
You work hard for your money and wisely choose to defer a portion of your salary for your retirement years. Your retirement plan is designed to help you grow your savings to an appropriate amount to support you in your retirement years.

As you are aware, the plan is only as effective as you make it. If you defer too little, or make unwise investment decisions there is a chance that you will not reach your goals. Similarly, if you drain your plan balance over the years, you understand you will find a shortfall in retirement. What many participants do not think about is being responsible for the security of their savings as well.

Cyber fraud has been a growing concern globally for years. Individuals are typically very careful to keep their security measures (passwords, authentication codes, etc.) private with regards to their banking and email accounts. However, in the past few years there have been breaches of major companies containing individuals' personal information. Unfortunately, much of that personal information has become accessible by bad actors on the dark web.

Participants need to be vigilant with their retirement savings accounts as well. In the past 12 months there have been a slew of cases of attempted fraud, some successful, enacted on plan participants' retirement savings. These attempts have occurred across a multitude of recordkeepers. The good news is that virtually all recordkeepers have security as a prominent priority and are constantly updating their security technology and protocols. But, their security can only go so far if participants are not being equally vigilant.

The following are a few prudent tips for you to ensure the security of your retirement savings accounts:

- Use multiple levels of security and authentication – if your plan's recordkeeper comes out with a new level/type of authentication, engage it immediately.
- If you frequent a website, or have an account with a company, whose website and information has been compromised, change all your passwords. For example, Yahoo recently had a large breach – a breach containing passwords – if you ever had a Yahoo account you should change your password.
- Make sure your password is strong – utilize letters, capitalization, numbers and symbols. Don't use recognizable words or the same password for multiple purposes and create a password at least 14 characters in length. Also, consider changing your password on a frequent basis.
- Never send your authentication to anyone requesting it, only use on sites which you navigated to independently of any outside request.

- Check your retirement account on a regular basis for any irregularities.
- Immediately contact your plan administrator and/or the recordkeeper if you receive any update that sparks your concern – do not wait, the money could leave the U.S. quickly.

As your employer we are always looking out for your wellbeing. We trust that the plan is in good hands with our recordkeeping provider. We have reviewed their cyber security protocols and technology, but still want to provide a gentle reminder that your involvement is crucial in maintaining the security of your account as well.

**We want your savings experience to be as simple and easy as possible. If you have any questions please contact your human resources department.**