Introduction to Cybersecurity

Who is the course for?

- Staff and managers looking to protect themselves from cybersecurity threats
- Staff whose businesses are seeking Cyber Essentials certification

Course objectives

- To explain what cybersecurity is about, and why it is important
- To explain the principal types of threats and risks
- To show staff how they can reduce the risks of attacks

Features

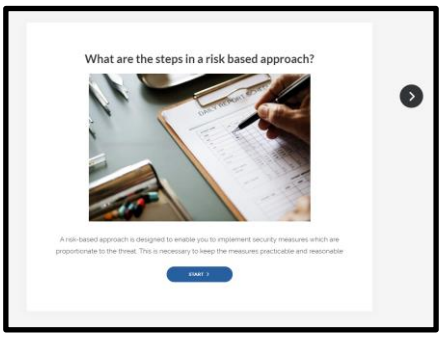
- Based on over thirty years' experience in information management education, training and research
- Based on over twenty years' experience in online and blended education
- Checklists to link learning to CyberEssentials audits
- Cloud based software as service delivery to wide range of platforms

Who are we?

AGLC have been trading for 10 years. We supply learning solutions to a wide range of organisations from local small companies to UK Dept of BEIS, Universities and the World Bank amongst other global agencies, and our collaborators include academic environmental management experts

This learning is designed to help organisations seeking to comply with the Cyber Essentials scheme train their staff about cybersecurity

It is not designed for technical specialists, but for all staff on the grounds that most cyber security attacks start with the staff not the technology



Content

1. **Fundamentals of information security**
   - The need for cybersecurity
   - The threat from staff
   - Information assets register
2. **Protecting your business from external threats**
   - Protecting your devices with firewalls
   - Deploying device firewalls
   - Protecting the perimeter of your information systems
   - Deploying firewalls to protect the perimeter
3. **Using settings to protect your information**
   - Changing default settings supplied with devices
   - Changing default settings supplied with applications
   - Strong passwords
   - Password policies that balance technical security with behavioural factors
4. **Using permissions to protect your information**
   - Controlling the information and physical environment
   - Measures to provide access appropriate to a job role
   - Measures to protect access to admin level information and functions
5. **Protecting your information from viruses**
   - Anti-malware software
   - White listing of websites and applications
   - Control of access to websites and applications not on the whitelist
6. **Using patching and updates to protect your information**
   - The importance of software updates to operating systems and applications
   - Managing automatic updates
   - When to manually update

Contact us at
sales@aglcltd.com
+44 7921600428