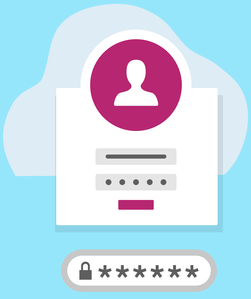
4 Steps to Better Cybersecurity

Whether you are back in the office or still taking video calls from home in your coziest pair of sweatpants, data security is something that you can never be casual about. No matter your location, there is always a chance of your clients' information falling into the wrong hands. There are technological tools to help protect you from a data breach, but they need to be paired with an ever-vigilant eye on risk mitigation. Are the following systems and habits in your toolkit?



Secure Portals

Email is our primary method of communication, but it's not always the most secure. Even with two-factor authentication, strong passwords updated frequently, and an army of trained attack poodles guarding your devices, you may be your own worst potential security risk. It's too easy to accidentally reply to or forward an email to the wrong contact. And if that email contains private client details, you are potentially liable for any harm that may arise. One solution is to use a secure web portal when transferring sensitive information. Sure, it may not save as much time as shooting emails back and forth, but sending and receiving information through a secure, restricted access website could certainly save you some trouble.

Redaction

Redaction isn't reserved just for the CIA and secret memos about UFOs. When corresponding with clients and sending or receiving sensitive information, ask yourself whether you actually need to include key pieces of data. If you can get along without it, omit it. Or, if you need to reference it, redact it. Strive to maintain privacy while still communicating to clients what they need to know. We're in the habit of only providing the last four digits of a person's social security number, but you may want to fully or partially redact employer identification numbers, phone numbers, spouse and dependent names, banking information, and signatures.

Encryption

If your device is lost or stolen, encryption could be your last line of defense. Most operating systems include options for encryption - you just have to turn the feature on. You should encrypt both your computer and smartphone and, of course, don't lose your password or encryption key! If you're having trouble tracking your plethora of passwords, consider a password management system. That's a better solution than simplifying or reusing your passwords. You'll also want to back-up your data consistently and often so that you can continue to access files that were lost with your device.

A Keen Eye

No matter how many firewalls, passcodes, and castle moats you employ to protect your data, a careful, cynical eye is still one of the best security tools at your disposal. A phishing attempt doesn't need to originate from a little-known crown prince with a unique business opportunity. Spelling and grammatical errors may still be a dead giveaway, but advanced antagonists will be more subtle. Look at those links before you clickthrough. Are you heading to a trusted destination? Does that URL look a little off? Or is the sender's email address close, but not quite what you'd expect to see?

For more information visit the AICPA Member Insurance Programs Resource Center

To learn about our Cyber Liability available through AICPA Member Insurance Programs visit us here

Sources

Kepczyk, R.H. (2019, December 16). Tax security: It's the law! *AICPA.*
https://www.aicpa.org/interestareas/privatecompaniespracticesection/qualityservicesdelivery/informationtechnology/tax-security-its-the-law.html

Ference, S.B. (2017, March 1). The armor of awareness. *Journal of Accountancy.*
https://www.journalofaccountancy.com/issues/2017/mar/defense-from-cyberattacks-at-cpa-firms.html

Bonner, P. (2015, November 13). Tax ID theft victims may obtain copies of fraudulent returns. *Journal of Accountancy.*
https://www.journalofaccountancy.com/news/2015/nov/tax-id-theft-victims-may-obtain-bogus-returns-201513385.html