

Tech Scam Risk Management

By Wilhelm Dingler

Insightful lessons can be learned by reviewing professional liability issues. With this in mind, Gallagher Affinity provides this column for your review. For more information about liability issues, contact Irene Walton at irene_walton@ajg.com.

New work-from-home paradigms, the proliferation of mobile technology, and electronic documentation for everything have all created challenges for the accounting profession. A very important aspect of these challenges is keeping a sharp eye out for those who would leverage that technology for nefarious purposes.

Instances of phishing, social media scams, and other unsavory activities are proliferating. This article explores some of the challenges faced by accountants and some risk-management suggestions as to how to deal with them.

IRS Scams

Phishing, the practice of sending fraudulent communications that appear legitimate, often comes through email and text messaging. The IRS has been warning about these scams, and regularly publishes information about tax scams, identity theft, and the like.¹ The IRS also publishes an annual “Dirty Dozen” tax scams.² The IRS makes it clear in many of its resources that the IRS does not initiate contact with taxpayers via email, text message, or social media channels; the agency does not call to demand immediate payment and will always first send a written notice and bill; the IRS does not solicit debit or credit card information over the phone; and the IRS does not demand payment via wire transfer, gift card, or other such payment method.

Practice Tip: Always verify the source of any request to take action that comes via email, text message, or social media referral. There was a time when commerce was conducted via paper, and it

was a common theme then to “know your endorser.” The spirit of that warning is equally valid in the electronic age. Be sure you (or your client) are, in fact, communicating with the IRS.

Phishing, Smishing, Spear Phishing

Phishing is a dangerous and an increasingly common type of cyberattack.³ The goal is to steal money, gain access to sensitive data and login information, or to install malware on the victim’s device. Smishing is the same as phishing, but the scammer utilizes SMS/text messages.

There are instances when e-scammers hijack an accountant’s database, emails, etc., and there are occasions when they hijack a client’s email. Let’s say you receive an email from a client asking you to transfer money to someone. If you seek confirmation from the client via email and the e-scammer has compromised the client’s email, you will receive a response from the thieves, not your client.

Practice Tip: Pick up the phone and call the client to confirm the ACH transfer request. Also be sure to modify your practices and amend your engagement letter to specify the need for client requests for transfers to be in writing and verified by you via telephone, a Teams or Zoom meeting, or other appropriate method to confirm the identity of the requestor.

This will help ensure that any client’s direction is, in fact, his or her wish. It may behoove you to include a provision in your engagement letter that the client must notify you within 48 hours of any cyber-attack they encounter so you can ensure your systems have not been compromised.

Hacks and Malware

Sometimes spear phishing emails impersonate a client to gain access to your systems. Other times, scammers use embedded code in an email to launch a trojan horse so that they “become” a new client with access to your secure site. Once


access is gained, they will look for ways to compromise various credentials, including your tax prep software information as well as tax preparer identities.

Practice Tip: You may have noticed in some emails: “Caution: This email originated from outside of the firm. Do not click links or open attachments unless you recognize the sender and know the content is safe.” Heed this warning! Sometimes something as simple as a two-point identification (where two different people confirm a request and its legitimacy) will thwart such endeavors.

Social Media

Many e-scammers use social media to generate false “advice” for tax savings. Some may claim an avenue to take advantage of a special program, such as the Employee Retention Credit, and then lead viewers to consult with their “highly successful professionals.”

Practice Tip: Your clients may press you to consider such social media come-ons. Remind them that such actions might result in a negative audit, fines, and criminal charges from taxing authorities.

One may think the above recommendations are cumbersome, but are they more cumbersome than putting your insurance carrier on notice that your client suffered a significant loss related to an email scam in which you were a duped? The “cumbersome” actions of trust but verify is far preferable to having to defend one’s actions before a judge and jury. 

¹ www.irs.gov/privacy-disclosure/report-phishing

² www.irs.gov/newsroom/dirty-dozen

³ www.cisco.com/site/us/en/learn/topics/security/what-is-phishing.html

Wilhelm Dingler is a shareholder, practice group leader, and board of directors member with Bullivant Houser in Seattle. He can be reached at wilhelm.dingler@bullivant.com.