SCHNEIDER DOWNS
Wealth Management

Cybersecurity Must Be a Priority for Plan Fiduciaries

Most 401(k) plans have access to a large pool of funds, making them an attractive target for cybertheft. And while stolen funds are devastating, unauthorized transactions aren't the only goal of cybercriminals. 401(k) accounts contain a plethora of sensitive personal information that can entice hackers interested in perpetrating identity theft and other forms of fraud. Because of these risks, it's important for fiduciaries to understand cybersecurity and to follow established safety protocols aimed at keeping their plans secure.

Growing Risks for Plans

According to a 2022 survey by Callan, cybersecurity is a top concern for plan sponsors, and nearly a third of sponsors polled stated that they intended to review and audit their plans' security practices. Their concerns aren't unfounded. While the exact number of cyberattacks on 401(k) plans is unknown, successful breaches can be highly damaging. For example, one lawsuit alleged that more than $245,000 was stolen from a retirement account over a two-month period.

Multiple Avenues of Attack

Most people know not to share passwords or use public computers to check sensitive information. But even if participants and fiduciaries follow these basic protocols, they might still be at risk. One of the most common forms of cyberattack is phishing, where a cybercriminal sends a fake message that resembles official correspondence and baits the recipient to enter their personal information. But in addition to phishing, hackers could target the plan's hosting servers directly to gain access.

Some of the concerns about cybersecurity are around the plan assets themselves. As more plans begin to offer cryptocurrency options, some experts worry that this could make 401(k) accounts even more vulnerable – in fact, a 2021 study showed that cyberattacks on cryptocurrency were among the top three types of crime reported to the FBI.

DOL Guidance

The Department of Labor (DOL) has issued guidance for plan fiduciaries that outlines their responsibility to ensure their plans are safe and provides best practices for cybersecurity. The DOL clarifies that ensuring cybersecurity is part of a fiduciary's duty to protect plan participants, and many of the techniques that they recommend involve regular security checks and procedural clarity. The department states that plans should have a clearly outlined security procedure and access protocols to ensure that no one can access plans except participants and fiduciaries. They also recommend strong and up-to-date data encryption, regular security training and audits and strict vetting for service providers.

By adopting the DOL's recommended practices, fiduciaries can provide an extra level of safety and security for plan participants. Sponsors should have processes in place to address breach notifications, system restoration and the evaluation of service providers with cybersecurity in mind. Just as risk is inherent in markets, it will always be present in the online management and administration of retirement plans. It's therefore incumbent upon plan sponsors to adopt prudent processes to detect and deter breaches as well as mitigate damage resulting from cyberattacks.

Continued on back

Sources:

https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices.pdf

https://www.plansponsor.com/cybersecurity-preventing-plan-leakage-top-mind-sponsors

https://www.cnbc.com/2021/03/16/labor-department-falls-short-on-401k-cyber-protections-gao-says.html

https://info.groom.com/28/837/uploads/best-practices.pdf

https://www.techtarget.com/searchsecurity/feature/Cryptocurrency-cyber-attacks-on-the-rise-as-industry-expands

---