

Ten things to do today

Simple cyber security steps for charities

None of this needs a technologist. Almost none of it needs a budget.

Information Security Panel | October 2026

Why this matters for charities

Over the last twelve months, according to the UK government's own survey:

28%

of charities identified a cyber breach or attack: around 57,000 organisations

1 in 4

charities experienced a phishing attack, the most common and most disruptive kind

19%

of charities have a formal plan for responding to a cyber incident

The good news: the ten steps that follow cost little or nothing, and you can start on most of them today.

Source: DSIT and Home Office, Cyber Security Breaches Survey 2025/26, published 30 April 2026.

1 Turn on multi-factor authentication (MFA)

Your password plus a second check, such as a prompt or code on your phone.

99.2%

of account-compromise attacks can be blocked by MFA

38%

of charities currently require it

Every account that matters

Switch it on for every email, banking and cloud account.

Start at the top

Trustees, the CEO and the finance team are the accounts criminals want most.

Prefer an authenticator app

App prompts are stronger than text-message codes, but any MFA beats none.

Sources: Microsoft Research, MFA effectiveness study (2023); DSIT and Home Office, Cyber Security Breaches Survey 2025/26.

2 Use long, unique passwords

The NCSC recommends three random words. Long beats complicated.

coffee - **brick** - **trumpet**

Easy for you to remember. Hard for a criminal to guess.

Make it long

Three random words give you length without a jumble of symbols.

Never reuse

One password per site, so a single leak cannot open every door.

Use a password manager

It remembers them all, so you only need one strong password.

Source: National Cyber Security Centre (NCSC), three random words guidance.

3 Keep software up to date

Updates fix weaknesses that criminals already know about. Let them install themselves.



Laptops

Turn on automatic updates



Phones

Turn on automatic updates



Tablets

Turn on automatic updates



Replace devices that no longer get security updates.

An old phone or laptop with no updates stays vulnerable, however careful its user is.

4 Treat email with healthy scepticism

Three habits that catch most scam emails.

Hover over the sender

Check the real address, not just the display name.

Hover over the link

See where it really goes before you click.

Feel rushed? Stop.

Urgency is a scammer's favourite tool. Check with someone first.

1 in 4 charities experienced a phishing attack in the last year. It remains the most common and most disruptive type of attack.

Source: DSIT and Home Office, Cyber Security Breaches Survey 2025/26.

5 Tighten your social media

What you share publicly helps criminals write a convincing scam.

Do

- Set personal profiles to private
- Be sparing about what you post, especially roles, rotas and travel plans

Don't

- Trust an advert just because the platform is well known
- Announce who is away, or who signs off payments

6 Be wary of QR codes and apps

Both are easy ways to slip a fake website or a harmful app onto your phone.

QR codes

Type the web address into your browser rather than scanning. A sticker can easily cover a genuine code.

Apps

Only install apps from the official Apple App Store or Google Play.

Be very suspicious of any app asking for accessibility permissions.

They let an app read your screen and tap buttons for you, which is exactly what fraudsters want.

7 Refuse phone-scam pressure

No reputable bank, HMRC, police force or phone company will ever:

- **Ask you for a one-time code**
- **Tell you to ignore a security warning**
- **Pressure you to act in the next sixty seconds**

Hang up.

Ring back on a number you find independently.

159

Worried about a call from your bank? Dial 159 to reach it safely.

Source: Stop Scams UK, 159 service.

8 Distrust voices and faces

AI can clone a convincing voice, and fake a face on a video call.

3

seconds

of audio produced an 85% voice match in McAfee's tests. A voicemail greeting is enough.

Agree a verbal callback procedure

For any unusual money or data request, even from people you know.

1. **Pause**
   Do not act on the call, message or video itself.
2. **Call back**
   Use a number you already hold, not one you were given.
3. **Confirm**
   Use an agreed code word or a second person before money or data moves.

Source: McAfee Labs, The Artificial Imposter (2023).

8 Distrust voices and faces



9 Sign up to Cyber Essentials

The UK government's basic cyber-hygiene certification, run by IASME.

Proves the basics are in place

Covers the controls that stop the most common attacks.

Opens doors to contracts

Increasingly required to bid for public-sector work.

Includes cyber insurance

£25,000 of cover for eligible UK organisations with turnover under £20m.

Annual fee by organisation size (plus VAT)

Size	Staff	Fee
Micro	0-9	**£320**
Small	10-49	£440
Medium	50-249	£500
Large	250+	£600

Only 16% of charities have heard of the scheme.

Sources: IASME pricing and insurance pages, checked October 2026; DSIT and Home Office, Cyber Security Breaches Survey 2025/26.

10 Back up your data, and test the restore

Follow the 3-2-1 rule.

3 copies of your data

2 different types of media

1 kept off-site or offline

Test a real restore at least twice a year.

Without a tested restore, you have a hope, not a backup.

Your checklist: tick them off



- [ ] **1** Turn on MFA, starting with trustees, the CEO and finance
- [ ] **2** Use three random words and a password manager
- [ ] **3** Switch on automatic updates; replace unsupported devices
- [ ] **4** Hover over senders and links; stop when rushed
- [ ] **5** Make personal social media profiles private
- [ ] **6** Type web addresses; install apps only from official stores
- [ ] **7** Hang up on pressure; ring back on a number you find
- [ ] **8** Agree a callback procedure for money and data requests
- [ ] **9** Get Cyber Essentials certified
- [ ] **10** Back up 3-2-1, and test a restore twice a year

Where to get help

Suspicious email

Forward it to report@phishing.gov.uk

Suspicious text

Forward it to 7726

Unexpected bank call

Hang up and dial 159 to reach your bank safely

Lost money or been hacked

Report Fraud: reportfraud.police.uk or 0300 123 2040. In Scotland, call Police Scotland on 101.

Free, practical guidance

NCSC Cyber Action Toolkit and small organisations guidance at ncsc.gov.uk

Rehearse an attack

NCSC Exercise in a Box: a free practice session for your team

Sources

DSIT and Home Office, Cyber Security Breaches Survey 2025/2026 (30 April 2026)
https://www.gov.uk/government/statistics/cyber-security-breaches-survey-20252026/cyber-security-breaches-survey-20252026

Microsoft Research, How effective is multifactor authentication at deterring cyberattacks? (May 2023)
https://www.microsoft.com/en-us/research/publication/how-effective-is-multifactor-authentication-at-deterring-cyberattacks/

NCSC, The logic behind three random words
https://www.ncsc.gov.uk/blog-post/the-logic-behind-three-random-words

McAfee, Artificial imposters: cybercriminals turn to AI voice cloning
https://www.mcafee.com/blogs/privacy-identity-protection/artificial-imposters-cybercriminals-turn-to-ai-voice-cloning-for-a-new-breed-of-scam/

Stop Scams UK, Stop, hang up, call 159
https://stopscamsuk.org.uk/campaign/get-help-now/

IASME, Cyber Essentials frequently asked questions (pricing)
https://iasme.co.uk/cyber-essentials/frequently-asked-questions/

IASME, Cyber Essentials cyber liability insurance
https://iasme.co.uk/cyber-essentials/cyber-liability-insurance/

NCSC, Report a scam email
https://www.ncsc.gov.uk/collection/phishing-scams/report-scam-email

City of London Police, Report Fraud
https://www.reportfraud.police.uk/

NCSC, Cyber security advice for small to medium sized organisations
https://www.ncsc.gov.uk/section/advice-guidance/small-medium-sized-organisations