Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Cyber security checklist for charities and not-for-profits

- [ ] Turn on multi-factor authentication where possible.
- [ ] Check automatic updates are on and install updates as soon as possible.
- [ ] Back up important files and device configurations often. Test your backups on a regular basis.
- [ ] Use a reputable password manager to create strong, unique passwords or passphrases for your accounts.
- [ ] Provide cyber security training, particularly on how to recognise scams and phishing attempts. Use access controls and review them often so staff can only access what they need for their duties. This will reduce potential damage caused by malware or unauthorised access to systems.
- [ ] Use only reputable and secure cloud services and managed service providers.
- [ ] Test cyber security detection, incident response, business continuity and disaster recovery plans often.
- [ ] Review the cyber security posture of remote workers and connections. Make sure staff are aware of secure ways to work remotely such as not accessing sensitive information in public.
- [ ] Report a cybercrime, incident or vulnerability to protect yourself from further harm at cyber.gov.au/report
- [ ] Join ASD's Cyber Security Partnership Program. This free program provides advice and insights on the cyber security landscape.

Protecting your charity or not-for-profit from cyber attacks is an ongoing process. Review your cyber security often to strengthen your resilience. Seek help from an IT professional if you are unsure.

For more resources and advice, visit:
www.cyber.gov.au/protect-yourself/staying-secure-online/cyber-security-for-charities-and-not-for-profits

If you require assistance due to cybercrimes or incidents, ASD's ACSC is available to help. You can contact our 24/7 hotline at 1300 CYBER1 (1300 292 371) or visit the Report and Recover page at cyber.gov.au/report-and-recover