

THE CHECK BEFORE YOU PAY

Charity money, spent on the cause.

Charities run on trust, volunteers and tight budgets, and the Charity Commission says phishing is the most common kind of cyber-enabled fraud they experience.

How it happens here

1. Payday approaches

Staff pay, or a payment to a supplier or grantee, is about to go out.

PRESS CHECK HERE**2. New details arrive**

An email to HR or finance, in a staff member's name, gives a new account for their pay.

3. The address looks right

It comes from a spoofed or lookalike address, so it seems to be from somebody you know.

4. The pay goes

Unless somebody checks with the employee on separately sourced contact details, the pay goes to the fraudster.

Before any payment to new or changed bank details

- 1 Never change a supplier's, grantee's or employee's bank details because of an email alone.
- 2 Ring them on the number already on your records, not one in the email.
- 3 Ask for the request on the supplier's own amendment form and check it against past payments.
- 4 Two people authorise every payment and every bank detail change, volunteers included.
- 5 For a first payment to new details, send a small amount and have the payee confirm receipt by phone.

If money has gone

Ring your bank's fraud line at once, then report to Report Fraud on 0300 123 2040 or reportfraud.police.uk (Police Scotland on 101 in Scotland).

Also on day one in England and Wales: tell the chair, keep a record of what happened and when, and consider a serious incident report to the Charity Commission.

What your sector's own bodies say

- Use dual authorisation for all financial transactions; if fraud happens, act quickly, preserve evidence, report to Report Fraud, and consider a serious incident report to the Commission. (Charity Commission, Protect your charity from fraud, November 2024)
- Review how employee bank details are changed and approved, and verify requests with the employee using separately sourced contact details. (Charity Commission, Alert for charities: fraudsters impersonating staff, December 2019)

Where Jatzo fits. Jatzo does not replace the call. It helps whoever reads the email notice that it needs one, before anybody pays.

Check before pay details change

Anybody unsure about a request to change where pay goes presses Check in Outlook or Gmail and sees a score out of 100 with the reasons.

Your treasurer hears at once

When anybody checks a message scoring High risk or above, an email goes to addresses you choose at your own domain, such as your treasurer's.

More at jatzo.co.uk/for-teams/charities

A separate check on supplier invoices

Invoice Fraud Analyser, a Windows program, compares the bank details on each supplier invoice with the ones you confirmed for that supplier.

See what is aimed at the charity

The organisation threat report counts the checks that reached Suspicious or above by kind of attack, the last 30 days against the 30 before, and names nobody.

The Charity Commission opened 603 cases relating to fraud between November 2023 and October 2024. That counts fraud of every kind, not only fraud that began with an email. (Charity Commission, Regulator refreshes guidance as it reveals 600 cases related to fraud, November 2024.)

UK Finance recorded £41.3 million lost to invoice and mandate fraud across 2,305 cases in 2025, 68% of it from business accounts. Criminals intercept emails or take over an email account, then pose as a supplier, a solicitor or a builder with new bank details. (UK Finance, Annual Fraud Report 2026, June 2026.) Report Fraud replaced Action Fraud in December 2025; the number did not change.