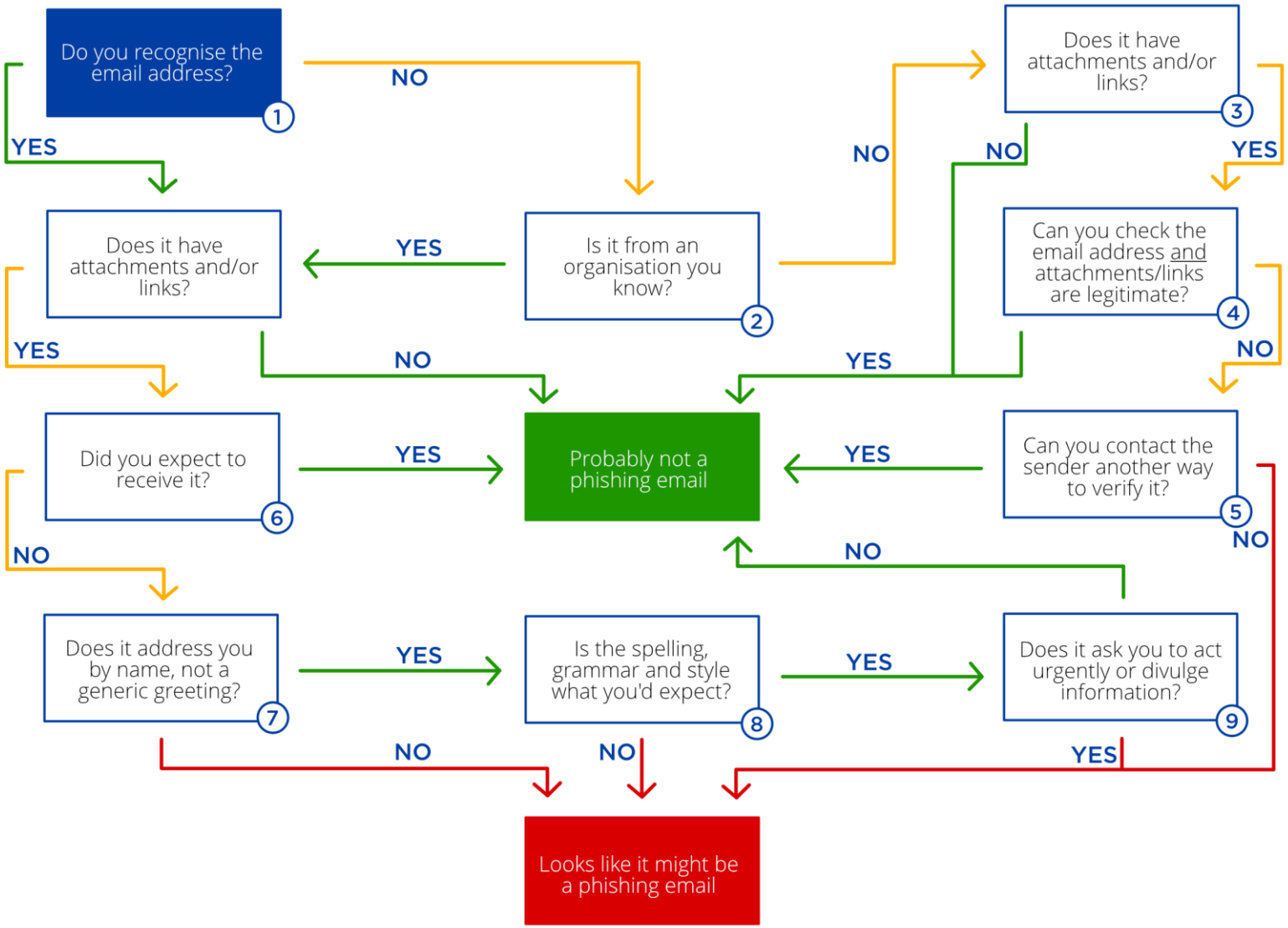
Phishing Flowchart

South West Grid for Learning Trust Ltd, Belvedere House, Woodwater Park, Pynes Hill, Exeter, EX2 5WS
Registered in England and Wales, Company Number 5589479. Charity Number 1120354. VAT Reg. Number 880 8618 88

SWGfL
Safe, Secure, Online



The SWGfL Phishing Flowchart is here to help you analyse emails you're not sure about. Remember that it might not be right all the time! Here's how to use it:

1. Start at the top left: "do you recognise the email address?" This is the actual address (e.g. infosec@swgflorg.uk), not just the 'display name' (e.g. "SWGfL Security Team).
2. "Is it from an organisation you know?" Here, you're looking at the email address to see if it's consistent with their website address (URL) and any emails they've sent you in the past.
3. "Does it have attachments and/or links?" If it does, these could be an attacker's way of trying to get something from you.
4. "Can you check the email address and attachments/links are legitimate?"
    - As in steps 1 and 2, look at the actual email address. It should match their genuine website (if you search through Google or another search engine).
    - Attachments can contain malware, so if you're not sure about the authenticity it's worth checking with your ICT or Information Security Team whether you can scan them for malware before opening.
    - You can hover your mouse over links to check where they will take you if clicked. This should be consistent with the sender's genuine website address.
5. "Can you contact the sender another way to verify it?" If you can speak to them in person, or over the phone (using a number you already have, or can find through their genuine website), that's the best way. You could also email them, but not by replying to the email they've sent you. Instead, create a new email and use the email address you already have, or one from their genuine website.
6. "Did you expect to receive it?" This is an important step: think carefully about how other people or organisations use email,and whether the email you're checking out fits in with this. If the timing or content don't fit, it's a warning sign. You could use the "can you contact the sender another way to verify it?" step here.
7. "Does it address you by name, not a generic greeting?" If some of the other criteria above are not checking out, and it's not addressed to you personally (particularly if it claims to be from a larger organisation whose technology should be able to address emails to you), it may well be phishing.
8. "Is the spelling, grammar and style what you'd expect?" Following on, if there are spelling or grammar mistakes, and/or a peculiar style, alongside other warning signs, that suggests it might be phishing.
9. "Does it ask you to act urgently or divulge information?" Equally, alongside other warning signs, adding time pressure or asking you to provide information is a classic sign of phishing.