The effectiveness of policing cybercrime

Dr Paul Stephens
Director of Computing, Digital Forensics & Cybersecurity
paul.stephens@canterbury.ac.uk
http://www.canterbury.ac.uk/computing
Triage

1st Priority - IMMEDIATE
2nd Priority - DELAYED
3rd Priority - MINOR
4th Priority - MORSE

- Known good/bad lists
- Encryption/compression
- File Signature/extension mismatch
- Keyword searching (including Internet/Email)
- Deep Thought (Enhanced Preview) and ECTEG: Dismiss/Lower Priority vs Accept/Higer Priority
- Problems: Low hanging fruit

Canterbury Christ Church University
Focus of teaching
Real lives, real crimes: A study of digital crime and policing

- HMIC(FRS) Report

Daniel, Blackmail Victim

**About**

Daniel called the police because he was being blackmailed by someone whom he had met on a dating website.

**Communication Channel**

Daniel uses his mobile phone for calls and has a laptop which he uses at home and on a personal communications as well. He also uses social media for connec.tion and sometimes online chatting.

**Level of Online Experience**

Daniel claims to have very good experience online, but his trust is kept updated on the latest security measures. He knows that there are lots of scams involving online, especially through online dating sites, but he did not even think that he would be caught until it happened.

**Day 1, 10:00**

I had been a member of a legitimate dating site for a while. I received a notification that I had had a match. I connected with my match online and things progressed quickly.

**11:00**

I then had an online video call with my match. The call became explicit quickly and I was encouraged to perform a sexual act.

**12:30**

It was all too much. I knew that I had to tell someone. I called the police on 101 and told them that I was being blackmailed.

**1:30**

I was put through to an online crime team who took my details. I was told to keep records of what was said and not to have any more contact with the blackmailer.

**1:45**

It was really important to have this voice contact with the crime team as I was not thinking clearly. I really needed that reassurance.

**11:30**

I received a really prompt response. Two police officers came to my house on the same day. They took my details and collected evidence by copying the messages which had been sent to me and by taking photographs of the on-screen activity.

**12:30**

The police gave me a crime reference number before leaving and told me to remove the contact online and get in touch with anyone I knew who was good with IT.

**13:30**

I felt really reassured by their advice. It was good to know that they had heard of similar cases. It made me feel that I was not the only idiot out there.

**11:30**

I was sent a link to the password-protected video which had been posted online. I was told that I had to transfer more cash if I wanted the video to remain private. I was also told that the video would be accompanied with claims that I was a child molester.

**12:30**

It was one thing to have an embarrassing video posted to my friends. It was another to have claims of child molestation attached to it.

**13:30**

I contacted a friend who works in IT. He advised me to change my online security settings and to set up an alert that would inform me if anything was uploaded online about me. This was good advice. I wish the police had given this type of advice to me.

**15:30**

The police contacted me a couple of weeks later to say that the case was closed because the blackmailer had been tracked to the Ivory Coast.

**16:30**

I tried to forget about the incident. I did not ever think that I would get my money back or that the person would be caught.
Can we continue to effectively police digital crime?

Graeme Horsman

https://doi.org/10.1016/j.scijus.2017.06.001
Could we be facing an era where digital crime can no longer be effectively policed?

- Increasing computer usage and volume of digital crime
  - Conviction rates not following suit
- High profile cases with digital forensics elements (Michael Jackson’s death, Dr Harold Shipman, Iain Watkins, Oscar Pistorius)
- Case backlogs, cyber-dependent, cyber-enabled, supporting evidence
- Privacy aware, digital natives, encryption, Deep Web, Prism Break
Could we be facing an era where digital crime can no longer be effectively policed?

- Locard’s exchange principle not applying so strictly to digital traces
- Detection is difficult – time-based, competency-based
- Scale – Internet, multiple jurisdictions and devices, size of storage media, non-cooperation of many countries
- Lack of reporting – feeling of stupidity, embarrassment factor
Conclusions of HMIC Report – Police Service

- Establish **scale** and **impact** of digital crime
  - National and local level
  - How to **respond** to it
- Create **effective leadership**, and **governance arrangements** and **strategies** at all levels to **manage the threat** digital crime poses
  - Engaging with those in **police service** and **private sector** who are able to provide **expertise**
Conclusions of HMIC Report – Chief Constables

- Appropriate and continuing training and guidance for all likely to deal with digital crime and its victims

- Officers and staff understand the significance of online anti-social behaviour

  - Able to provide effective support and advice to those that are its victims
Conclusions of HMIC Report – Chief Constables

- Capability to examine digital devices appropriately, effectively, and speedily
- Appoint chief officer responsible for ensuring staff understand which cases should be referred to Action Fraud and which require an immediate response
- Referrals from National Fraud Intelligence Bureau are dealt with effectively
Other responses

- Prevention and awareness training from an early age
- Improvements in digital investigation technology, tools and techniques
- Pushing of responsibilities for policing onto companies hosting activity
  - Facebook and fake news
  - Google and the right to be forgotten
  - Target advertisers rather than hosts (bad publicity)
Other responses

- Legislation, e.g., Regulation of Investigatory Powers Act (RIPA)
  - Criminal **offence to refuse to decrypt** encrypted data if requested as part of a **criminal investigation**
  - Penalty **two years or five years** for terrorism
British police are on the brink of a totally avoidable cybercrime crisis

- [https://www.wired.co.uk/article/british-police-cybercrime-hacking](https://www.wired.co.uk/article/british-police-cybercrime-hacking)
- Legislation for ‘offensive policing’
- Technology platforms to start doing the some of the policing
- More resources…
Live Data Forensics

- How do we handle encrypted/network/volatile data?
- Critique and rewrite ACPO Guidelines?
- Automation, is it possible?
- How do we measure the effect we have on a system?
Dealing with Encryption and Complexity
Dealing with Better Encryption
Discussion, Ideas and Questions?

paul.stephens@canterbury.ac.uk