# SCAM EMAILS

## How to spot the warning signs

**FROM**
- You do not recognise the sender (or the email address)
- You know of the sender, but the email is unusual, unexpected or its tone out-of-character
- The sender’s email address is suspicious looking

**DATE / SUBJECT**
- The email was sent at an unusual time
- It’s a reply to an email you never sent. Or the subject line and content do not match

**TO**
- You were cc’d along with other people who you do not recognise
- The email was sent to an odd-looking group of people

**HYPERLINKS**
- The email contains a hyperlink with a misspelt URL to a known company’s website
- When hovering your mouse over the hyperlink, the link-to web address is different to the one displayed

**ATTACHMENTS**
- You were not expecting an email attachment
- The attachment is a potentially dangerous file type (only .txt files are always safe to open)

**CONTENT**
- The email does not address you by name
- The email requests you to click on a link, open an attachment, or disclose confidential information
- The message is strange, contains spelling mistakes or bad grammar

---

It's estimated* that fraud costs UK charities as much as £2 billion per year, damaging not only the finances but also the good name of the charities affected. As one of Europe’s largest charitable foundations, we have produced this checklist to help you spot scam emails, a medium widely used by criminals to defraud people and organisations.

Our **security centre** provides more tips about how to avoid falling prey to fraud. If you believe your organisation has become a victim of fraud, please report it to the **Action Fraud helpline** – 03000 123 2040.

---

* Source: Annual Fraud Indicator 2017