Understanding

USI CONSULTING GROUP

Safeguarding your 401(k) account

People who worry about an attack on their personal information and bank and credit card information should also consider how to keep their retirement accounts safe from hackers.

When people hear about hackers getting access to card numbers and other personal information, they probably worry about identity theft as well as their bank and credit card accounts. Another thing they should think about is their retirement account.

While there hasn't been a large-scale attack on 401(k) plans yet, some retirement plan providers have begun to discover breaches in plan participants' accounts. Even a limited breach is a big deal when what's at risk is someone's life savings and future financial security.

How can you protect your account?

If you are a participant in a 401(k) plan, there are steps you can take to protect your savings, starting with **monitoring your account**. One reason 401(k) plans are becoming a target for hackers is that many participants don't check their accounts very often and are unaware of their balances and of any activity. Although daily checking isn't necessary, it is important to review your 401(k) account periodically. Look for any unauthorized activity, such as loans or withdrawals, and confirm that your home address, phone number, and email address are all correct and current as well.

Another way to keep your account secure is to **regularly change your password**. Make sure it is strong (using both uppercase and lowercase letters, numbers, symbols, etc.) and that it's different from the passwords you use for other accounts. Some plan providers use a multifactor authentication process, where participants get a code sent to them by email or text, to allow online account access. They may also alert participants of any online account changes by regular mail or using a verified email address.

Participants should also be careful when receiving communications regarding their accounts. Phony emails that contain links or attachments could infect your computer with malware or lead you to a fake site to gather your personal information. This is known as phishing. **Keep your antivirus, anti-malware, and firewall software up to date**, and pay close attention to details in the email that may suggest that it's a fake, such as multiple misspellings in the text or if it's sent from an unknown email address. Also, do not give out any information over the phone if you receive an unsolicited or suspicious call.

(Continued)

Inform your employer or plan provider immediately if you suspect hackers are trying to compromise your account or if you discover any unauthorized account activity. And if you are the victim of any other kind of identity theft, be sure to alert your plan provider.

> In today's digital world, combatting cyber fraud is an ongoing effort. 401(k) plan participants can do their part by proactively following security measures, routinely monitoring their plan accounts, and reporting any suspicious activity as soon as it is discovered.

If you have questions about your workplace retirement plan, please contact your Human Resources department or your retirement plan provider's customer service center.

USI CONSULTING GROUP