

IDENTITY THEFT

Did you know that logging into someone's email or social networking account without their permission could be illegal? Or that pretending to be someone else online could be identity theft? Find out what identity theft is and how you can prevent it by reading this factsheet.

What is identity theft?

Identity theft is when someone pretends to be someone else to get a benefit or cause harm. An identity thief collects personal information about another person, such as their name, address, date of birth and passwords, and uses that information to take on the other person's identity.

Facebook, Twitter and YouTube all ban this type of behaviour.

Is identity theft illegal?

Yes. It is illegal to have anyone else's identity information with the intention of committing a crime. It is also illegal to make, supply or use identity information with the intention of committing a crime.

For example, it is illegal to use someone's name or photo to create a fake online profile of that person with the intention of harassing them. That's because their name and photo are identity information and online harassment is a crime.

Did you know...

Online, it is illegal to:

- Access or change password-protected information on purpose and without permission. For example, logging into someone else's email or social networking accounts without their permission.
- Access or change information held in a computer without permission in order to commit a serious crime. (A serious crime is a crime that has a long prison sentence, like identity theft or fraud.) For example, logging into someone else's email or social networking accounts without their permission to impersonate them or steal something that belongs to them.
- Intercept (look at or stop) any communication passing over the internet. For example, hacking a wifi connection to read someone's email.
- Menace, harass or offend someone. For example, posting threatening messages on someone's Facebook wall.
- Trick someone to get something. For example, using someone else's credit card number to buy stuff without their permission.



How does identity theft happen 'online'?

Making fake profiles

Creating or using profiles on social networking sites under a fake name or using another person's identity is 'identity theft' and can be illegal.

Some social networking sites also have their own rules about creating more than one profile per person or creating profiles under fake names. Profiles breaking those rules may be removed from the site.

Example

Samantha created a Facebook page using Kelly Parker's identity information and photo under the name 'Kelly Porker'. The identity information Samantha used included Kelly's home address,

her school, date of birth and some photos. Samantha's actions could be considered identity theft with the intention of committing a crime – cyber bullying and online harassment.

Hacking into real profiles

An identity thief may be able to get into your online accounts in a few different ways. For example, you or someone you know might give them your password. Or they might use a computer or smart phone that has your log-in information saved.

An identity thief may also be able to hack into your online accounts by guessing the answers to your security questions. Any details you post to your profile—like your school and your favourite bands—may be used as clues to guess the answers to these questions. Once a person answers the security questions correctly, they can change your password and lock you out. A number of Facebook accounts have been taken over this way.

Finally, some computer viruses are programmed to record your log-in details and pass them along to identity thieves.

Example

15 year old Leon wanted to play a prank on his friend Jason. He thought it would be funny to log onto Jason's email account and send emails to their friends to embarrass Jason. Leon knew Jason's password because Jason had told it to him one time when they were online at Leon's house. Using the password Jason had given him, Leon logged on to Jason's account, and he read and deleted some of the emails in Jason's inbox. Then he sent an

email to Jason's girlfriend, calling her names and telling her that he wanted to break up. Leon was worried Jason would find out so he changed Jason's password to make it difficult for him to log in again.

Because Leon logged on to Jason's email without Jason's permission, he has committed a crime. Even if someone tells you their password, using it to get into their account without their permission is against the law. If Leon logged on to Jason's account with the intention of harassing Jason's girlfriend, he might also be charged with identity theft.

What can I do to prevent identity theft?

- **Be careful with passwords.** Avoid sharing them with others. Pick passwords that aren't easy to guess, and that have a combination of numbers, symbols and capital and lower case letters.
- **Be careful when picking security questions.** Avoid questions that can be answered using the information on your profile. Pick questions that aren't easy to guess.
- **Be careful when using a public computer, or when letting other people use your computer or smart phone.** Make sure to log out of your accounts on public computers, and to click "don't remember my password". Think about setting up a pin number for your smart phone or a password for your computer so people can't use them to get into your accounts without your permission.
- **Be careful when shopping or banking online.** Avoid buying stuff on websites that seem dodgy.

- **Be careful with your information on social networking sites.** Avoid adding people you don't know or trust and limit the amount of information you share.
- **Be careful when clicking links or downloading files.** Avoid downloading files from people or sites you don't know or trust.
- **Use antivirus software and keep it up-to-date.**

What can I do if I think my identity has been stolen?

- Report it to the website administrator (e.g. Facebook, Twitter and YouTube)
- Contact [ACCC SCAMwatch](http://www.scamwatch.gov.au)
 - <http://www.scamwatch.gov.au>
 - Phone: 1300 795 995
- If you have a question or need legal advice you can send a **Lawmail** at www.lawstuff.org.au/nsw_law/LawMail. Lawmail is a FREE legal advice and information service.

Other useful links

For useful tips and information on being safe online, check out the following websites:

- www.cybersmart.gov.au
- www.staysmartonline.gov.au/teens
- www.thinkuknow.org.au

This information was last reviewed on 10 April 2012. This factsheet provides information about the law in NSW. It does not provide legal advice. If you need advice, or if you would like information about the law in a state or territory other than NSW, please send us a Lawmail at <http://www.lawstuff.org.au>