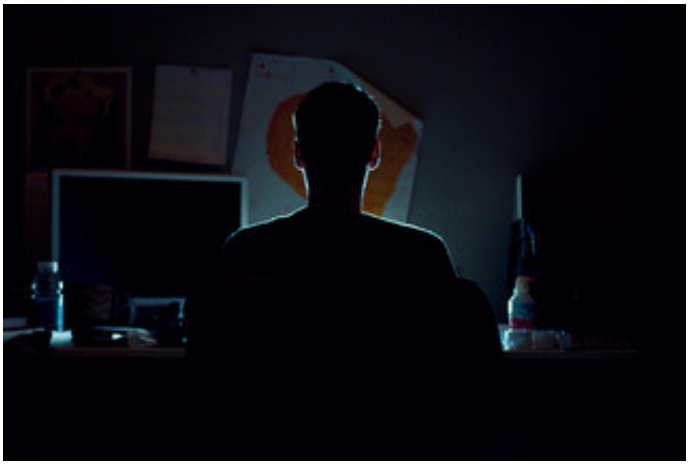
How to tackle cyber crime before people even know they're a victim

March 19 2015, by Cassandra Cross



What if the police told you that you were being scammed – would you continue to send money? Credit: Flickr/jacobfg , CC BY-NC-ND

An estimated A$75,000 is lost by Australians everyday to online fraud, according to the Australian Competition and Consumer Commission (ACCC).

Given that this is based on reported crime, the real figure is likely to be much higher. It is well known that fraud, particularly online fraud, has a very low reporting rate. This also doesn't even begin to encompass non-financial costs to victims. The real cost is likely to be much, much higher.

There are many challenges to policing this type of crime, and victims who send money to overseas jurisdictions make it even harder, as does the likelihood of offenders creating false identities or simply stealing legitimate ones.

But despite these challenges police have started to do something to prevent the impact and losses of online fraud.

By accessing financial intelligence, police are able to identify individuals who are sending money to known high-risk countries for fraud. They then notify these people with their suspicions that they may be involved in fraud. In many cases the people don't even know they may be victims or involved in online fraud.

Project Sunbird

This proactive approach was originally pioneered by Queensland Police Service. Another example is Project Sunbird, a collaborative project between the West Australian Police (WAPOL) and the West Australian Department of Commerce (Commerce) which first started in 2012.

Project Sunbird focuses on people who are sending money to five known high-risk countries in West Africa: Nigeria, Ghana, Benin, Togo and Sierra Leonne. This is not to say that these are the only countries involved in fraud, rather it recognises that a large amount of money is transferred to these "hot spot" countries.

There are five stages to Project Sunbird: identification; intervention;' interruption; intelligence; and investigation.

Identifying potential victims is conducted by WAPOL, who access financial intelligence of individuals who are sending money to these five specific countries. They screen this list to formulate a list of individuals

they suspect are fraud victims.

This list is passed to Commerce, who send a letter to each person, notifying them that they may be victims of fraud. The letter encourages the individuals to stop sending money and invites them to contact Project Sunbird staff to discuss.

If they continue to send money, they will receive a second more targeted letter, which outlines further details of their likely involvement in fraud and provides a fact sheet for fraud victims.

The third stage is focused on the interruption of payments and funds transferred to West Africa and is primarily undertaken by Commerce.

The fourth stage is the gathering of intelligence from letter recipients from both agencies which feeds into the fifth stage, being the investigation, which is led by WAPOL and can focus on local offenders if relevant, or make the appropriate referrals to an overseas law enforcement agency.

Sunbird shows promising results

Initial results from Project Sunbird have been very positive. Between March 2013 and July 2014, 1,969 first letters were sent to individuals.

Financial intelligence indicates that approximately two thirds (66%) stopped sending money, with a further 14% reducing the amount of money transferred (transactions are examined three months prior and three months subsequent to the month the letter is received). Of those who continue to send money and receive a second letter, 44% stopped sending money and a further 33% reduced the amount being sent.

While these early results indicate the success of Project Sunbird, the

displacement effect of this approach is unknown. Analyses are currently unable to determine if victims stop sending money altogether, or if they simply stop sending money to the five countries currently targeted, and continue to send money to other countries.

The types of fraud uncovered by Project Sunbird are many and varied. These include romance, investment, lottery and inheritance fraud to name a few. The reach of offenders and their ability to manipulate and exploit victims is endless.

Individual reactions to receiving this letter are generally positive. For some, it was literally a lifesaving letter, with two individuals contacting WAPOL to advise that they were on the verge of suicide prior to receiving the letter.

While many are unaware that they are being defrauded, others have suspicions and the letter may be an important step in helping them to recognise and confirm their fraud involvement. It also provides a non-threatening means of discussing this with police, which is vital given the stigma and negative stereotypes associated with this type of victimisation.

The intelligence advantage

The use of financial intelligence provides an important shift in the way police deal with online fraud, to a proactive, victim oriented approach, compared to the more traditional reactive, offender based methods.

Australia is fortunate to have infrastructure in place whereby the financial intelligence needed by police to identify potential fraud victims is available to them. Not all countries have this information available to them, which limits their ability to implement a similar approach.

This approach also recognises online fraud as a legitimate crime type, which can have devastating consequences for its victims. By intervening in such a proactive manner, it is attempting to reduce and limit the losses incurred by unsuspecting victims. It is much easier for police to interact with a victim early on who has only lost a small amount of money, compared to picking up the pieces further down the track when the victim may have lost everything.

The South Australian Police have now launched a similar project based on the Sunbird model. In addition, the ACCC launched the National Scam Disruption project in August 2014, taken from the Sunbird approach which targets potential victims in New South Wales and the Australian Capital Territory.

In December 2014, the ACCC reported that it had contacted 1,500 potential victims, of which 60% had stopped sending money (similar results to Project Sunbird).

At this stage however, no other jurisdiction in Australia or overseas has implemented the collaborative approach used in Project Sunbird, with either police or a consumer protection agency taking sole ownership in their jurisdiction. There is currently no national, coordinated approach in Australia.

Some still send money

Despite its initial success, this approach is not foolproof and there are individuals who continue to send money overseas despite police intervention.

For these people, their journey to the realisation of their true circumstances will take a little bit longer (if at all). There is also the possibility that some will continue to send money to countries outside the

five currently targeted.

There is still much work to be done, including the obvious potential to expand this approach to all Australian jurisdictions and encompass a wider number of countries.

But Project Sunbird represents a small light in what can seem like a never ending tunnel on tackling cyber crime.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation