Quick Digital Accounting Security Assessment

Are you keeping an eye on safety while running your firm in a digital world?

Areas of high risk for accounting professionals

How secure are your firm's workflow and systems for handling tax and other confidential information in the age of Digital Accounting? (If you're not sure of an answer, check 'Yes')

Email

Does your firm request or share documents with clients & others using unencrypted email?

☐ YES   ☐ NO

Could your staff easily be deceived by a fraudulent email that appears to come from management, a client, bank, taxing authority and/or software vendor providing a login link or requesting a funds transfer / payment that appears to be routine due to lack of awareness and cybersecurity training? (If you're not sure, check 'Yes')

☐ YES   ☐ NO

File Sharing & Storage

Does your firm use consumer-level online file sharing programs for confidential documents?
(ex. Dropbox, Google Drive, OneDrive, etc.)

☐ YES   ☐ NO

Does your firm store sensitive / confidential information on local hard drives, servers or removable storage (USB drives) without encryption? (If you're not sure, check 'Yes')

☐ YES   ☐ NO

Does your firm store all digital files in one place only, without an encrypted online backup system?

☐ YES   ☐ NO

Password Management

Do staff members store login credentials on spreadsheets, written notes or use other unprotected methods?
(If you're not sure, check 'Yes')

☐ YES   ☐ NO

Does your firm store sensitive / confidential information on local hard drives, servers or removable storage (USB drives) without encryption? (If you're not sure, check 'Yes')

☐ YES   ☐ NO

Do your staff and / or clients share the same login credentials?

☐ YES   ☐ NO

Do staff members use the same password for multiple logins? (If you're not sure, check 'Yes')

☐ YES   ☐ NO

Policies

Do staff or management ever use public Wi-Fi to access confidential information without additional security protection? (If you're not sure, check 'Yes')

☐ YES   ☐ NO

Is sensitive information on paper documents easily accessible to everyone in your office and / or emptied when no longer needed with regular bin disposal?

☐ YES   ☐ NO

Hardware / Software

Does your office use hardware that's more than 5 years old (computers, routers, modems, firewalls)?

☐ YES   ☐ NO

Is there a newer version available of your firm's computer and mobile device operating systems and / or key software that has not yet been updated or is obsolete? (If you're not sure, check 'Yes')

☐ YES   ☐ NO

Planning

Is your firm operating without a plan of action for what to do in the event of a cyber security breach?

☐ YES   ☐ NO

Is your firm operating without adequate cybersecurity insurance? (If you're not sure, check 'Yes')

☐ YES   ☐ NO

Scoring of Answers

To find your score, count up how many questions were answered 'Yes'.

1–3
LOW

Possible but less of a target for cyber criminals.

4–6
MODERATE

Needs attention because there are some high-risk gaps.

7–14
HIGH

Some critical vulnerabilities exist, and your firm is an easy target for a cyber attack.

RISK LEVEL