Safety and Security

IC3 Digital Literacy Certification, Global Standard 6 (GS6)

2 objectives · Certiport IC3 Digital Literacy GS6

Managing device security goes beyond a strong password. Multifactor authentication, regular malware scanning and safe handling of devices when they change hands protect both your data and the people who use the device next.

Every objective and its key skills

7.1 Manage device security

Authentication factors fall into three types: something you know (password, PIN), something you have (phone, security key) and something you are (fingerprint, face).

Antivirus or anti-malware software detects, blocks and removes harmful software such as viruses, ransomware and spyware.

7.2 Be aware of the physical and environmental impact of digital tools and technologies

Poor posture and long periods at a desk can cause neck, back and wrist pain; adjust the chair, screen height and keyboard position.

Electronic waste (e-waste) contains hazardous materials such as lead and mercury and valuable metals that can be recovered, so it should never go in ordinary rubbish.

Common pitfalls

- Two passwords, or a password and a security question, are both 'something you know', so they are not true multifactor authentication.
- Throwing batteries or electronics in household rubbish can cause fires and pollution, and may be illegal in many places.

ExamDragon, examdragon.com/ic3. Independent exam preparation, not affiliated with or endorsed by Certiport or Pearson VUE; written in our own words from Certiport's IC3 Digital Literacy GS6 objectives.