Getting to the heart of the matter

01: Carolyne Burge

Putting an end to online banking crime provides more than enough motivation to come to work each day.

Ten years ago, Carolyne Burge worked in one Australia's 'Big Four' banks, examining cheques to determine whether they were genuine. Over the past decade, scams to prise money from unsuspecting victims have dramatically increased in form and volume, and Carolyne's job has evolved too.

Today, she works for the Australian Federal Police, investigating a wide variety of fraudulent activity, ranging from employment scams to money laundering. But the crimes she investigates all share a common feature: they are perpetrated via the internet.

Criminals use computer technology and the internet to steal money from unsuspecting, innocent people, usually by sending out millions of fraudulent emails to random email addresses in the hope they will get a response.

Carolyne is a member of the Joint Banking and Finance Sector Investigation Team (JBFSIT) in the AFP's High Tech Crime portfolio. Before joining the AFP, she managed Westpac Banking Corporation's Electronic Fraud Team, where she went from examining cheques to investigating electronic deception when the bank experienced a spate of phishing attacks in 2003.

'Phishing' is a particular type of criminal activity, where bank customers are targeted through spam emails. The emails direct victims to a fraudulent website, where their banking and logon details are stolen.

As part of a cooperative partnership between the AFP and the private sector, Carolyne was seconded from Westpac to the Australian High Tech Crime Centre banking team in April 2004. Since September 2006, Carolyne has been employed directly by the AFP as an unsworn member of the JBFSIT.

Her role includes investigating internet banking fraud matters as well as liaising with financial institutions, overseas and State law enforcement agencies, telecommunications agencies and other private sector partners.

"When I first began this job, working with a law enforcement organisation was a new experience for me, but I was welcomed as part of the AFP team right from the start," Carolyne said.

Carolyne often deals with people who have been duped by employment scams known as mule recruitment. Known as 'mules,' these people have responded to spam emails or advertisements purporting to be from someone looking for a financial manager. After supplying their bank account details, the mules receive money into their account. They are then directed to transfer funds overseas, after retaining a portion as their salary. Unfortunately, this is a form of money laundering and the mules, often unknowingly, are acting illegally.

"The hard part is explaining to the person, who quite often has been looking for employment for some time, that the job is not genuine," Carolyne said.

"They are actually partaking in a money laundering scam which carries serious offences."

Helping victims to get their money back is one of the reasons Carolyne comes into work each day. Recently she worked as part of a team that helped put an end to a transnational scam. The investigation and prosecution concentrated on an offender who was compromising Australian bank accounts while based in Vietnam. This multi-jurisdictional investigation was the first for the AFP in this crime type, and resulted in a conviction for the offender and restitution orders for the Australian bank victims.

"The collaborative approach that brings together law enforcement and private sector stakeholders to combat technology-enabled crime makes my job very satisfying," Carolyne said.

"I have learned to be open and honest and to keep trying even when things aren't going as well as I would like them to."