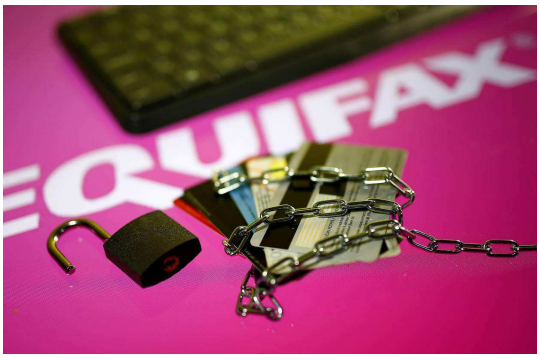
THE WALL STREET JOURNAL.

WEALTH MANAGEMENT | PRACTICE MANAGEMENT

How Advisers Are Protecting Client Data

Two-factor authentication, phishing drills and other methods are being used guard against cyberattacks



The Equifax data breach has spurred cybersecurity concerns among wealth managers. Here, an Equifax photo illustration. PHOTO: REUTERS

By Veronica Dagher

Nov. 1, 2017 12:41 p.m. ET

With the Equifax Inc. data breach stoking clients' concerns surrounding the safety of their personal information, more financial advisers are tightening their cybersecurity measures or looking to do so.

Among the steps some registered investment advisers are trying to keep client data safe: regularly using encryption, conducting cyber-security drills with staff and hiring consultants to help them check out vendors' security procedures before hiring them.

WSJ Wealth Adviser spoke with several advisers to get some ideas and tips. Here, they share some of their data-security procedures.

Ben Brown, founder
Entelechy, Bethesda, Md.

The former information-technology consultant uses long, randomly generated passwords for every online service he uses and encourages clients to do the same via a password manager such as LastPass.

Mr. Brown also enables two-factor authentication wherever available and asks clients to do so, too. The two-factor process requires that a consumer provide not only a username and password but also a piece of personal information when accessing an account. With some accounts, the business will text a piece of information, such as a number, to the consumer's cellphone, which the consumer must then input before gaining access online.

But Mr. Brown has a point of caution on two-factor authentication: He suggests clients and employees disable text-message preview on their cellphones (where they often receive authentication codes) and make sure all of their devices used for multifactor authentication have strong passcodes. This way, if a crook steals clients' passwords and

cellphones, they won't be able to log in the client's accounts on various websites without also unlocking the phone.

Kyle Moore, founder
Quarry Hill Advisors, St. Paul, Minn.

Mr. Moore uses the virtual private network Encrypt.me to ensure he has a secure connection to the internet at all times. He also doesn't store any data on his computer. He uses Dropbox Business for his online file storage and all files in Dropbox are double-encrypted using Boxcryptor, an encryption program that works with cloud services.

"Everything is in the cloud," he says.

Part of his reason for using virtual storage stems from security concerns about the physical world as he's heard stories of office break-ins where an adviser's hard drive was stolen.

Keeping files in the cloud guards against physical threats, but cloud storage itself doesn't guard against cyber threats, which is why encryption is important, he says.

Rob Siegmann, owner
Total Wealth Planning, Cincinnati

Mr. Siegmann's firm regularly trains staff to be on the lookout for cyberattacks. Whenever staffers get a suspicious email, for example, they are to report it to him or another cyber-trained expert in the office. If it turns out to be malicious, Mr. Siegmann will make a screenshot of the email and send it to the rest of the firm—lauding the employee who didn't fall for the phishing attempt.

The firm also uses a service called KnowBe4 to create spoof phishing emails to send to the firm on monthly basis. So far, employees have been diligent to not click on these spoofed emails, he says.

"I believe these monthly phish drills are preparing us for a spear-phish attempt that will come," he says.

Peter Lazaroff, chief investment officer
Plancorp LLC, St. Louis

Mr. Lazaroff's firm works with a cybersecurity consultant who does due diligence on Plancorp's vendors. For example, the consultant will check that the vendor's sites are secure facilities, with physical as well as electronic measures to protect information, such as onsite security,

If Plancorp has significant concerns about the ability of a vendor to meet these standards, the consultant will try to find a similar vendor who does.

"There are always going to be new threats, so it's essential to have internal and external resources dedicated to protecting client data," he says.

Write to Veronica Dagher at veronica.dagher@wsj.com