Australian Government
Serious Financial Crime Taskforce

We're targeting:

Cybercrime affecting the tax and superannuation systems

Financial crime is constantly evolving, and technology plays an increasingly significant role.

The Serious Financial Crime Taskforce (SFCT) is hardening Australia's tax cyber ecosystem by putting in place new strategies to protect Australians from these criminals through collaboration with the community and key government stakeholders, both domestically and internationally.

We are strengthening capability across government agencies to identify and deal with cyber criminals. We also want to help you to make sure you don't fall victim to identity theft, scams, or cybercrime.

Criminals we are on the lookout for:

Cyber Criminals use technology to gain access to information and sensitive data which can be used to facilitate a range of crimes, including tax crime and identity theft.

There are a range of different kinds of cyber criminals including:

- data thieves | hackers | phishers | code writers | data buyers

These criminals could be anyone from a teenage hacker living next door to a member of an offshore crime syndicate.

Behaviours to look out for:

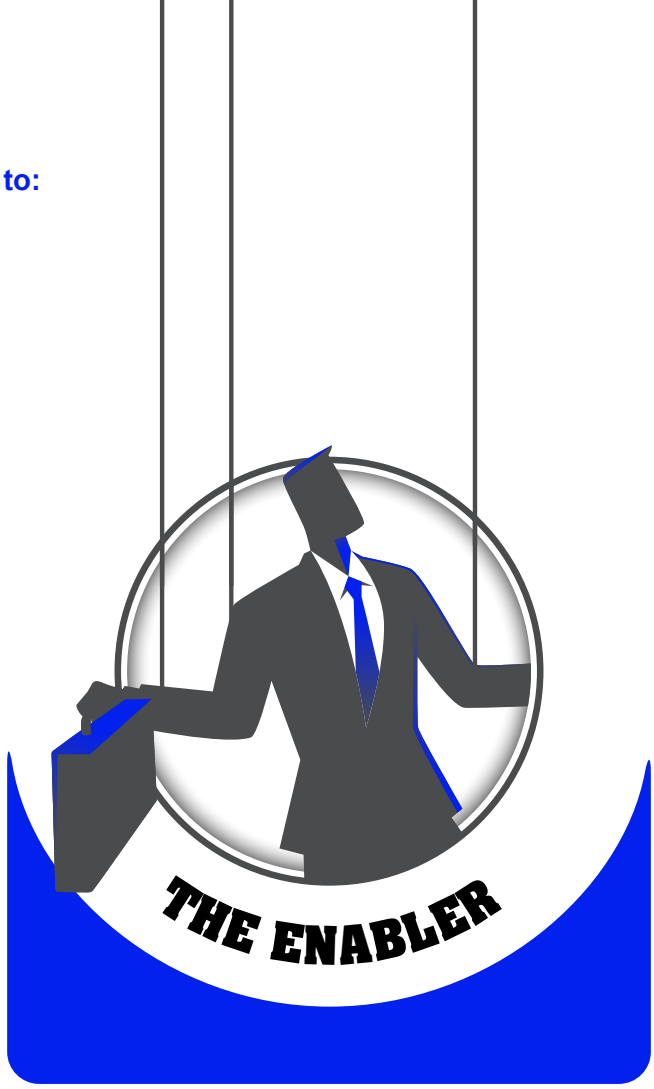
- They often use illegal marketplaces (facilitated by the dark web) to enable the sale of illicit goods, services and information.
- Crime is provided as a service. For example, some criminals sell names and information related to individuals and criminal syndicates. Other criminals buy and then use these identities and information to carry out serious financial crimes that harm people, businesses, banks and government agencies (and therefore the Australian public).
- Stolen identities and information, and phishing schemes can be used to steal from superannuation and share trading accounts, and purchase goods and services using the victim's funds and ID.
- Meanwhile, others provide hacking services, or 'testing services' that seek to compromise the security and information of government agencies, banks, businesses and other organisations.

Other criminals The Cyber Criminal can be linked to:

Work by the SFCT reveals that most serious financial crime schemes are overseen by a 'controlling mind' who is the key instigator and beneficiary of the financial crime. Often, these individuals are members of or linked to organised (international) crime syndicates or groups.

Hardcore criminals offend whenever opportunities arise and work with professional 'enablers' to conduct and conceal their crimes.

Proceeds of serious financial crime may be used to fund other crimes that cause considerable harm to the community – such as drug and human trafficking, sexual exploitation and terrorism.



Professionals who use their skills, structures and networks to help facilitate serious financial crime.

Enablers can work in a wide range of professional roles such as lawyers, accountants, tax advisers, labour providers, service providers or bankers.

As enablers require advanced professional skills, as well as a network that facilitates interaction with other criminals, many may be older or more advanced in their careers.

How you can help:

- Protect yourself: Individuals and businesses can be targeted by cyber criminals – ensure that you have security measures in place to protect your information.
- Be cautious using free Wi-Fi hotspots. They're unsecure networks so it's easier for cyber criminals to intercept your information. Avoid making financial and tax transactions when you're connected to public Wi-Fi.
- Never click on links, open attachments or download a file in emails, text messages or social media posts unless you are sure the message is genuine.
- Take notice of unusual activity in your accounts and report it straight away.

If you have a tip-off or any concerns, please call the ATO tip-off hotline on **1800 060 062** or go to **www.ato.gov.au/SFCT** for further information.