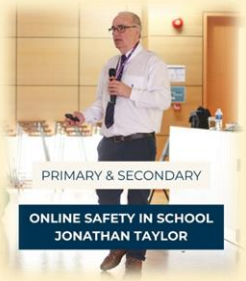
Online Safety for Schools



Recognising Online Spam or Scams

This guide is designed to help users recognise common phrases, introductions, and warning signs used in scam and spam emails. Scammers rely on urgency, fear, trust, and authority to trick people into clicking links, opening attachments, or sharing personal information.

Common Scam Email Introductions

- "Dear Customer" or "Dear Valued User" instead of using your real name
- "Greetings" "Good Evening" "My Dear" "Friend" "Dear Friend"
- "We have detected unusual activity on your account"
- "Your account will be suspended/closed today"
- "Immediate action required"
- "Final notice" or "Last warning"
- "You are entitled to a refund / compensation"
- "We are contacting you regarding a problem with your payment"
- "Congratulations! You have been selected"
- "A loved one has tried to contact you"
- "This message is from your bank / HMRC / NHS / Amazon / PayPal"

Common Phrases Used to Create Urgency or Fear

- "Act now" or "Respond immediately"
- "Failure to respond within 24 hours will result in…"
- "Your account has been compromised"
- "Suspicious login attempt detected"
- "Unusual payment activity found"
- "Legal action may be taken"
- "Your benefits may be stopped"

Requests That Should Raise Concern

- Requests for passwords or PIN numbers
- Requests for bank details or card numbers
- Requests to confirm personal information by clicking a link
- Requests to download or open attachments
- Requests to buy gift cards or vouchers
- Requests to move money to a 'safe' account
- Requests to pay a fee to receive winnings or refunds

Warning Signs to Look Out For

- Spelling or grammar mistakes
- Email address does not match the organisation it claims to be from
- Links that look odd or shortened
- Attachments you were not expecting

- Messages that pressure you to keep it secret
- Logos or branding that look slightly wrong
- Emails sent at unusual times

Safe Actions to Take

- Do not click links or open attachments
- Do not reply to the email
- Do not share personal or financial information
- Contact the organisation directly using a trusted phone number or website
- Delete the email or mark it as spam
- Ask a trusted family member or friend for advice
- Report scams to Action Fraud (UK) or your email provider

Remember: Genuine organisations will never rush you, threaten you, or ask for sensitive information by email.

Presented by: Jonathan Taylor MSc
www.onlinesafety4schools.co.uk
onlinesafety4schools@ymail.com

Online Safety 4 Schools

Online Safety 4 Schools