The top cyber security tips for small to medium business

These are the tips that CERT Australia considers to be the most critical for businesses to use to reduce cyber security risks.

The tips are listed in the priority we believe offers the most benefit to the organisation. However, they need to be considered within the context of specific risks to the organisation or the sector.

1. **Keep your software patches up-to-date and use supported versions of software.** This includes the operating systems and applications, as well as email, database and web servers, configured to update automatically where possible. Additionally, use software from reputable sources to prevent accidentally installing hidden malware. **Why?**

   Patching your organisation's systems and programs is the key to keeping malware from infiltrating the computers. Each and every unpatched program can become an entry point for an attacker.

2. **Develop a backup strategy for your critical data.** A good strategy includes daily backups, an additional weekly or monthly backup, with both offline copies as well as offsite storage of at least the weekly backup media. Test that you can recover with backup data. **Why?**

   A sound backup strategy will ensure you have access to your information in the event of a cyber security incident. Having an offline backup also reduces the impact of ransomware attacks. See the CERT Australia guides on Resilient Backups and on Ransomware at **www.cert.gov.au/advisories** for more information.

3. **Change the default passwords across all systems to something new**, so that they cannot be easily guessed. Also use unique passwords for access to all systems, including for each website subscribed to, and change these individual passwords regularly. **Why?**

   So that an attacker will not automatically obtain access to all your systems in the event that a password for one website or system is discovered.

4. **Install security software that includes a firewall, anti-virus and anti-spyware.** Ensure that it is updated automatically. Using spam filters can reduce the amount of spam that your business receives. **Why?**

   Security software helps to protect your organisation against malicious or otherwise unauthorised incoming network traffic.

5. **Create non-administrator level accounts.** By default new computers usually have a single user account with Administrator privileges. Splitting this into two reduces

the opportunity for an attacker to gain control of your system. Use the non-Administrator account for all day-to-day activities, in particular for accessing email and web browsing. **Why?**

Administrator level accounts are targeted by attackers as they can potentially give full access to a system. Creating non-Administrator level accounts and using them for day-to-day activities reduces the risk of network compromise.

6. **Recognise and follow safe online practices.** Ensure that staff understand how they should use email and the internet, and learn safe browsing habits. Educate staff to be wary of unsolicited emails or phone calls, and to be cautious of opening attachments or clicking on weblinks sent via email. **Why?**

   Tempting a user to access malicious attachments and websites is a common technique used to install malicious code on a computer, which can lead to information theft or network compromise.

7. **Secure any remote access services**, such as disabling remote access if it is not needed, or using "IP whitelisting" and strong passwords if remote access is required. Also secure all other public facing services like your organisation's web server, such as through independent website testing for vulnerabilities like SQL injection. **Why?**

   Users with remote access can be targeted by attackers to attempt to gain unauthorised access to the network, for example in ransomware attacks. See the CERT Australia guide on Ransomware at **www.cert.gov.au/advisories** for more information. Attackers may also take advantage of security flaws in the website for defacement or to make the site unavailable.

8. **Protect critical information** by controlling physical access and using encryption when this information is stored on portable devices or removable media. **Why?**

   Controlling physical access minimises the risk of resource theft, destruction or tampering. Encryption helps ensure only those authorised to access information stored on portable devices and removable media are able to do so.

9. **Automatically log information relating to network activities and computer events.** Best practice is to retain logs and regularly review them to help detect malicious activity. If staffing levels do not permit regular log analysis, at least retain logs for use in retrospective investigations. **Why?**

   Sound logging practices improves the chances that malicious behaviour will be detected by highlighting any changes to the normal behaviour of a network, system or user. Logs can show how a cyber security incident came to pass and, therefore, what can be done to prevent similar occurrences in the future.

10. **If you do not have a dedicated IT Manager, assign at least one person in your organisation to have responsibility for information security** (such as passwords, backups, anti-virus updates). Ensure this person keeps up to date with cyber security threats and makes colleagues aware of potential issues. **Why?**

    Appointing a person with these responsibilities will ensure information security is a consideration in your organisation's day-to-day activities.