CPA
Practice Advisor



form of authentication is a password, but given the rise of tax-related identity theft and phishing schemes that accounting firms face, a password is no longer enough ...

**Jim Boomer** • Jun. 27, 2017

You've probably noticed more and more of your email and bank accounts requiring multi-factor authentication before allowing you to log into your accounts online.

When you try to log in to your email from a new computer or access your bank



form of authentication is a password, but given the rise of tax-related identity theft and phishing schemes that accounting firms face, a password is no longer enough to protect the private information of your firm and your clients.

According to the security platform Endgame, there are two major methods that attackers use to steal usernames and passwords: attacking the users directly and attacking the websites people use. Attacking users directly might involve sending scam emails to customers of a certain bank, prompting them to enter usernames and passwords into a fake login page. Attacking a website involves exploiting a vulnerability in the website itself, stealing the usernames and passwords of everyone who uses the site. These are usually the large-scale data breaches that make the news, like when the IRS's "Get Transcript" system was hacked, comprising the personal information of more than 700,000 taxpayers.

## Authentication methods

While a hack of your firm's systems may never reach the scale of the IRS data breach, you don't want to be the one that has to alert your clients that their personal information has been compromised. That's why any system that houses sensitive data should be configured to require the use of two or more different authentication methods. Strong authentication requires two or more of the following:

1. **Something you know.** Providing a password or correct answers to previously established security questions are the most common examples. This is the most common authentication method and also the least expensive in terms of initial cost. Perhaps not surprisingly, it's also the least secure of the three. In 2016, Yahoo announced that a hacker had stolen information from a minimum of 500 million accounts in late 2014. The information stolen included not only email addresses and passwords but also security questions and answers.

2. **Something you have.** This is some physical object in the possession of a user.



biometric authentication into their hardware.

Even with the use of multi-factor authentication, a thief in physical possession of your laptop or tablet will be able to defeat it, so it's important to physically secure your property and use encryption as well as authentication.

Last month, I asked whether your accounting firm is serious about security. Serious software providers and accounting firms are moving beyond passwords to require multi-factor authentication for the firm's staff and clients. When evaluating software vendors, the ones who can apply multi-factor technology are probably the better choice. It may up the nuisance factor, but it's what you need to do to make sure your clients' information is secure.

—

Jim Boomer is CEO of Boomer Consulting.

Firm Management • Security • Technology