Fighting high tech crime

Modern technology and the popularity of the internet have led to the emergence of new crime types on a global scale.

High-speed internet connections have increased the speed at which criminals can steal information such as usernames, passwords and financial information.

Rapid growth in internet use from the mid 1990s and the simultaneous increase in cyber crime in a world suddenly without geographic limits meant traditional law enforcement approaches were less effective. A coordinated national approach that connected to international law enforcement was the only way to beat crime online.

The Australian High Tech Crime Centre (AHTCC) was formed in July 2003, and right from the beginning it harnessed expertise from across both the public and private sector to deal with this unfamiliar form of crime. In a global law enforcement first, the AHTCC seconded employees from the five major banks to work side-by-side with police to investigate the financial impacts of cyber crime.

To discover levels of online criminal activity, the AHTCC seconded staff from the Australian Bureau of Statistics and researchers from the Australian Institute of Criminology. Secondees from Customs and the Australian Securities and Investments Commission focused on detecting and deterring online criminal activities within their areas of expertise while those from the Department of Defence concentrated on protecting the national information infrastructure.

In addition, members of State and Territory police forces were seconded to the AHTCC, an important step in ensuring that online crime could be investigated and prosecuted no matter where in Australia it occurred. Strong partnerships with industry were also key, especially in the banking and finance sector, the telecommunications sector and particularly Microsoft.

Another initiative was to provide easily accessible forms on the AHTCC website so members of the public could report any type of online crime.

Following two reviews of the capacity to deal with technology enabled crime, on 1 March 2008 the AFP formed a new functional area, High-Tech Crime Operations, which absorbed the AHTCC.

The HTCO portfolio focuses on combating all types of cyber-crime, including online fraud, phishing, mule recruitment, computer intrusion and online child sex exploitation. HTCO is also responsible for all covert surveillance activity undertaken in the AFP, including telephone interception.

Phishing is the use of spam emails purporting to be from a legitimate bank, and usually containing links to fraudulent websites with the intent of gathering a person's internet banking logon details.

Mule recruitment is an attempt to get a person to receive stolen funds using his or her bank account and then transfer those funds to criminals overseas. These bogus jobs are often advertised on the internet, or offered in spam emails.

National Coordinator High Tech Crime Investigations Peter Sykora has led the HTCO Investigations and Intelligence teams since July 2007. Federal Agent Sykora first joined the AFP in August 1985, and is an experienced investigator.

In addition to Canberra-based staff, Federal Agent Sykora is responsible for managing teams in Sydney and Melbourne, including investigators from the major banks who work alongside AFP members as part of the Joint Banking Finance Sector Investigation Team (JBFSIT) to help stop internet banking fraud.

The JBFSIT, which was formed in 2004, conducts investigations relating to internet banking fraud, phishing and related criminal matters, including fraudulent job recruiting websites and identity theft.

"The AFP's Joint Banking Finance Sector Investigation Team is a unique model, and one of the world's first," Federal Agent Sykora said.

"A lot of our work is very different to the traditional policing model, and is based on mitigation, prevention and education."

The JBFSIT receives information every day from a number of financial institutions. It collates regular reports for the Banking and Financial Services sector which outline emerging trends and issues.

The Internet Policing Team is another important component in the fight against internet crime. Recently highlighted in the ABC's Four Corners television program, the team works to shut down underground forums where hackers sell malicious software, mule recruitment websites and online paedophile networks.

One of the difficulties faced by the Internet Policing Team is that many of the websites used by criminals are hosted overseas. Internationally, the AFP collaborates with policing organisations such as Interpol, the FBI, the Royal Canadian Mounted Police and New Zealand Police as part of the global response to cyber-crime. They share information about suspect websites and work together to shut them down and prosecute the offenders who either create the sites or use them for illegal activities.

In many cases, the best option for policing organisations is to shut down access to offending websites by disabling the Internet Protocol (IP) address that the site is using.

A recent success for HTCO was Operation Carpo, which was carried out in collaboration with Western Australia Police. A Perth man was arrested for possessing 56,000 credit card details, 53,000 usernames and passwords, and 110,000 domain names.

Botnets are networks of computers used by criminals to gain unauthorised access to computers, gather usernames and passwords, or conduct denial-of-service attacks. Criminals use malicious software to infect computers, which in turn spread the virus to other computers and create the botnet network.

"The AFP works in partnership with the Defence Signals Directorate (DSD) and the Australian Security Intelligence Organisation (ASIO) to mitigate attacks on Australia's national information infrastructure," Federal Agent Sykora said.

Regular meetings are held by the AFP, DSD and ASIO to form and implement strategies to prevent, mitigate and investigate online attacks.

The AFP also runs educational campaigns to teach the public how to protect themselves from internet crime. As an example, the ThinkUKnow campaign is aimed at teaching parents, teachers and carers how to keep children safe from internet sex predators.

The AFP is a sponsor of the International Youth Advisory Congress which gives young people from around the world an opportunity to meet and discuss cyber-safety and put forward ideas on how to help their peers use the internet safely.

"The AFP will continue to intercept and prevent online crime," Federal Agent Sykora said.

"Our ongoing commitment is to stay at least one step ahead of the criminals who are involved in any form of online crime."

01: Federal Agent Peter Sykora