At Ease Online

How To Spot A Scam Email

A straightforward guide to the most common warning signs - so you can stay one step ahead.

Knowing how to spot a scam email is one of the most useful things you can do to stay safe online. Scam emails - sometimes called phishing emails,they are designed to look convincing, and they're getting better at it. But there are almost always warning signs. Once you know what to look for, they become much easier to recognise.

1. The sender's email address looks odd

The name shown in your inbox might say "HMRC" or "Your Bank" - but the actual email address behind it often tells a different story. Look carefully at the full address. If it contains random letters, numbers, or a domain that doesn't match the organisation (for example, hmrc@gov-update.net instead of @hmrc.gov.uk), treat it with suspicion.

2. It creates urgency or panic

Scam emails often use phrases like "Act now", "Your account will be suspended", or "You have 24 hours to respond." This pressure is deliberate - it's designed to make you act before you think. Legitimate organisations will not rush or threaten you.

3. It doesn't use your name

A genuine email from your bank or a company you deal with will almost always address you by name. If an email starts with "Dear Customer", "Hello" or just your email address, be cautious.

4. Poor spelling, grammar, or something looks slightly off

Unusual formatting, a logo that doesn't look quite right, or awkward phrasing can all be signs of a scam. Trust your instincts - if something feels off, it probably is.

5. It asks for personal or financial information

Legitimate organisations - including banks, HMRC, and the NHS - will never ask for your password, bank details, or personal information by email. If an email asks you to enter or confirm these details, do not do so.

6. It contains a suspicious link or attachment

Be very cautious about clicking links or opening attachments in unexpected emails, even if they appear to come from someone you know. If you hover your mouse over a link (without clicking), you can usually see the actual web address it leads to. If it looks unfamiliar or unusual, do not click!

At Ease Online

7. It sounds too good to be true

Prize notifications, unexpected refunds, and unclaimed windfalls are classic tactics. If something sounds too good to be true, it almost certainly is.

If you're not sure If an email claims to be from your bank, HMRC, a delivery company, or any other organisation and you're not certain it's genuine, contact that organisation directly - using a phone number or website you already know and trust, not the details in the email.

If you've already clicked a link or shared information Don't panic. Read our guide: What to Do If You Think You've Been Scammed Online.

Suspicious emails can also be forwarded to report@phishing.gov.uk - a free reporting service run by the National Cyber Security Centre (NCSC).

Want to feel more confident online?

These are the warning signs to know - but if you'd still like a little extra reassurance, that's exactly what we're here for. At Ease Online offers calm, patient digital support for older adults, at a pace that suits you.
Book your audit today.