

Cyber security Assessment



1. Cyber security only relates to protecting personal or sensitive electronic information.
 - True
 - False

2. Small charities are less vulnerable to cyber attacks than large corporations or government agencies.
 - True
 - False

3. Who is ultimately responsible for a charity's cyber security?
 - The head of IT or Chief Information Officer
 - The Chief Executive Officer
 - The charity's Responsible Persons (its board or committee members)

4. What is the first thing a charity should do to identify cyber security risks?
 - Install a firewall for its network
 - Consider the information it holds that could be valuable to an attacker and prioritise its protection
 - Ensure individuals have strong passwords on their work devices, including computers and phones
 - Revoke access to the internet for part-time staff and volunteers

5. What should a charity do if it identifies a data breach?
 - Follow the Office of the Australian Information Commissioner's guidance on data breach preparation and response
 - Contact the ACNC to notify of the breach
 - Replace the device or system that led to the breach occurring
 - Reprimand the person responsible

6. Of the following, select the cyber security risks.

- A trusted, long-time charity employee having unauthorised access to files they shouldn't have access to.
- Sending new volunteers to a cyber security training session before they start work.
- Clicking on a link in an email from an unfamiliar source to see if its contents are legitimate.
- Having a shared password for a shared charity computer written down on a notepad next to the computer.

7. Select the correct option to complete the sentence. A charity shouldn't...

- Keep a written register of the passwords for its critical assets
- Store back-ups of important information in the 'cloud'
- Publicly acknowledge a data breach if it occurs
- Use a two-step process for logging in to a computer or device
- Issue devices such as tablets and phones to part-time staff or volunteers

Answers



1. False. Cyber security applies to all electronic information. But if a charity handles personal or sensitive information, it must be particularly careful about how it is protected.
2. False. Small charities can be especially vulnerable to cyber attacks.
3. A charity's Board or Responsible Persons are ultimately responsible for a charity's cyber security.
4. To identify the risks, the first thing a charity should do is consider the information it holds that could be valuable to an attacker and prioritise its protection.
5. A charity should respond to the breach in line with OAIC's guidance, which follows a four-step process: contain, assess, notify, and review.
6. The cyber security risks are:
 - A trusted, long-time charity employee having unauthorised access to files they shouldn't have access to
 - Clicking on a link in an email from an unfamiliar source to see if its contents are legitimate
 - Having a shared password for a shared charity computer written down on a notepad next to the computer
7. A charity shouldn't keep a written register of the passwords for its critical assets