Cyber Security Essentials for New Accounting Practices

ACCA | PureCyber

Why Are Accountancy Practices a Target for Cybercriminals?

Accounting firms hold **valuable personal and financial information** about clients and the business itself. This makes them prime targets for **phishing**, **data breaches**, and **ransomware attacks**. It's not only larger firms that are targets for cyber criminals – their aim is to target any vulnerabilities that cause disruption and lead to a potential financial gain. This renders smaller and new firms, who often have minimal to no cyber security process in place, as even bigger targets.

GDPR Responsibilities and Regulatory Expectations

Under **UK GDPR**, *Article 32* specifically mandates that firms must understand:

- **What data they hold**
- **Where it is stored**
- **What controls are in place to protect it**

The **Information Commissioner's Office (ICO)** expects even micro-businesses to demonstrate reasonable efforts to protect data.

Proactive steps can mitigate penalties in the event of a breach.

Practical Cyber Security Measures for Start-Ups

1. Password Policy & Access Management

Tools such as cloud-based accounting platforms offer scalability and cost-efficiency but must be properly secured. Key practices include:

- Using a **password manager** to maintain strong, unique credentials
- Enabling **multi-factor authentication (MFA)** across all systems
- Limiting admin access and enforcing **least-privilege principles**

2. Staff Awareness and Training

Human error is a leading cause of data breaches. Ongoing cyber awareness training helps staff detect and prevent phishing and social engineering attacks.

- **84%** of UK businesses experienced phishing attempts last year.
- Training should be refreshed at least **twice a year**.

3. Backup Your Data

- **Regular Backups:** Schedule frequent backups of all critical data.
- **Offsite Storage:** Use secure, remote/cloud-based locations for backup storage.
- **Recovery Testing:** Test recovery processes regularly to ensure business continuity.

4. Develop an Incident Response Plan

- **Preparation:** Have a clear, documented incident response plan in place.

- **Roles and Responsibilities:** Define roles and responsibilities within the response team.
- **Testing:** Regularly test and update the incident response plan.

5. Secure Physical Access

- **Access Control:** Implement physical access controls for sensitive areas.
- **Surveillance:** Use surveillance cameras and monitoring systems.
- **Visitor Policies:** Establish strict visitor policies to prevent unauthorised access.

Cyber Health Checklist

Use this checklist to monitor and maintain your cyber resilience:

Control Area	Action	Frequency
Data Management	Map data storage, classify sensitivity	Annually
User Access	Review user privileges and admin roles	Monthly
Password Security	Enforce use of password manager and MFA	Ongoing
Patch Management	Automate system and software updates	Monthly
Backups	Verify off-site/cloud backups and test restore	Weekly
Cyber Awareness Training	Conduct staff training on phishing and threats	Every 6 months
Incident Preparedness	Maintain and test response plan	Bi-annually
Certification	Complete or renew CE/CE+	As required
System Testing	Schedule vulnerability scans or pen-tests	Annually

Cyber Essentials

Cyber Essentials will help you to understand how to protect your organisation, whatever its size, against a whole range of the most common cyber-attacks.

- **Cyber Essentials (CE) Standard:**
  A government-backed, self-assessed certification. Suitable for start-ups and sole practitioners. Successful applicants may also receive **cyber liability insurance**.
- **Cyber Essentials Plus (CE+):**
  A more advanced, **externally audited** certification. CE+ is the next stage of your Cyber Essentials journey and looks to reinforce your cyber security compliance.

Cyber Insurance

Cyber Essentials certification, which starts from £320, can provide up to £25,000 of cyber insurance cover for eligible UK organisations. While this offers a useful safety net, the cover is limited and may not be sufficient to meet the potentially significant costs of a cyber attack, such as business interruption, legal liabilities, or reputational damage. ACCA practices, which hold sensitive client financial data, should therefore carefully assess their risk exposure and consider taking out standalone cyber insurance to ensure they have adequate protection.

Find out more about the Cyber Essentials scheme here: https://iasme.co.uk/cyber-essentials/.

Cyber Security Essentials for New Accounting Practices

Getting Secure: Your Next Steps

1. Begin with the **Cyber Essentials Standard** certification
2. Implement **strong access controls** and **regular backup** routines
3. Schedule **staff training** and monthly cyber health checks
4. Prepare and test an **incident response plan**
5. Plan for an **annual vulnerability scan** or **penetration test** as your firm grows

The ACCA & **PureCyber** partnership has been forged to support ACCA members and their businesses, from start-ups to established practices on their journey to improve their cyber resilience.

ACCA members receive a 10% discount on PureCyber Managed SOC, Penetration Testing & Consultancy Services, offered individually or as part of our subscription packages.