The cybersecurity checklist for SMBs

Reduce risks and alleviate total data loss



Maintain a strong password policy

Avoid using common passwords such as birthdate, name, etc. Use long passwords with a combination of numbers and special characters.

Be on the lookout for phishing emails and phone scams

Be wary of suspicious emails, hyperlinks, and calls. When in doubt, report it.

Conduct an annual security assessment

Know where your baseline currently stands each year and what can be improved.

Make sure back-ups are up to date

Plan certain dates to perform back-ups or automate the process.

Enforce mandatory cybersecurity training sessions

Holding regular training including the latest threat trends keep all employees up-to-date.

Monitor user access

Ensure the right users have the correct access to certain data and documents.

Use multiple layers of security

Multi-factor authentication confirms the users identity with other devices and platforms.

Have clear guidelines on data management

Create a document about data and file classification, storage, access, and disposal that all employees will follow.

Continually re-examine policies and procedures

Determine various checkpoints throughout the year to ensure policies and procedures are still applicable or need to be updated.

Deploy endpoint security

Only having antivirus is not enough.

Regularly evaluate BYOD policies

Revisit BYOD policies as the organization changes. (Ex: remote working)

Update all software when updates are available

Keeping software up to date reduces vulnerabilities and security holes that hackers are looking for.

creativeIT

1300 143 493 | http://www.creativeit.net.au

Unit 220, 757 Bourke Street, Docklands, Vic 3008