CPA
Practice Advisor

PRODUCT & SERVICE GUIDE

7 Tips to Keep Client Data Safe During this Work-from-Home Tax Season

The past year has brought with it some significant changes to the way the world does business. Kitchens, bedrooms and living rooms have become offices. Conference rooms have been replaced with online meetings. While many have settled into ...

Jan. 06, 2021

The past year has brought with it some significant changes to the way the world does business. Kitchens, bedrooms and living rooms have become offices. Conference rooms have been replaced with online meetings. While many have settled into this work-from-home norm, others (like tax professionals and accountants) are about to embark on yet another challenge—tax season.

For most tax professionals and accountants, email remains the tool of choice for sharing information electronically with clients. It is quick, easy and everyone has it —even at home. However, using email alone puts confidential information at risk.

To keep client data safe when working from home this tax season, it is important to understand potential risks when sharing information electronically, and how to manage these risks effectively. Consider the following.

Phishing attacks are on the rise.

Phishing occurs when a perpetrator impersonates a trusted email sender in an attempt to get the recipient to click a bad link. In doing so, the user unknowingly installs malware or ransomware on their computer. While much has been written about phishing attacks disguised to appear as if they are coming from a person's bank or social media network, the pandemic has created yet another opportunity for hackers—COVID-themed phishing attacks.

When using email to share important information, remember you are volunteering that information into a system that is frighteningly easy to compromise. And while it may be tempting to run socially distanced business activities from your email inbox, think twice before sharing important information.

Recipients can't always be trusted.

The grim reality is people are often careless in how they manage their own privacy. This is especially true when they, like you, are trying to run everything from their own home office. Their internet connection might be public or shared with neighbors. Malware may also be running on their home computer and there's nothing you can do to stop or prevent it. When sending financial details to someone over email, you not only have to trust the security on your end, but on the recipient's end as well. This trust can be a gamble as home and work lives become intertwined.

The cloud is probably safer than your computer.

Generally, cloud storage services are much more secure than a laptop. This is especially true when using the same computer for work that you use at home. A clever password or seemingly unimpeachable security habits are often no match for a talented hacker attempting to steal or hold for ransom the data on your hard drive by hacking your home internet connection. The cloud is a more secure method for sharing and storing data.

Your internet connection is not as secure as you think.

Most people assume that a home Wi-Fi connection is as secure as connecting at the office. This is seldom true. Passwords are rarely strong enough and too often they are shared with family members and guests. When working from home, it's critical that access to your internet is restricted. This means using a strong password and changing that password frequently. Some routers can be configured so that they will broadcast two separate Wi-Fi networks in a house with different network names and passwords. This is a good option for keeping family activity on one network and business activity on another.

Privacy laws are different throughout the world.

Another problem with email is that messages often travel through foreign jurisdictions on their journey from the outbox to the intended inbox. This means that if your email bounces onto a server in a region where privacy isn't protected, it can (and most likely will) be read by someone other than the intended recipient.

SMS is never secure.

Most of us know that we shouldn't send important information over text message. But it can be very tempting when text messaging is the new "in-person" meeting. What many people don't consider is that when we use SMS to share a private message or document, we're putting that critical information into a position of discoverability for any hacker with the right tools. End-to-end encryption doesn't mean much if a hacker can code his way into a local cell tower and impersonate someone's device. While it can be tempting in these times to substitute text messaging for those quick in-person chats you used to have in the office, be careful what you share over SMS.

Digital signatures are easy and effective. Use them.

Believe it or not, in today's pandemic environment many accounting practices continue to invite clients into their offices to sign tax documents. There is absolutely

no reason to do this when digital signatures can be easily and securely acquired. When you bring someone into your office, even when masks are worn, all parties are at risk. Digital signatures are a safer alternative to in-person transactions.

=========

Dave Martin is vice president of Verifyle, a provider of secure messaging and file sharing solutions.

Product & Service Guide • Tax • News