Cybercrooks are targeting retirement accounts, and there's no guarantee you'll get your money back

Paul Gores, Milwaukee Journal Sentinel 5 days ago

Beth Bennett didn't check on the balance in her employer-sponsored retirement account very often. "Maybe every couple of months I'd go online and take a look at it," said Bennett, of Madison, Wisconsin. When she logged in to view her account in November, she expected to see a balance of more than $80,000. Instead, she saw a balance of only about $8,000. "I was very shocked by that. I thought there must be some mistake here," she said.

She soon found out it was no mistake. "Indeed, my money had been systematically withdrawn over the past couple of months," Bennett said she learned after contacting her employer's retirement plan adviser and the mutual fund company that held the money. Someone had stolen her identity and was able to pose as her, changing Bennett's mailing address, redeeming big chunks of her mutual funds and having checks mailed to new locations – first to the Minneapolis-St. Paul area and then New York City. A bank cashed the first two checks, but when Bennett discovered the heist, payment was stopped on a third check.

But another shock was still in store for Bennett. When she contacted a representative at the mutual fund company, no immediate guarantee was made that she'd ever see that money again. "When I tell people they're like, 'What?' And then the next thing is, 'Well, surely they have to make sure you get your money back.' And then when I say, 'Well no, no one will tell me I'm going to get my money back,' that's when it gets scary. And that's when you get people's attention," Bennett said.

Unlike with stolen credit cards, a saver's losses to fraud in retirement investment accounts aren't limited by federal law, although mutual fund companies typically say they'll reimburse funds lost to fraudulent activity. It's an issue to be aware of as cyberattacks on retirement funds rise. "Hackers are finding it's getting harder to hack bank accounts, so they're saying where else is there more money? Where can we go? And they've started to discover 401(k) accounts, they've started to discover retirement funds," said Ed Mierzwinski, senior director of the federal consumer program for the U.S. Public Research Interest Group.

At a 2019 forum for institutions involved in retirement planning, industry expert Larry Goldbrum, of Reliance Trust, told attendees that while overall cyberfraud and account fraud was down – cyberfraud amounted to $14.7 billion in 2018 – fraud in retirement accounts was rising, according to a report by the National Association of Plan Advisors.

Cybercriminals today are "looking for any possible route into people's financial transactions, and they are increasingly focusing their efforts outside financial institutions' firewalls," said Steven Silberstein, chief executive officer of Financial Services Information Sharing and Analysis Center, an industry consortium dedicated to reducing cyber-risk in the global financial system.

"In other words, directly at the public," Silberstein said. "E-mail compromises, spear phishing and social profiling are some of the key tactics being used to target all types of assets, including retirement accounts." In spear phishing, cyberbandits send emails, purportedly from a known or trusted sender, in the hope of persuading potential victims to reveal confidential financial information.

The good news in Bennett's case is that American Funds, the mutual fund company that holds her retirement savings, has agreed to restore the money she lost, even though at first Bennett said representatives gave her no assurance of reimbursement. Still, what happened to Bennett serves as a cautionary tale that people with 401(k) accounts and other types of retirement savings accounts need to be on guard.

"The scenarios continue to evolve, so while our nearly 7,000 member financial institutions are constantly developing their cyberdefenses, it's also critical for consumers to practice good cyberhygiene and be on the lookout for suspicious activity," said Silberstein, of the Financial Services Information Sharing and Analysis Center. When crooks gain entry to consumer bank and retirement accounts, the point of entry more often than not is the victim's email account, said Kevin Bong, director of cybersecurity for the accounting and consulting firm Sikich. Oftentimes, people's account passwords, obtained in data breaches and then sold on the "dark web" to cybercriminals, are used to break into an email account and take it over without the victim knowing it.

“We’re definitely seeing that by getting just that one account – usually your email account – they use that to figure out, ‘Here’s my bank, here’s where my retirement accounts are,’” Bong said. “You’ve probably got a different password on your retirement account than you do on your email address, but what do you do if you forget that password? Well, you click ‘Forgot Password’ and they email a link to reset your password. So with access to your email address, they really have access to all those other things in a lot of cases.”

Bennett doesn’t know how a crook got into her American Funds account and started draining it. American Funds said its system wasn’t hacked and that it sends out notices via postal mail when things like changes of address take place online.

Bennett is executive director of the Wisconsin Newspaper Association. Her retirement savings tool is what’s known a Simple Plan, a tax-deferred, employer-sponsored account with some similarities to 401(k) and 403(b) plans that is tailored for smaller employers.

Asked about Bennett’s case, American Fund issued a statement: “Our mission is to help people save for a secure retirement. When one of our customers is the victim of identity theft, we hold ourselves accountable to immediately conduct a thorough examination of what happened and take appropriate action. We use instances like this to strengthen our practices and conduct additional staff training if needed. We have communicated to the customer that her savings, including any accrued dividends or appreciation, will be reinstated. We will work with law enforcement to aid in their investigation.”

Mierzwinski, of the U.S. Public Research Interest Group, said people can’t assume whomever holds their retirement money will reimburse them after a hack, but he said the biggest companies typically do.

Charles Schwab, for example, states online it will “cover 100% of any losses in any of your Schwab accounts due to unauthorized activity.” Fidelity also says it will reimburse customers for any financial losses resulting from unauthorized activity on Fidelity accounts. American Funds states on its website: ”We review each report of unauthorized access thoroughly, file appropriate notices with law enforcement agencies, and, in the event of a financial loss, we assess the facts and circumstances for potential reimbursement to your account.”

Companies do need to investigate the hacks for fraud and make sure law enforcement is notified a crime has taken place, experts said.

How to protect yourself

Cybersecurity experts say if retirement savers have access to their accounts online, one of the best things they can do is make it very hard for hackers to take over their accounts. Here are some tips they recommend:

- Make sure any computer or device used to access accounts is protected by a firewall and has current antivirus and antispyware software.
- Be wary of responding to, opening attachments in or clicking on links in emails that ask for your financial information.
- Open and read any letters or paper statements from your mutual fund or money manager to see if everything looks accurate, and notify them promptly if it appears unauthorized activity has taken place. Investment firms often also will send letters via postal service to let clients know if any changes have been made to details like a home address.

Sikich’s Bong said one important way of increasing security for an account is a strong password that isn’t used for any other types of online accounts. Long passwords with phrases such as “Dogcatfish22” are better and easier to remember than shorter ones, he said.

“It’s a lot longer so people can’t break it as easily,” Bong said. Mierzwinski said retirement accounts could be particularly vulnerable because account holders might neglect looking at their statements. In some cases, they’ve been told over the years just to let the money grow and not check on it too frequently. That advice isn’t prudent anymore in an age of cybercrime.

“You know it’s just a statement, but open it,” he said. Bennett said she wants people to know they need to check regularly on their retirement savings. “If it can happen to me, it can happen with everybody,” she said.