kaspersky

HOW TO

Detect scams

How to get better at detecting scams, spam mail and infected links

1 Do it yourself

Only ever access your internet banking or shopping sites by typing the address into your browser, or selecting them from ‘favourites’ or ‘bookmarks’ that you’ve created yourself. **Never go to a website from a link in an email**.

2 Look for the ‘S’

Make sure that the URL you are visiting is secure by checking if it starts with **HTTPS** rather than **HTTP**, or has the **padlock icon** in the address bar. This will reduce the likelihood that you’re on a scam site.

3 Treat everything with caution

Treat all unsolicited emails with caution: **don’t click on links or open attachments in emails you weren’t expecting or are not sure about**. If you’re not sure, telephone or text the person who sent it to double check.

4 Does it look fishy?

Spot a phishing email by looking out for any of the following: impersonal greeting, typos, threatening language, or strange attachments. **If it looks fishy, it generally is**. Above all, remember that legitimate organisations will not send you requests for personal information – this is a key indicator that something’s not right.

5 Optimise security

Make sure all your devices are **protected with up-to-date internet security software**.