CLIENT SERVICE | September 27, 2024

6 Steps to Help Participants Safeguard DC Assets

McKinsey cybersecurity experts give tactics to protect against scammers.

Reported by ALEX ORTOLANI

In the second quarter of this year, there were 877,536 phishing attacks, according to a report by the Anti-Phishing Working Group, a not-for-profit coalition of cybercrime experts.

According to APWG, phishing via phone calls and text messages is being used with "increasing frequency" to attack bank customers and payment service users. Meanwhile, Cofense Inc., an email security firm, notes that hackers often use times such as open enrollment and 401(k) updates to hack into participants' accounts.

Plan advisers are, ideally, working with their plan sponsors on a consistent basis to stay up to date on their cybersecurity practices. The Department of Labor recently updated its cybersecurity guidance, reinforcing that guidance applies to all covered employee retirement benefit plans and health and welfare plans.

But what can plan fiduciaries do to help protect their employees from email, text and social media scams?

Justin Greis and Charlie Lewis, partners in consultancy McKinsey & Co., say via email that "no single control is a silver bullet to protect savers from becoming victims." But they do provide six steps that fiduciaries can share with participants to help protect them from harm:

- *Identify* — A participant should know where their accounts are, how they are set up and who is accessing them. Keeping an inventory of accounts, statements, balances, brokers and advisers is the first step. A person can only protect what is on the radar.

- *Protect* — Where possible, participants should use modern authentication tools like passkeys and biometric-based (e.g., facial recognition or fingerprint) authentication. If they must use passwords, they should be unique, complex and changed periodically. They should always use multi-factor authentication and be alert for phishing and smishing attacks—false emails and text messages—as they are the leading and most successful ways criminals get access to savings accounts.

- *Detect* – If a hack is suspected, a participant should freeze their credit and monitor for changes to a credit file. If they do not have a credit monitoring service, they should be encouraged to get one to alert them when fraudsters are attempting to open accounts or access a credit file without authorization. If the platform has alerts built in, they should be sure to have them activated for things such as logins, password changes, balance changes, transfers, transactions, etc. If they have a broker or wealth manager relationship, they should establish clear and secure protocols for how transactions are executed related to their accounts.

- *Respond* – If an alert or change is detected, participants should act quickly. They can review identity theft policies that are often included as part of credit monitoring or even homeowners/renters' insurance policies. They may have more resources at their disposal than they initially realize.

- *Recover* – Savers should keep copies of accounts and balances and know who to call if there is an attack. Time is of the essence, and they can often recover funds if they move quickly and enact a plan fast. Every account, broker, bank and financial institution

has a different process, so knowing who to call and how to engage the process on the right timeframe is critical.

- *Govern* – Participants should periodically review their accounts and do digital health check-ups to ensure passwords are secure and they are taking advantage of the latest security features. New security functionality is often rolled out but may be turned off by default, so it is best to stay up-to-date and take advantage of new features as they are released.

Meanwhile, plan advisers and sponsors should stay up to date on the latest trends and development in digital threats, the consultants note.

"Companies should not treat cybersecurity requirements as an 'add-on'—or worse yet, an afterthought—but rather a critical set of ingredients that must be baked-in from the very beginning to ensure their products, services and platforms are secure from the outset," they wrote.

Tags cybersecurity, Department of Labor (DOL),