Texts claiming your account is locked, or benefits are at risk
- Unfamiliar transactions or profile changes in your account

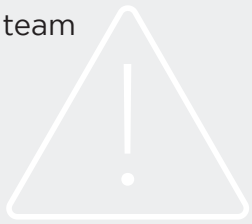
The retirement plan recordkeeper and service providers likely take certain precautions to protect data and accounts; however, ensure that you use good judgment as an additional layer of security.

What to Do if You Think You've Been Targeted or Your Account is Compromised

01 Contact your retirement plan recordkeeper's fraud or customer service team

02 Notify your employer's HR or benefits team

03 Review account activity for unauthorized transactions



Action Items for Participants

Consider the following action items to keep your financial accounts safe:

- Pause before you click. Cyber criminals may impersonate your retirement plan's recordkeeper or benefits office. Make sure any communications received via email or text are legitimate before opening.
- Protect your login credentials. These should not be provided to anyone, even your financial advisor. If you plan to provide access to your financial accounts to an advisor or trusted third party, it is best to have them set up with their own credentials.
- Check your retirement account regularly. Tip! Set up a reminder to check your account monthly or quarterly.
- Review the full guidance from the DOL and consider how it applies to your retirement accounts.[iii]
- Ask your employer if they offer cybersecurity or fraud prevention training and review it regularly to stay current on new scams.

Taking simple steps can help protect yourself and your retirement savings!

---

[i] U.S. Department of Labor, Employee Benefits Security Administration, *Online Security Tips*, April 2021, https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/online-security-tips.pdf.

[ii] U.S. Department of Labor. Employee Benefits Security Administration. "Compliance Assistance Release No. 2024-01: Cybersecurity Guidance Update." September 6, 2024.
https://www.dol.gov/agencies/ebsa/employers-and-advisers/plan-administration-and-compliance/compliance-assistance-releases/2024-01. [iii] U.S. Department of Labor, Employee Benefits Security Administration, *Online Security Tips* (Washington, DC: U.S. Department of Labor, April 2021), https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/online-security-tips.pdf.