AUCYBER

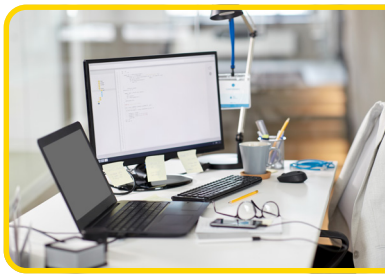
Holiday Cybersecurity Checklist

Cybercriminals don't take holidays but your business should be able to. Use this quick checklist to ensure your systems stay protected while your team takes a well earned break.

People

- [ ] Enable out-of-office alerts without exposing personal details.
- [ ] Remind staff not to click on unexpected holiday-themed emails or attachments.
- [ ] Confirm key contacts for incident response during the break.
- [ ] Limit access for temporary or departing staff before holidays.

Devices

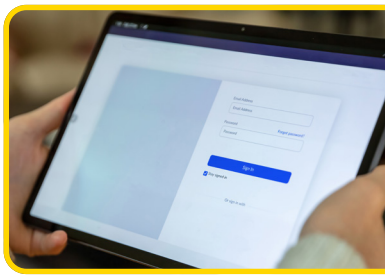


- [ ] Ensure all laptops and endpoints have the latest security patches installed.
- [ ] Enable full-disk encryption for portable devices.
- [ ] Verify endpoint protection is active and updated (EDR/AV).
- [ ] Require MFA for all remote logins.

Data

- [ ] Confirm backups have completed successfully and are stored securely offsite.
- [ ] Test a data restore from backups before the break.
- [ ] Encrypt sensitive files shared externally.
- [ ] Restrict file-sharing permissions for non-essential users.

Access



- [ ] Review and disable unused admin accounts.
- [ ] Rotate privileged account passwords before the holidays.
- [ ] Check MFA enforcement across all critical systems.
- [ ] Ensure monitoring and alerting remain active 24x7.

Need a second set of eyes before you switch off?
Speak with our team today. Visit aucyber.com.au