The New Era of Cybercrime

Everybody's talking about cybercrime, and the hacks and thefts at giant organizations. In all likelihood, you may know someone who's been affected by hacks at major retailers for instance. Perhaps you may think you're too small a fish to be a target. But that is far from the case: According to the 2016 Internet Security Threat Report, Symantec's annual analysis of cybercrime at the close of 2015, the World experienced the largest data breach ever publicly reported. An astounding 191 million records were exposed. It may have been the largest mega breach, but it wasn't alone. In 2015, a record-setting total of nine mega-breaches were reported. (A mega-breach is defined as a breach of more than 10 million records.) The total reported number of exposed identities jumped 23 percent to 429 million.[1]

Are you thinking about cyber fraud as much as you should, or are you counting on your banking institutions, tax planner and financial advisors to protect you? The truth is they can only do so much. Everyone who has access to your finances must take precautions. And that includes you. It's enough to make you paranoid—and maybe that's a good thing.

Perils of Cyberfraud

Here's an example: Take your typical, fairly active investor—one who typically contacted their advisor by email, and frequently used funds from their accounts to close business deals with a variety of partners. But then, a fraudster expertly mimicked this client's requests for funds and managed to steal a large amount of money, all in sums that were a shade under the $250 thousand level that would bring on a full-bore federal investigation.

Now you may be thinking, "I'd never fall for such a scam." But to sit down and look at the emails, they seemed completely legitimate. They used the correct email address, with no indication that the emails (and funds) were being diverted elsewhere—not even after a forensic analysis. The language used in the emails was eerily similar to the client's typical communications. In all likelihood, the fraudster had been monitoring the client's emails for some time, and so was able to make the fraudulent communications seem "normal."

The firm releasing the funds to a third party, followed its Compliance Policies and

Procedures and did what it was supposed to do: The advisor confirmed that the transactions had been verified with the client. The advisor, who was accustomed to communicating with that same client by email, affirmed that they had. Everyone did what they were supposed to do—but still, the theft took place.

Think about a typical busy day. You're in the throes of multi-tasking, you're busy, you get an email. Most of us aren't taking the second look and asking about fraud. But today you have to, as phone calls can get diverted to a third party—and if that person has the right answers to your identity questions, you could be deceived.

What can I do?
We all have to take a wider view of cybersecurity, identity theft and fraud. Internet fraud is increasing; scams are getting more sophisticated. It's hard to imagine that, with all the cautions you think you have in place, fraud could still bite you. But it can.

Here are a few recommendations that you can start following today. No matter how large or small your accounts, these steps can help make them a little more secure.

1. **Work with your advisor** by verifying any disbursement requests directly with a phone call. He or she may already be making this change but if not, consider starting this practice today. Taking the extra step of old-fashioned communication may help prevent you from being victimized.
2. **In addition to disbursement requests**, verify new bank instructions via phone-do not rely on email.
3. **Do NOT rely on Caller ID** – it can be manipulated. Always call any of the institutions or business relationships you have back at the phone numbers you have on record.
4. **Check email addresses carefully**. Imposters will often setup similar looking email accounts to impersonate various institutions or the people you work with directly at those firms. Look carefully to make sure the email account you are corresponding with is the correct one.
5. **Ask Questions.** Everyone at the firms who hold your hard earned dollars and investments should follow that cliché of public safety, "if you see something, say something." Ask the people you work with directly what steps they are taking to ensure your information is protected.
6. **Consider engaging in a credit monitoring service.** It's not the complete answer but it helps.

7. **Don’t rely on what you think you know about technology.** Whatever you may know about information technology and security, fraudsters know more—this is their business.

Is it paranoia if everybody is really against you? That question used to be funny. In the era of cybercrime, though, a little paranoia can go a long way toward protecting your assets and your reputation.

---

[1]2016 Internet Security Threat Report, April 2016, Symantec, page 6

Please contact our firm for additional information

WEALTH DESIGN GROUP

Gary L. Pevey, CFP, CLU, ChFC
3445 American River Drive, Suite B
Sacramento, Ca. 95864
916-480-0669
gary@wealthdesigngroup.com