Cyber-Safe Detectives: Protecting Your Digital World

1. Risky. You should close the pop-up immediately and do not click on it or enter any personal details. (2 marks)

Working: The pop-up is a classic phishing attempt designed to steal personal data.

1 mark for identifying as risky, 1 mark for the correct action (closing/not clicking).

2. Risky. You should not reply to the message, block the user, and tell a trusted adult immediately. (2 marks)

Look for: Identifying the risk of sharing location/identity and the need to involve a trusted adult.

Good: It is risky. I should not tell them where I go to school.

Better: This is risky because they are a stranger. I should block them and tell my teacher or parent.

Best: This is a risky situation. I must not reply, block the user to prevent further contact, and report the incident to a trusted adult immediately.

What moves an answer up: Moving from 'good' to 'best' requires identifying the specific action of reporting to an adult, which is a key safety protocol.

3. Risky. You should use a strong password that is not related to your personal life, using a mix of letters, numbers, and symbols. (2 marks)

Working: Passwords containing birthdays or pet names are easy for others to guess or for software to crack.

1 mark for identifying as risky, 1 mark for suggesting a stronger, non-personal password.

4. Risky. The 'extra file' could be malware or a virus that harms your computer or steals your data. (2 marks)

Look for: Understanding that unknown downloads can contain malicious software.

Good: It is risky because the file might be bad.

Better: It is risky because downloading extra files can give your computer a virus.

Best: This is risky as the 'extra file' is likely malware designed to damage your device or steal personal information, so you should never download it.

What moves an answer up: The 'best' answer explains the 'why' behind the risk (malware/data theft) rather than just saying it is bad.

5. Check your privacy settings to ensure only friends can see it, and make sure the photo does not reveal your location or school uniform. (2 marks)

Working: Digital footprints are permanent; checking privacy settings limits who can see your data.

1 mark for mentioning privacy settings, 1 mark for mentioning checking for personal details/location.

What a secure answer looks like

A secure answer demonstrates an understanding that personal information should never be shared with strangers and that digital platforms require caution. Students should prioritise reporting concerns to a trusted adult.

If your child is stuck

Ask your child: 'If a stranger walked up to you in the park and asked for your address, would you give it to them?' Explain that the internet is just like that park, but with more people.

Common mistakes to watch for

Children often think that if a website looks 'official' or 'fun', it is safe. They also frequently underestimate how easy it is for others to guess passwords based on common personal details like pet names.