could be making your company vulnerable to hacks and other cyberattacks.

Matt Peterson • Jan. 07, 2016

They're just old habits. You likely do them without even thinking. But these 10 habits could be making your company vulnerable to hacks and other cyberattacks. Are you committing one or more of these 10 risky behaviors?

1. Sharing Passwords

It may not seem like a big deal to share your password with a coworker that you're

a password app to keep all your passwords safe, and use a different one for every one of your accounts.

3. Using Unsecure Internet Connections

Getting work done at the airport or while you're sitting at your local Starbucks may seem like a good idea at first, but if you have confidential information on your device, it is a serious data security risk. Public internet connections make your information accessible to anyone who has the know-how to access it. Only use secure internet connections to get work done, and save public connections for personal browsing purposes.

4. Not Purging Files

Some documents that contain sensitive information eventually become obsolete or outdated. When this occurs, it's important that you purge the files from your system. The longer these documents are on your computer, the more likely it becomes that they'll be compromised. If you need regular reminders to purge old documents, you can set file retention policies through eFileCabinet.

5. Using Unencrypted USB Drives

It's quick and easy to grab a USB drive and save some files to it before you leave the office. But it's important that you ensure the drive you're using is encrypted. If you were to lose an unencrypted drive, anyone who found it could access the information you stored.

6. Not Reporting Lost Equipment

We're only human, and sometimes we lose things. But when you lose a work-related device—whether it's a laptop or a USB drive—you may be tempted to keep it quiet to

avoid any repercussions. (Or you may just think it's not that big of a deal.) It's

laptop and run, or to copy some information off of your screen. Always keep your laptop within easy reach when in a public area.

8. Not Using Privacy Screens

Whether you're at work or working remotely, it's important that you use privacy screens when working on confidential documents. Any time you step away from your computer, lock it with a privacy screen so that passersby can't see the information you are working on. Failing to do so is an easy way to compromise clients' personal data.

9. Using Personal Mobile Devices

It's common practice these days to connect your mobile device to the wireless network at work. But if that connection can access private information, it should only be accessed with secure devices. Your smartphone does not have the security necessary to protect your company's data and maintain compliance.

10. Carrying Unnecessary Info When Traveling

When you're traveling for business, it's essential that you have access to the files and information that you need. However, you should never have more files than are absolutely necessary for your trip. If your laptop becomes lost or is compromised in some other way, every file on the computer is now at risk; the fewer files stored on the computer, the better. Your best option is to use a secure, encrypted, cloud-based document management software like eFileCabinet. This will give you full access to all the documents you need without having to store them directly on your computer.

———————

Matt Peterson is the CEO of Lehi, Utah based eFileCabinet, Inc. Founded in 2001,

Security • Small Business