Terminology

This activity will support you in establishing learner's background knowledge of the digital landscape and cyber resilience.

Introductory Questions

To begin conversations on the topic area, the following introductory questions could be discussed as part of a group:

What do you think of when you hear the word "cyber"?

Cyber - relating to or characteristic of the culture of computers, information technology, and virtual reality.

What does it mean to be "resilient"?

Resilient - able to withstand or recover quickly from difficult conditions.

Cyber Resilience

Provide learners with a copy of the explanation below. Ask them to highlight any words they haven't heard before or don't understand and discuss.

Being cyber resilience means being able to protect yourself from cyber attacks and being able to respond and cover if you are targeted.

Cyber attacks happen when someone attempts to gain access to a computer, computing system or computer network without permission, with the intent to cause damage.

Cyber attacks aim to disable, disrupt, destroy or control computer systems or to alter, block, delete, manipulate or steal the data held within these systems.

Extension: ask learners to come up with their own definition for 'cyber resilience'. This can then be used throughout the remaining activities.

Cyber Attack

Name an example of a way someone might attack your computer or network?

- Malware attack
- Phishing attack
- Password attack
- Cyber scams
- HMRC scam texts
- Delivery scam texts
- PayPal scam emails
- TV Licensing scam, emails and texts
- Social media competition scams
- Scam bank text messages
- Dating and romance scams