5 Security Tips to Help Accountants Work from Anywhere

When you're up against a deadline, using your personal laptop, smartphone, or tablet can help you better serve your clients. Here's how to use a personal device for work without compromising security.

Your firm is well prepared for deadlines, but oftentimes your clients don't make it easy. When you're waiting for a client to send a crucial file, you're working on their schedule, not your own. For many accountants, that means you're stuck in the office, too. But why does it have to be that way?

Only 5 percent of respondents consider themselves very likely to open an email from an unknown sender when they are using a personal device. But when using a work device, that figure doubles.

The smartphone in your pocket and the laptop at your home are more than capable of handling your workload, and many accounting firms are implementing Bring Your Own Device (BYOD) programs that allow their employees to do exactly that. The biggest concern against using those tools, of course, is security. Is it possible to keep your clients' data secure on a personal device? New research suggests so: a recent survey found that employees are actually more cautious when using a personal device for work purposes.

Meanwhile, 14 percent of those polled said they would be very likely to open unrecognized file extensions included in an email on a personal device. Again, things change when that device isn't their own: 27 percent are very likely to click on a random file when using a work system. Since unsecured emails and attachments are among the most prevalent data security threats, this is no small concern.

Data security is a much bigger task than simply avoiding malicious emails and files, however. Here are five best practices to help you secure your personal device at work and minimize risk for yourself and your firm.

Store data in the cloud

One of the biggest security hazards for BYOD is employees storing secure work data on their personal devices, which aren't subject to the same safeguards as your work computers. In fact, fifteen percent of employees store data on personal devices. If your personal device is lost or stolen, the risk is doubled: not only do you risk your sensitive data falling into the wrong hands, your company loses all of your hard work as well.

Be careful in public

Working from an airport lounge or cozy cafe may sound nice, but you must be aware of the data you are accessing and who is around you — other people might also want access to that information.

83 percent of respondents to one study said they have used a computing device in a public place while having confidential data on the screen.

Remain aware of your surroundings when you use a personal device for work when out of the office, and if you're accessing sensitive client information, try to find a corner to work in where your screen can't be seen.

Don't ignore update notifications

In a CIO magazine report, industry expert Fred Mouawad explained that many

businesses are beginning to trust third-party services when it comes to security, and the focus has shifted on managing internal users. One major example of this is making sure employees update their personal devices.

Many routine software updates are used to improve security, even among your seemingly inconsequential apps. You don't need IT oversight to find success here. Just pay attention to those "An app needs your permission to update" notifications, or turn auto updates on, and you'll be able to keep up.

Use secure networks — or encrypt everything

Many organizations that are embracing BYOD are also realizing the need to use a secure connection with personal devices. For your firm, this means practicing strategies like connecting to corporate Wi-Fi instead of a mobile network whenever you can.

If you can't use a secure network and somebody needs you to respond something when you're logged into a public network, make sure data is being encrypted in transit. Some email add-ons and professional file-sharing solutions will even handle this for you.

Don't change passwords too often

Conventional wisdom is to change passwords frequently to stay ahead of threats. The problem is that changing too often tends to lead to weaker passwords because — let's face it — it's a challenge to remember and rotate between several complex passwords. In fact, a recent report from the Federal Trade Commission said that people who change passwords frequently usually do so in predictable ways, and would be better served using stronger passwords and changing them less frequently. One password change every six months is often sufficient.

Learn more

Using personal devices for work can help you hit your deadlines while saving time and adding flexibility to your life, but only when data is secure. Following these five tips can help you get the most out of your devices while minimizing worry.

CITRIX®

ShareFile
North America | 1 800 441 3453
Worldwide | +1 919 745 6111
United Kingdom | +44 800 680 0621
Australia | +1 800 089 572

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States