talk money with Ecstra Foundation

Finance facts: Identity theft

What is identity theft?

Identity theft occurs when someone (a 'scammer') pretends to be you and uses your personal information without your permission. This information could include your name, birth certificate, student ID card, library card, Tax File Number, Centrelink Reference Number, credit card details, or any other data that helps to identify who you are or how to find you. They might use this information to open credit cards, make purchases, or even take out loans in your name, which can mess up your finances and cause many headaches.

Identity theft can also extend to stealing your online identities, such as social media accounts. If someone gains access to your social media accounts without your permission, they can impersonate you online, potentially posting harmful or misleading content or even scamming your friends and followers. This can damage your reputation and is as upsetting as someone stealing your personal information for financial gain.

Did you know?

- Identity theft is a growing problem
- Identity theft refers to the use of identifying information of an actual person (living or dead) instead of a fictitious identity
- Scammers may only need to obtain a small amount of your personal information if they can find out more about you from public sources.

How do you prevent identity theft?

Identity theft can happen to anyone. Scammers have stolen and used the identities of people of all ages and walks of life.

You can reduce your risk of identity theft by taking some simple steps to protect your personal information:

- Always keep your personal information secure
- Ask questions before you share your information
- Use strong passwords and add an authentication step
- Be alert and check your bank details and personal details regularly.

Passwords

These days, passwords are the key to our online lives. If someone gets hold of your password, they can access your email, social media, bank accounts, and more. That means they can pretend to be you and do things you don't want them to do, like stealing your money, sending messages pretending to be you, or accessing your private information.

It is very important to protect your password and never give it out to anyone, not even your friends. By keeping your password safe, you're protecting yourself from identity theft and other online threats.

How to protect your passwords

A weak password is an easy way to become a victim of fraud! Passwords that are easily guessed include ones with your name, your date of birth, or a pet's name. It's crucial to use strong, unique passwords for each account and never share them with anyone you don't trust. If the number of accounts you have has become too large to manage, it may be worth looking into buying an app that keeps your passwords stored securely and random password generators that will select a unique password.

Six tips for setting up secure passwords:

1. Set up secure passwords to begin with. Ensure the password is 12 or more characters long, including punctuation marks throughout and upper-case and lower-case letters
2. Don't always use the same password
3. Keep passwords in a safe place offline and online
4. Install anti-malware software on your computer
5. Use multi-factor authentication
6. Be vigilant.

Did you know?

Multifactor authentication requires users to provide two or more pieces of evidence, or 'factors', to verify their identity. These factors often include:

- Something you know—password or PIN
- Something you have—a smartphone or a security token that generates a temporary code
- Something you are—biometric data like fingerprints, facial recognition or voice recognition.

Finance facts: **Identity theft**

Beware of phishing emails and messages

Phishing is like fishing, but instead of trying to catch fish, scammers are trying to catch your personal information. They do this by pretending to be someone trustworthy, like a bank or a company you know, and sending you emails or messages asking for sensitive information like your passwords or credit card numbers.

These messages often look real, but if you give them your information, the scammers can use it to steal your money and do other things you don't want them to do.

So, it's important to be cautious and never share personal information in response to unsolicited messages.

If you've accidentally opened a phishing email but have not clicked or downloaded anything, be sure to:

1. Unsubscribe
2. Mark it as junk email so that your email account can do a better job of sending malicious emails directly to your spam folder
3. Scan your computer for ransomware, viruses or other malware, just in case.

If you have clicked on a link in a phishing email or message, do not panic and follow these steps:

1. **Disconnect your device:** This will reduce the risk of malware spreading to other devices on your network, prevent the malware from sending out sensitive information and keep someone from remotely accessing your device
2. **Back up your files:** If you regularly back up your files using methods like an external hard drive, a USB thumb drive or cloud storage, then you may only need to back up files that have been updated or created since the last backup
3. **Scan your system for malware:** After you have disconnected your device from the Internet, run a complete scan with your antivirus program
4. **Change your credentials:** Malware may be used to grab your sensitive information, including online usernames and passwords, credit card and bank account numbers, and other identifying information.

Case study: Adam's drivers licence

When Lian took her son Adam to get his driver's licence, she expected to witness an important milestone in his life. Unfortunately, she was met with a shocking surprise—he had already been issued with a driver's licence.

After a police investigation, it was discovered that the scammer had obtained Adam's personal information from a phishing email to obtain the fake licence. The scammer had created a number of fake identities from phishing emails and used that information to obtain credit cards. It took a number of years to resolve the issues this created for Adam.

Glossary

Malware	is short for malicious software. Malware is a file or code, typically delivered over a network, that infects, disrupts or gives unauthorised access to a computer system by an attacker.
Phishing	is a type of cyber-attack in which a scammer disguises themselves as a trustworthy entity to trick individuals into providing sensitive information. It is usually done through deceptive emails, messages, or websites that mimic legitimate sources.
Scammer	someone who tries to trick people into giving them money or personal information dishonestly. They often use deceitful tactics, like pretending to be someone trustworthy or creating fake offers or opportunities to lure their victims. Scammers can operate through various channels such as phone calls, emails, text messages or social media.

Links

eSafety Commissioner—Identity theft

Scamwatch

ASIC—Financial Scams

About Talk Money with Ecstra Foundation

Talk Money with Ecstra Foundation is designed to help Australian students learn money lessons for life, to be confident talking about money and to make informed financial decisions. We offer facilitator led workshops for Years 5–10 students and additional resources to reinforce learnings. The program is provided at no cost to schools, enabling more students across Australia to access financial education at key life stages.

About Ecstra

Ecstra Foundation is an independent charitable foundation committed to building the financial wellbeing of Australians within a fair financial system. Ecstra launched Talk Money in February 2022.

talkmoney.org.au

1800 651 636

talk@talkmoney.org.au