onwallstreet

Updated Monday, March 31, 2014 as of 9:05 PM ET

30 DAYS 30 WAYS

DAY 30

Protecting Digital Assets: Advisors on 'Front Line'

by: Andrew Welsch

As modern life increasingly moves online, advisors, clients and their devices are at risk of being hacked, compromised or having critical information stolen. Because they handle such sensitive information, advisors are in a position to help protect clients' digital assets, experts say.

"They not only can make a difference – they are the difference. They are on the front line," says Chris Valenti, CISSP, Information Security Liaison at First Clearing, an affiliate of Wells Fargo Advisors.

FRAUD

Valenti says advisors need to be aware of when email accounts may be compromised because catching inauthentic emails can prevent serious damage to a client's account. In emails, watch out for nonsensical or generic greetings, and links that do not go to actual websites, says Valenti.

If an advisor is concerned about the validity of an email or a request for sensitive information and account transfers, Valenti suggests calling the client and politely verifying the authenticity of the request. A quick, polite phone call can prevent major headaches.

Wire fraud is a prevalent threat to clients, says Al Caiazzo, head of Risk and Quality at First Clearing. He adds that communication between advisors and clients is a key step in protecting digital assets.

"FAs need to be communicating with clients about these sorts of issues and these sorts of problems," says Caiazzo.

MOBILE DEVICES

In addition to information contained in emails, advisors must be aware of the safety of information stored on their smart phones and tablets, warns Dennis Noto, chief information officer of Trust Company of America, an independent custodian for RIAs.

Noto says advisors need to be sensitive to what kinds of information they are storing and sending from their mobile devices as they can be just as vulnerable to hacking as desktop computers. The smartphone, he says, is the most

hacked device in the world.

If independent advisors are running their own websites, then should think carefully about security risks and hacking, he says, as the security protections might be inadequate.

“These are the things that advisors don’t think about,” says Noto.

PROACTIVE APPROACH

He also recommends advisors encrypt data on their computers and devices, including data-at-rest (e.g. documents that they aren’t accessing). If having an internet firewall is the equivalent of having a lock on the front door, then encryption of data-at-rest is like having a secure safe in the basement.

“You have to break into the house, but you also have to break into the vault to get at sensitive information,” explains Noto.

First Clearing’s Valenti and Caiazzo recommend advisors be proactive about security and about educating themselves about best practices, whether via their firms or government resources.

But most importantly, advisors need to have a positive attitude towards incorporating security in their daily practice, says Valenti. Viewing it as a nuisance or burden that gets in the way of work is the wrong attitude to have, he warns.

“You have to have security embedded in the task at hand,” urges Valenti.

Read more:

- **Security Strategies for HNW Clients**
- **Estate Planning: Don't Miss Digital Assets**
- **Advisors Beware: Single Data Breach 'Can Bring Down' a Practice**
- **Do Wealthy Clients Need an Escape Route?**

Previous Days

Day 29
Do Wealthy Clients Need an Escape Route? »

Day 28
Smart Ways to Work With Tech Entrepreneurs »

Day 27
Do Your HNW Clients Need Special Insurance Coverage? »

Day 26
Estate Planning: Don't Miss Digital Assets »