

Digital Detectives: Internet Safety Mastery

Learning objective: To identify potential online risks, understand the importance of digital footprints, and apply strategies for staying safe, respectful, and responsible online.

Read each flashcard carefully. Test your knowledge by covering the answer side, then reflect on how you can apply these digital safety rules in your daily life.

What is a 'Digital Footprint'?

A digital footprint is the permanent trail of data, posts, photos, and interactions you leave behind whenever you use the internet.

Define 'Personal Data' and give three examples.

Personal data is information that can identify you. Examples include your full name, home address, school name, phone number, and passwords.

What is a 'Phishing' attempt?

Phishing is when someone sends a deceptive message or email pretending to be a trustworthy source to trick you into revealing sensitive information.

Why is it important to use a strong, unique password for every account?

Using unique, complex passwords prevents 'credential stuffing', where a hacker uses a password from one compromised site to access all your other accounts.

Explain the role of a 'Moderator' on a website or game.

A moderator is a person or software tool that checks content to ensure users are following community rules and staying safe from inappropriate behaviour.

What does it mean if a website address begins with 'https' and shows a padlock icon?

It means the connection is encrypted, which helps protect the data sent between your device and the website server from being intercepted.

What is the 'Think Before You Post' rule?

It is a reminder to consider the long-term impact of your digital actions, ensuring that everything you share is kind, accurate, and safe.

How should you respond if you encounter 'Cyberbullying'?

Do not reply, save the evidence (screenshot it), block the person, and report the behaviour to a trusted adult immediately.

Why should you be cautious about 'Privacy Settings' on social platforms?

Privacy settings control who can see your information, keeping them strict ensures that only your trusted friends and family can view your content.

Explain why you should never meet an online 'friend' in person.

Online personas can be fabricated. You have no way of verifying the true identity or intentions of someone you have only met through a screen.