

# Kit's Cyber-Safety Challenge: Staying Secure Online

*Learning objective: To understand the importance of online safety, privacy, and how to respond to potential risks when using digital devices.*

Read each question carefully. Think like a digital detective! Use the provided definitions to master your internet safety knowledge.

## What is a 'Digital Footprint'?

The permanent record of all the websites you visit, messages you send, and photos you post online.

## What are the three essential rules for a 'Strong Password'?

It should be long, contain a mix of letters, numbers, and symbols, and never be shared with others.

## Define 'Phishing'.

When someone sends a fake message or email pretending to be a real company to trick you into revealing private details.

## What is 'Personal Information' that you should never share online?

Your full name, home address, school name, telephone number, or passwords.

## What should you do if you encounter something online that makes you feel worried or uncomfortable?

Tell a trusted adult immediately and use the 'Report' or 'Block' function.

## What is a 'Privacy Setting'?

A control on a website or app that limits who can see your profile, posts, and personal information.

## Define 'Cyberbullying'.

Using digital devices to intentionally say mean, hurtful, or threatening things to someone else.

## Why is it important to check if a website is 'Secure'?

To ensure your data is encrypted and protected from hackers; look for the padlock icon in the browser bar.

## What does it mean to be a 'Trusted Adult'?

A responsible person you know in real life, such as a parent, carer, or teacher, who can help you resolve online problems.

## Explain why 'Anonymity' online can be misleading.

People may pretend to be someone they are not (like a different age or gender) because they are hidden behind a screen.