National Cyber Security Centre
PART OF THE GCSB

Ministry for Ethnic Communities
Te Tari Mātāwaka

**Keeping your organisation safe online**

**Why is cyber security important for community groups and organisations?**

This page has advice and some steps you can take to protect your community group or organisation from cyber security threats. There's also a separate guide for individuals.

This advice is based on the most common and serious threats.

- Updates – keep the software on your devices up to date to patch any holes in the security.
    - Keep your community group or organisation's devices updated. This includes phones, computers, WiFi routers, and anything else that connects to the internet – including smart devices.
    - Use automatic updates where possible.
- Two-factor authentication (2FA) – adds extra security to your accounts by requiring a password and one more step, such as a code from an app on your phone.
    - Note: This is called multi-factor authentication (MFA), two-step verification (2SV) and many other names.
    - Turn on 2FA on all your community group or organisation's accounts.
    - If possible, try using a form of 2FA that is phishing resistant, which means you can't be tricked into giving it over. This may be a physical security key or something like a fingerprint or face ID.
- Keep track of your online accounts – make sure ex members don't keep their access to accounts after leaving the community group or organisation.
    - If you have more than one person accessing the same account, make sure they all have different logins, and all have 2FA turned on.
    - Keep a list of all user accounts and deactivate any that aren't needed, such as when staff leave.
    - Keep a register of any devices you have given to your members and remember to get them back and factory reset them if that person leaves the organisation. You may also need to change physical codes for building access.
- Check who has access to your online accounts – people in your community group or organisation should only have access to things they need.
    - If one person's account gets 'hacked', these steps limit the harm an attacker can do.
    - Regularly check and remove unnecessary permissions.
    - If you have a single "admin" account that multiple people use, monitor it for unusual activity. Try to limit having these sorts of accounts, especially for daily tasks.
    - These rules also apply to administrator access to devices, such as routers.

- Review your contracts with service providers – if you have hired anyone to run IT services for you.
    - Make sure that they have cyber security protections in place to meet your community group or organisation's needs.
- Know how all your accounts and systems work together – understanding the connections helps you know where an attacker could get in.
    - Review the connections between your systems, for example, email, cloud storage, and accounting platforms.
    - Consider using a Virtual Private Network (VPN) for extra online safety. Using a VPN hides your online activity from anyone who might try to track you. This is especially good if any members of your community group or organisation connect remotely.
- Keep your people 'cyber smart' – the people in your community group or organisation are more likely to be targeted than your systems.
    - Train all staff in basic cyber security. The Own Your Online website Own Your Online | NCSC has a wide range of advice and tips to help keep yourself secure online and how to spot scams.
    - Remind them that this is important for their personal accounts as well as the ones they use for your organisation.
    - We have a guide for individuals as well. [LINK placeholder]
- Plan for an incident – having a response plan in place is important to keep people from panicking when an incident happens.
    - An incident response plan outlines who does what during an incident. Templates are available here Incident Management | NCSC
    - Include a plan for what to do if phones, computers, or other systems fail. Keep this plan updated.
    - Keep contact details of everyone required and backup details if the main way to contact them is broken (such as email).
    - Keep the plan somewhere outside your system as well, in case you can't get to it.