December 2019

Cybersecurity - What Plan Participants Can Do to Protect Their Accounts and How Plan Sponsors Can Help

Karen R. Paulson, CIMA®, PRP
Managing Partner & Senior Consultant

Retirement plan providers invest significant resources to protect participant accounts from cyber theft. Yet, security vulnerabilities can still be exploited if participants are not proactively engaged in protecting their own accounts.

Recently, a plan participant I know learned this firsthand when he became a victim of attempted cyber fraud. The participant, who did not register his account online with his plan's record keeper, was over age 59 ½ and was eligible for in-service distributions. A fraudster posing as this individual managed to successfully set up an account and request a distribution by wire. Luckily the wire was rejected, but the record keeper ended up mailing a check. Fortunately, the check was mailed to the participant's correct home address, which averted the ultimate theft. But the lesson from this story is clear. Plan participants need to take an active role in better protecting their retirement plan accounts.

While it may not occur to plan sponsors that encouraging cybersecurity best practices should be among their duties, the realities of account hacking and theft warrant an "all hands on deck" approach to mitigate cyber risks as much as possible. In partnership with their plan providers, plan sponsors are in a great position to proactively raise awareness and provide periodic reminders to employees about the importance of being vigilant over their own accounts.

Below are some things plan sponsors can do to help plan participants understand the importance of and, more importantly, take action to bolster their account security:

1. Remind participants to register their accounts online. Oftentimes people have the misguided notion that they are safer if they don't register their accounts online. But this is not necessarily true. As the participant in this story learned, a fraudster may be able to get access to an unregistered account and enter original information that could then be used to perpetrate a fraud.

2. Encourage participants to implement two-factor authentication. Two-factor authentication provides an additional layer of security beyond a password and generally includes entering a one-time passcode that is sent to another device belonging to the account owner. Other types of multi-factor authentication may include additional identity verification for financial transactions, verifying one's identity on an unrecognized device, or answering additional security questions. While these extra steps may seem inconvenient, an extra layer of security protecting your participants' financial assets is well worth a bit of extra effort.

3. Partner with the plan provider to develop a strategy for periodically communicating cyber protocols to participants. Most plan providers have created participant communication flyers that describe their specific cyber protocols, account verification procedures, and methods they offer to help participants protect their accounts. While most providers have added traditional two-factor authentication, some are now beginning to implement voice biometrics as well. As cybersecurity technology continues to evolve, it is important to keep participants informed on current account protection practices.

4. Encourage participants to read the plan provider's Customer Protection Guarantee (if there is one) and understand the specific steps they must take to be eligible for the Guarantee. Many plan providers are now offering cybersecurity guarantees, which generally state that the provider will fully restore a participant's account as long as the participant has registered the account, has not shared the log-in credentials with anyone, and has notified the provider immediately if they suspect fraud. However, each provider's guarantee program is unique, and some are more restrictive than others. If your plan provider offers this type of guarantee, it should be available on the retirement plan website. Most participants will probably not know to look for it, so bringing it to their attention can help.

Data security for retirement plans has been a top priority for plan providers, but plan participants need to do their part to keep their assets safe and secure. Plan sponsors can help support this effort by engaging with plan providers to educate participants and encourage them to take an active role in protecting what may be their largest financial asset.

FIDUCIARY INVESTMENT ADVISORS

Fiduciary Investment Advisors, LLC ("FIA")

FIA is an independent institutional consulting group with over 20 years of investment consulting experience. FIA is an employee owned firm with 100% of the firm's revenue derived from fees clients pay for investment advice. Our mission is to provide customized investment consulting services to assist our clients in achieving their investment and financial objectives, while fulfilling their fiduciary obligations. Our clients include corporate retirement plans, endowments & foundations, public plans and private clients. Our consulting services include:

- Investment Policy Statement Review/Creation
- Retirement Service Provider Search (RFI/RFP)
- Plan Benchmarking
- Investment Menu Analysis and Design
- Total Plan Fee Analysis (full fee disclosure)
- Fiduciary Governance Consulting
- Investment Fund Performance Measurement, Analysis and Reporting
- Risk-Based Model Portfolio Construction
- Employee Communication and Education
- Asset Allocation Analysis
- Investment Manager Searches
- Liability Driven Investment ("LDI") Strategies for Pension Plans
- Quarterly In-Person Meetings with Finance/Investment Committees
- Strategic Guidance on Relevant Topics of Interest

For More Information Please Contact:

Karen R. Paulson, CIMA®, PRP
Managing Partner & Senior Consultant
Fiduciary Investment Advisors, LLC
100 Northfield Drive
Windsor, CT 06095
Direct: (860) 697-7413
Email: kpaulson@fiallc.com