A 15-MINUTE SECURITY CHECK
FOR CHARITIES



Is your charity's website an easy target?

Six quick checks to help you see whether your website is vulnerable to criminals, and what you can do about it.

magnetic

Anna Hessenbruch · November 2026

WHY THIS CHECKLIST

Your website can tell strangers more than you think.

After the recent PHP vulnerabilities, I wanted to know how many charities might have website weaknesses they're unaware of. So I looked at 40 of the UK's largest charities by income, using only what any visitor's browser can already see.

40
of the UK's largest charities reviewed

39%
show which software their website runs on

23%
have an email domain fraudsters could send fake emails from

Most of these fixes are quick, and you can run every check yourself.

The PHP flaw targeted a specific Windows set-up, so it largely passed charities by. Everyday risks sit closer to home, such as old software, email domains others can send from, and sites that show which software they run. In the government's 2025 survey, around 30% of UK charities reported a breach or attack in the past year.

Work through the six checks, or turn to page 6 and let an AI run them for you.

Sources: UK Government, Cyber Security Breaches Survey 2025. magnetic's review of publicly visible website and email settings at 40 of the UK's largest charities, October 2026.

THE CHECKS

Six checks to run on your own site

Each takes about a minute. Every check explains what it looks at and why it matters, then points you to a free tool.

01

Does your site always use a secure connection?

This checks whether your site always loads with https:// and a padlock, which means information passing between visitors and your site is encrypted.

Without it, anything a supporter types, such as their name, email address or card details, can be read or changed on its way to you, for example on public wifi.

FREE CHECK

ssllabs.com/ssltest

Enter your web address and wait a minute or two. A grade of A or A+ is good. B or lower is worth raising.

ASK WHOEVER RUNS YOUR SITE

Is every page forced onto https, and is HSTS switched on?

02

Does your site show what it's built on?

Many websites display the name and version of the software behind them, such as WordPress 6.4, in their code.

When a weakness is found in a particular version, criminals use automated tools to search the internet for sites running it. Showing your version can put your site on that list.

FREE CHECK

builtwith.com

Enter your web address and look under 'CMS' and 'Web Server'. A version number next to the software name means anyone can see it.

ASK WHOEVER RUNS YOUR SITE

Do our pages show our software name or version, and can that be hidden?

03 Is your website software up to date?

Most charity websites run on a content management system, such as WordPress or Drupal, with add-ons called plugins and themes. Each part needs regular updates.

Updates often close security holes that are already publicly known. Out-of-date software is a common way into a website.

FREE CHECK

sitecheck.sucuri.net

Enter your web address and look for warnings about outdated software, plugins or known vulnerabilities. It only sees what's public, so a clean result is a good sign rather than a guarantee.

ASK WHOEVER RUNS YOUR SITE

Are our core software, plugins and themes updated regularly, and who checks them?

04 Could someone send email pretending to be you?

This checks three settings, called SPF, DKIM and DMARC, that tell email providers which emails genuinely come from your domain.

If they're missing, criminals can send emails that appear to come from your charity, for example asking supporters to donate to a fake account. Phishing was the most common attack on UK charities in the government's 2025 survey.

FREE CHECK

mxtoolbox.com/dmarc.aspx

Enter your domain, the part after @ in your email address. Look for a DMARC record with p=quarantine or p=reject. If it says p=none, or finds no record, fake emails can still reach inboxes.

ASK WHOEVER RUNS YOUR SITE

Do we have SPF, DKIM and DMARC in place, and is DMARC set to quarantine or reject?

05

Does your site use browser safety settings?

Websites can send instructions, known as security headers, that tell visitors' browsers how to behave safely on your site.

If harmful code slips onto a page, for example through a compromised plugin or advert, these settings can stop it running or limit what it can do, such as copying details typed into a form.

FREE CHECK

developer.mozilla.org/en-US/observatory

Enter your web address and look at the grade. A or B is good. C or lower means some protections are missing, and the results show which.

ASK WHOEVER RUNS YOUR SITE

Do we use a Content-Security-Policy and the other standard security headers?

06

Who keeps all of this up to date?

This check is about people rather than technology: whether someone is responsible for keeping your website and email settings secure over time.

Settings change when the site is updated, suppliers change or new services are added. Each fix above lasts as long as someone owns it.

FREE CHECK

internet.nl

Run the website test and the email test, and save the scores. Repeat every quarter. If a score drops, something has changed and needs a look.

ASK WHOEVER RUNS YOUR SITE

Who is responsible for our website and email security, and how will we know updates are done?

FOR PAID BUSINESS AND ENTERPRISE ACCOUNTS

Let an AI check your site for you

This route is for organisations with a paid business or enterprise account, such as Claude Team or Enterprise, or ChatGPT Business or Enterprise. These accounts can usually browse websites for you, and by default your conversations are kept out of model training.

1

Switch on browsing

Use Claude with its Chrome extension, or ChatGPT in agent mode. Your administrator may need to turn this on.

2

Say it's your organisation's site

Give your charity's name and your role, and sign in with your work email if you can.

3

Be ready to show it's yours

If the AI asks, open your website admin or domain settings, or add the short verification record it suggests.

PROMPT TO COPY AND PASTE

I manage the website for [charity name] and I'm responsible for its security. Please review our own site, [yourcharity.org], and our email domain, using only publicly visible information. Check whether the site forces a secure connection, reveals its software or version, runs out-of-date software and sends the standard browser-security headers, and whether our domain could be used to send fake email (SPF, DKIM and DMARC). Then look for any other publicly visible risks. Explain everything in plain, everyday language for non-technical staff, avoiding jargon. For each issue, say how serious it is, what could happen, and what to ask the people who run our site. If you can't see something directly, say so and name a free tool that would show it.

FOR ANY AI, INCLUDING FREE VERSIONS

Free checkers, then a plain-English explanation

This route works with any AI tool, including the free versions of Claude and ChatGPT. The checkers gather the facts and the AI explains them.

1

Run two free checkers

internet.nl (run both the website test and the email test) and sitecheck.sucuri.net. Enter your own web address or domain.

2

Copy the results

Copy the text from each results page. Screenshots work too.

3

Paste them into the AI with this prompt

Add your results underneath the prompt and send.

PROMPT TO COPY AND PASTE

I manage our charity's website. Below are results from free security checkers for our own domain, [yourcharity.org]. Explain each finding in plain, everyday language for non-technical staff, avoiding jargon. Say how serious each one is, what could happen, and what to ask the people who run our site. Point out any other risks the results suggest. Where something sits outside these results, say so instead of guessing.

IF SOMEONE ELSE RUNS YOUR SITE

Questions to ask about your site

Most charities have someone else run their website, which works well when it's clear who owns security. Send these questions and look for specific answers.

- [ ] Is every page forced onto https, with HSTS switched on?
- [ ] Are our core software, plugins and themes updated regularly, and who checks them?
- [ ] Do our pages show our software name or version, and can that be hidden?
- [ ] Do we use a Content-Security-Policy and the other standard security headers?
- [ ] Do we have SPF, DKIM and DMARC in place, with DMARC set to quarantine or reject?
- [ ] Who do we call, and how quickly will you respond, if the site is hacked or goes offline?

Want a hand with any of this?

I help purpose-led organisations get the essentials sorted, in plain language. I can run these checks with you, or take on the whole job.

magneticconsulting.dk · anna@magneticconsulting.dk