LiteHaus
INTERNATIONAL

Scam Awareness & Safety

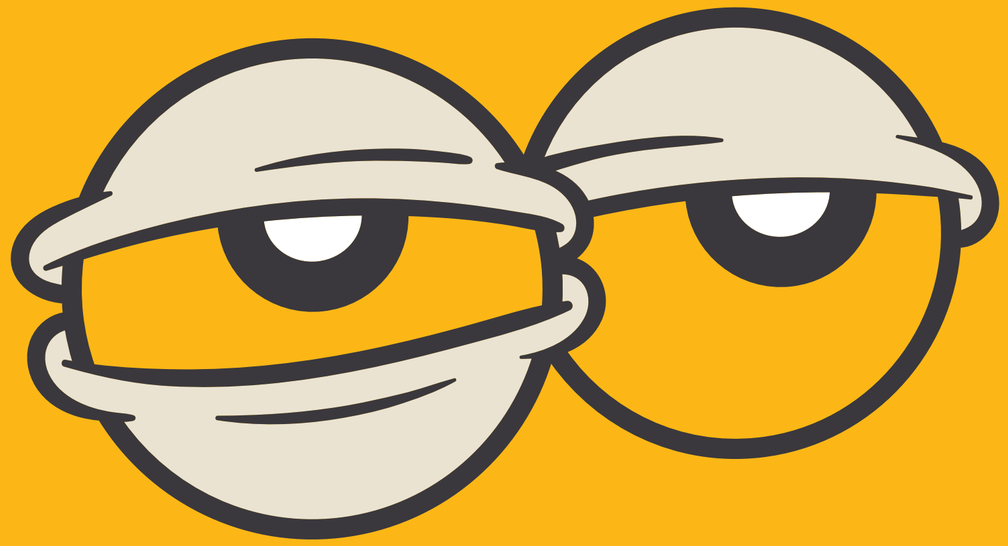
What is a Scam?

LiteHaus
INTERNATIONAL

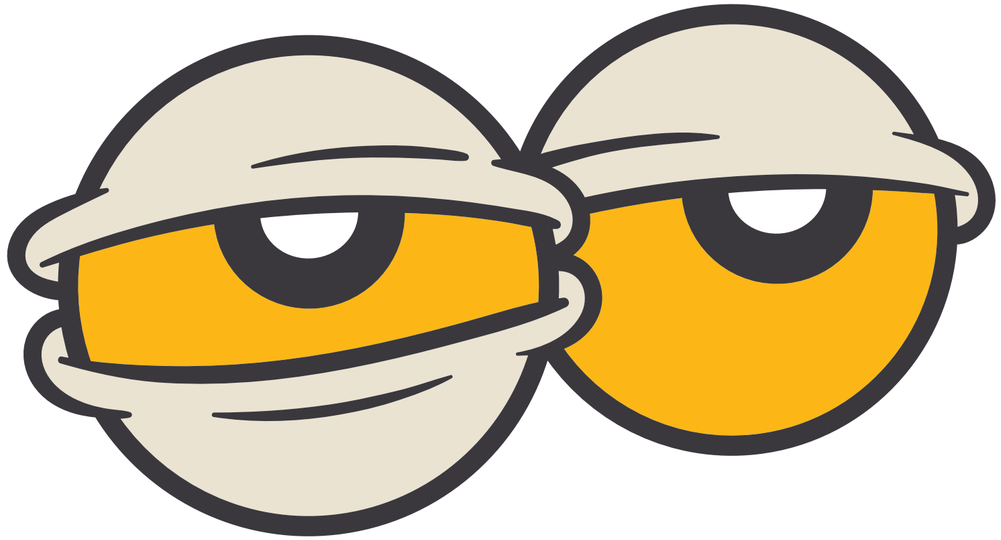
What is a Scam?

- A scam is an illegal trick, and a form of fraud.
- Scams usually try to solicit money or personal information illegally from people.
- Scams target people of all backgrounds, ages and income levels across Australia.
- All of us may be vulnerable to a scam at some time.
- •Scams succeed because they look like the real thing and catch you off guard when you’re not expecting it.
- Scammers take advantage of new technology, new products or services and major events to create believable stories that may convince you to give them your money or personal information.

Who do they target?



LiteHaus
INTERNATIONAL



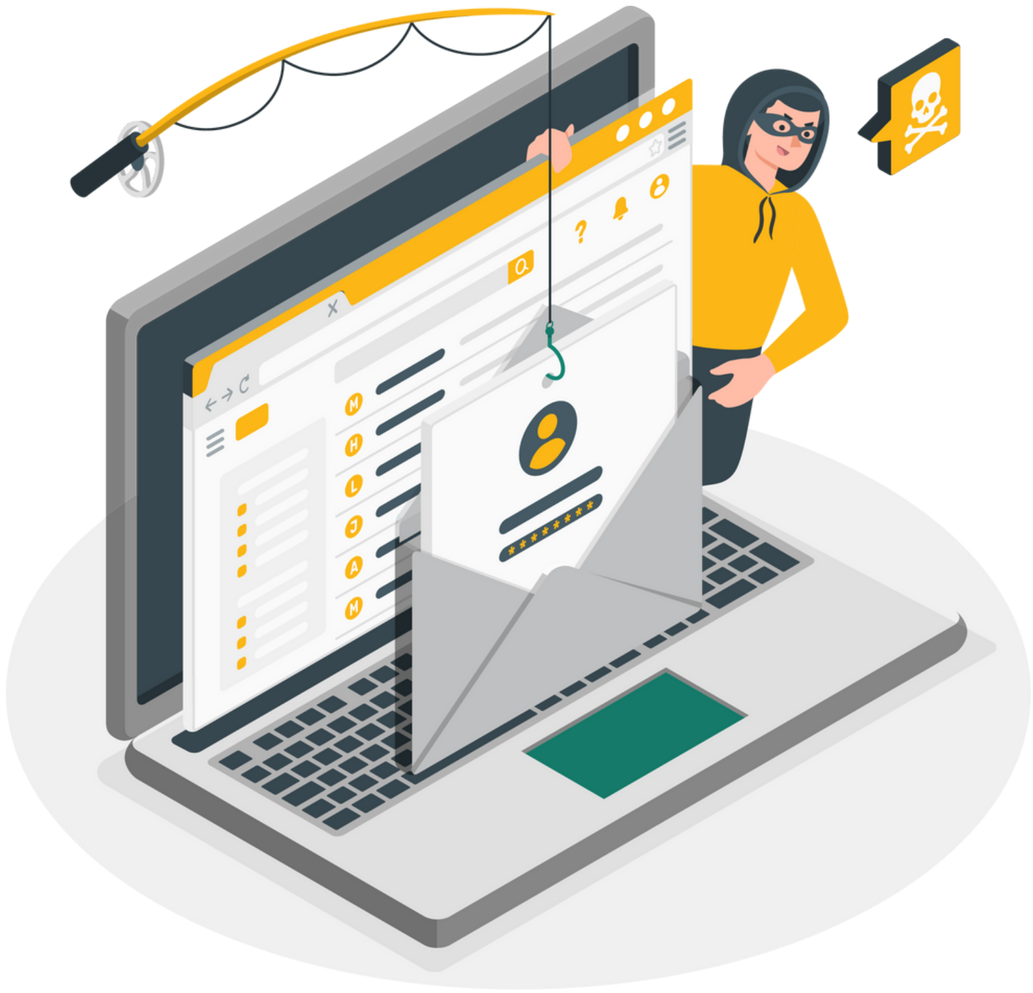
Who do they target?

Scams can target anyone, however, usually elderly people, teenagers, or people who are not so familiar with technology are targeted.

Scammers target these people because they perceive them as easier potential victims, less aware of online threats, and therefore more likely to trust them.

What to look out for with scammers

LiteHaus
INTERNATIONAL



Phishing

- Phishing is a form of fraudulent activity where scammers send emails pretending to be somebody they are not.
- Usually, scammers pretend they are from a well recognised company or public institution.
- Scammers may even go as far as pretending to be your boss of your company, a family member, or someone you know that is travelling overseas.

Phone calls & text messages

Scammers may call or text message you pretending to be from a big company most people use. Common examples include:

- telecommunications companies (i.e. Optus, Telstra, Vodaphone)
- banks
- E-commerce companies (i.e. Amazon)
- superannuation funds
- the Australian Taxation Office
- other Government departments.

Scammers may claim there is something that is wrong with your order, your account or your bills to secure personal information such as your name, phone number, credit card details, or customer registration numbers.

This is typically done under the guise of a survey.

These can often seem very authentic.

Websites

- Sometimes when you are exploring a website there might be an annoying pop-up or a completely new page on the website that you cannot go back on.
- You will have to close the tab to get rid of it, but often it may tell you there is a virus on your computer or you are being fined for illegal activity.
- This will require you to click and call ‘them’. At this point, a scammer may try to sell you a fake antivirus software or pay a bill.
- Scammers may even try to get remote access to your computer so that they can go through your files and get you to log into your bank.
- Scammers will do whatever they can to get money out of you.

Dating Apps

- Relationship scams are a significant issue.
- Scammers may fake an identity and build an online relationship with you, via dating sites or social media.
- Scammers may con you into thinking you are in a relationship, build your trust, before asking for money.
- They will ask for photos, etc that they can later manipulate and use to blackmail you. This is particularly prevalent as artificial intelligence (AI) apps grow in usage.

How to deal with scammers to prevent being scammed

LiteHaus
INTERNATIONAL

How to deal with scammers to prevent being scammed

- Trust your instincts. If something does not feel ‘right’, it probably is not.
- Never send money to anybody you do not know, especially if they have contacted you randomly.
- Avoid clicking on links which feel ‘dodgy’.
- ·Seek advice from your parent or guardian, or a teacher. They would rather you ask now than have to help you once it is too late.
- Do your own research. The Federal e-Safety Commission. **Video: Connecting safely online**

If you find yourself facing scammers and they are continuing to trying to contact you, do the following:

Block their numbers/emails.

Report them to the Federal e-Safety Commission.

Record and screenshot anything that may help with the reporting, this can be used to build a case for you.

Speak to your parent or guardian or a teacher for help.

Lookout for yourself and lookout for others, if you see signs you need to try and help.

Sometimes people can be so stuck into the belief of the scam that they refuse to believe otherwise. Be patient with them and continue to do the right thing, help them to see the flaws in the scam.

What if I am scammed?

LiteHaus
INTERNATIONAL

What if I am scammed?

If you are scammed you have the following options:

- If it is immediate threat to life or risk of harm, call 000 and report to the police immediately.
- Speak with your parent or guardian or a teacher, immediately.
- Report the incident to cyber.gov.au and they will take the case and try to help you.

The Queensland Government offers many training programs in digital skills.

Some areas include:

- Cybersecurity
- Coding
- Data Security
- And much more if you are interested in other areas.

Any Questions?

LiteHaus
INTERNATIONAL