DOL Issues Participant Tips for Protecting Retirement Savings Online

July 5, 2023

RELATED PRACTICES Retirement Plans, Employee Benefits and Executive Compensation

The DOL recently issued eight tips about how participants can protect their online retirement savings accounts. As we previously reported here, plan cybersecurity practices have been a focus of the DOL. The DOL included the following tips, which retirement plan sponsors should make their participants aware of:

1. Register, set up, and regularly monitor online retirement accounts.
2. Use a strong and unique account password and update passwords regularly (*e.g.*, every 120 days).
3. Use multi-factor authentication (*i.e.*, two-step verification), which is an effective way to prevent an unauthorized person from accessing an account.
4. Keep contact information up to date, provide multiple communication options, and close unused accounts.
5. When checking an online retirement account, do not use a public Wi-Fi network, which can be accessed by criminals.
6. Avoid phishing scams that target passwords, account numbers, and sensitive information and may be part of an unexpected text message or email and may include spelling errors or poor grammar.
7. Install antivirus software and keep applications and software up to date.
8. If a participant is a victim of a cybersecurity attack, they should contact the FBI or the Department of Homeland Security to file a report.

As part of this guidance, the DOL also notes that plan fiduciaries have a responsibility to take steps to protect the retirement plan against cybersecurity risks, including ensuring that plan recordkeepers and service providers appropriately safeguard participant information. The DOL participant tips are available here.

© 2026 Haynes and Boone, LLP