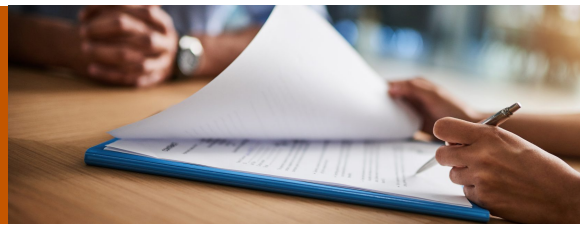
Cybersecurity Risks for Retirement Plans

SEPTEMBER 8, 2026 | BY: THE EMPLOYEE BENEFIT PLAN TEAM



When most people think about cybersecurity, they think about email accounts, customer databases, or credit cards.

A 401(k) plan may not be the first thing that comes to mind.

But retirement plans contain valuable assets and sensitive participant information—and that makes them an attractive target for fraudsters.

Consider everything connected to a typical plan:

- Employee names and Social Security numbers
- Bank account information
- Payroll data
- Participant account balances
- Distribution requests
- Plan and trust accounts
- Access to third-party systems

A compromised account or fraudulent transaction can become a serious problem very quickly.

What can plan sponsors do? Start with the basics.

- **Limit access**. People should have access to the information and systems they need—and no more.
- **Use strong authentication**. Multi-factor authentication can provide an important additional layer of protection.
- **Verify unusual requests.** A request to change banking information or initiate a large distribution deserves additional scrutiny, as well as controls around proper reviews and approvals.
- **Review who has access.** Employees change jobs and responsibilities. Access should change with them.
- **Document your controls.** Having a procedure is helpful. Being able to demonstrate that the procedure is actually followed is even better.

When we think about controls around a retirement plan, we're not just thinking about whether numbers reconcile. We're also thinking about whether the processes surrounding those numbers help protect plan assets and participant information.

We're always happy to discuss the control considerations we see during 401(k) audits.

RELATED SERVICES

Employee Benefit Plan Audits