BUSINESS

Milwaukee Journal Sentinel
JSOnline.com

Sunday, December 23, 2018

D

Are cybercriminals targeting your 401(k)?

401(k) ADVISER
MICHAEL J. FRANCIS

Ever apply for a credit card, shop at Target or stay at a Marriott? If so, it's time to wake up to the very real possibility that, due to some recent large data breaches, your personal information is now available to anyone motivated enough to go on the dark web and buy it.

To a cybercriminal, the 401(k) industry looks like a big candy store with over $5 trillion in liquid assets and largely automated systems. Armed with your name, social security number, date of birth, address and any personal information available on social media, your 401(k) account is vulnerable. Not surprisingly, since these large-scale data breaches have occurred, industry insiders report a sharp increase in the number of attempts to steal 401(k) assets.

Sophisticated criminals, with little fear of being caught, use stolen personal data to gain access to your account. Once successful, they change your contact information on file, then pose as you to your plan's help desk asking to withdraw or borrow money for some imaginary emergency. They request the money be wired to a domestic bank account and then quickly move the money offshore, never to be seen again.

Here are some steps you should take now to protect your 401(k) assets:

Check your account regularly. Make sure your 401(k) service provider can connect with you. You're looking for any unauthorized activity. This includes any changes to your contact information. All current 401(k) record-keeping platforms attempt to notify the account holder when changes are made to their contact information. This is why you want to make sure they have either a phone number or email address to contact you when any changes are made to your account.

If you get a notice of a change you didn't initiate or see any activity in your account that looks suspicious, contact your human resources department immediately. Also make sure your 401(k) provider is set up as an approved email source, so any email it sends you doesn't get caught in your spam folder.

Use a unique and strong password. Your 401(k) account is likely one of your largest liquid assets, it deserves its own password. Consider changing your password every year.

Beware of phishing scams that ask you to click on a link embedded in an email or open an attachment from someone unknown to you. This is one of the most common tricks cyberthieves use to get you to hand over sensitive personal information or download malware onto your computer that can transmit all your key strokes. Install ant-virus, anti-malware and firewall software on your computer to prevent thieves from hacking your personal computer.

Avoid using public computers and public Wi-Fi networks when logging into your retirement account. You never know who could be tracking your activity. When you've finished looking at your account, immediately log out of your account and close the browser.

Never share your login username or password with anyone, including your financial adviser. As soon as you do, you will likely forfeit any protections offered by your plan's online service provider as you will be deemed to have authorized outside access to your account.

Inquire with your 401(k) service provider or human resources department about the availability of advanced security measures. Dual factor authentication is now standard on most 401(k) platforms, with additional security available from certain service providers such as account lock features and biometric/voice recognition software. The best safety measure may be for employers to "de-automate" the distribution process.

Protections have caveats

Understand there is no federal insurance standing behind your 401(k) account. Generally speaking, 401(k) record keepers, whose systems you rely on to protect your assets, will cover 100 percent of any losses due to unauthorized access. But caveats abound regarding what conditions you must satisfy to demonstrate the theft was not the result of your or your employer's carelessness or inattentiveness.

Some of the 401(k) service agreements we have reviewed make statements like, "We will reimburse you for 100 percent of the assets taken." Then in the fine print state, "Our obligation to reimburse applies only in the event such unauthorized activity is due to our failure to implement our contractually agreed upon security protocols." If you have not taken any of the precautions described above, there is a very real possibility the service provider will not make you whole.

For this reason, it's a good idea to ask your employer about the existence of any insurance that would make you whole in case of a successful breach of your account. While these steps may seem like a lot, it's well worth it to protect the retirement savings you've worked so hard to accumulate.
