# Hack-Proof Your 401(k) Account

Americans hold over $20 trillion in 401(k)s and other retirement accounts—yet federal safeguards to protect these accounts from theft are lacking. Cyber thieves have begun targeting retirement accounts more frequently in the past few years. While there is not a lot of public data on retirement account theft, The Wall Street Journal reported on lawsuits by account holders looking for reimbursement of 401(k) accounts.

In 2019, Heide Bartnett discovered $245,000 was wrongfully distributed from her 401(k) after receiving a statement in the mail. Bartnett believes that a hacker was able to access her account online, possibly using the Forgot Password feature, where they added their address and bank account information. The scammer was then able to initiate the distribution to the bank account they owned.

Bartnett filed a lawsuit against Abbot (her former company) and Alight Solutions, the benefits administrator. She was able to recover part of the distribution through taxes withheld and from the fraudulent bank account, but she is seeking the full balance plus damages. Bartnett had to continue working longer than anticipated and has affected her thinking about retiring for good.

Currently, consumers have better protection for their savings accounts and credit cards. The Government Accountability Office (GAO) has requested that the Labor Department improve protections for 401(k) investors.

According to the GAO, cyberattacks on 401(k) providers could lead to “severe financial ramifications.” The Labor Department currently does not have minimum security requirements for plan providers. For now, your clients must take security into their own hands.

## Savvy Cybersecurity actions

There are steps you can take to help protect your retirement accounts from being hacked. Many of the Savvy Cybersecurity principles can be applied to these types of accounts for better protection.

### 1. Set up an online account

First, be sure you set up an online account with your 401(k) provider. This will allow you to access your account more easily and will also ensure that an impersonator cannot make an account in your name. Of course, when making your account, there are cybersecurity best practices you should follow to keep it secure.

**2. Use a strong and unique password**

When setting up your online account, you must create a good password. Do not use a password you have used elsewhere.

**3. Enable two-factor authentication**

In addition to having a unique password for your account, you must also enable two-factor authentication. Two-factor authentication protects your account even if a hacker has your password, they will still need the one-time security code to access your account.

If your 401(k) provider does not offer two-factor authentication, raise the security issue to them. Any sort of financial firm should be offering this level of security.

**4. Check accounts regularly**

Lastly, check your account regularly for any unusual activity. If your provider offers text or email notifications, sign up for those so you are notified any time a change is made to your account. At the very least, you should log into your account monthly to check your balance and contact information.

Source:  Horsesmouth.com