

MEDIA RELEASE



Michael Daley MP
Minister for Police

John Hatzistergos MLC
Attorney General

Tuesday 27th July 2010

Would You Post that on a Billboard? Then Don't Post it on Facebook

NSW Attorney General John Hatzistergos and Minister for Police Michael Daley today urged NSW residents to be aware of new, increasingly sophisticated forms of fraud and ID theft.

Speaking at a conference on fraud and ID theft organised by Crime Stoppers, Mr Daley said that NSW Police detectives were seeing new scams, where personal information gleaned off social networking sites was then used to target victims over the phone, or by email.

"For all its benefits, technology has made it easier than ever for criminals to separate people from their hard-earned money," he said.

"In the past, criminals have sourced their information about an individual by rummaging through garbage bins for bank statements, tax returns, any documents which can be used to compile a profile on a person.

"These days, social media and networking sites are routinely 'surfed' to compile a profile on a target individual.

"The people compiling the profiles are not necessarily the people who will scam you. The information-compilers will often on-sell their data to scammers," Mr Daley said.

The advice follows new figures released by the Attorney General showing that since new laws targeting identity crime were introduced, police have issued some 50 court attendance notices. The DPP has also advised that 18 matters involving 111 counts are currently being prosecuted in the District Court.

"These new offences, which commenced on 22 February this year, recognize that crime is evolving, and that criminals are now dealing in information that can be used by others to commit crimes like fraud" Mr Hatzistergos said.

The laws make it a crime to sell, use, or possess identification information with criminal intent.

"These figures showing the number of charges since the laws commenced demonstrate that Police are working hard to stamp out a crime that costs the Australian community nearly \$1 billion a year" he said.

Mr Daley gave an example of a recent scam through which a woman was told in an online chat room that they thought their mum went to school with the target's mum.

The alleged offender then asked for the victim's maiden name – a common security question for various accounts to verify a person's identity.

Mr Daley said that once a scammer has personal information such as your date of birth, address, occupation or mother's maiden name – it can be very easy for them to convince a victim that they are from a legitimate Government agency.

"There have been approximately 120 reports since mid-February of a new scam that involves the scammer contacting the victim, and purporting to work for the Australian Tax Office or another Government Agency or a bank," he said.

"These scammers use information gleaned off social-networking sites or chat-rooms to convince their target that they are from a legitimate organisation.

"Scammers are typically excellent salesmen, they are people who can 'read' individuals.

"They know how to appeal to a person's weaknesses, be it a person willing to pay money to secure a fictional lottery win in Nigeria or a beautiful Russian bride.

"So I'd ask the community to protect their online information and to remember that if the offer is too good to be true, it probably is," Mr Daley said.

Tips and Hints:

- Never put any information about yourself on a social networking wall that you would not feel comfortable also putting on a billboard on a busy road;
- Is the person who wants to be "friended" actually who they say they? Make sure you know the people you are adding as friends;
- Ensure your security settings are up to date and your page is not available to everyone.
- Information which can be used by criminals includes; date of birth, address, photos and images suitable for ID Theft, occupation, pets names (a common password choice), when people are going on holidays, or information about the purchase of a new home, car or holiday house.

Background:

In the current scam, the offender convinces the recipient that they have been selected from a number of people who are eligible to claim a reward for continually paying their taxes or they have been overcharged bank fees or Government fees.

The caller promises to have funds electronically sent to their bank account if the details of this (with other personal identification details) are supplied verbally.

The details provided then allow the offender to withdraw funds from the victim's bank account.

The offender could also request that money be sent via Western Union as a form of "advance". This is represented as a Service Fee, Transfer Request or a Rebate Fee.

Very recently these representations have been made by email, with very authentic looking logos and a convincing, but fake, Tax Office form. The email may also direct victims to a bogus ATO website and request personal identification and financial information.

Any person who believes they may have received such telephone call or email of this nature is advised to report the matter to the local police.

Under no circumstances should they respond to or engage in further communication with the caller / sender of suspicious email.