Police target cyber crime after teenager’s death

Police Scotland today announced its support for an international multi-agency operation to target cyber-crime in the Philippines following an investigation into the death of a Scottish teenager.

Daniel Perry, 17, from Fife, who died in July 2013 at the Forth Road Bridge, had been the victim of an alleged sextortion attempt. Inquiries by Scottish detectives revealed an electronic online trail, which led to the Philippines and links to organised crime groups there.

The authorities there have, over the past two days, targeted a number of organised crime groups involved in cyber-crime and have arrested a large number of people as part of Operation Strikeback. Inquiries by the Philippines National Police are on-going to establish the circumstances of the involvement of individuals in relation to Daniel’s death and Police Scotland will continue to liaise with the authorities in Manila.

Police Scotland has worked with a number of international agencies, including Interpol, NCA CEOP, Homeland Security Investigations, US Immigration and Customs Enforcement and the Philippines National Police, through a cyber-crime taskforce, to provide information to the authorities in the Philippines to assist with their operation.

Following the conclusion of the operation, Police Scotland issued a strong prevention message to anyone who may fall victim to such crime.

Senior officers in Scotland have also highlighted that regardless of where in the world criminals operate to target

the vulnerable, the reach of law enforcement is global and every effort will be made to bring offenders to justice.

Assistant Chief Constable Malcolm Graham, Major Crime and Public Protection, (and former Commander of Police in Edinburgh) said: “Daniel’s death last year led to a major criminal inquiry which ultimately led officers to the Philippines.

“The enforcement action over the past two days by the Philippines National Police has been supported by Police Scotland. We have had officers in Manila observing and assisting in the past few days, working with a wide range of partners including Interpol, the Foreign and Commonwealth Office, the Philippines National Police and CEOP and law enforcement from other countries.

“Our message is clear: Our focus is on keeping people safe and there is no hiding place – anywhere in the world – if you are a criminal and you undertake this type of activity, which preys on those who might be the most vulnerable and susceptible to coercion and blackmail.

“A young Scottish teenager lost his life as a result of this online activity. The impact on his family, friends and wider community cannot be imagined. I hope that the efforts of law enforcement and our partners in Scotland and globally helps to provide some reassurance to Daniel’s family and the wider public that we are determined to tackle this type of criminality.”

Detective Chief Inspector Gary Cunningham, of Specialist Crime Division Major Investigation Team East, led the investigation into Daniel’s death. He travelled to Manila to liaise with the authorities in the Philippines. He said: “Our investigation has been supported by a range of partners in the UK and abroad and that’s been a significant factor in helping us understand the circumstances which led to Daniel losing his life.

“Daniel was a victim of a crime which uses threat and intimidation to coerce people into parting with money. This is an organised criminal activity, which is there for one reason – to generate profit by exploiting the vulnerability of others. It’s an abhorrent crime and in this case a young man lost his life, which is something his family and friends have to live with. We have been thorough and relentless in our pursuit of answers to why Daniel died.

Police Scotland is committed to supporting victims of cyber-crime and targeting offenders. Superintendent Danny Hatfield, Safer Communities, said: “Victims should not suffer in silence. If you suspect you are the victim of such a crime, report it to the police immediately. We will listen. We will investigate. We will act. This operation demonstrates that and should provide confidence to any member of the public who believes they are being targeted in this way.

“There are some basic, common-sense steps which can be taken to minimise the risk and threat from online criminals. They relate to computer hardware and software and personal online safety. By taking these steps it reduces opportunities for criminals online and will increase individuals’ safety. Police Scotland is committed to keeping people safe and we see no difference between delivering that policing focus on the streets of our communities or online.

“Work is on-going across Police Scotland to ensure our response to such incidents is as professional as possible. Officers from Specialist Crime Division and Contact, Command and Control are developing that response to ensure victims get the right level of service when coming forward and reporting crime to us.”

Johnny Gwynne, Director of the NCA’s CEOP Command, said: “Criminals who think that by sitting behind their computer in a foreign country they can blackmail or sexually abuse members of the UK public with impunity should know they are wrong.

With partners in the UK and around the world, we will pursue them with any means at our disposal.

“Everyone, particularly young people, should realise that there are dangers to sharing anything online that they would not want family and friends to see. But there is help out there if you do. Click CEOP on our website to report abuse, and you can get advice and support from the NSPCC by calling 0808 800 5000, or from Childline on 0800 1111.

“Guidance for children and young people on staying safe online, as well as information for parents and teachers, can be found can be found at www.ThinkuKnow.co.uk.”

John Logue, Director of Serious Casework at the Crown Office and Procurator Fiscal Service said: “The global nature of sexual cyber crimes means law enforcement agencies in Scotland need to work more closely than every before with their counterparts around the world to ensure that we remain one step ahead of those who engage in these appalling acts. The Crown Office has directed the Scottish end of Operation Strikeback from the outset. We cannot comment on a live investigation but we can reassure the public that cyber crimes committed against Scottish citizens will be treated extremely seriously and borders will present no barriers to that. ”

Daniel’s mother, Nicola Perry added: “The manner of Daniel’s death is every parent’s worse nightmare. After being targeted by complete strangers online, he was left so traumatised by his ordeal that he chose to take his own life.

“Whoever was at the other end of that computer did not know Daniel. They didn’t care that he was a loving and caring person with his whole life ahead of him. To them, he was just another faceless victim to exploit for cash.

“Losing Daniel has left us all devastated and we are still trying to come to terms with what has happened. I would like to thank the police officers who have supported our family

during this extremely distressing time and for keeping us up to date with the progress of their investigation.

“If we are to make sure that no other parent or family member loses a loved one in the way that we have lost Daniel then people must take care when talking to others online and not share intimate pictures or personal information that could be used against them.

“Since Daniel’s death we have been overwhelmed by the kind words and sympathies expressed by so many people across the country. We would now ask that our privacy be respected as we continue to grieve.”

Key prevention steps:

Computers

* Install good anti-virus and spyware software as well as a firewall

* Don’t open unsolicited and unverified attachments

* Use security passwords which are not obvious or easy to guess

* Turn of computers when not in use

* Disconnect or cover webcams

* Exercise caution when downloading or installing programmes

Personal

* Don’t post personal information or images you would not want family or friends to see

* Don’t provide personal information online simply because it has been requested

* Be suspicious – not everyone online will be who they claim

to be

* Set up a separate email account to access social media – don’t use a work email or existing personal account

* Use privacy and security settings on social media sites so you know who is viewing content

* Encourage friends and family to use appropriate privacy and security settings

* Close unused social media accounts down

* Report anything you are unhappy with to site administrators

Victims

* You are the victim of a criminal act – it’s not your fault

* Do not respond to threats – the more you respond, the more demanding they will become

* Police Scotland will take all complaints of this kind seriously and will conduct a thorough investigation

* Victims will be supported and signposted to external guidance agencies

* Victims should contact the police on 101. In an emergency use 999

* Police Scotland is working the Scottish Government and many partners across the public and private sector to keep people safe online

Offenders

* Police Scotland will take all complaints of online extortion seriously

* Complaints will be rigorously investigated

* All investigative tools, including covert and overt techniques, will be used to gather evidence and identify offenders

* We will work with a range of partners

* We will arrest and report offenders where sufficient evidence has been gathered