Six Easy Steps to Keep Your Plan Assets Safe

Cyber fraud is a growing concern globally. Individuals are typically very careful to keep their bank account and email authentication information safe, but they aren't always smart with the rest of their personal information.

Participants need to be vigilant with their retirement savings accounts as well. In the past year we've seen a slew of cases of attempted fraud – some successful – against retirement savings plan participants across a multitude of recordkeepers. The good news is that virtually all recordkeepers view security as a prominent priority and diligently update their technology. However, their security can only go so far if the participant isn't being equally vigilant.

Educate your plan participants on the following tips to ensure the security of their retirement savings accounts.

1. Use all available levels of authentication. If your plan's recordkeeper comes out with a new type of authentication, your participants should implement it immediately.
2. If participants frequent a website or have an account with a company whose website and information has been compromised, they should change all of their passwords for all online accounts.
3. Remind participants to use strong passwords. Utilize letters, capitalization, numbers and symbols. Don't use recognizable words. Don't use the same password for multiple purposes. Have the password be at least 14 characters in length. Consider changing passwords frequently. Using a password manager can make this task less unwieldly.
4. Don't send authentication information to any third parties, and remind participants to limit authentication access to use on sites which are navigated to independently – not through a link or other prompt.
5. Check your participants' accounts frequently and address any irregularities, and remind participants to keep an eye out, too.
6. Ask participants to immediately contact you if they receive any "updates" that look suspicious so you can notify your recordkeeper.

Keep your participants in the know. We recommend communicating with participants on the importance of remaining vigilant when it comes to cybersecurity – it's one of the most important investments your participants can make.

For more information on keeping your plan assets safe from cyberattack, please contact your plan advisor.