Cybersecurity Breaches Threaten Advisors Who Work From Home

April 1, 2020

Working from home may be convenient for advisors and others, but it also can draw out bad actors preying on cybersecurity weaknesses of home networks, said Wes Stillman, CEO of RightSize Solutions, a technology and cybersecurity firm.

“In these disastrous times, we are seeing the nation come together, but we are also seeing a huge increase in cyberattacks against those working at home,” Stillman said during a webinar hosted by RightSize Solutions on Tuesday.

The topics of security and compliance discussed during the webinar, “Cyber Security Work-from-Home Best Practices,” are not new but are especially relevant now as people are pushed out of their offices by the pandemic, he added.

Phishing attacks, in which fraudsters send fake emails to solicit private information, are the number one way schemers attack advisors and the public, Stillman said. If a client has been hacked, an advisor may receive a fake email that looks like it is from the client, but actually is from someone trying to take advantage of the current situation.

“Verify all email and website addresses,” he warned. In many cases, advisors have the same concerns as the general public and should react the same way. “Do not open strange files or give out any private information of yourself or a client.”

But advisors have more to worry about when it comes to cybersecurity than the general public.

Advisors need to use multi-factor authentication for their clients and themselves for email and for access to the advisory firms’ web portals, he said. Virtual private networks (VPN) can add a layer of security but VPNs they also can slow down the internet service, he added.

Once an advisor makes the switch to working at home, he or she needs to change the default password on the computer router, he said.

Susan Glover, president of Susan Glover & Associates, an operations and technology consulting firm, told advisors they should log onto the internet through their company’s platform, not their home internet, while working at home. “If you download client information onto your home computer, it stays there.”

Stillman added that all home devices used for work should be registered to the firm’s domain and all devices should meet compliance regulations.