# ONLINE SAFETY TIPS

## To protect your devices and accounts

*Guidance from The Cyber Helpline, created for individuals working in charities*

Whatever devices you use and however you connect, there are simple steps you can take to protect your accounts and devices and stay safe online.

## Introduction

Our phones, laptops and social media accounts hold more information about our lives than ever, which makes them attractive targets for criminals. A handful of simple online safety habits can help keep you better protected, both at work and at home. This helpsheet contains advice from The Cyber Helpline, a UK charity supporting victims of cybercrime, digital fraud and online harm.

## What does it mean to protect your devices and accounts?

Charities are exposed to many of the most common cyber threats, including phishing, email compromise and social engineering. Protecting your devices and accounts means keeping them secure so that criminals can't get into the charity's information, finances or systems.

Criminals often target people rather than technology. Impersonation fraud is a common example, where they pose as a colleague, senior manager or trusted organisation
A convincing message can be enough to get someone to click a link or open an attachment, and that can give them access to your accounts and information, putting the charity and the people it supports at risk. That's why staying alert to every message you receive is one of your best protections.

***No single step will keep you completely safe, but together these habits make a real difference.***

ACKNOWLEDGEMENT
The Cyber Helpline
The Cyber Helpline

Published 2026. © Fraud Advisory Panel for England and Wales, 2025. Fraud Advisory Panel will not be liable for any reliance you place on the information in this material. You should seek independent advice.

# Good habits to protect your charity's devices and accounts

Use these steps to secure a new or compromised device.

## Phones

- If you think your device has been compromised, reset it to factory settings. This wipes off most malware. But be careful when you restore from a backup, because the malware could be hiding in it. Use a backup from before the problem started, or start fresh and only copy over your photos, contacts, and documents. Then download your apps again from the official app store.
- Enable two-factor or multi-factor authentication (2FA or MFA) on your accounts.
- Don't jailbreak your device or use jailbroken devices.
- Keep the operating system and apps updated.
- Use device-based biometrics, such as face recognition, backed by a unique password.
- Limit what your apps can access. If an app doesn't need your location, camera, or contacts to do its job, turn that permission off. For the ones that do need it, choose "only while using the app."
- Turn off Bluetooth, location services, and NFC (the tap-to-pay feature) when you're not using them.
- Use end-to-end encrypted messaging apps.

## Laptops

- If you think your computer is infected, erase the drive and reinstall the operating system from scratch.
- Enable full disk encryption.
- Use robust passwords.
- Set up regular, automated backups.
- Switch on your device's built-in firewall to block unauthorised connections from the internet.
- Review account permissions regularly.
- Use HTTPS and security-focused browser extensions.
- Limit data sharing in privacy settings.

# Account security

Every account should be protected so that only authorised people can get in. Wherever possible, use passkeys, a stronger alternative to passwords that lets you sign in with the same thing you already use to unlock your device: your fingerprint, your face, or your device PIN.

## Where passwords are still needed, these 8 habits make them much harder to break:

1. **Make them strong and unique.**
   Use a passphrase made of three random words, or let a password generator create one for you.
2. **Never reuse a password.**
   If one service is breached, every account sharing that password is at risk.
3. **Check for compromise.**
   Use a service such as Have I Been Pwned to see whether your password has leaked, and change it immediately if it has.
4. **Turn on multi-factor authentication (MFA).**
   It asks for a second check when you log in, such as a code sent to your phone or one from an authentication app.
5. **Be careful with password books.**
   A physical ledger can help, but keep it secure so it doesn't become the root cause of a breach, especially in a shared household.
6. **Protect your recovery questions.**
   Have your password manager generate and store random answers.
7. **Store passwords safely if you can't use a manager.**
   Don't keep passwords in unsecured documents on your device. Write them down offline and keep them somewhere secure, or use a cloud key vault protected by MFA.
8. **Use a password manager.**
   These store your passwords with strong encryption. For extra protection, pair it with an email alias service such as Apple's Hide My Email, which gives each account its own address, so attackers can't link your accounts or reuse a leaked login elsewhere.

## Social media and unsecured communication channels

Knowing how a charity operates and how its teams are structured helps criminals carry out social engineering and gain unauthorised access to accounts. All staff should therefore be careful about sharing charity information online or outside official charity channels.

### In particular:

- Do not share details of charity systems or team structures
- Do not publish direct dial numbers for individual team members
- Be alert to unsolicited calls or emails asking about the charity or its staff
- Make sure support teams verify staff identity before giving help, especially with password resets
- Provide a way for staff to report third-party contact or confidential charity information they find online

# Extra layers

- Automate app updates.
- Use a VPN, especially on public Wi-Fi networks.
- Enable device tracking, so you can locate and remotely wipe a lost or stolen device.
- Use biometric authentication.
- Set up emergency contacts on your phone for quick access.
- Protect sensitive documents with encrypted cloud storage or local encryption.
- Keep learning about cybersecurity threats and best practice, and schedule regular audits to adjust your measures.

## Checklist

### *Ask yourself:*

1. Can I use passkeys? ☐
2. Have I enabled MFA wherever possible on accounts? ☐
3. Is my anti-virus software up-to-date? ☐
4. Are my devices encrypted, locked and backed up? ☐
5. Have I reviewed app permissions and removed what I don't need? ☐
6. Have I checked what I share publicly on social media? ☐
7. Do I schedule regular security audits of my devices and accounts? ☐

If you need more help, access free support from The Cyber Helpline at **thecyberhelpline.com/gethelp**