AICC ARTIFICIAL INTELLIGENCE COLLABORATION CENTRE

Spotting AI Scams

What is an AI scam?

AI scams happen when someone uses AI to trick, imitate, or steal from others.

What makes AI different?

AI now makes scams more personal and believable. Scammers can use your online posts, emails, or social media to tailor scam messages just for you. This makes them seem genuine.

Remember: It's about TRUST... not fear

Here are simple steps you can take to avoid AI scams:

- **T** **Take a moment**, pause before you act
- **R** **Recheck**, double-check who is really contacting
- **U** **Use trusted sources**, only respond to official sites or numbers
- **S** **Stay calm**, don't let urgency or fear rush your decision
- **T** **Tell someone**, report it or share your concern

AICC ARTIFICIAL INTELLIGENCE COLLABORATION CENTRE

Spotting AI Scams

Here are some AI scams you should be aware of:

T

R

U

S

T

Voice Cloning

What it looks like:

- A phone call sounds like a family member, friend, or colleague asking for urgent help or money.

How it works:

- AI copies a person's voice from short clips online or social media.

Help to recognise it:

Unusual requests or tone. Check if they avoid video or follow-up by text. Examples: A "daughter" calls saying she's stranded and needs bank details to pay a taxi.

Deepfake Videos

What it looks like:

- A video shows a celebrity, politician, or boss saying or doing something unexpected.

How it works:

- AI edits real footage to make fake content appear real.

Help to recognise it:

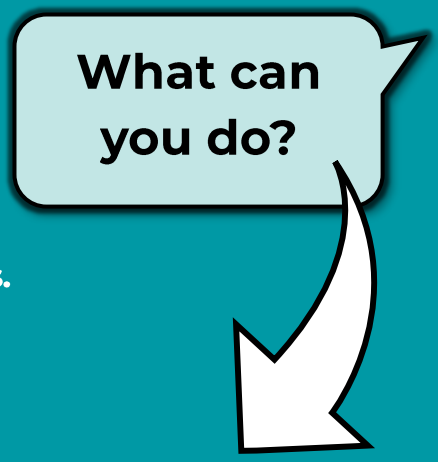
The speech looks slightly off, or a facial expression doesn't match the words. Examples: A fake video of a politician using racial slurs or offensive language.

Produced by the AICC – Responsible AI Hub: **aicc.co/responsibleai** (Created Nov 2025)

AICC ARTIFICIAL INTELLIGENCE COLLABORATION CENTRE

Spotting AI Scams

How to spot an AI Scam:



Step 1 : Check the source

- Use official websites or verified contact details.

Step 2 : Pause and think

- Scammers often try to make you act fast.

Step 3 : Verify people

- Call or message the person using known contact details.

Step 4 : Notice small errors

- Spelling, tone, or slightly wrong facts can give them away.

Step 5 : Listen carefully

- AI voices sound flat or emotionless. Respond unexpectedly to see how they react.

Step 6 : Protect your data

- Never share banking or personal information unless you are sure about who you are speaking with.

STOP	CHECK	ACT
Don't click links, open attachments, or reply	Verify using a trusted route by contacting them yourself	Report the scam and warn others after you secure your accounts

Produced by the AICC – Responsible AI Hub: **aicc.co/responsibleai** (Created Nov 2025)

AICC ARTIFICIAL INTELLIGENCE COLLABORATION CENTRE

Spotting AI Scams

Here are some AI scams you should be aware of:

T

R

U

S

T

Phishing with AI Chatbots

What it looks like:

- You receive a highly convincing message or email that seems like it was written by a real person.

How it works:

- AI analyses your social media and email patterns to personalise messages to gain trust.

Help to recognise it:

Use real interests or contacts but includes a suspicious link or immediate action to take. Examples: Hi John, I say your post of Facebook, here's more information about the event (including a strange link).

Fake Customer Support

What it looks like:

- You click a "support" link or phone number that looks official.

How it works:

- AI chatbots or fake websites copy real company branding.

Help to recognise it:

The website URL is slightly wrong (e.g., amaz0n-support.com). Example: You google "PayPal help" and a fake number is listed at the top.

Produced by the AICC – Responsible AI Hub: **aicc.co/responsibleai** (Created Nov 2025)