

Call spoofing training available

Published on 28 October 2025

Online training to help investigators understand call spoofing technology

News 2 mins read

Call spoofing is when criminals change their caller ID to hide the real source of the call, appearing as trusted organisations like banks or government agencies. For investigation teams, understanding this technology is crucial as it's behind thousands of fraud cases and affects how evidence can be analysed.

Fraudsters use readily available software to mask their real phone numbers, making traditional call tracing more complex. When investigating these crimes, teams need to understand the technical mechanisms behind spoofing to properly interpret evidence and build strong cases.

While there are legitimate uses for call spoofing – such as businesses displaying main customer service lines – the criminal applications create significant challenges for investigation teams trying to identify perpetrators and trace communications.

Specialist training

Online training has been developed specifically to help investigation teams understand call spoofing technology and its implications for evidence gathering.

The course covers essential areas including:

- what call spoofing is and types of spoof calls
- how spoof calls are technically created
- white SIM technology and its applications
- how call spoofing impacts digital evidence
- methods for analysing relevant datasets

To access the training you will need to log in to College Learn.

[Go to call spoofing training](#)

Related training

Strengthen your investigation capabilities this Cyber Security Awareness month by taking a look at our other e-learning courses. You will need to log in to College Learn to access this training.

- [eSIM awareness](#)
- [Deepfakes](#)
- [Dark web](#)
- [Cryptocurrency](#)

Tags

Cybercrime