Inspecting policing
in the public interest

Real lives, real crimes

A study of digital crime and policing

December 2015

© HMIC 2015

ISBN: 978-1-78655-060-6

www.justiceinspectorates.gov.uk/hmic

Contents

Foreword

The public has the right to demand swift action and good quality advice about how best to deal with those who commit digital crime from every police officer or member of staff with whom they come into contact – from the first point of contact to an experienced detective. Many of those who took part in this study, police and non-police, told us that it is essential that every officer should be equipped to provide victims of digital crime with the help and support that they have a right to expect from those charged with the duty to protect them.

This study has helped HMIC better to understand the effect that digital technology is having on crime and policing. In due course, it will inform our all-force inspection programme, to assess the local response to digital crime and how well each force is progressing.

We hope that it will help chief constables and the College of Policing to provide guidance and good practice to forces so that victims of these crimes get the best possible service.

Stephen Otter QPM
HM Inspector of Constabulary

1. Introduction

1.1. This report is intended to help HMIC better to understand the effect that digital technology is having on crime and policing. We hope that, in turn, it will help chief constables and the College of Policing to provide guidance and good practice to forces so that the victims of these crimes get the best possible service.

1.2. We have worked to the following terms of reference:

> "Her Majesty's Inspectorate of Constabulary (HMIC) should undertake a thematic study in order to develop HMIC's understanding of the effect of digital technology on crime and policing. The study will be conducted for the purpose of informing future HMIC inspections of police forces and law enforcement agencies. HMIC will work with: the College of Policing; the Home Office and police forces in order to achieve a comprehensive understanding."

1.3. We visited six police forces between 19 January and 27 February 2015. We worked closely with non-governmental organisations which represent victims of crime and we have been supported by a group of critical readers and members of various advisory bodies. Uniquely, we worked with Uscreates, a private sector company, to undertake in-depth interviews with victims of digital crime so that their stories may be told in our report. We are grateful to all those who gave of their time freely to help us.

1.4. Those who commit digital crime create victims. Those victims demand and deserve the support and help of the police, as much as any other victim of crime. We have set out in this study the accounts of some victims to highlight the personal impact that digital crime has had upon them. Digital crime is not a lesser crime; it is as pernicious and disruptive as any other and merits an equal response.

Background

1.5. In 2013, 36 million adults (73 percent) in Great Britain accessed the internet every day, 20 million more than in 2006 when directly comparable records began.[1] The percentage of people who use a mobile phone to access the internet has more than doubled between 2010 and 2013, from 24 percent to 53 percent.[2]

1.6. This rise in use is particularly driven by young people. The 2013 annual report of the independent regulator and competition authority for the United Kingdom communications industries reported that 91 percent of children live in a household with internet access.[3] In 2013, children aged 5-7 years spent, on average, 6.7 hours each week online; children aged 8-11 years, 9.2 hours; and children aged between 12 and 15 years, 17 hours.[4]

1.7. Further, in 2013, the Office for National Statistics reported that those aged between 16 and 25 years were most likely to participate in online activities that focused on leisure and recreation, such as social networking (93 percent), downloading software (55 percent) and telephoning or making video calls over the internet via a webcam (40 percent).[5]

1.8. But at the centre of what makes the internet and technological devices such powerful tools for good, lies their potential to be used for bad.

1.9. For the police, the task of investigating and apprehending offenders is made substantially more difficult if they need not set foot inside the jurisdiction of the United Kingdom at any time during the preparation for, and execution of, the crime.

1.10. Anonymity and activity beyond the jurisdiction are a potent mix to help the would-be offender.

[1] *Internet Access - Households and Individuals*, statistical bulletin, Office for National Statistics, August 2013, page 1.

[2] *Ibid.*

[3] *Op cit*, page 22, figure 2.

[4] *Op cit*, page 55, figure 31.

[5] *Internet Access - Households and Individuals*, statistical bulletin, Office for National Statistics, August 2013, page 4.

Digital crime

1.11. People use different terminology to describe this area of crime. In our view, it is essential that a common language is adopted so that we may all understand what it is we are considering. In June 2014, national policing leads, practitioners and policy makers developed four definitions which we adopt throughout this study. We set them out verbatim:

- "**Digital footprint:** that is, the trail of data that is left behind by users of digital services. In an investigative context, this typically relates to mobile and online communications, travel and financial transactions by offenders and victims.

- "**Internet-facilitated crime:** where the internet and smartphones are used in planning or committing traditional criminal or terrorist activity. This ranges from online abuse as part of a neighbourhood dispute to communications between terrorists planning attacks.

- "**Cyber-enabled crimes:** such as fraud, the purchasing of illegal drugs or firearms and child sexual exploitation which can be conducted on or offline, but online may take place at unprecedented scale and speed. This might include terrorism, for example, where cyber-enabled fraud is used to fund terrorist activities.

- "**Cyber-dependent crimes:** which can only be committed using computers, computer networks or other forms of information communication technology. They include the creation and spread of malware for financial gain, hacking to steal important personal or industry data and denial of service attacks to cause reputational damage for criminal purposes or terrorism."[6]

1.12. We have adopted the term 'digital crime' to encompass all the above definitions.

[6] *Report on operationalising the Digital Intelligence and Investigation Capabilities Framework - Improving the intelligence and investigative response to an evolving digital environment,* College of Policing, July 2014, page 6.

An important general point

1.13. Modern technology is an integral part of people’s lives. The police service must respond accordingly. Almost any crime is now capable of involving modern technology, be it in organising its commission through e-mail or social media messages between conspirators, using technology itself to perpetrate the offence, or taking a picture of the aftermath of the crime, such as photographing an assault victim as he or she lies injured in the street with a view to sharing it online.

1.14. As such, it is no longer appropriate, even if it ever were, for the police service to consider the investigation of digital crime to be the preserve of those with specialist knowledge.

1.15. The public has the right to demand swift action and good quality advice about how best to deal with those who commit digital crime from every officer with whom they come into contact – from the first point of contact to an experienced detective.

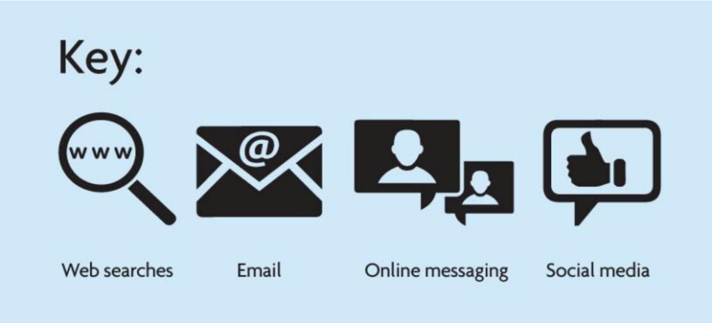
1.16. It is for the police service at large to recognise that dealing with victims of digital crime is now commonplace. Treating such crime as ‘specialist’ or requiring expertise that is provided only by the few is outdated, inappropriate, and wrong. Every officer must be equipped to provide victims of digital crime with the help and support that they have a right to expect from those charged with the duty to protect them.

1.17. In due course, as part of our all-force inspection programme, we will assess the local response to digital crime and how each force is progressing. This report will enable HMIC and those who lead our police forces better to understand what needs to be done to ensure that they respond effectively to digital crime and provide the best possible advice, support, and service to its victims.

2. Our findings

2.1. Throughout this report, we have set out examples of how digital crime is committed, using real examples from victims. We have deliberately selected examples of everyday crimes in order to reinforce the point that digital crime is commonplace. The law which is applicable in each case is set out in annex A.

2.2. The symbols in the examples have these meanings:



2.3. In chapter 3, we set out the issues which the victims of digital crime face, and their experience of the police response.

2.4. In chapter 4, we consider the extent to which the police service is able to gauge accurately the size of the threat posed by digital crime.

2.5. In chapter 5, we look at the level of understanding of the threat posed by digital crime and the way in which the police service is equipping its staff in terms of learning and training to provide an appropriate response to it.

2.6. In chapter 6, we specifically consider how police forces are responding to online anti-social behaviour.

2.7. In chapter 7, we consider the extent to which police forces have developed the technical and specialist capability to deal effectively with digital crime.

2.8. In chapter 8, we set out the structures, leadership arrangements and external partnerships which the police service has put in place in order to combat digital crime, both at a local and national level.

2.9. In chapter 9, we consider the work of Action Fraud and the National Fraud Intelligence Bureau.

2.10. Thereafter, in chapter 10, we draw together the specific areas which we consider the leaders of the police service should have at the forefront of their collective minds so that victims of digital crime are provided with the best possible service, at a national and local level.

2.11. Throughout this report, we indicate how well police forces (based on our findings in the six forces that took part in this study) are responding to particular aspects of digital crime by using a progressive bar across the page. It is a simple and clear indication of how far the police service has come, and how much further it needs to travel to reach a good standard.

3. What did the victims think?

3.1. We have put the victim at the centre of our study into digital crime. Every victim suffers the consequences of the offender’s behaviour and the specific cases in this report provide a powerful testimony to the distress and disruption that digital crime can cause to those who suffer as a result of it.

3.2. Based on our discussions with victims of digital crime, we set out in this chapter the common themes that emerged from the victims’ contact with the police service.

3.3. We spoke to eight victims who generously provided very detailed descriptions of their experiences of being victims of digital crime. We did this to help us better to understand how the police service should respond effectively to their needs. However, we recognise immediately that our sample size of victims of digital crimes is not large enough to draw statistically valid conclusions.

Are people aware of the threat of digital crime?

3.4. Although, for the most part, victims of crime are aware of what has happened to them when the crime is committed in a tangible way (such as an assault or a burglary where the victim is able to see the consequences of the offender’s actions), the picture is different when the crime is a digital crime.

3.5. The victims with whom we spoke were broadly unaware of the threat that digital crime posed to them. They were generally unaware too of the prevalence of such crimes and, on occasion, they were uncertain about the specific offence which had been committed.

3.6. This uncertainty meant that victims were not able to take steps to prevent the crime or its repetition, and many were unsure about what action they should take in response to what was happening to them. This included whether they should contact the police.

3.7. Victims reported to us that, where they took action to report what had occurred to the police in terms of a specific offence, the response that they received was positive.

3.8. However, where the victim was uncertain about whether what had happened to them amounted to a crime, the response that they received from the police was not satisfactory.

> "The police asked me what the crime was. I think it's theft, fraud – I don't really know. Deception?... My frustrations were not so much with the time they took to send someone out to me, as I know they are busy, but with the lack of understanding of what the crime was from every officer I came into contact with."
> ***Paul – online auction site fraud victim***

3.9. In some instances, we were told that the victim had to wait several days before a police officer visited because his or her case was not considered important. Some victims were passed immediately to Action Fraud, regardless of whether that was the appropriate course of action. And other victims commented on what they considered to be a lack of police action once the crime had been reported.

3.10. While we understand that the police's response must be determined in part by the clarity with which a victim conveys his or her account in the first instance, it cannot be right for the victim to have to tell the police the specific offence which has been committed. It is the police's job to identify any criminality from the victim's account and act accordingly.

3.11. In one force, we were told that a police call handler has just seven minutes to assess a caller's account of what has happened and provide an appropriate response. When victims are upset, confused or frightened, such rigidity is not conducive to providing an appropriately tailored response or giving the victim confidence that he or she is believed and is being taken seriously.

3.12. Better understanding the needs of the victim would improve the police response and reduce the number of negative experiences about which victims told us.

Do the police provide adequate support and advice to victims?

3.13. We found a mixed picture about the extent to which the police provided good quality advice to victims of digital crime. Although the picture was not uniform, the following is an example of the positive reaction that good policing secures from a victim of digital crime.

> "I was reassured by the police that the suspect's reach went only as far as Facebook. They gave good advice, like asking me if there was anyone in my network that I could ask further IT advice from."
> ***Daniel – blackmail victim***

3.14. And victims identified areas where they would like to see a greater police presence to help to thwart would-be offenders.

> "It would have been good to have some police presence on chat room sites, in the way that they may drop by a pub in the evening if there had been problems there."
> ***Judith – stalking victim***

3.15. We were also provided with examples where good quality advice and guidance was not provided.

> "They told me to change my phone number to stop receiving the [stalking] texts, but why should I? It's my phone. In the end, I worked out how to make sure all messages coming from his number went into a special folder so I wouldn't see them."
> ***Judith –stalking victim***

3.16. We consider such advice to be wrong in principle and dangerous in practice as it might have led to the loss of evidence which could be later used to support a prosecution against the offender.

3.17. In several cases, the victim's perception of an investigating officer's competence was not directly related to the depth of the officer's knowledge of digital crime. Instead, it was based on the officer's ability to provide thoughtful advice and practical guidance about what the victim could do to protect him or herself from any further criminality.

Why do victims of digital crime delay in contacting the police?

3.18. Not one of the victims with whom we spoke contacted the police immediately after the crime was committed. Such consistency caused us to explore this issue further and three main reasons were given. We consider each in the paragraphs that follow.

Embarrassment

3.19. Broadly, this emotion broke down into two distinct parts: first, the victim's perception that he or she was doing something which others might think of as inappropriate; and, secondly, the idea that the victim had contributed to the crime because of the actions which he or she took.

> "I felt embarrassed and silly. People do form relationships online, but I realise that not everyone will get it."
> ***Judith – stalking victim***

3.20. This reaction is entirely understandable. In our view, what will help victims to overcome them is having the confidence that the police officer to whom they recount what has occurred will treat them with dignity and respect and without casting judgment.

“I can sort this out myself”

3.21. Many digital crimes occur as a result of the victim voluntarily using modern technology. Many victims will have been using the greater freedom provided by technology to set up online accounts, to manage their personal and business affairs and to conduct their social lives, either wholly or partly online. They may well have used modern technology successfully for many years and consider themselves to be adept at understanding and controlling it. And undoubtedly they will have encountered technical difficulties in using the technology and overcome these themselves.

3.22. It is not surprising, therefore, that many victims consider their first encounter with digital crime as something that they should seek to overcome themselves – after all, they will have had the experience of addressing successfully non-criminal difficulties in the past.

3.23. Again, while entirely understandable, it is important for those who are victims of digital crime to appreciate that they are exactly that – victims of crime. And the prompt reporting of what has happened may help the police to secure a positive outcome for the victim.

Perception of police skills

3.24. There remains a perception among digital crime victims that the police are not well-equipped to deal with what has happened to them. The police are seen as responsible for investigating crimes that have a physical manifestation, such as an assault or a burglary. Victims do not yet see the police as the first port of call when they suffer a digital crime.

3.25. Victims reported to us that they often contacted the police only after their attempts to rectify the position had failed, or when they felt out of their depth in dealing with what had occurred. For some, notifying the police was a plea for reassurance and protection.

3.26. Interestingly, we found that in cases of online fraud, victims tended to contact their bank rather than the police.

3.27. Raising public awareness that the police service takes digital crime seriously and will investigate it competently lies at the heart of ensuring that victims contact the police in a timely fashion.

Is there consistency of approach?

3.28. Digital crime is not confined by geographical boundaries within which police forces operate. Unlike an assault or a burglary, for example, where the location of either can be clearly identified and a police force charged with investigating it, digital crime may cross police force boundaries, locally, nationally and internationally.

3.29. In such instances, a common and consistent approach must be adopted.

3.30. We identified a number of cases where two different police forces were involved in the same investigation. In one, a victim of online harassment received conflicting information from the police about what she could do to stop further harassment. In another, a victim of online marketplace fraud was told by an officer from each of two forces that the other force would investigate – although neither did.

3.31. We also found a difference in approach between police forces. While we recognise that police officers should not be straitjacketed in the response that they provide, it cannot be right that an officer’s response was the following:

> “[t]he police told me that it wouldn't be ‘crimed’ as if they dealt with all cyber [sic] crime it would be all that they did! This made me feel angry. I see police deal with cases with far less value. I see these cases being hauled through the court.”
> ***Paul – online auction site fraud victim***

3.32. Such a response is never acceptable.

Do the police recognise the impact of digital crime?

3.33. In cases where the police recognised the emotional upset to the victim which the digital crime had caused, we were told that sensitive and appropriate reassurance and support were provided. Reassurance is often the response which victims are seeking. Where it was given, the victim’s experience of the police was positive.

3.34. We found examples of digital crimes where victims welcomed the sensitivity and understanding of the officers concerned, and they judged their interaction with the police as positive as a result.

> “I was completely overwhelmed, in total shock. I couldn’t believe what was happening. I panicked and transferred the cash without thinking. I was embarrassed. It was so stupid. As soon as the police arrived, they said they had heard of similar cases, which made me feel that I’m not the only idiot”
> ***Daniel – blackmail victim***

> “The police officer was great, really empathetic and I felt as if she was on my side and taking the matter seriously. She said she wasn’t just going to call, but visit him, so she could suss him out face-to-face.”
> ***Judith – stalking victim***

3.35. However, the experience was not universal.

> “The police response was that I shouldn’t have posted the phone. I know what I did was stupid, but that wasn’t helpful.”
> ***Paul – online auction site fraud victim***

3.36. Generally, our case studies suggest that police officers appear to have difficulty in empathising with the victim’s situation – possibly because of their lack of awareness and understanding of the digital lives that some people lead. Recognition of the victim’s vulnerability and the support that he or she needed tended to be based on individual officers’ personal judgment.

3.37. This is a different approach to more traditional crime, where Victim Support is offered as a matter of course. Only one of the eight victims with whom we spoke had been offered the services of Victim Support in the first instance.

3.38. Dealing with any victim of crime in an understanding and respectful way is the daily bread and butter of a police officer’s working life. The fact that the crime was a digital crime should not make any difference to the officer’s approach.

Do the police recognise and collect evidence of digital crime?

3.39. Many victims mentioned that they had carefully collected the evidence of the digital crime but that the investigating officer had not taken it, when offered.

> “I found the branch where my money had been sent and offered to give it to the police to stop it happening to someone else. The police told me to contact Action Fraud. When I contacted Action Fraud they didn’t take it from me but told me to leave the matter to them. I never heard anything else from Action Fraud or the police.”
>
> ***Jane – ‘romance fraud’ victim***

3.40. When this was put to police officers, it transpired that there was a lack of understanding about what to do with such material.

> "Do you print off the Facebook page, write it down, or ask the victim to save it for later?"
> ***Police officer***

3.41. Better awareness of what to do when investigating digital crime is essential, both to preserve the integrity of any evidence available and to instil confidence in the victim that the crime will be properly investigated.

Do the police keep the victim informed of progress?

3.42. Once a victim has summoned up the courage to report a digital crime, it is essential that he or she is updated about the progress of the investigation. Many victims mentioned that they were not kept so informed and some reported that they were not even told when the investigation had been closed.

> "The police never told me if this will go down on the thief's record. It would have been nice to know."
> ***Warren – theft of smartphone***

> "I'm really disappointed that I haven't heard anything back on the case. I feel like there's no progress and two years have gone by. If there is insufficient evidence for the case and they're not going to take it up, I'd just like to get feedback on that."
> ***Simon – 'boiler room' fraud victim***

3.43. And even when contact was maintained, we were told of one instance where the investigating force wrote to the victim in a tone which was inappropriate.

> "I received a letter from the investigating police force saying that they had assessed the case. It said that fraud investigation was resource intensive and they were not taking it further. It said my case might be passed on to Action Fraud. The letter was so generic. It felt like a circular. There was no reference to my circumstances, no signature, no reference to previous correspondence. My hopes had been so high; then they were dashed. I felt more upset than I did after the crime itself."
> ***Jane – 'romance fraud' victim***

3.44. The goodwill of victims towards police, and their trust in them, will be lost easily and quickly if they are not told what is happening in their case, and in a polite and appropriate way.

What do young people think?

3.45. We have set out in paragraph 1.7 the fact that the use of the internet and modern technology is commonplace among those aged up to 25 years – and undoubtedly for many over that age as well. They are the everyday means by which social communication is maintained and young people regard their use as part of their everyday lives.

3.46. Because of this, we spoke with representatives of the National Society for the Prevention of Cruelty to Children. They conducted an online discussion with young people aged between 13 and 20 to find out their experiences of dealing with the police in the context of any difficulties which they encountered online. They also took the opportunity to invite the audience to comment on what the police service could do better when providing its response.

3.47. Although not based on case studies that we undertook, we consider it helpful to set out the comments which were made to representatives of the National Society for the Prevention of Cruelty to Children to complete the picture of the victims' experience.

> "Young people would not go to the police about online issues, because the police just say to them block the person who is bullying and everything will be okay. When the actual case is that bullies won't stop, because they're blocked; they will find other ways to get to the victims online."
>
> "I think the police need to make young people feel like they can contact the police - not like they are wasting police time or like their issues are trivial."
>
> "I want the police to be approachable and actually do something about it, rather than be unreliable."
>
> "Maybe a way of making young people report an issue and have the confidence is if the police actually make the effort to reach out to younger people and raise more awareness. Make young people feel supported and that they've 'got our backs'."
>
> "I would like the police to be more understanding, follow-up on things and not to ignore the issue."
>
> "Online issues don't get taken seriously. The police literally treat it like it's virtual."

3.48. It is clear from these typical comments that the police service has some way to go to secure the confidence of the upcoming generation in the area of digital crime.

How does the police response compare between digital and non-digital crime?

3.49. Throughout this report, we have provided case studies involving some who have been the victims of digital crime. We have included a case study of a victim of attempted burglary between chapters 9 and 10, for comparative purposes.

3.50. Although generalised conclusions cannot be drawn from this limited number of accounts, the contrast between their experiences could not be more stark.

3.51. In the case of the victim of attempted burglary, he knew of the precautions that he should take to protect his home and property in the first instance; he knew that a crime had been committed when the offenders sought to burgle his home; he knew that his first port of call to report the incident should be the police; and he did so immediately.

3.52. Not for him was there uncertainty about what had happened, what he should do or what others might think.

3.53. In turn, the police response to a more familiar crime was markedly different from that provided to victims of digital crime. The police provided advice about how to prevent a further burglary attempt on two different occasions within 24 hours of the first attempt. The victim was visited by two community support officers after the immediate response officer had attended.

3.54. The police offered the victim the services of Victim Support on two occasions.

3.55. And so, we have two crimes, two different approaches by the victims and two different responses by the police. If the position is replicated across more crimes, it is clear that there is some way to go before the victims of digital crime can be assured that they will receive the same response from the police as victims of more familiar crimes.

Conclusion

3.56. There is nothing to suggest that the experiences of victims of digital crime which we have included throughout this report are not representative of what happens to a substantial proportion of victims of such crimes. However, as we have said at the beginning of this chapter we recognise immediately that our sample size of victims of digital crimes is not large enough to draw statistically valid conclusions. Nonetheless, we consider that their experiences are sufficient to identify those areas of police work that need attention. We consider these to be:

1. showing that the police service takes digital crime and its impact seriously;
2. better tailored support and advice to victims of digital crime;
3. better awareness of how to investigate digital crime and the evidence required to support such an investigation;
4. a more consistent and co-ordinated response by the police within and across force boundaries; and
5. keeping the victim of digital crime better informed of progress in the investigation.

3.57. We leave the last words of this chapter to a victim of digital crime whose eloquence in conveying her thoughts does not warrant any further explanation.

> “As a result of my experience, I felt violated, both emotionally as well as financially. After it happened, it occurred to me that, had I been robbed/burgled in the accepted sense, I would have been visited and questioned by someone.
>
> “Because it was over the internet, with no hard evidence/finger prints, etc., my complaint was as invisible as the person who had stolen from me – more so because the hard evidence I did have was of no interest to anyone.
>
> “Ultimately I think I have been left realising what I already acknowledged, namely that the emotional damage is as important, if not more so, than the financial. That is what the police need to recognise. I lost some money but emotionally the scars are a lot deeper.”
> ***Jane – ‘romance fraud’ victim***

Jane Romance fraud victim

ABOUT

Jane called the police after realising that the person to whom she had been chatting online, and to whom she had been sending money, was defrauding her.

58 Years old

Female

Nurse, also cares for her parents

In her words "I like writing emails because they're like corresponding by letters."

1 2 Most used devices

1 2 3 Online most for...

COMMUNICATION CHANNELS

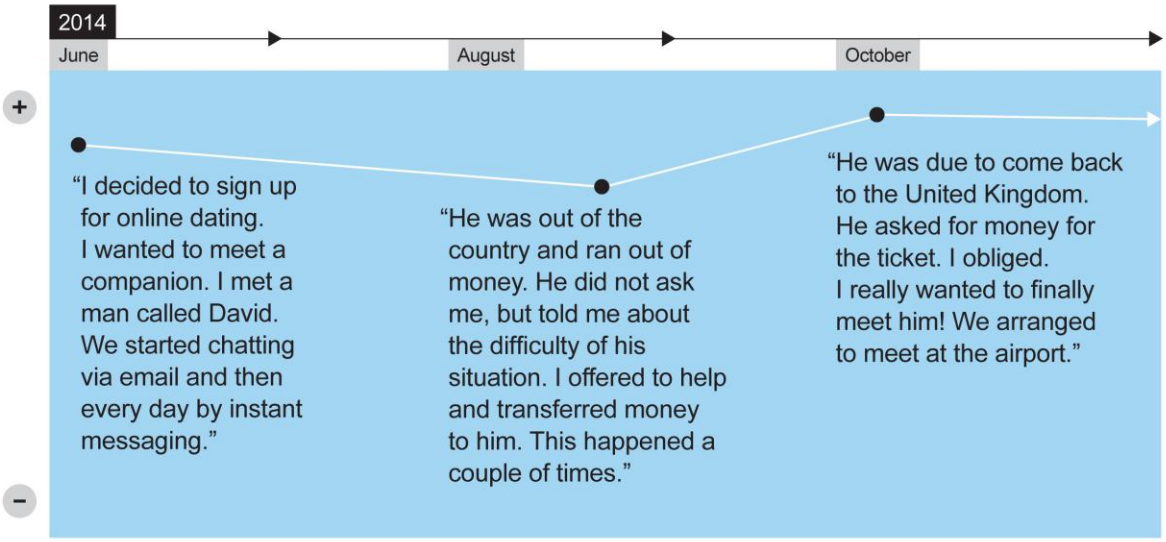
She does not use computers much at work, but has a laptop that she uses at home for researching on the web and for emails.

ONLINE EXPERIENCE

This was her first experience of the online dating world. She 'took the plunge' after a friend suggested that she gave it a try. She hoped that online dating sites would be a way to meet a new companion, after the passing of her husband. It took her a long time to get to that point – "I am not very internet savvy".

Level of online experience

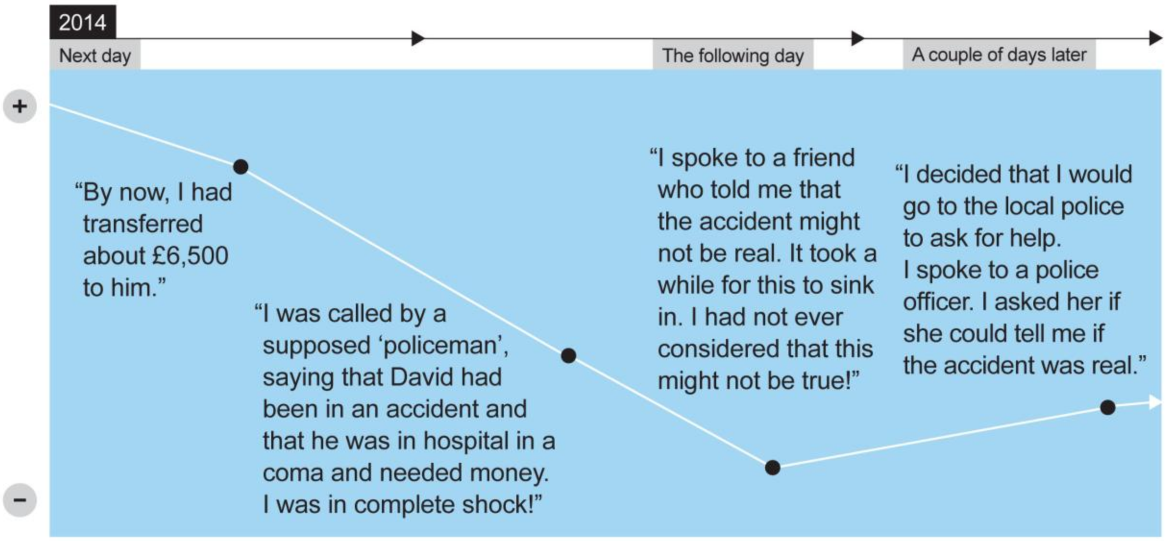
Novice ● Average Expert



"I decided to sign up for online dating. I wanted to meet a companion. I met a man called David. We started chatting via email and then every day by instant messaging."

"He was out of the country and ran out of money. He did not ask me, but told me about the difficulty of his situation. I offered to help and transferred money to him. This happened a couple of times."

"He was due to come back to the United Kingdom. He asked for money for the ticket. I obliged. I really wanted to finally meet him! We arranged to meet at the airport."

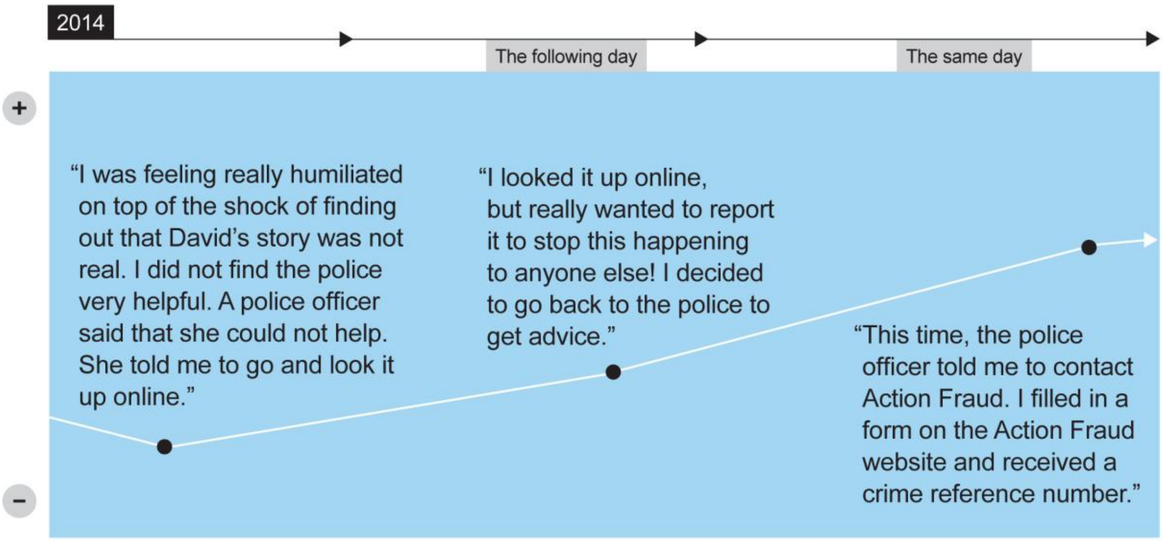


"By now, I had transferred about £6,500 to him."

"I was called by a supposed 'policeman', saying that David had been in an accident and that he was in hospital in a coma and needed money. I was in complete shock!"

"I spoke to a friend who told me that the accident might not be real. It took a while for this to sink in. I had not ever considered that this might not be true!"

"I decided that I would go to the local police to ask for help. I spoke to a police officer. I asked her if she could tell me if the accident was real."



2014

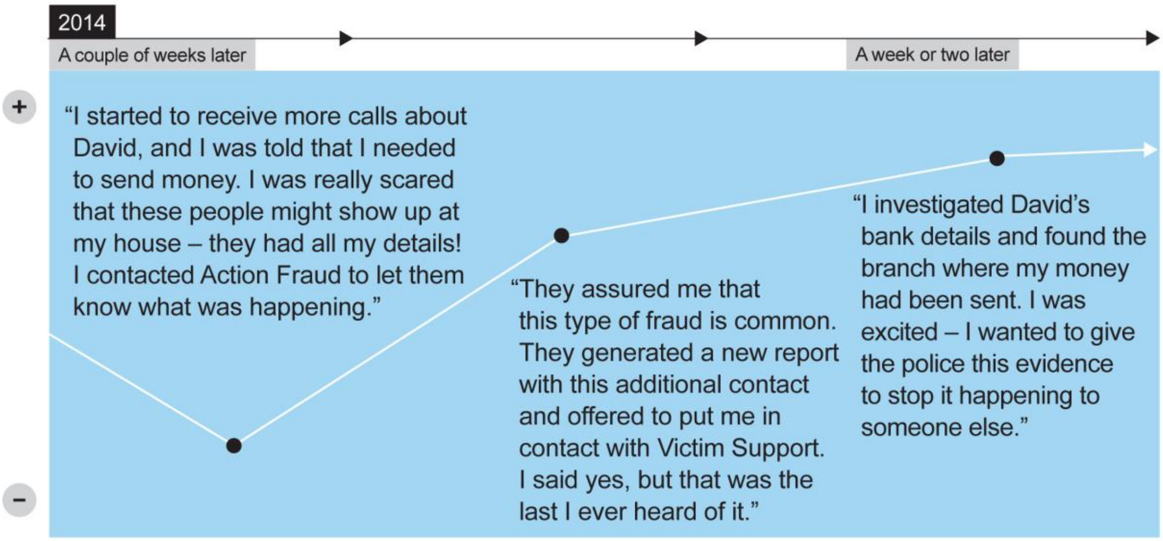
The following day

The same day

"I was feeling really humiliated on top of the shock of finding out that David's story was not real. I did not find the police very helpful. A police officer said that she could not help. She told me to go and look it up online."

"I looked it up online, but really wanted to report it to stop this happening to anyone else! I decided to go back to the police to get advice."

"This time, the police officer told me to contact Action Fraud. I filled in a form on the Action Fraud website and received a crime reference number."



2014

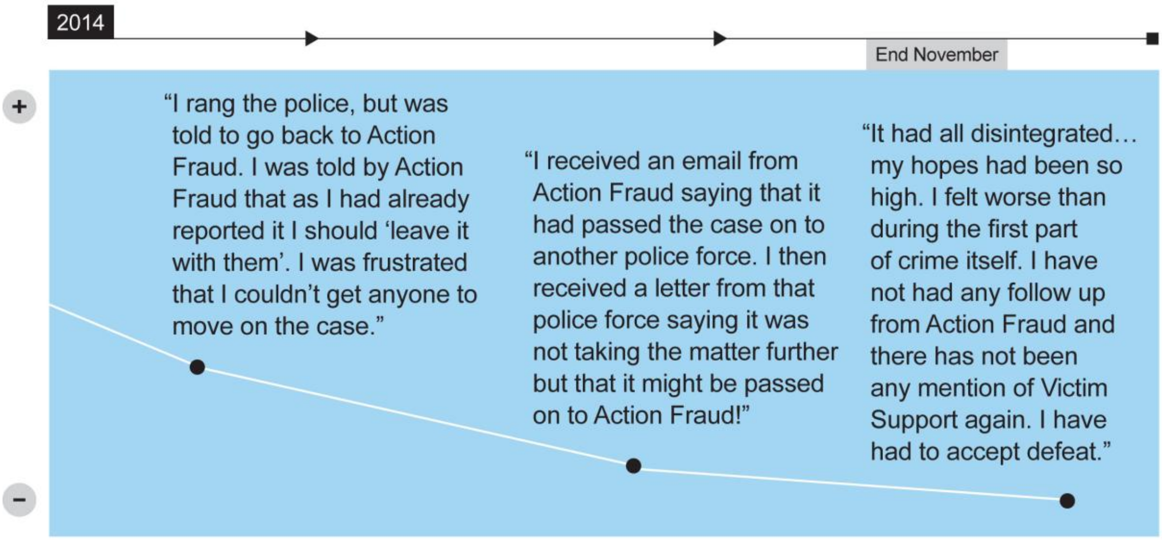
A couple of weeks later

A week or two later

"I started to receive more calls about David, and I was told that I needed to send money. I was really scared that these people might show up at my house – they had all my details! I contacted Action Fraud to let them know what was happening."

"They assured me that this type of fraud is common. They generated a new report with this additional contact and offered to put me in contact with Victim Support. I said yes, but that was the last I ever heard of it."

"I investigated David's bank details and found the branch where my money had been sent. I was excited – I wanted to give the police this evidence to stop it happening to someone else."



2014

End November

"I rang the police, but was told to go back to Action Fraud. I was told by Action Fraud that as I had already reported it I should 'leave it with them'. I was frustrated that I couldn't get anyone to move on the case."

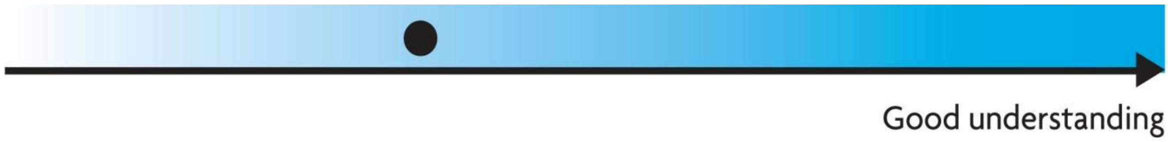
"I received an email from Action Fraud saying that it had passed the case on to another police force. I then received a letter from that police force saying it was not taking the matter further but that it might be passed on to Action Fraud!"

"It had all disintegrated… my hopes had been so high. I felt worse than during the first part of crime itself. I have not had any follow up from Action Fraud and there has not been any mention of Victim Support again. I have had to accept defeat."

4. Do the police know the scale of digital crime and how do they respond?

4.1. In order for the police service to provide a sufficient and effective response to digital crime, it has to understand at a national and local level the size of the challenge which it is facing.

Do the police understand the scale of digital crime?



4.2. Understanding the current and future demand that the criminal use of digital technology does, and will, place on police forces is central to providing an effective and efficient policing response. Such understanding allows forces to make sound, evidence-based decisions in relation to critical areas, such as operational structures, procurement, and learning and development.

4.3. Understanding the way in which digital crime is committed also enables the police service to identify those who are most likely to be vulnerable to this form of crime. In turn, this will help to inform the most appropriate response and to provide guidance to help to prevent likely individuals from becoming victims in the first place, or repeat victims thereafter.

4.4. Given the importance of such information, we considered the extent to which forces collected data in order to develop strategies, risk assessments, tactical implementation plans and local profiles[7]. We found that little information was obtained. Given that fact, some forces have developed responses based on professional judgment. As a consequence, those forces are now some way along their journey of building an effective response, while others remain ‘in the starting blocks’.

4.5. However, we are pleased to see that the issue has been recognised and that steps are being taken to understand the scale of current digital crime activity.

4.6. We consider that an important element in generating reliable information about the scale of digital crime is the adoption of a flagging system which enables local and national statistics to be produced.

[7] In 2014 the Home Office provided guidance on the development, distribution and effective use of local profiles. See: *Serious and Organised Crime Local Profiles: A Guide*, Home Office, November 2014

4.7. An only partially successful voluntary scheme in which participating forces could choose to flag reported crimes that fall within the definition of cyber-crime was replaced from 1 April 2015 with a mandatory system (now known as the online flag). This requires all police forces to flag all crimes which they record:

> "[w]here the officer believes that on the balance of probability the offence was committed, in full or in part, through a computer, computer network or other computer-enabled device".[8]

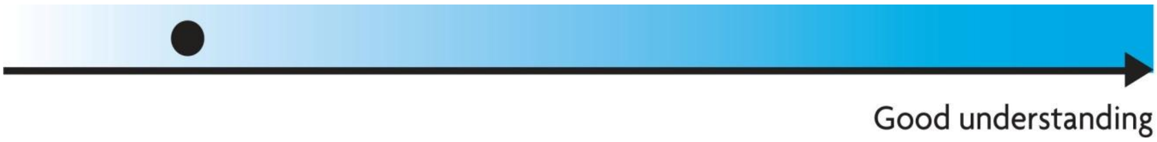
4.8. Those forces which took part in the previously voluntary scheme already have some insight into the scale and targeting of digital crime and now, under the mandatory scheme, the remaining forces will be able to plug the gap in their knowledge.

4.9. The Home Office, as the owner of the process of flagging, has recognised that the aggregation of the forces' returns will:

> "provide a national and local picture of the extent to which the internet and digital communications technology are being used to commit crimes. This will give an insight into the scale and nature of online crime, and it will greatly enhance the development of policies to tackle them and protect victims."[9]

4.10. We encourage all forces to contribute accurately and comprehensively to the system of flagging in order to build up a national picture. However, we recognise that the extent to which this will happen is dependent on the recording officer recognising that the crime which he or she is considering is a digital crime. This reinforces the need for adequate training and we return to this theme in chapter 5.

Do the police understand the impact of digital crime?



4.11. Finding out the extent to which digital crime is being perpetrated in any given police force remains only part of the story in devising a national and local response. The other, equally important data centre on the impact that digital crime has on its victims.

[8] *Additional data requirement*, Home Office, 2015, paragraph 1.1.6.

[9] *Ibid*.

4.12. Our case study concerning Daniel, page 38, illustrates the positive victim reaction when a police officer recognised the impact that the crime had on the victim, not only in a physical sense (such as the loss of money) but also in an emotional sense (such as the creation of fear that the victim is vulnerable to further crime and that his or her personal details are now known across the internet).

4.13. Beyond that, forces need also to be aware of the local community's perceptions of digital crime as a local police response does have a role to play in helping to safeguard and support victims of digital crime, and help to prevent others from becoming victims themselves.

4.14. Some forces that helped us during our study have made the decision not to rely solely on numerical data when shaping their response to digital crime. Instead, they have developed their understanding by consulting with their communities in order to identify their fears and concerns. This has enabled those forces to construct a more comprehensive response to the occurrence of digital crime, its prevention and its aftermath.

4.15. We encourage all forces to look at the impact of digital crime in the round. The use of public surveys and consulting local business fora are two ways in which forces can obtain a broader understanding. One force intends to use its staff as a proxy for the wider community in an information-gathering exercise.

4.16. These are sensible initiatives and we encourage their use.

Conclusion

4.17. The police service needs to establish the scale and impact of digital crime, at both the national and local level, and how to respond to it.

Megan Account hacking victim

ABOUT

Megan called the police because her son's online accounts had been hacked.

43 Years old

Female

Works as a systems manager

In her words "Life as a single mum is very busy. I am always juggling the logistics of it all".

❶ ❷ Most used devices

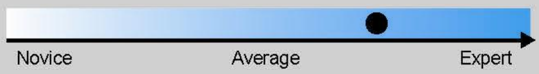
❶ ❷ ❸ Online most for...

COMMUNICATION CHANNELS

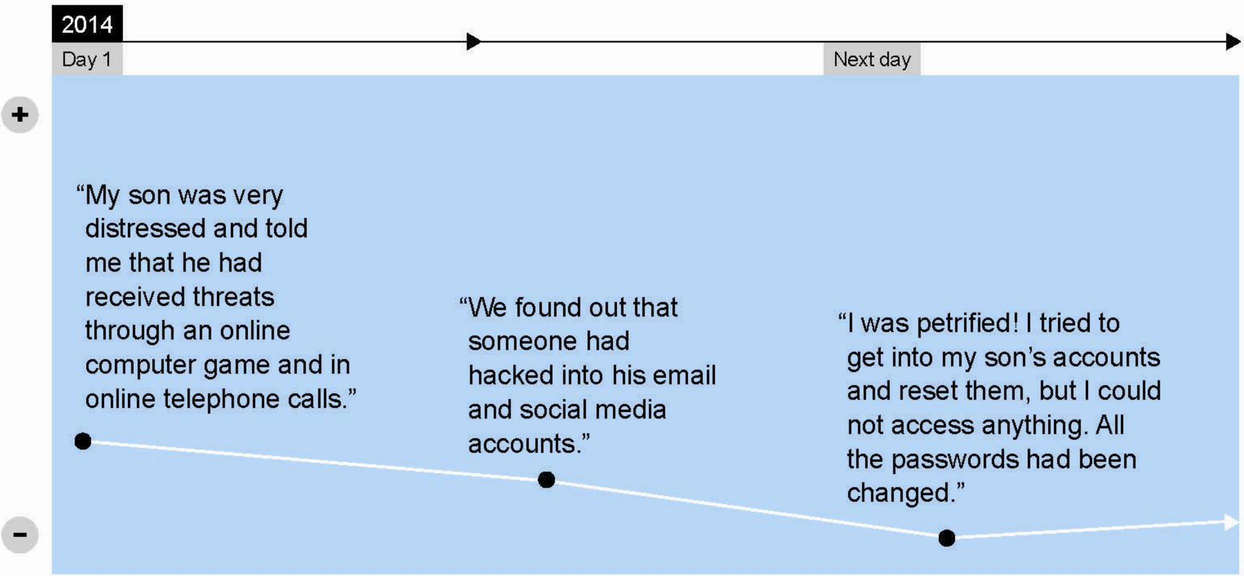
She uses her mobile 'phone "constantly" and shares a laptop with her daughter. She is active on social media sites, especially Facebook and Instagram.

ONLINE EXPERIENCE

She is online, either on her 'phone or laptop most of the day. She considers herself to be "pretty aware" of how the online social world works, but feels she does not know much about technology and internet security – "this was a very steep learning curve for us".


Level of online experience

2014

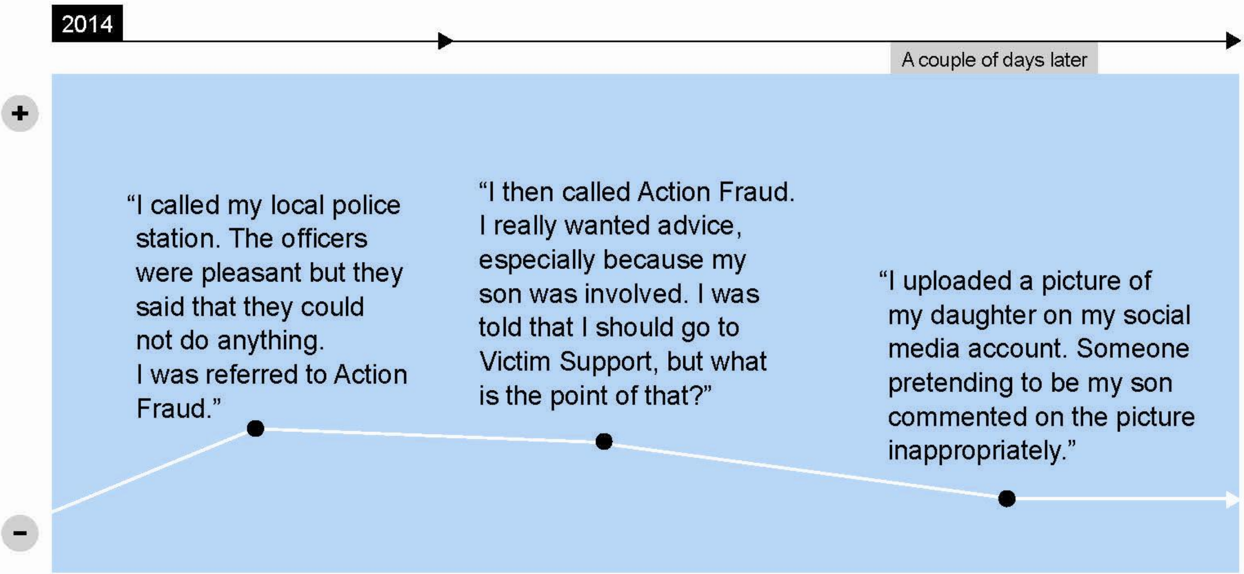


"My son was very distressed and told me that he had received threats through an online computer game and in online telephone calls."

"We found out that someone had hacked into his email and social media accounts."

"I was petrified! I tried to get into my son's accounts and reset them, but I could not access anything. All the passwords had been changed."

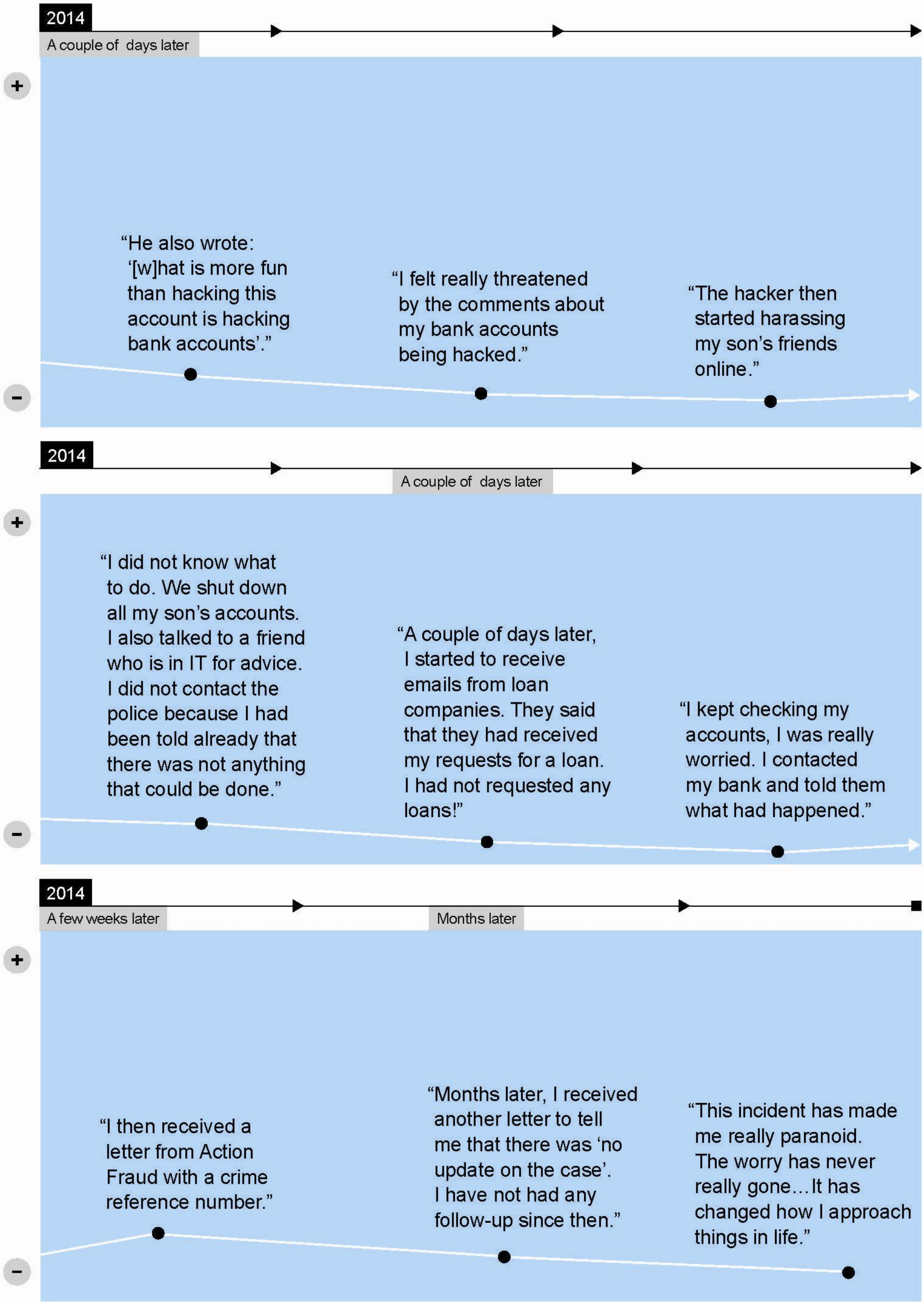
2014



"I called my local police station. The officers were pleasant but they said that they could not do anything. I was referred to Action Fraud."

"I then called Action Fraud. I really wanted advice, especially because my son was involved. I was told that I should go to Victim Support, but what is the point of that?"

"I uploaded a picture of my daughter on my social media account. Someone pretending to be my son commented on the picture inappropriately."



2014

A couple of days later

+

“He also wrote: ‘[w]hat is more fun than hacking this account is hacking bank accounts’.”

“I felt really threatened by the comments about my bank accounts being hacked.”

“The hacker then started harassing my son’s friends online.”

-

2014

A couple of days later

+

“I did not know what to do. We shut down all my son’s accounts. I also talked to a friend who is in IT for advice. I did not contact the police because I had been told already that there was not anything that could be done.”

“A couple of days later, I started to receive emails from loan companies. They said that they had received my requests for a loan. I had not requested any loans!”

“I kept checking my accounts, I was really worried. I contacted my bank and told them what had happened.”

-

2014

A few weeks later

Months later

+

“I then received a letter from Action Fraud with a crime reference number.”

“Months later, I received another letter to tell me that there was ‘no update on the case’. I have not had any follow-up since then.”

“This incident has made me really paranoid. The worry has never really gone…It has changed how I approach things in life.”

-

5. How well are the police training their officers in digital crime?

5.1. As we have set out in paragraph 1.14 to 1.16, the police response to digital crime should be capable of being provided by every police officer and member of police staff who deal directly with the public. Digital crime's prevalence is such that it is no longer the exclusive domain of a specialist squad at a regional or national level, even if it were right that that had ever been the appropriate response.

5.2. We recognise, however, that bringing the handling of digital crimes within the general skillset of every police officer and member of police staff means that it is essential that they, in turn, have the necessary understanding of the technology.

5.3. We found a mixed picture when we considered the extent to which police officers and staff knew of, and were trained in, digital crimes and modern technology.

5.4. On the one hand, an officer summed up his views about social networking by commenting:

> "I am 46 years old. I do not have a computer; what do I know about Facebook?"

5.5. On the other, another said:

> "I do not see it as digital or cyber-crime; it is just crime that needs investigating. It is my job."

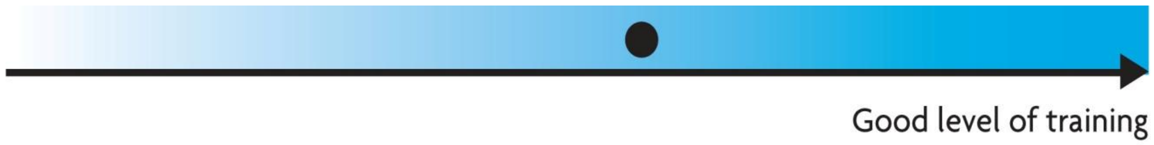
5.6. Better understanding and appropriate training are crucial to ensuring that digital crime is dealt with appropriately by every officer and member of police staff, and that victims are treated properly.

5.7. Many with whom we spoke recognised this need but were uncertain how to go about obtaining evidence from digital media. They spoke of their lack of confidence that they were providing an effective service to the public. One said:

> "[s]taff feel frustrated with their lack of ability to deal with digital investigations."

5.8. Awareness that more is required in this area is the first step in providing a better service.

What advice and training is provided to staff?



5.9. Learning about digital investigation is currently provided for specialist and non-specialist staff. There are three courses provided by the College of Policing.

5.10. Non-specialist learning is predominantly provided through an online learning programme provided by the National Centre for Applied Learning Technologies.[10]

5.11. This programme was launched in November 2013. It is aimed at all frontline police officers and staff. The learning programme is divided into four modules:

- cyber-crime and digital policing;
- cyber-crime and digital policing – investigations;
- digital communications, social media, cyber-crime and policing; and
- cyber-crime and digital policing introduction.

5.12. We understand from data provided to us by the College of Policing that in 2014-15, 172,762 modules were completed.

5.13. A classroom-based course, entitled ‘mainstreaming cyber-crime training’, is designed for ‘first responders’. The contents of this course are currently being reviewed by the College of Policing.

5.14. This training course was rolled out nationally in February 2014. Between then and April 2015, 4,394 officers successfully completed it.

5.15. In addition, a level of training intended to ensure the provision of specialist knowledge within forces is provided by the digital media investigators course.

5.16. This course has only been available since January 2015. We understand that there are approximately 800 funded places available during the 2015-16 financial year. The course includes five days protected online learning and a further five-day classroom-based course. It is anticipated that the current Home Office funding for this course will stop in March 2016.

[10] The National Centre for Applied Learning Technologies, commonly referred to in the police service as NCALT, is a collaboration between the College of Policing and the Metropolitan Police Service. It assists the 43 Home Office police forces in England and Wales and the wider policing community in adopting new learning technologies.

5.17. We comment further on this course at paragraphs 7.19 to 7.22**.**

5.18. With regard to the online training programme, we found good examples of frontline leaders using it as a group training tool, to encourage interaction between members of the team. Working through the training material together facilitates group discussions and enables specific points of learning to be highlighted. Staff commended these sessions as “beneficial and interactive”.

5.19. These instances seem to be isolated. More generally, we found a different picture.

5.20. The content and the format of the online training programme were considered broadly suitable by staff, but we heard consistent criticism of the equipment with which they were provided. We found examples where staff were expected to undertake the online training on computers from which the sound cards had been removed, thereby preventing them from listening to the online learning package.

5.21. Further, staff complained about the insufficiency of time with which they were provided to complete the training programme. In one force, so-called protected training days which staff are expected to use to maintain their continuous professional development were cancelled on a routine basis because of operational requirements.

5.22. This caused pressure on those undertaking the training when they eventually did find time to do so, and some with whom we spoke admitted to “clicking through” the online packages without paying them much regard, simply so that they could complete the training programme. In one instance, we were told that:

> “[t]o be honest, the probationer does the online training for the shift on nights.”

5.23. There are clear management issues here that need to be addressed.

5.24. The mainstream cyber-crime training course began in February 2014. For 14 months, the course was subsidised to try to ensure that as many officers as possible completed it. Some forces decided that the course did not meet their requirements. As it was a national course facilitated locally, those forces amended the standard course to include additional training aspects which they considered were absent from the national programme.

5.25. Home Office funding for this training course stopped in April 2015.

5.26. The College of Policing has responded to these criticisms and is currently rewriting both the online and mainstream cyber-crime training packages. We understand that it intends to provide two-tier training: cyber awareness in an online format; and cyber for investigators, the content of which will be integrated into the professionalising investigation programme.[11]

5.27. It is the College's intention that every police officer and member of police staff who is involved in the investigative process should have the appropriate level of knowledge and understanding in order to provide a professional response to the challenges which digital technology presents.[12]

5.28. We agree.

5.29. However, we do not underestimate the challenge which the removal of funding by 2016 for two of these three courses will present to police forces which are already financially constrained. We accept that chief officers will need to take hard decisions about which training should be funded at a local level.

5.30. All that we propose to say here is that the substantial increase in digital crime and its potential to cut across all types of crime indicate to us that raising the skill base of every police officer and member of staff who is likely to be required to deal with such crimes is essential.

5.31. And we make the point that just as digital crime occurs in every police force area in England and Wales, so should the training requirement, wherever it is facilitated.

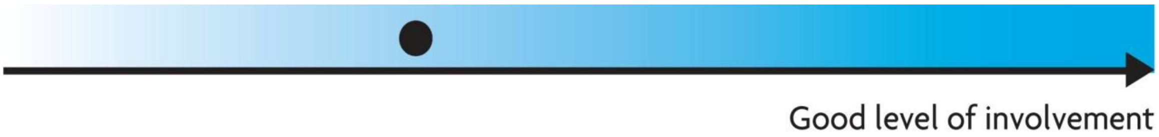
5.32. We want to make one further point. In addition to redesigning the appropriate training packages, digital skills profiles should be completed. They should be for all frontline staff, starting with those who have first point of contact with the public, call takers, front desk staff, operational police officers and police community support officers, and carry through to those in specialist roles.

[11] The Professionalising Investigation Programme is designed to ensure that staff are trained, skilled and accredited to conduct the highest quality investigations. See: www.app.college.police.uk/app-content/investigations/introduction/#pip.

[12] In June 2015 the national policing lead for cyber crime training and development wrote to all chief constables. In his letter he outlined proposals for the development of mainstream cyber-crime training, and the role of forces in implementing those proposals.

5.33. Once a baseline of core skills for each role has been established, the training framework can be developed and career pathways identified. This should help to inform the requirements of the training programmes being considered and better tailor them to the needs of the staff concerned. The College of Policing has already commissioned a training needs analysis which should help to inform such profiles and aid course design.

How is the private sector involved?



5.34. No matter the breadth and depth of the training provided by the College of Policing, there are highly technical enquiries, usually connected to serious organised crime or counter-terrorism, which require specialist knowledge.

5.35. There is a general acceptance that the College of Policing is unable to provide that level of specialised training, and, because of the relative infrequency of the need, there are strong arguments to support the assertion that it is not cost-effective for the College to do so.

5.36. The issue is likely to be exacerbated as the speed of technological advances which facilitate digital crime is likely to continue to outstrip the police service’s ability to keep pace.

5.37. The use of third party training providers is a clear way forward. They have the benefit of: allowing the police service to require a bespoke training programme to address an identified need; reducing costs in training development; buying training provision at a time when it is needed rather than maintaining a training infrastructure which may not be sufficiently used; and allowing the police service to benefit from the private sector’s knowledge base.

5.38. This approach has been adopted in the police counter-terrorism network, where, in April 2015, an agreement was reached in principle to scope options for designing a National Digital Exploitation Service to support counter-terrorism policing. This is intended to maximise the exploitation of digital technologies by encouraging engagement and collaboration between law enforcement agencies and security partners.

5.39. In support of counter-terrorism network requirements, a training development pathway has been created. It has 5 levels of accreditation: foundation; intermediate; advanced (levels 3 and 4); and expert. The training provided is to industry standards and is accredited by CESG.[13]

5.40. It also incorporates an online element produced by the Open University and, in the paragraphs which follow, we have set out the way in which one force has capitalised on the work of the Open University.

5.41. In that force, applicants for a specialist role are required to have completed a specific online course provided by the Open University before making their application.

5.42. The Open University has an introduction to cyber security course as part of its Future Learn project. The course provides online learning which is designed to develop the individual's knowledge of personal digital security. The course is modular in format and takes 24 hours to complete. In addition to traditional course materials, such as filmed lectures and reading material, the course provides an interactive user forum to support discussion between students and facilitators. The course allows unlimited participation and is free to access.

5.43. The clear benefit to the force in question is that the learning provided through the course is directly relevant to the workplace. Such benefits have also been recognised by the counter-terrorism network which has incorporated the course into the training pathway for its officers.

5.44. Indeed, it has gone further. Following consultations with the Open University, counter-terrorism policing has purchased a three-year licence for the course. This will run parallel to the current open source version of the course, and guarantees that its staff will be able to access fit for purpose training within a relatively short timescale.

5.45. We were told that the aspiration for the course is that it will be shared with security partners and, if possible, police forces in the longer term.

5.46. We have gone into detail about this example as we are convinced it provides a substantial opportunity for the police service as a whole to forge links with external providers and build strong working relationships with others who can help the police to meet the threat of digital crime.

[13] CESG was formerly known as Communications – Electronics Security Group. It is the information security arm of GCHQ, the Government Communications Headquarters, and the national technical authority for information assurance in the United Kingdom.

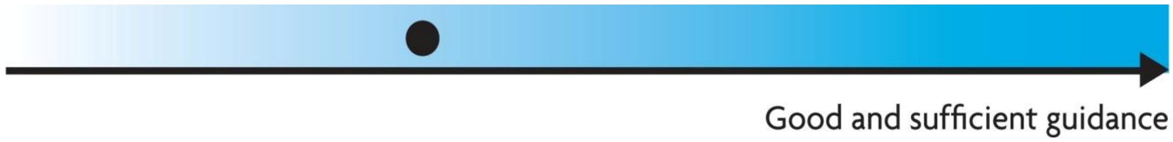
5.47. The link between the police’s training needs and academic institutions which also provide learning in this area of work is clear. We would welcome future initiatives that enable police officers and staff to undertake approved and regulated training programmes which are recognised by academic or vocational qualifications.

5.48. There are issues to be resolved concerning the commissioning, quality assuring and licensing of external sources of training. We consider that the College of Policing is ideally placed to act as the co-ordinator for these initiatives. It should set out the framework within which the private sector may play a crucial role in augmenting home-grown training programmes so that every aspect of digital crime is with the grasp of those who are required to investigate it.

Useful resources

> **Future Learn**

What further guidance is available to staff?



5.49. In addition to formal training, forces often use their local intranets as a source of guidance and learning for staff.

5.50. On more than one occasion, senior officers told us that “all that they [the staff] would need is on the intranet”. Unfortunately, we found that, often, this confidence was misplaced.

5.51. Our study found that the guidance available to support frontline staff through force intranet sites varied considerably. Often, what guidance existed was hidden within other unrelated guidance, and it was seldom reviewed to ensure that it remained accurate and up to date. As a result, if staff members were able to locate the relevant page on the intranet, they had little confidence in its accuracy or relevance.

5.52. We encountered this problem for ourselves during our study. One senior officer told us that all the required information was on the force intranet. We were invited to search for it. We tried. We could not find it and we enlisted the help of local staff. They too were initially not able to find it. The relevant guidance was eventually found after 90 minutes of diligent searching by a number of technology-literate individuals. The guidance was inadequate.

5.53. We have much sympathy with the police officer or member of staff who, upon carefully trawling through the intranet to find the help that he or she is seeking and then finding it inadequate, decides not to undertake the exercise a second time.

5.54. Forces need to ensure that their intranets are better maintained and contain current, accurate and useful information for staff dealing with digital investigations and enquiries.

5.55. On a more positive note, a number of forces were piloting projects which provide frontline staff with digital tablets. This allows initial responders immediate access to the force intranet and to other sources of information. One of the best examples we saw was from a response officer who attended the report of a courier fraud. At the scene of the incident, she was able to access not only guidance on how best to investigate such an incident but also what advice should be provided to victims. This is a good example of how forces are able to use digital technology to support frontline staff.

Conclusion

5.56. Each chief constable needs to provide appropriate and continuing training and guidance for all those within his or her force who are likely to deal with digital crime and its victims.

Daniel Blackmail victim

ABOUT

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

43 Years old

Male

Works in finance

In his words: "I work long hours in the city centre. I often come home after a busy day and do more work from home."

1 2

Most used devices

COMMUNICATION CHANNELS

He uses his mobile 'phone often and has a work laptop which he takes home and uses for personal communications as well, mainly for email, Facebook and sometimes online chatting.

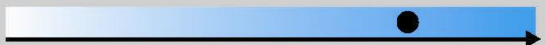
1 2 3 4

Online most for...

ONLINE EXPERIENCE

He considers himself very experienced online, but still finds it hard to keep updated on the latest security measures. He is aware that there are lots of risks involved online, especially in scams through online dating sites, but he did not ever think that he would be caught out until it happened.

Level of online experience

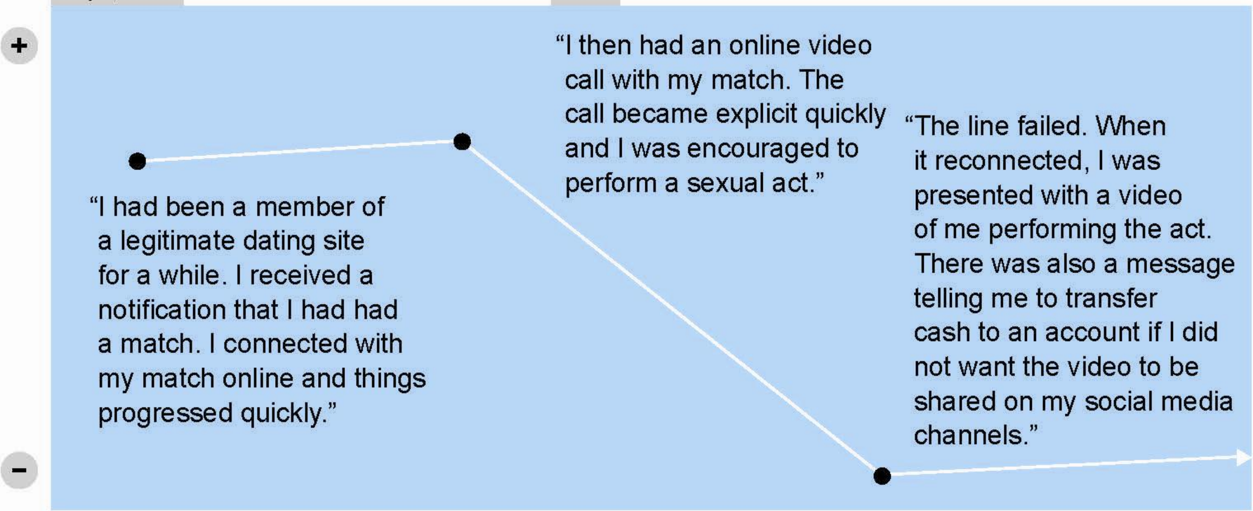


Novice Average Expert

2014

Day 1, 10:00

11:00



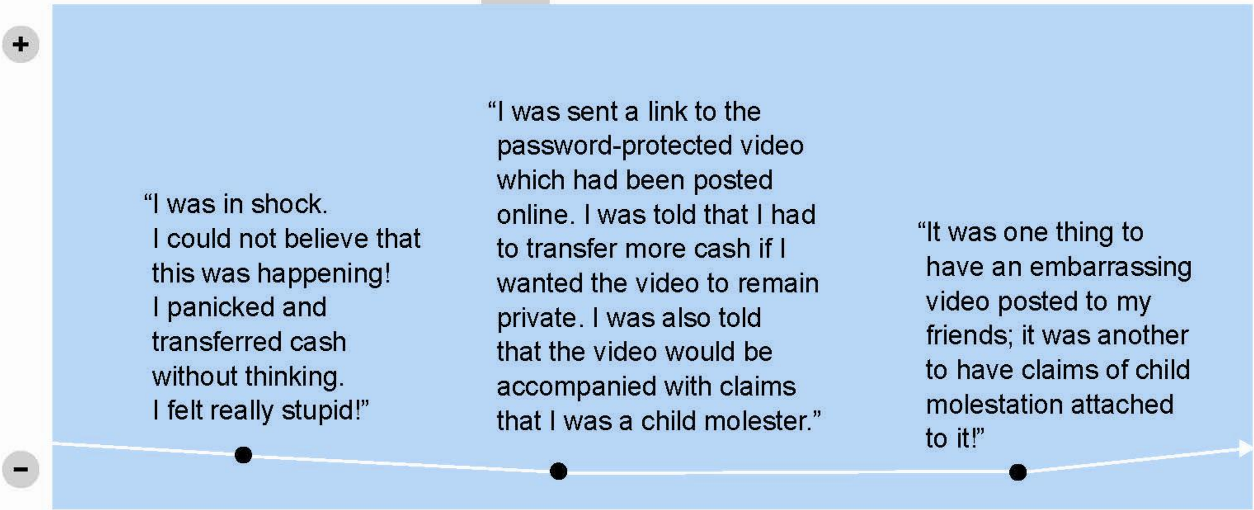
"I had been a member of a legitimate dating site for a while. I received a notification that I had had a match. I connected with my match online and things progressed quickly."

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

"The line failed. When it reconnected, I was presented with a video of me performing the act. There was also a message telling me to transfer cash to an account if I did not want the video to be shared on my social media channels."

2014

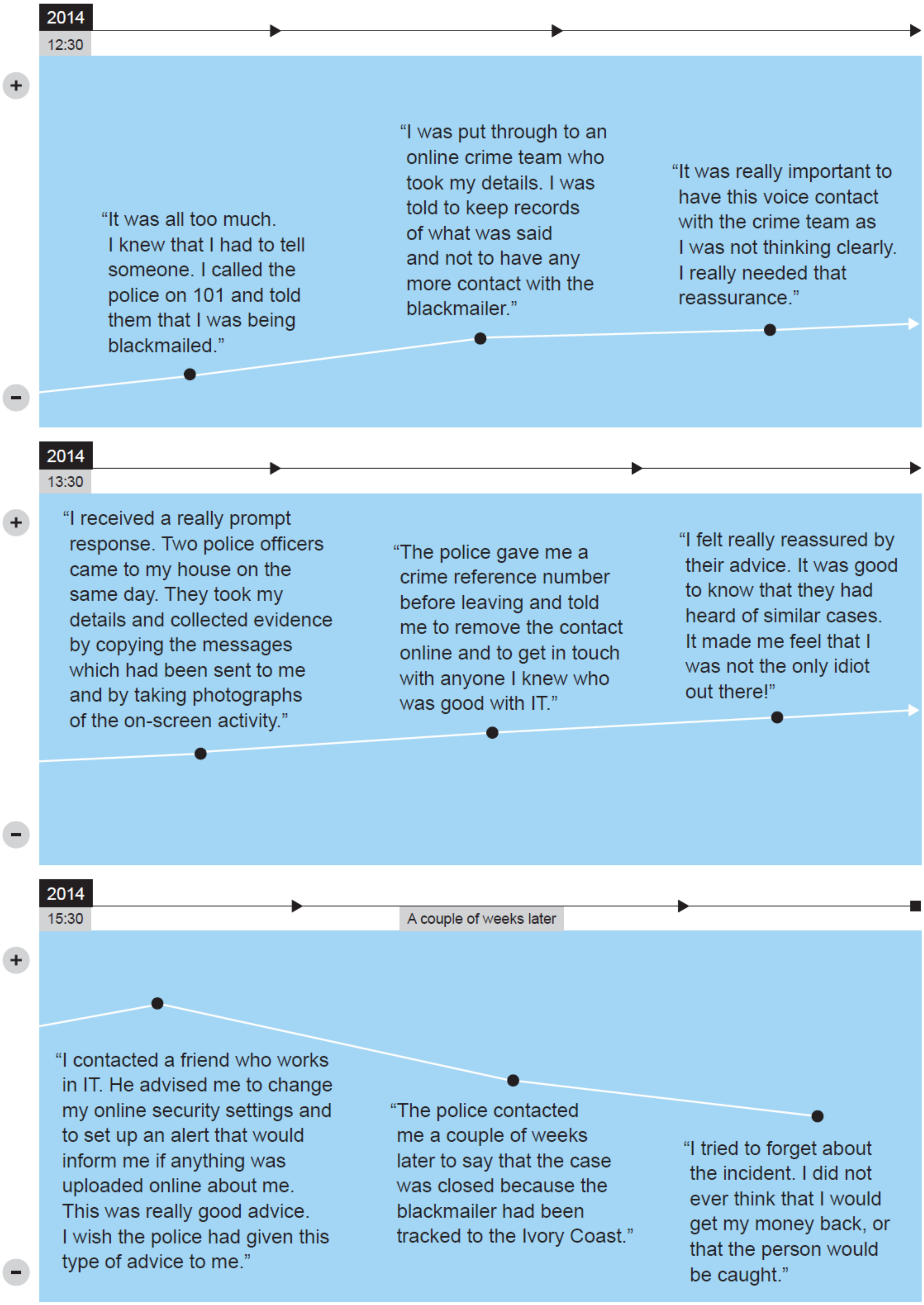
11:30



"I was in shock. I could not believe that this was happening! I panicked and transferred cash without thinking. I felt really stupid!"

"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."

"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!"



2014
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."

"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."

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

2014
13:30

"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."

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

"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!"

2014
15:30

A couple of weeks later

"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 really good advice. I wish the police had given this type of advice to me."

"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."

"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."

6. How are forces responding to online anti-social behaviour?

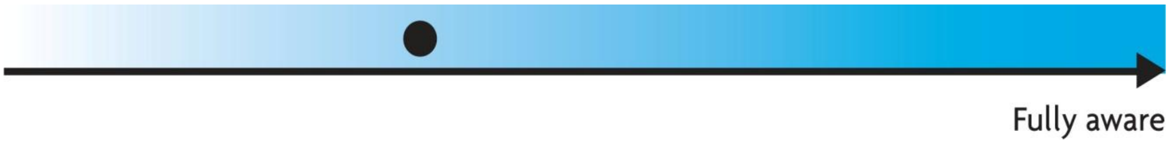
6.1. The increasing willingness of individuals to organise their social events, to strike up, maintain and close down friendships and relationships, and to report their lives online for others to follow and comment upon has led to a substantial increase in social media sites.

6.2. There has been a corresponding increase in the number of complaints that social media sites are being used as vehicles by some to engage in anti-social behaviour directed towards others – be they former friends or partners, or even strangers because the victims' social media profiles have singled them out for unwarranted attention.

6.3. One officer told us that:

> "[m]ost of our time is spent dealing with social media bullying and harassment offences."

Are officers aware of relevant resources and advice?



6.4. Our study has led us to conclude that one of the inhibitors to an effective policing response to this problem is a lack of awareness of what resources and advice are available to staff. A group of frontline managers told us that:

> "staff feel frustrated with their lack of ability to deal with investigations that involved social networking sites".

6.5. We were told of one case which illustrates the point. A complaint was made to neighbourhood police officers which involved the misuse of a social media site. The officers contacted the relevant social networking company based in the United States of America requesting a statement and the account user's details. The company declined to provide the details. Consequently, the officers considered the enquiry to be complete and this element of the investigation was closed.

6.6. The officers did not consider making further enquiries with specialists within the force who could have advised on the correct course of action to be taken.

6.7. We considered the guidance which was available to staff to support them in dealing with online incidents of anti-social behaviour. Our starting point was with the social networking sites themselves.

6.8. A representative of one social media site told us that:

> "[t]here is a knowledge gap with officers not being trained in digital investigations. They do not know how to obtain the most basic of information."

6.9. We understand that initiatives are in place to address this apparent lack of knowledge. For example, one leading social media company has provided free training to the 43 forces about how to obtain evidence from social media organisations.

6.10. The same representative told us that the company had provided guidance to all forces which could be made available to police officers and staff in order to help them advise the public. This included:

- tips to help the public to stay safe online;
- how to help a person who is posting messages online that indicate that they are at risk of suicide or in need of urgent help;
- how parents and families can respond if their child has been the target of online bullying; and
- how education staff can respond when a student has been the target of bullying.

6.11. It is possible that other social media sites and victims' groups may be prepared to help the police to raise the awareness of police officers and staff. Our view is strengthened by a brief trawl of other social media and relevant websites. Each has a substantial bank of information which police officers and staff would find of help when supporting those who come forward to them as victims of online anti-social behaviour.

Useful resources can be found at:

> Help a Friend in Need

> Empower Educators

> Empower Teens

> Empower Parents and Families

> Think Before You Share

National Society for the Prevention of Cruelty to Children

> Safety Online

> Online Abuse

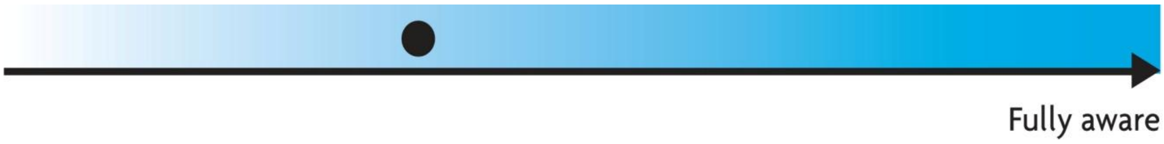
> Share Aware

> Your Guide to the Social Networks Your Kids Use

Suzy Lamplugh Trust

> Is it stalking?

Are the police aware of the vulnerability of victims?



6.12. As we have said throughout this study, a significant cause for concern is the police’s failure fully to recognise the vulnerability of the victims of digital crime. This may be more apparent when the victim suffers a significant fraud that has deprived him or her of thousands of pounds or is a victim of blackmail, but it is also relevant when the offence is one of anti-social behaviour.

6.13. The essential point to remember is that the gravity of the offence and its impact on the victim is not lessened because it is carried out online. In some ways, the vulnerability of the online victim may be increased because the number of people who become aware of the allegation or who read the script of the offender cannot ever be fully known. As a result, many victims are left with the fear that they will be recognised as they walk down the street as a result of what their online assailant has said about them.

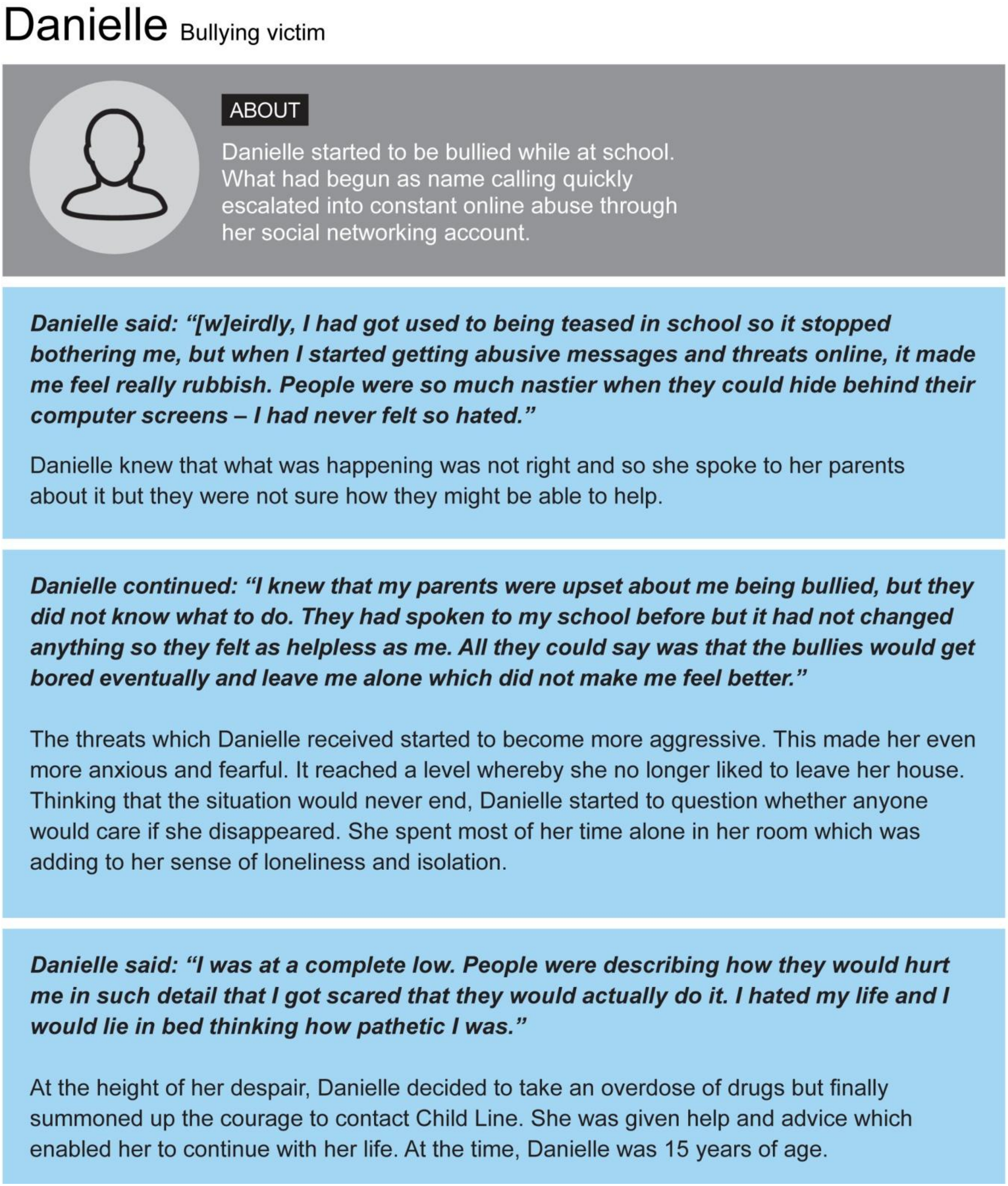
6.14. We found that some police officers and staff were dismissive of complaints about the misuse of social media sites. We were met with comments such as:

> “[w]hat do they [the victim] expect us to do about it?”
>
> “I do not use social media; how am I supposed to investigate it?’

and with regard to a domestic abuse incident, we were told that:

> “[h]e will not carry out the threat to stab her; otherwise he would not have posted the threat online.”

6.15. These comments demonstrate a worrying lack of understanding both of the threat and risk to the victim and, as a consequence, a failure positively to support them. We set out below an example with which we were provided which captures how victims can suffer as a result of such behaviour.



Danielle Bullying victim

ABOUT

Danielle started to be bullied while at school. What had begun as name calling quickly escalated into constant online abuse through her social networking account.

Danielle said: "[w]eirdly, I had got used to being teased in school so it stopped bothering me, but when I started getting abusive messages and threats online, it made me feel really rubbish. People were so much nastier when they could hide behind their computer screens – I had never felt so hated."

Danielle knew that what was happening was not right and so she spoke to her parents about it but they were not sure how they might be able to help.

Danielle continued: "I knew that my parents were upset about me being bullied, but they did not know what to do. They had spoken to my school before but it had not changed anything so they felt as helpless as me. All they could say was that the bullies would get bored eventually and leave me alone which did not make me feel better."

The threats which Danielle received started to become more aggressive. This made her even more anxious and fearful. It reached a level whereby she no longer liked to leave her house. Thinking that the situation would never end, Danielle started to question whether anyone would care if she disappeared. She spent most of her time alone in her room which was adding to her sense of loneliness and isolation.

Danielle said: "I was at a complete low. People were describing how they would hurt me in such detail that I got scared that they would actually do it. I hated my life and I would lie in bed thinking how pathetic I was."

At the height of her despair, Danielle decided to take an overdose of drugs but finally summoned up the courage to contact Child Line. She was given help and advice which enabled her to continue with her life. At the time, Danielle was 15 years of age.

6.16. Danielle’s is not an isolated example. Police officers, parents, social workers and school teachers would recognise her experience in respect of a large number of individuals who have come to their attention.

6.17. It is, therefore, all the more disturbing that one officer told us:

> “[i]t is just kids on Facebook’.

6.18. Such a response is indefensible.

Conclusion

6.19. Each chief constable needs to make sure that his or her officers and staff understand the significance of online anti-social behaviour, and that they are able to provide effective support and advice to those who are its victims.

Judith Online stalking victim

ABOUT

Judith called the police when she started being stalked in an online chatroom, by someone whom she considered to be a friend.

48 Years old

Female

Full time Mum

In her words "The people in that chat room are my friends. We speak everyday."

1 2

Most used devices

1 2 3 4

Online most for...

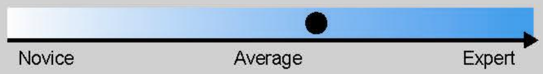
COMMUNICATION CHANNELS

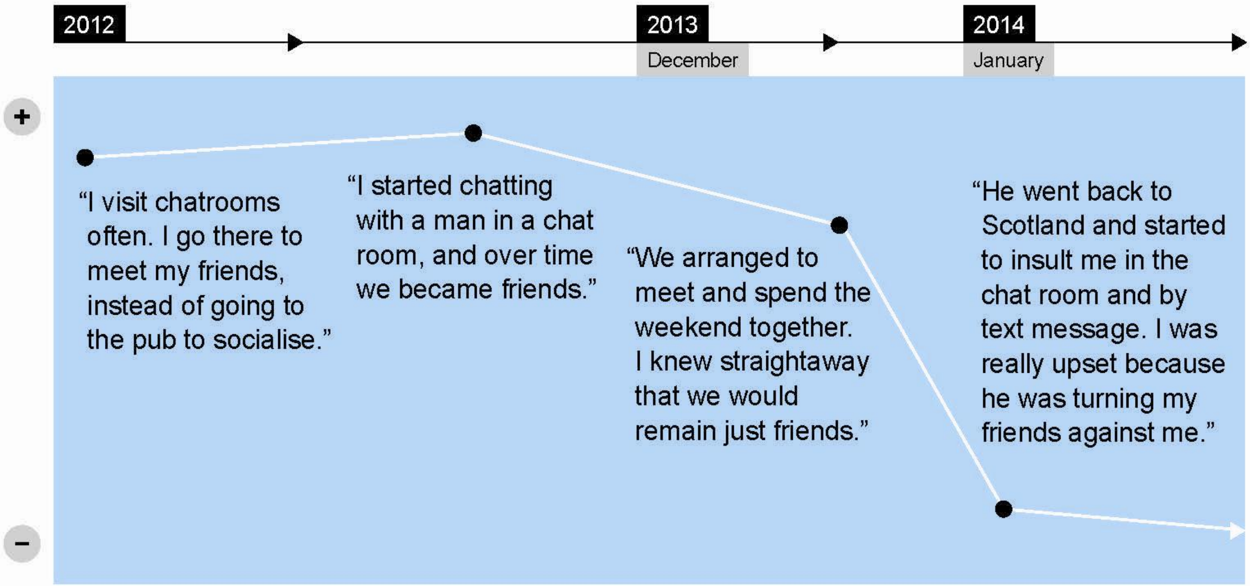
She uses her mobile 'phone and laptop and is active on social media sites. For the last six years, she has been using a chatroom regularly – "you get to know a lot of people".

ONLINE EXPERIENCE

She previously had a six year relationship with someone whom she met on a chat site. Her son had been involved in a potential modelling scam that she identified, but she did not report it – "It is not that serious".

Level of online experience



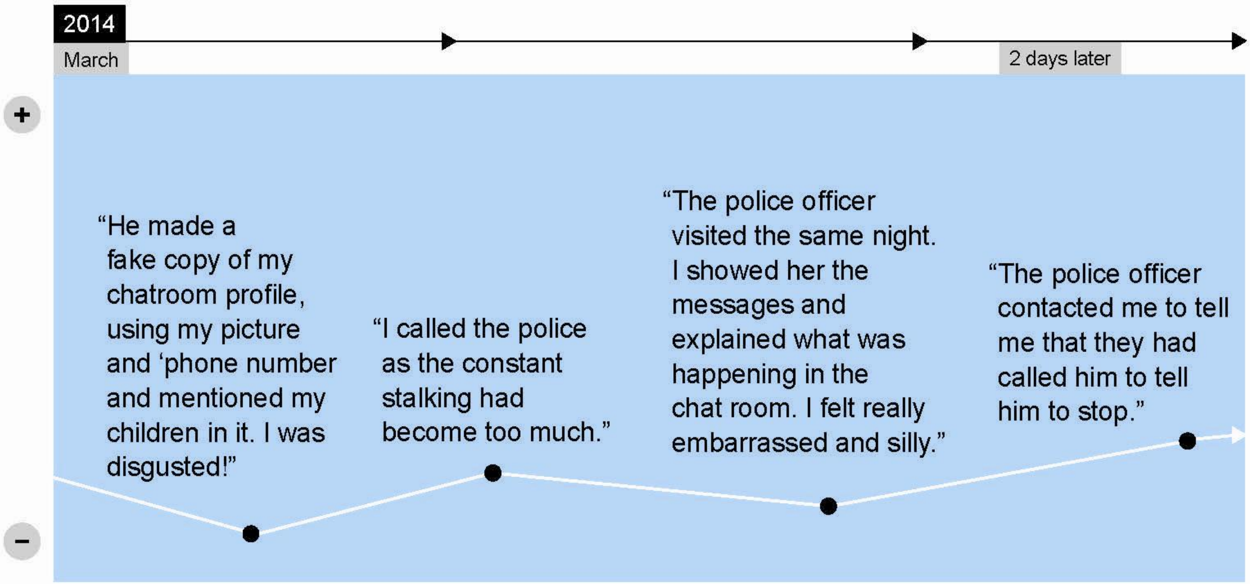


"I visit chatrooms often. I go there to meet my friends, instead of going to the pub to socialise."

"I started chatting with a man in a chat room, and over time we became friends."

"We arranged to meet and spend the weekend together. I knew straightaway that we would remain just friends."

"He went back to Scotland and started to insult me in the chat room and by text message. I was really upset because he was turning my friends against me."

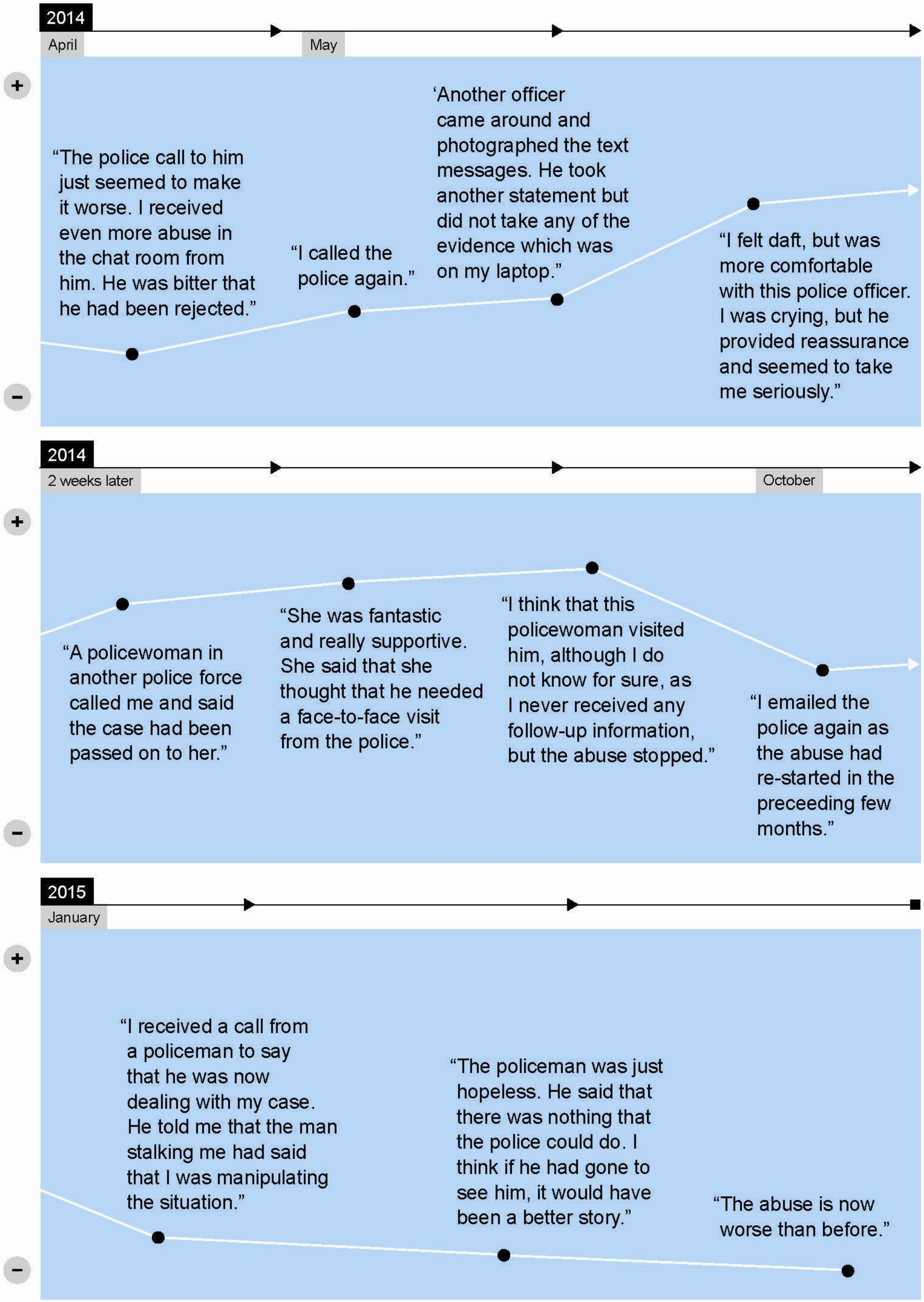


"He made a fake copy of my chatroom profile, using my picture and 'phone number and mentioned my children in it. I was disgusted!"

"I called the police as the constant stalking had become too much."

"The police officer visited the same night. I showed her the messages and explained what was happening in the chat room. I felt really embarrassed and silly."

"The police officer contacted me to tell me that they had called him to tell him to stop."



"The police call to him just seemed to make it worse. I received even more abuse in the chat room from him. He was bitter that he had been rejected."

"I called the police again."

'Another officer came around and photographed the text messages. He took another statement but did not take any of the evidence which was on my laptop."

"I felt daft, but was more comfortable with this police officer. I was crying, but he provided reassurance and seemed to take me seriously."

"A policewoman in another police force called me and said the case had been passed on to her."

"She was fantastic and really supportive. She said that she thought that he needed a face-to-face visit from the police."

"I think that this policewoman visited him, although I do not know for sure, as I never received any follow-up information, but the abuse stopped."

"I emailed the police again as the abuse had re-started in the preceeding few months."

"I received a call from a policeman to say that he was now dealing with my case. He told me that the man stalking me had said that I was manipulating the situation."

"The policeman was just hopeless. He said that there was nothing that the police could do. I think if he had gone to see him, it would have been a better story."

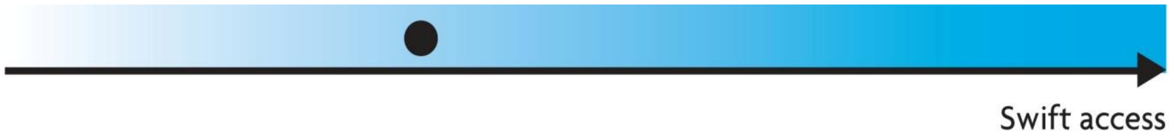
"The abuse is now worse than before."

7. What specialist resources are available to investigators?

7.1. There are very few criminal offences committed in the 21st century where some digital evidence does not exist. The need to retain digital evidence needs to be understood by every police officer in England and Wales, and the ability to identify and recover it needs to be a basic skill that all investigators possess.

7.2. Beyond that, we have sought to understand what specialist support is available to officers in the investigation of digital crime. This support can take the form of technical equipment, trained officers who are able to provide advice and guidance, and specialist investigative capability.

Are investigators able to access digital evidence quickly?



7.3. Each force that we visited during the course of our study had specialist digital forensic capabilities. The size and remit of these units varied, however. Their primary function was to undertake the forensic examination of seized digital devices for evidential purposes. The types of devices examined by these specialist units included computer hard drive units, laptops, tablets, gaming devices, satellite navigational devices and mobile telephones.

7.4. In some instances, the demand placed on these units has outstripped their capacity. This has resulted in significant backlogs. This issue has been the subject of comment in previous HMIC inspections relating to child protection, the most recent of these being *Online and on the edge: Real risks in a virtual world – An inspection into how forces deal with the online sexual exploitation of children*[14]. While we recognise that this issue is of particular importance within the child protection arena it is also equally relevant to all other areas of police investigation.

7.5. During our study, the most common complaints that we heard from police officers and staff related to the length of time that it takes for digital devices to be examined.

[14] See: Online and on the edge: Real risks in a virtual world. An inspection into how forces deal with the online sexual exploitation of children, HMIC, 2014, page 25. See: www.justiceinspectorates.gov.uk/hmic/publications/online-and-on-the-edge-real-risks-in-a-virtual-world

7.6. This has had an impact on the willingness of victims to co-operate because, often, their entire social life is organised through their digital devices. To be deprived of them for a significant period of time is not something that they are prepared to accept. A response officer stated that:

> ”[v]ictims are now reluctant to hand over expensive devices because of the delays.”

7.7. In order to reduce this backlog, some forces have resorted to the outsourcing of the examination of devices to private companies. In one force, we found that over £180,000 had been spent in one year on outsourcing examinations. Despite this, the force still had a nine month backlog of exhibits awaiting examination. One senior officer responsible for digital forensic capability told us:

> “[w]e cannot afford backlogs and we cannot afford to outsource.”

7.8. Other forces have responded to this challenge by providing triage equipment located within police stations. This provides frontline officers with the technology to perform basic analysis of telephone handsets or, as was the case in one particular force, computer hard drives.

7.9. The triage process allows investigators to determine which devices to seize at a crime scene to prioritise the sequence in which to examine devices, and quickly to extract information which might progress an investigation.

7.10. Those frontline staff with whom we spoke during our study were positive about the triage process. They provided evidence of how it had benefited investigations, and we were told that it had resulted in a reduction in the demand placed on the forensic digital capability of those forces.

7.11. On that basis, we hoped to find data that provided a strong argument in favour of the use of triage equipment by frontline investigators. Unfortunately, the collection and analysis of such information are not widespread.

7.12. However, others indicated that they were not persuaded by the use of triage equipment. On a number of occasions, we were told that its use presented “too great a risk” and that officers “might miss something” by using it. One digital forensic manager told us that he was “not a fan of [triage equipment].” However, this opinion was apparently based on intuition, as he also admitted that he had not conducted any research in arriving at his conclusions.

7.13. Whatever the merits of the triage approach, it appears often to be the case that, where it is not adopted, decisions have been made without any reference to empirical evidence. Instead, the judgment is left to middle-ranking managers who are able to influence force policy, sometimes on the flimsiest of evidence.

7.14. During our fieldwork, we found only one force that was using triage equipment in the analysis of computers. This was within a public protection unit where staff used the equipment to identify indecent images which were stored on computers while the suspect was held in custody.

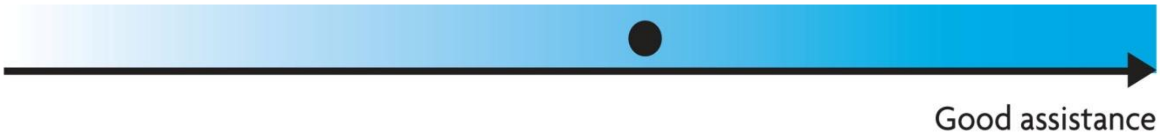
7.15. The decision to use triage equipment had been made after an analysis of the following: the demand within the public protection unit for digital forensic examination; the capacity of the forces digital forensic unit; and an assessment of the risk presented to the public by the release of a suspect from custody without charge while digital forensic examinations took placed. We were informed that the there had not been any negative consequences as a result of the decision to use triage technology.

7.16. The Home Office Centre for Applied Science and Technology[15] has reviewed a wide range of triage devices by testing them within operational scenarios. The results are available to all forces, and their findings should enable operational staff to make an informed decision on the purchase and use of triage tools.

7.17. We recognise that the use of triage equipment is a decision for individual forces to take. However, its use to gather intelligence and evidence in a very timely manner serves to accelerate investigations and so ensure speedier justice for victims. In addition, it reduces the risk of backlogs, caused by an imbalance between demand and resources in the more established digital forensic arena.

7.18. Having hundreds of computers in a backlog awaiting full examination does not support the victim and undoubtedly does not do anything to prevent further crime.

How do digital media investigators assist forces?



7.19. Frontline staff are often left frustrated by their inability to deal with digital investigations. The provision of digital media investigators is one potential means of addressing this frustration. The main function of the role is to advise on the development of an effective technology and data strategy for any investigation or policing operation.

[15] The Centre for Applied Science and Technology, also known as CAST, houses a team of scientists and engineers working within the Home Office. They provide expert advice and support to police forces.

7.20. The number of digital media investigators in each force and how they are deployed is ultimately a decision for the chief constable. They were initially intended to be part of major investigation or serious organised crime investigation teams. However, forces may deploy digital media investigators at a local level to support local investigation teams on volume crime.

7.21. Those undertaking the role are required to have extensive knowledge of communication data technology and successfully to have completed the College of Policing's digital media investigators course which is currently one of three training courses available for those involved in digital crime investigations.[16] We have commented on the potential difficulties which forces face with regard to the continuing funding of the digital media investigators course in paragraphs 5.29 to 5.31.

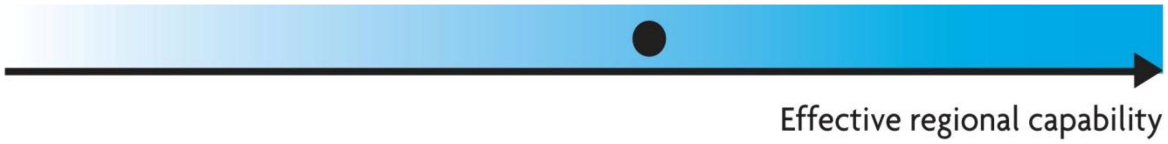
7.22. We found that forces had used digital media investigators in a number of different ways. In all but one force, the introduction of digital media investigators was still very much in the planning stage. The different models included:

- a centrally based, stand-alone unit of digital media investigators, with an additional out-of-hours capability;
- digital media investigators embedded within basic command units; and
- virtual teams of digital media investigators, comprising officers who have been appropriately trained, and who are available to provide advice and guidance as required, but who are deployed in other full-time posts.

7.23. Due to the relative newness of the digital media investigator role, we are unable to comment on the effectiveness of any specific operating model. However, we are sure that the function of the digital media investigator is an important one and that forces need fully to understand the potential demand on those who will perform the role, when deciding how best to use them.

[16] See paragraphs 5.9 to 5.16.

What regional capability exists to deal with digital crime?



7.24. In paragraph 1.11, we explained the component elements of what we have referred to as digital crime. Given the scope of digital crime and the breadth of the challenge presented by it, an effective response requires resources at a local, regional, national and international level.

7.25. The way in which digital crime is handled at the international and national levels stands outside the scope of our study. These levels of crime are overseen by the national cyber-crime unit which is part of the National Crime Agency. We have set out earlier the capability of local forces to deal with digital crime and, to complete the picture, we have considered the capability of forces to do so at a regional level.

7.26. Working in partnership with the national cyber-crime unit are the regional cyber-crime units. These are based within each of the nine regional organised crime units. The regional cyber-crime units provide an investigative capability for crimes that would generally fall within the cyber-enabled or cyber-dependent definitions which we explained in paragraph 1.11. In addition, they undertake a co-ordinating function, which, through regional meetings, enables them to provide updates on emerging national trends.

7.27. The development of the regional cyber-crime units is a very positive step toward combating cyber-enabled and cyber-dependent crimes. We found the relationship between the national cyber-crime unit, regional units and forces was good, with both the national and regional units providing effective support.

7.28. However, we found that, often, investigations were referred to the regional cyber-crime unit on a case-by-case basis, with little evidence of the application of referral criteria. Few to whom we spoke, including senior officers, were aware of any such criteria or, if they were, they recognised that they were inconsistently applied.

7.29. Because the regional units, at this time, still have some available capacity we found them willing to take on most of the cyber-related crimes referred to them.

7.30. However, we foresee that demand will very quickly outstrip the capacity of the regional units and it is therefore essential that an effective tasking and co-ordinating process is established. Without this, the regional units will soon be overwhelmed and important investigations might not be properly prioritised as they should be.

7.31. This will result in the responsibility for a significant proportion of complex digital investigations being returned to local investigators.

7.32. It is important that forces recognise this now, and ensure that they have access to sufficient capacity and capability, either independently or in collaboration, in order to avoid becoming over-reliant on the regional cyber-crime capability.

Conclusion

7.33. Each chief constable needs to make sure that his or her force has the capability: to examine digital devices in the most appropriate, effective and speedy way possible; and to provide sufficient local capability to deal effectively with digital crime.

Nathan Burglary victim

ABOUT

Nathan called the police after finding out that there had been an attempted burglary at his house.

66 Years old

Male

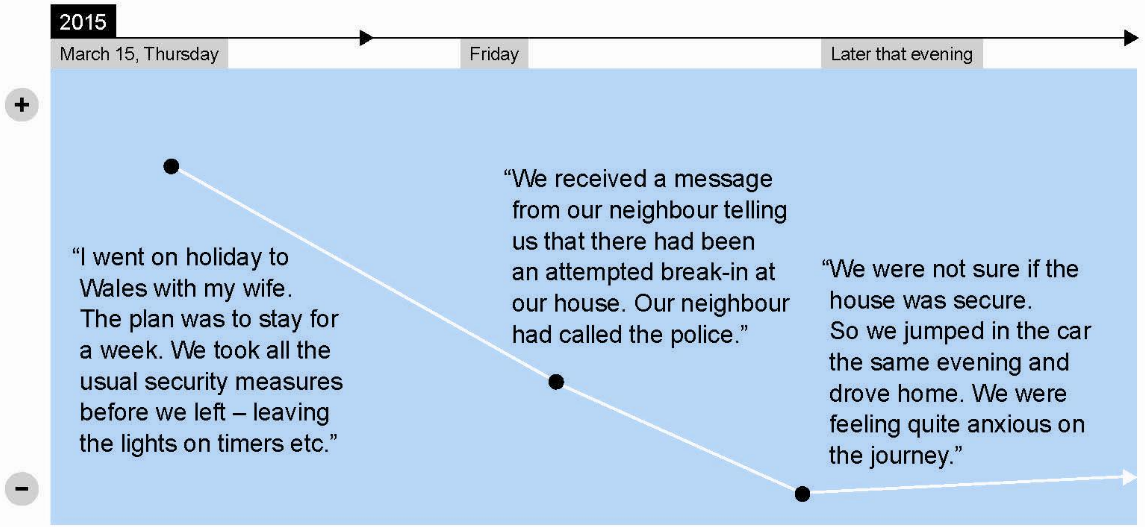
Works as a Civil Engineer

In his words “I do feel like a victim of crime, even if nothing was taken.”

LEVEL OF AWARENESS:

He has never been burgled before and feels that he has a good level of awareness about how to prevent break-ins. “We make sure that everything is secure; we have our lights on timers; and we let our neighbours know to keep an eye out and collect our post if we are away for a long period of time”.

He is also aware about community safety initiatives in the area. “I have received information about the police introducing neighbourhood watch to our area. I have been talking to my neighbours about how this might be done.”



2015

March 15, Thursday

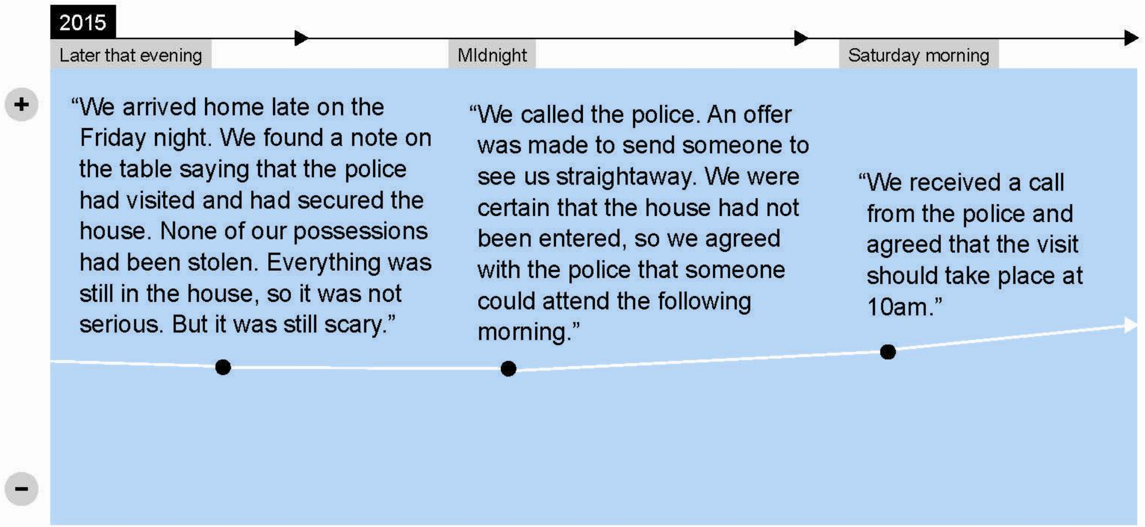
“I went on holiday to Wales with my wife. The plan was to stay for a week. We took all the usual security measures before we left – leaving the lights on timers etc.”

Friday

“We received a message from our neighbour telling us that there had been an attempted break-in at our house. Our neighbour had called the police.”

Later that evening

“We were not sure if the house was secure. So we jumped in the car the same evening and drove home. We were feeling quite anxious on the journey.”



2015

Later that evening

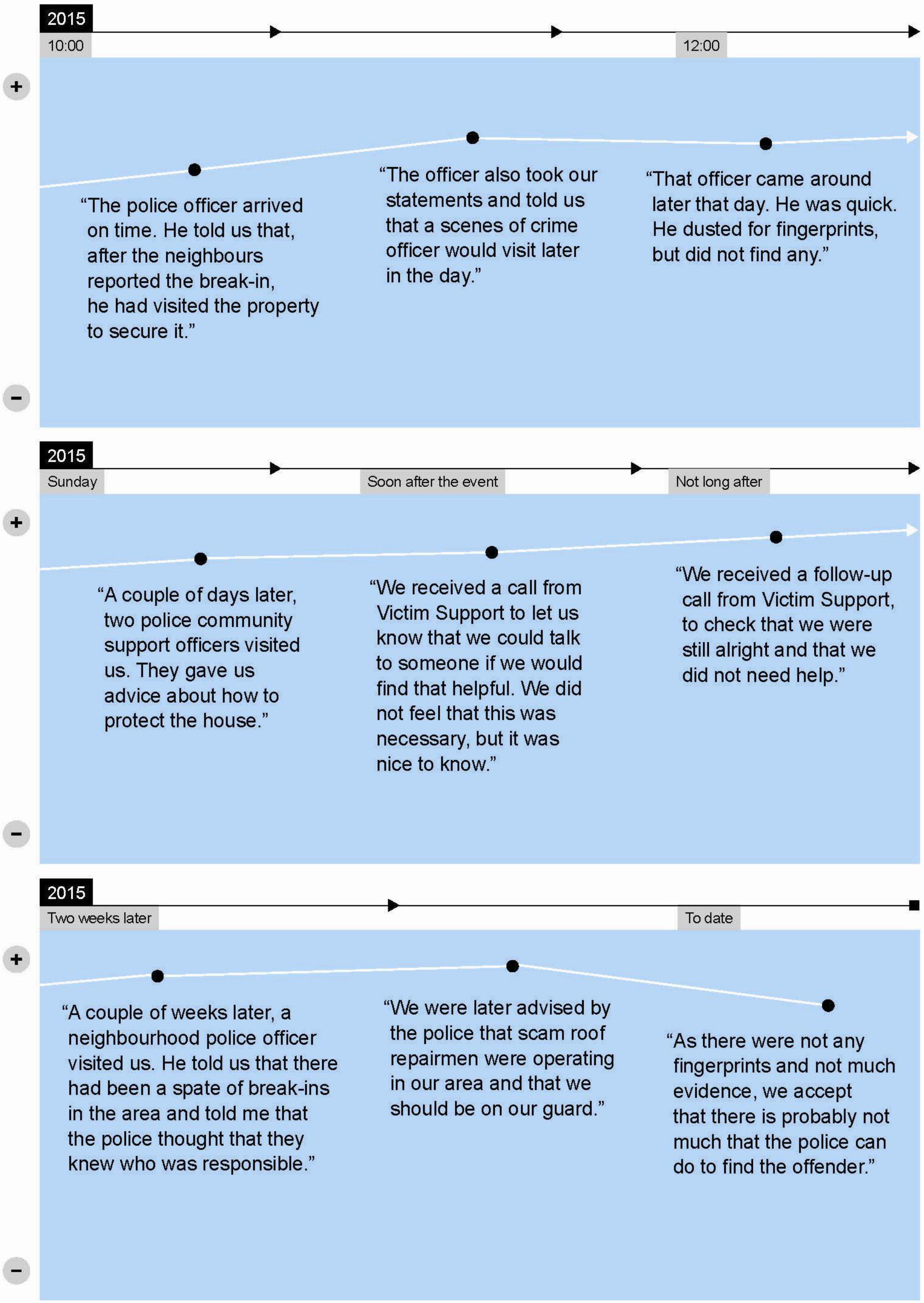
“We arrived home late on the Friday night. We found a note on the table saying that the police had visited and had secured the house. None of our possessions had been stolen. Everything was still in the house, so it was not serious. But it was still scary.”

MIdnight

“We called the police. An offer was made to send someone to see us straightaway. We were certain that the house had not been entered, so we agreed with the police that someone could attend the following morning.”

Saturday morning

“We received a call from the police and agreed that the visit should take place at 10am.”



2015

10:00

12:00

"The police officer arrived on time. He told us that, after the neighbours reported the break-in, he had visited the property to secure it."

"The officer also took our statements and told us that a scenes of crime officer would visit later in the day."

"That officer came around later that day. He was quick. He dusted for fingerprints, but did not find any."

2015

Sunday

Soon after the event

Not long after

"A couple of days later, two police community support officers visited us. They gave us advice about how to protect the house."

"We received a call from Victim Support to let us know that we could talk to someone if we would find that helpful. We did not feel that this was necessary, but it was nice to know."

"We received a follow-up call from Victim Support, to check that we were still alright and that we did not need help."

2015

Two weeks later

To date

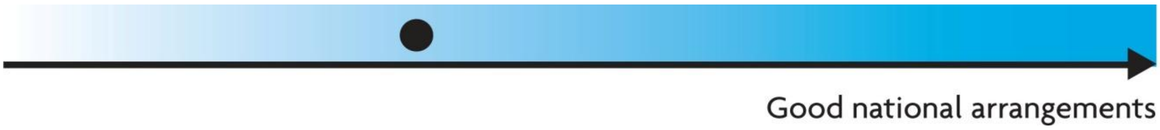
"A couple of weeks later, a neighbourhood police officer visited us. He told us that there had been a spate of break-ins in the area and told me that the police thought that they knew who was responsible."

"We were later advised by the police that scam roof repairmen were operating in our area and that we should be on our guard."

"As there were not any fingerprints and not much evidence, we accept that there is probably not much that the police can do to find the offender."

8. What are the governance and leadership arrangements for digital crime at a national and force level?

What are the national governance and leadership arrangements?



8.1. One of the 12 National Police Chiefs' Council's co-ordination committees that are designed to provide direction and oversee the development of policing policy is the crime operations committee. One of the national policing portfolios that reports to the crime operations committee is the digital intelligence and investigation portfolio. It was established in June 2014 when the chief constable of Essex, Stephen Kavanagh, was invited to "co-ordinate the response to digital intelligence and investigation."

8.2. As a consequence, the development of digital capabilities across the police service is being brought together under the Digital Intelligence and Investigation Framework[17], which was endorsed by chief constables in April 2015. A capabilities management group, chaired by Chief constable Kavanagh, has been established by the National Police Chief's Council, the National Crime Agency, the College of Policing and the Home Office.

8.3. The group will co-ordinate a number of existing strands of work which are directly related to digital crime but housed in different national portfolios, such as digital forensics, communications data, intelligence, economic crime, online child sexual exploitation, social media engagement and cyber-crime.

8.4. The immediate priority for the management group is the development of guidance to help forces establish the necessary capabilities to deal effectively with digital crime. If successful, this will help to establish consistency in the way that victims of digital crime are served across England and Wales.

[17] *Digital Investigation and Intelligence Policing Capabilities for a Digital Age*, National Police Chief's Council, April 2015. See: http://news.npcc.police.uk/releases/chief-constable-stephen-kavanagh-we-have-to-think-digital

8.5. While the police governance structure may now have been simplified, the funding arrangements remain complex. Funding is currently provided through a number of unco-ordinated streams which include the Communications Capability Development Programme,[18] the National Cyber Security Programme,[19] the Police Innovation Fund,[20] and a force's own funding from council tax precepts or the Police Grant. There are also examples of additional funding being made available through European and academic partnerships.

8.6. None of these funding streams has the development of digital policing capabilities as its core function. As a consequence, the ability to lead national change is reliant on the ability of the police service to bid successfully across a range of funding.

8.7. In the past, when aspects of digital crime were spread across a number of different portfolios, there lacked a central point of co-ordination to ensure that any secured funding was most effectively used.

8.8. We hope that, with the advent of a single portfolio, these funding issues will resolve themselves.

8.9. The purpose of this study has not been to inspect the suitability of national structures or, indeed, the effectiveness and efficiency of these individual portfolios. We can say that that the national policing leads with whom we have spoken are clearly passionate about this area of policing and are committed to improving the national policing response to the many and varied challenges presented by digital technology.

8.10. We are certain that the provision of effective digital investigation and intelligence policing capabilities will require the transformation of a significant proportion of the current policing model within England and Wales. Such transformation will require both governance and funding.

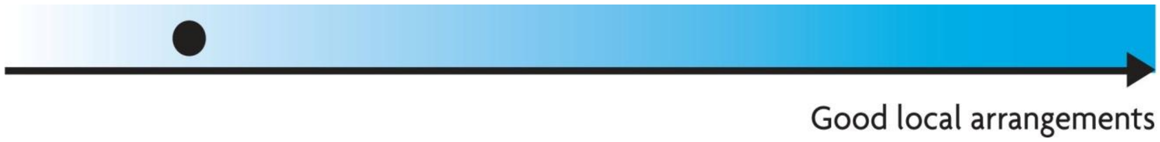
[18] The Communications Capabilities Development Programme is a government programme designed to ensure that police forces and the security and intelligence agencies have the capability to detect, prevent, disrupt and investigate crime.

[19] As part of the Strategic Defence and Security Review in 2010, the government of the day put in place the National Cyber Security Programme. This provided funding between 2011 and 2016 for the Government's response to cyber threats. See: *[t]he Strategic Defence and Security Review",* Her Majesty's Government, October 2010, page 47, paragraph 4.C.1.

[20] This is a Home Office fund of £50M for projects aimed at transforming policing through innovation and collaboration. See: www.gov.uk/government/organisations/home-office

8.11. HMIC regards the co-ordination of this area of business as a positive step. The next challenge is obtaining a secure source of funding in order to take forward the work that will be required to place the police service nationally in the best position possible to respond effectively to digital crime.

What are the governance and leadership arrangements at a force level?



8.12. The case for strong leadership and co-ordination nationally is duplicated at a local level. While the minimum levels of capability may be set at a national level, it is for forces, and in particular chief officers, to ensure that they are provided at a local level.

8.13. We found that the level of involvement of chief officers varied. Some were clearly engaged and had taken responsibility for putting in place clear management structures, strategies and tactical plans. Those tasked with the implementation of these tactical plans were empowered, as a result of effective governance structures, to take matters forward themselves. As a result, these forces were more advanced in the development of their response to digital crime.

8.14. In one force, there was a clear thread of commitment from the police and crime commissioner through to the force's implementation leads. There was a clearly identified chief officer who was able to task, analyse, authorise and, most importantly, co-ordinate change through a management board. A detective superintendent was identified as the strategic lead with four chief inspectors responsible for the implementation of the board's decisions. Tactical implementation plans were in place and there was clear evidence that these were being put into practice.

8.15. As part of this structured response, the force was able to ring-fence a budget, controlled by the chief officer lead, in order to improve the force's digital capability. This was the only force which we visited that had such dedicated funds. The availability of identified funding further facilitated the process of implementation. As one implementation lead commented:

> "the strong strategic structure enabled the implementation of the plan in a relatively straightforward manner."

8.16. This position was not achieved overnight. The original business case for change was written in 2013 and had been, in the words of one senior officer, “a slow burn”. However, the force is now in a position that allows senior officers to be confident that, in a relatively short period, they will be able to demonstrate real change in how the force responds to the needs of the public.

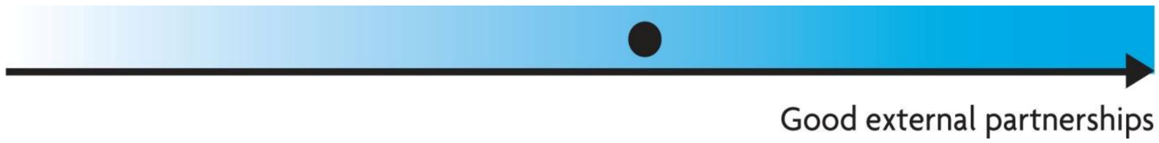
8.17. In other forces, the responsibility for effecting change had been devolved to middle-ranking officers. We found these officers to be well informed and passionate about this area of business. They were committed to driving forward improvements within their particular force and they had achieved impressive results, often by sheer force of personality and interpersonal skills.

8.18. However, while their commitment should be recognised and applauded, it was clear to us that these officers were hindered by the need to drive activity ‘upwards’. This involved gaining access to individual tiers of authority seeking endorsement along the way before any particular initiative could be presented to the relevant chief officer when, if approved, it was then driven ‘down’ and implemented as policy.

8.19. By way of example, we were presented with a strategic training plan in one force. It was an impressive document which provided detail of the various facets of the organisation and the training that was to be provided, by whom and by when. Unfortunately, in the absence of a clear ownership by chief officers it had not been approved, or, in one instance, even seen by senior managers. As a consequence, there was no guarantee that it could or would ever be implemented.

8.20. We consider that the transformation that is required with regard to digital crime cannot be provided by ad hoc arrangements and an over-reliance on middle managers. Irrespective of their personal knowledge and expertise, they do not have either the appropriate level of authority or the strategic oversight to ensure that the required capability is provided in a structured and effective manner.

What external partnerships have the police formed?



8.21. All the forces that took part in the study had, either individually, or in some cases through a regional capability, recognised the benefits of entering into partnerships with academia, businesses and partners within government.

8.22. In one force, such a partnership has resulted in the relocation of the force’s digital forensic services and staff to the local university's campus. This enables the force’s digital forensic teams to work alongside university staff and students. The force considers that this partnership provides a wide range of benefits which include: enhanced research opportunities within an operational environment; the ability to develop an internship scheme; and improved experiential and practical learning for students.

8.23. We also found that a number of forces were making good use of partnership arrangements at a national level, such as the Cyber-security Information Sharing Partnership, known as CISP.[21] This is part of Cert-UK, the United Kingdom National Computer Emergency Response Team,[22] which was formed in March 2014 in response to the National Cyber Security Strategy.[23]

8.24. CISP is a joint industry and government initiative which shares current threat and vulnerability information in order to increase awareness of the cyber threat and therefore reduce the impact on businesses within the United Kingdom.

8.25. We found that a number of forces were engaging with local businesses and raising awareness of the benefits that membership of the partnership provides. One force was seeking to establish, at a local level, a similar forum with membership open to business and individuals.

[21] This is a joint industry and government initiative, designed to share cyber threat and vulnerability information and therefore reduce the impact on United Kingdom business. See: www.cert.gov.uk/cisp/

[22] Cert-UK has four main responsibilities: providing national cyber-security incident management; supporting critical national infrastructure companies to handle cyber-security incidents; promoting cyber-security situational awareness across industry, academia and the public sector; and providing a single international point of contact. See: www.cert.gov.uk/

[23] See: *[t[he UK Security Strategy: Protecting and promoting the UK in a digital world*, Her Majesty’s Government, November 2011.

8.26. Other forces were using the same principle at a neighbourhood policing level. Subscribers to an alert service received online updates of emerging digital threats.

8.27. We commend these local initiatives to other forces which have yet to consider how best to ensure that their local communities are involved in responding to the threat which digital crime poses.

Useful resources:

> Cert-Uk

> Cyber-security Information Sharing Partnership (CiSP)

> Get Safe Online

> Cyber Street Wise

> Cyber Essentials

Conclusion

8.28. The police service needs to create effective leadership, and governance arrangements and strategies at all levels to manage the threat that digital crime poses, engaging with all those inside the police service and in the private sector who are able to provide expertise.

Simon Fraud victim

ABOUT

Simon called Action Fraud after he realised that he had invested money in scam operations.

67 Years old

♂ Male

Retired special needs teacher

In his words "I have retired recently and have been looking for ways to invest my money for my children and grandchildren!"

1 2

Most used devices

COMMUNICATION CHANNELS

He has a laptop at home and both a landline and a smart 'phone. He uses the internet sometimes, mainly to check the news. He has an email address, but doesn't send emails often.

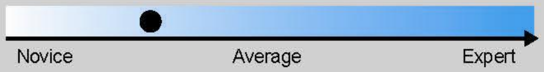
ONLINE EXPERIENCE

He is comfortable with technology "up to point." He doesn't feel he has much experience although "If I got taught, I would be alright".

1 2

Online most for...

Level of online experience



2-3 years ago

Day 1

"I received various 'phone calls offering me investments. One offered me higher interest rates than any bank."

1-3 weeks later

"The man was very persuasive. It really seemed like a good investment, so I transferred £30,000 to him. I thought that I was making a good investment. I was told that the interest would start accruing in a couple of months' time."

1-2 weeks later

"Not long after, I received another call about investing in rare metals. The man offered to meet me in person."

2-3 years ago

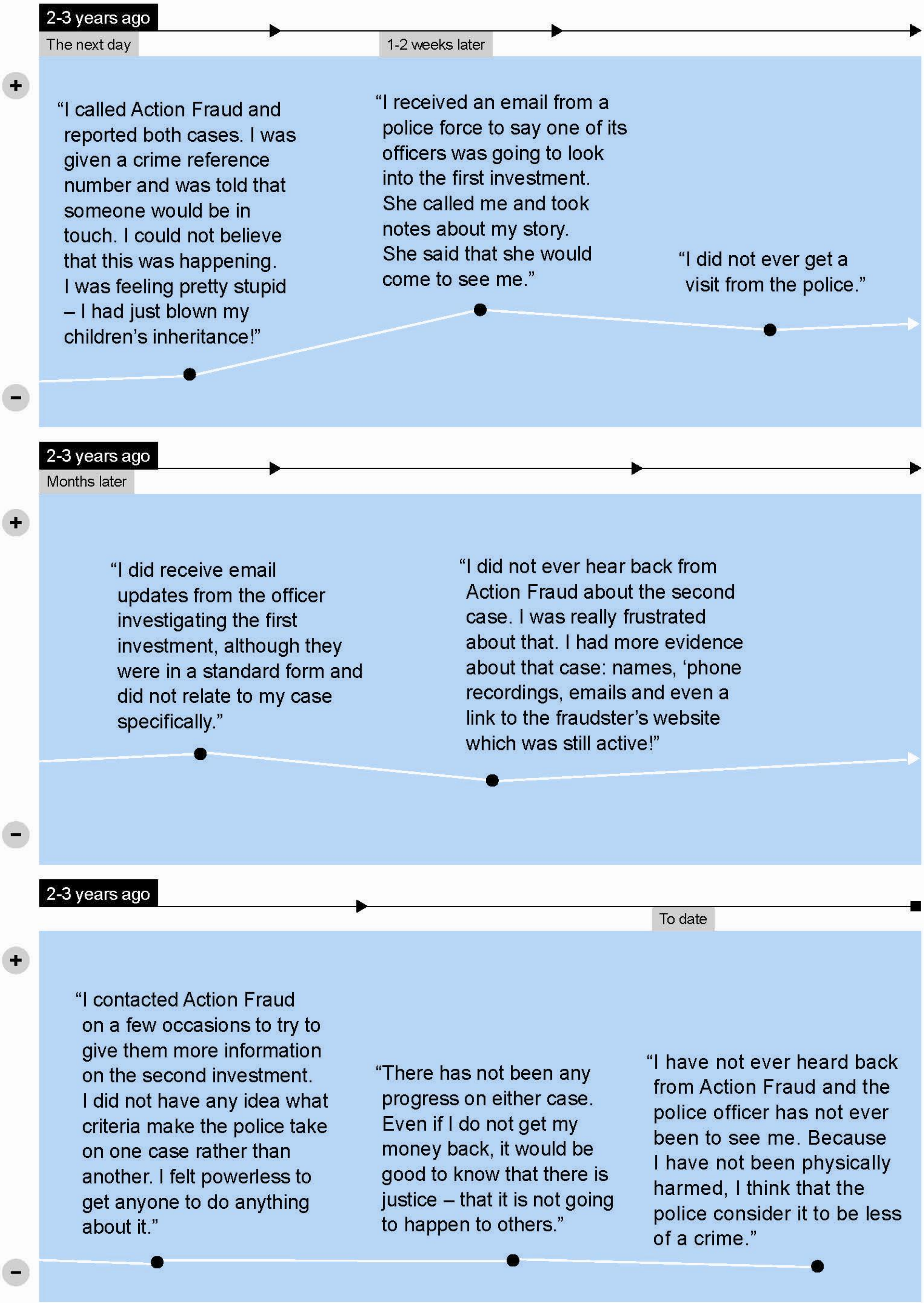
2 months later

"I went to London to meet him. He talked through all the details with me and I decided I that I would invest another £30,000 in rare metals. It seemed like another great opportunity."

1-2 months later

"A couple of months later, when talking about the investments to others, I was alerted to the fact that I might have been the victim of fraud. I was shocked. I really thought that I had made sound investments!"

"I was advised to contact Action Fraud. I do not know what I would have done if they had not been told to do that – I might have gone to the local police, but I do not know if that would have been the right way to go about it!"



“I called Action Fraud and reported both cases. I was given a crime reference number and was told that someone would be in touch. I could not believe that this was happening. I was feeling pretty stupid – I had just blown my children’s inheritance!”

“I received an email from a police force to say one of its officers was going to look into the first investment. She called me and took notes about my story. She said that she would come to see me.”

“I did not ever get a visit from the police.”

“I did receive email updates from the officer investigating the first investment, although they were in a standard form and did not relate to my case specifically.”

“I did not ever hear back from Action Fraud about the second case. I was really frustrated about that. I had more evidence about that case: names, ‘phone recordings, emails and even a link to the fraudster’s website which was still active!”

“I contacted Action Fraud on a few occasions to try to give them more information on the second investment. I did not have any idea what criteria make the police take on one case rather than another. I felt powerless to get anyone to do anything about it.”

“There has not been any progress on either case. Even if I do not get my money back, it would be good to know that there is justice – that it is not going to happen to others.”

“I have not ever heard back from Action Fraud and the police officer has not ever been to see me. Because I have not been physically harmed, I think that the police consider it to be less of a crime.”

9. How do forces, Action Fraud, and the National Fraud Intelligence Bureau work together?

What are the current arrangements?

9.1. With the volume of personal details now stored online, with the ability for another to obtain them and for that person then to remain unseen online, it is little wonder that fraud has become a growth industry in terms of digital crime.

9.2. Fraud, in all its guises, is one of the principal offences which does not respect police force boundaries, either within the United Kingdom or internationally.

9.3. As a result, it became clear that a national perspective needed to be adopted to reflect the ways in which fraud can be committed.

9.4. In 2006, structures were created which were designed to provide a more co-ordinated and nationally consistent response to fraud. The City of London Police became the national lead force for fraud with responsibility for the National Fraud Intelligence Bureau and the Home Office created the National Fraud Reporting Centre.

9.5. In 2009, the National Fraud Reporting Centre was renamed Action Fraud and, in 2014, it came under the control of the City of London Police.

9.6. Action Fraud provides the central point of contact for the reporting of fraud and online crime. It receives crime reports and information reports in one of four ways:

- directly from members of the public over the telephone;
- directly from members of the public via an online reporting process;
- directly from police forces, or other law enforcement agencies on behalf of victims; and
- directly from businesses using an online bulk reporting tool.

9.7. The National Fraud Intelligence Bureau processes the information received by Action Fraud. Following analysis, the bureau provides the police and other law enforcement agencies with:

- individual crime packages – these identify viable opportunities to undertake a criminal investigation or take disruptive action;

- victim profiles – these contain the details of all victims of crime and the type of crime to which they have been subjected. A monthly schedule of this information is forwarded to the police force which serves the address provided by the victim of the reported crime;

- force profiles – these provide statistical analysis of crime trends, crime types and emerging crime techniques used by offenders within force areas; and

- monthly threat updates – these support a national profiling of current and emerging fraud.

9.8. Neither Action Fraud nor the National Fraud Intelligence Bureau is responsible for the investigation of offences. That duty remains with the local police force or other appropriate law enforcement agency.

9.9. Action Fraud receives on average 25,000 reported crimes and a further 12,000 information reports per month.[24] This creates a significant amount of information that requires a database for it to be analysed. The database used by the National Fraud Intelligence Bureau is the ‘Know Fraud’ system. This system is used to identify links and patterns in offending.

9.10. A case in which there are so-called ‘solvability factors’ is highlighted and passed to a team within the bureau so that it may establish whether there is a realistic prospect of identifying the offender through a bank account, postal address, internet address or telephone number. Where this is the case, and the bureau considers that there are viable lines of enquiry to pursue the offender (for example, because he or she is thought to be within the jurisdiction), the matter is referred to the relevant police force or other law enforcement agency to pursue.

9.11. Cases in which there are no such factors or where there are no viable lines of enquiry remain on the ‘Know Fraud’ database for further analysis.

How is the victim kept in touch?

9.12. Upon reporting a crime, the victim receives an automatically generated letter. The letter provides a specific crime reference number and an explanation of the National Fraud Intelligence Bureau process. The letter also states that the victim will be provided with an update by letter within 28 days.

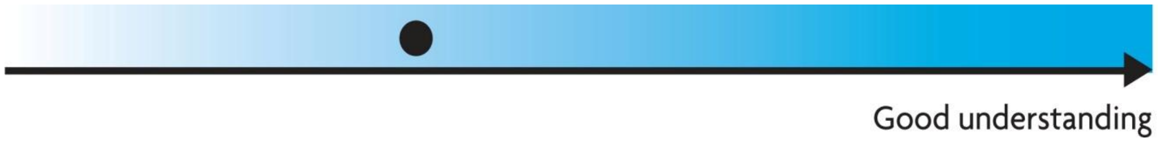
[24] An information report is a report from a member of the public or from a business which, according to the way in which crimes are recorded, falls short of being classified as a crime but which nonetheless alleges fraudulent activity. Such a report may still be used for intelligence purposes by the police.

9.13. Depending on the analysis undertaken by the bureau concerning the solvability factors and viable lines of enquiry in the case, the follow-up letter will state one of two conclusions; either that no further action will be taken at that time, and that the victim's details will remain on the database, or that solvability factors and viable lines of enquiry have been identified and that the case has been forwarded to a specific police force or law enforcement agency for further action.

9.14. Contrary to the usual position, the local force or agency to which such a crime will be forwarded is the force or agency where the viable lines of enquiry arise. This may not necessarily be the force or agency where the crime was committed or where the victim lives.

9.15. In order to ensure that the victim's local force is aware that a crime has been committed in its area, the National Fraud Intelligence Bureau provides each force with the details of every victim who resides within its area, on a monthly basis. These details include those victims whose cases remain on the 'Know Fraud' database because they do not have any solvability factors.

How well understood are Action Fraud and the National Fraud Intelligence Bureau?



9.16. During our study, we found very few police officers and staff who understood either their own roles and responsibilities or those of their force in relation to the investigation of fraud. In particular there was a lack of knowledge, at all ranks, regarding the functions of Action Fraud and the National Fraud Intelligence Bureau.

9.17. Consequently, the advice and support which the police should provide to the victims of such crime are poor. For example, on two occasions, in two separate forces, we were told by neighbourhood policing officers that they didn't understand the process and they would advise victims who reported frauds to call 101.

9.18. Misunderstanding the role of Action Fraud appears to be rife.

9.19. We conducted a group discussion in one force with call handlers and enquiry desk staff who commented that they would:

> "refer the victim direct to Action Fraud";
>
> "deploy a police officer to take a crime report from the victim";
>
> "transfer the victim to the criminal investigation department";

> "make an appointment for a police community support officer to speak to the victim"; and
>
> "transfer the victim to the force economic crime unit".

9.20. This clear lack of understanding among many who come into contact with victims about the right procedure to adopt was consistent across most police forces which helped us in our study, both at tactical and strategic levels.

9.21. Yet, all the forces which we visited had a nominated officer, at either detective sergeant or detective inspector level, to receive and manage those cases referred to the force from the National Fraud Intelligence Bureau. He or she was responsible for the case management of the investigations and was fully aware of the way in which fraud cases should be reported to Action Fraud and of the response that could be expected from the bureau. However, it appeared that these officers did not carry sufficient weight to ensure that the remainder of police officers and staff in their forces were equally well informed.

9.22. When we spoke to chief officers about National Fraud Intelligence Bureau referrals, they invariably directed us to those specialist middle-ranking officers. In all but one force, there was an absence of strategic leadership and direction, which resulted in a lack of performance management and priority setting in relation to the reporting and investigation of fraud.

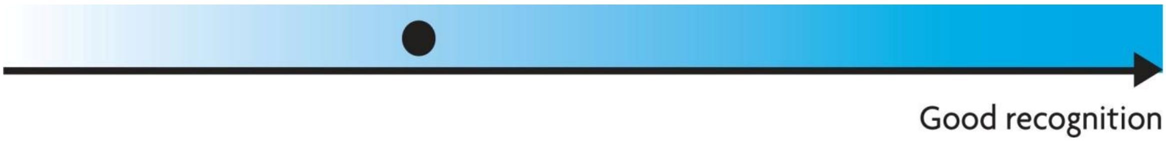
9.23. The numbers of crimes reported to Action Fraud annually have more than doubled since 2013. Despite this, fewer than 50 percent of forces regularly assess the impact of fraud in their strategic risk assessments.[25]

9.24. We are aware that the National Police Co-ordinator for Economic Crime wrote to every chief constable in March 2015 highlighting best practice. In his letter, he stressed that the entire process needed to be "owned by an accountable chief officer". He asked that every force notify him of its nominated chief officer.

9.25. By August 2015, he had received only 14 responses out of a possible 43.

[25] See: *National Fraud Capability Survey*", national police coordinator for economic crime, March 2015, page 10.

Do the police correctly recognise the need for an immediate response?



9.26. None of the victims who took part in our study initially contacted Action Fraud to report the crime. His or her first point of contact was the local force, and call handlers across all forces confirmed that they receive calls from victims of fraud on a daily basis. Therefore, the call handler's role is particularly important in identifying and responding to the needs of the victim.

9.27. We found good examples of staff identifying the need for an immediate police response. However, too often we found that the victim was directed to Action Fraud without a full assessment of the individual case. One detective sergeant with responsibility for the investigation of fraud was particularly frustrated:

> "[t]his should be our bread and butter but we get it wrong all the time. We tell people to contact Action Fraud rather than recognise that this is a call for service."

9.28. Our study's findings were supported in an earlier HMIC inspection, the report of which was published in November 2014.[26] There, the inspectors witnessed call handlers forwarding telephone calls from victims to Action Fraud, without making any attempt to establish the circumstances of the crime or the vulnerability of the victim.

9.29. Our case study concerning Megan, page 28, further illustrates this point. Megan reported to the police that her computer had been 'hacked' and she was immediately transferred to Action Fraud, despite the fact that there were clearly steps that the local force should have taken to remedy the situation. Consequently, when the offending against her continued, Megan did not contact the police again because she had already been advised that it was not a matter for them to investigate.

9.30. Our findings were echoed by the National Police Co-ordinator for Economic Crime following a survey of national fraud capability undertaken in March 2015.[27] In his letter to all chief constables, he asked forces to satisfy themselves that:

[26] *Crime-recording: making the victim count*, Her Majesty's Inspectorate of Constabulary, November 2014. This is available at www.justiceinspectorates.gov.uk/hmic/wp-content/uploads/crime-recording-making-the-victim-count.pdf

[27] See: *National Fraud Capability Survey*, national police coordinator for economic crime, March 2015.

> "[c]alls for service particularly from vulnerable victims receive the most appropriate support at the time they report and these cases are not just referred onto Action Fraud. The appropriate response in such cases is for a local force to take immediate action to prevent ongoing victimisation or financial loss and then to support the victim in reporting to Action Fraud."

9.31. We agree.

9.32. A further consequence of the failure of forces to respond appropriately is the loss of opportunity to take immediate action.

9.33. Action Fraud has advised us that, between April 2014 and March 2015, the total losses reported to it were approximately £3.5bn. A significant proportion of these monies were transferred initially from the victims' bank accounts to bank accounts in the United Kingdom. Invariably, these accounts were opened or operated by the offenders. Thereafter, however, the monies were likely to be transferred to other accounts, often within 24 hours of the original fraud.

9.34. This provides a limited window of opportunity for the police to respond in an attempt to prevent the loss of the monies entirely. And the possibility that immediate action might be taken to secure the monies for the victim is often the motivation behind the victim's call to the police in the first instance.

9.35. We have set out the way in which Action Fraud and the National Fraud Intelligence Bureau undertake their work in paragraphs 9.11 to 9.13. The bureau's analysis of individual crimes takes time. One force crime manager informed us that, in general, a crime reported to Action Fraud would take at least 30 days before it is allocated to an investigator in force.

9.36. This delay presents a substantial opportunity to the offender who has the ability to generate a complex money trail, often involving bank accounts outside the jurisdiction, to salt away the fraudulently-obtained funds.

9.37. To optimise the opportunities for the police to respond effectively, it is essential that calls for service are properly recognised and appropriately handled.

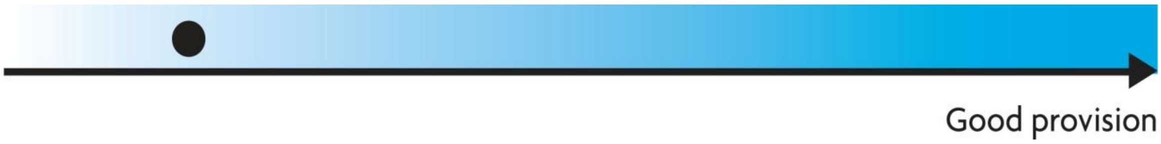
9.38. It is only right that we point out, however, that we did find some examples of individual members of police staff providing excellent service to members of the public.

9.39. Several of these related to ‘courier frauds’.[28] Recognising that these were calls for service, call handlers immediately deployed officers who were able either to prevent credit cards being stolen, or, in some cases, to arrest the offender.

9.40. A police community support officer provided a further good example of swift action. He received information that a member of the public had recently transferred money into a fraudulent bank account. The officer, recognising the urgency of the situation, contacted the bank and was able to prevent the funds being withdrawn.

9.41. These examples of good policing are commendable, but isolated; they should be standard procedure.

Do the police provide appropriate levels of care to victims?



9.42. While it is clear that Action Fraud is responsible for the recording of fraud and cyber-crime, local forces continue to be responsible for protecting their local communities against those who commit crime, and for supporting those who fall victim to it.

9.43. During our study, we found that there is a lack of an effective response to fraud at a local level. One chief officer told us that chief constables considered that they had: “given [fraud] in its entirety to Action Fraud.”

9.44. Our findings are supported by the national fraud capability survey undertaken by the office of the National Police Co-ordinator for Economic Crime which identified that:

> “at a strategic level, less than 50 percent of forces assessed the impact of fraud within their force strategic assessments”.

9.45. In the forces which we visited, we found limited awareness of the fraud victim profiles within their communities.

[28] Courier fraud is committed when the offender attends the address of the victim to collect his or her credit card, following a telephone conversation purporting to come from the credit card company in which it is falsely claimed that the victim’s card has been compromised.

9.46. This is especially disappointing given that the National Fraud Intelligence Bureau provides forces, on a monthly basis, with details of all victims of fraud and cyber-dependent crime in their force areas. We found that few were aware that these data either existed or, if they were aware, they did not use them for any beneficial purpose.

9.47. We have concerns, too, that the fact that the fraud is committed online remains a factor which distinguishes the level of police response from that provided in respect of other crimes.

9.48. In our case study concerning Simon, page 62, who was the victim of a 'boiler room'[29] fraud to the value of £60,000.He disclosed that he did not have any contact whatsoever from his local force.

9.49. In another case, another victim of fraud told us that he had lost £18,000 but that there had not been any follow-up action by his local force.

> "It was a really disappointing and upsetting outcome. We thought this would have been easy to solve. We had all the evidence and the police never came around to see us."

9.50. Yet, in the case of an attempted burglary, one victim described that within 72 hours of reporting the attempt, he had received visits from a response officer, crime scene investigators and police community support officers.

9.51. This disparity in approach is difficult to reconcile without reflecting on the manner in which the two crimes were perpetrated. The response is all the more concerning, given that Simon actually lost a substantial sum of money and the victim of the attempted burglary retained all his possessions.

9.52. Victim care is important. It enables forces to provide relevant and timely crime prevention advice to victims with a view to reducing the risk of repeat victimisation, which is particularly prevalent among fraud victims. It also provides a means by which the police can signpost victims to other agencies who can provide more bespoke support.

9.53. We found little evidence of effective care for fraud victims generally. One neighbourhood police officer told us that:

> "[w]hen I patrol my area I know who has been the victim of crime, except for those who have been the victim of fraud".

[29] A 'boiler room' fraud usually involves bogus stockbrokers, cold calling people to pressure them into buying shares that promise high returns. In reality the shares are either worthless or non-existent. See: www.actionfraud.police/fraud-az-boiler-room-fraud

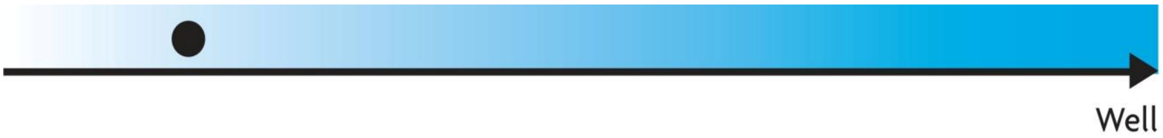
9.54. We found that some forces have begun to develop strategies; however, with the exception of one force, they have yet to be implemented.

9.55. That one force was able to demonstrate impressive results. It has established a victim care unit specifically for victims of fraud. By identifying those individuals who are vulnerable to repeat victimisation, the unit is able to provide them with bespoke advice. We recognise that this unit is in its infancy but very early results indicate a significant reduction in repeat victimisation and an increase in victim satisfaction.

9.56. An important element in the unit's initial success has been its recognition of the role that partner agencies play in the provision of victim care. As well as providing effective crime prevention advice, the unit directs victims to partner agencies. These agencies are then able to provide practical help to victims of crime.

9.57. Other forces will want to consider the effectiveness of their support and care for victims of fraud, including online fraud.

How do forces deal with referrals from the National Fraud Intelligence Bureau?



9.58. Referrals from the National Fraud Intelligence Bureau to police forces are increasing year on year. Between October and December 2014, the bureau referred 18,751 cases to police forces and other law enforcement organisations.

9.59. While the way in which forces are structured to handle these referrals is outside the scope of our study, we do want to express our concerns about the inconsistency in approach adopted between forces in handling the referrals at all.

9.60. The bureau only refers a case back to a local force after it has assessed it and decided that there are viable opportunities to undertake a criminal investigation or to take disruptive action. It is incumbent upon the force concerned to consider any such referral and to take appropriate action.

9.61. Indeed, we found forces which did adopt a policy of allocating and investigating all referrals from the bureau. However, we are also aware of other forces (not those who took part in our study) that impose a financial threshold on bureau referrals with the consequence that those victims whose loss is below a certain amount do not have their cases allocated for further investigation. We understand other forces impose arbitrary limits on the number of bureau referrals which they will investigate.

9.62. In one force, that limit has been set at 20 percent. We are unsighted about how a case is considered to be within the 20 percent band. Given that the force does not know when it makes that decision how many referrals it is to receive from the Bureau in any given time frame, we cannot understand how it decides whether a particular case falls within or outside the quota.

9.63. In seeking to help forces to identify what needs to be done, and in the absence of any authorised professional practice issued by the College of Policing, we cannot do any better than to cite the National Police Co-ordinator for Economic Crime. In his letter of March 2015 to chief constables, he set out best practice in relation to the management of fraud referrals from the National Fraud Intelligence Bureau.

9.64. In an abridged form, he said that there should be:

- a clear and auditable process for the receipt of National Fraud Intelligence Bureau case dissemination;
- a clearly understood and transparent process for the dissemination of cases to appropriately skilled investigators;
- an identified individual, responsible for case management, progress tracking, and reporting back to the National Fraud Intelligence Bureau;
- the ability to test the provision of victim care in relation to calls for service coming into local contact centres or police enquiry desks;
- an identified subject matter lead at senior management team level; and
- an accountable chief officer to monitor and manage performance, including the support given to local victims.

9.65. We entirely agree.

Conclusion

9.66. Each chief constable needs to appoint a chief officer to ensure that his or her staff understand which cases should be referred to Action Fraud and which require a more immediate response, and that referrals from the National Fraud Intelligence Bureau are dealt with effectively.

10. Conclusions

10.1. The aim of this study has been to set out our views about the current preparedness of the police service to deal effectively with digital crime and its victims. This has not been an inspection in the traditional sense. We recognise that the speed of developments in this fast-moving and ever-increasingly technological era requires a different approach from HMIC.

10.2. Here, we have drawn together those areas of policing which, if put into effect, will enable the police, at all levels, to provide the best possible service to victims of digital crime. This will also help HMIC to identify those areas which will contribute to our annual all-force inspections.

10.3. The police service needs:

- to establish the scale and impact of digital crime, at both the national and local level, and how to respond to it;

  paragraph 4.17

- to create effective leadership, and governance arrangements and strategies at all levels to manage the threat that digital crime poses, engaging with all those inside the police service and in the private sector who are able to provide expertise.

  paragraph 8.28

10.4. And each chief constable needs:

- to provide appropriate and continuing training and guidance for all those within his or her force who are likely to deal with digital crime and its victims;

  paragraph 5.56

- to make sure that his or her officers and staff understand the significance of online anti-social behaviour, and that they are able to provide effective support and advice to those who are its victims;

  paragraph 6.19

- to make sure that his or her force has the capability: to examine digital devices in the most appropriate, effective and speedy way possible; and to provide sufficient local capability to deal effectively with digital crime; and

  paragraph 7.33

- to appoint a chief officer to make sure that his or her staff understand which cases should be referred to Action Fraud and which require a more immediate response, and that referrals from the National Fraud Intelligence Bureau are dealt with effectively.

paragraph 9.66

Annex A Legislation

In Annex A we have included a brief statement of the offence or offences which may have been committed by the perpetrator in the victim stories contained within this report. We have set out the maximum sentence in relation to each offence to provide an indication of how serious the offences are.

Based on Jane's account, the offence committed is fraud by false representation, contrary to section 2(a), Fraud Act 2006.

Section 2 states:

(1) A person is in breach of this section if he—

(a) dishonestly makes a false representation, and
(b) intends, by making the representation—
(i) to make a gain for himself or another, or
(ii) to cause loss to another or to expose another to a risk of loss.

(2) A representation is false if—

(a) it is untrue or misleading, and
(b) the person making it knows that it is, or might be, untrue or misleading.

(3) "Representation" means any representation as to fact or law, including a representation as to the state of mind of—

(a) the person making the representation, or
(b) any other person.

(4) A representation may be express or implied.

(5) For the purposes of this section a representation may be regarded as made if it (or anything implying it) is submitted in any form to any system or device designed to receive, convey or respond to communications (with or without human intervention).

Section 1 states:

(3) A person who is guilty of fraud is liable—

(a) on summary conviction, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum (or to both);
(b) on conviction on indictment, to imprisonment for a term not exceeding 10 years or to a fine (or to both).

Based on Megan's account, the offence committed is unauthorised access to computer material, contrary to section 1, Computer Misuse Act 1990

> **Section 1 states:**

(1) A person is guilty of an offence if—

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer.

(b) the access he intends to secure is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

(2) …

(3) A person guilty of an offence under this section shall be liable

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

(b) on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both;

(c) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both.

Based on Daniel's account, the offence committed is blackmail, contrary to section 21, Theft Act 1968.

Section 21 states:

(1) A person is guilty of blackmail if, with a view to gain for himself or another or with intent to cause loss to another, he makes any unwarranted demand with menaces; and for this purpose a demand with menaces is unwarranted unless the person making it does so in the belief—

(a) that he has reasonable grounds for making the demand; and

(b) that the use of the menaces is a proper means of reinforcing the demand.

(2) The nature of the act or omission demanded is immaterial, and it is also immaterial whether the menaces relate to action to be taken by the person making the demand.

(3) A person guilty of blackmail shall on conviction on indictment be liable to imprisonment for a term not exceeding fourteen years.

Based on Judith's account, the offence committed is harassment, contrary to section 2, or stalking contrary to section 2a, Protection from Harassment Act 1997.

Section 1 states:

(1) A person must not pursue a course of conduct—

(a) which amounts to harassment of another, and

(b) which he knows or ought to know amounts to harassment of the other.

Section 2 states:

(1) A person who pursues a course of conduct in breach of section 1 is guilty of an offence.

(2) A person guilty of an offence under this section is liable on summary conviction to imprisonment for a term not exceeding six months, or a fine not exceeding level 5 on the standard scale, or both.

Section 7 states:

(1) This section applies for the interpretation of sections 1 to 5.

(2) References to harassing a person include alarming the person or causing the person distress.

(3) A "course of conduct" must involve conduct on at least two occasions.

Section 2(A) states:

(1) A person is guilty of an offence if—

(a) the person pursues a course of conduct in breach of section 1(1), and
(b) the course of conduct amounts to stalking.

(2) For the purposes of subsection (1)(b) (and section 4A(1)(a)) a person's course of conduct amounts to stalking of another person if—

(a) it amounts to harassment of that person,
(b) the acts or omissions involved are ones associated with stalking, and
(c) the person whose course of conduct it is knows or ought to know that the course of conduct amounts to harassment of the other person.

(3)The following are examples of acts or omissions which, in particular circumstances, are ones associated with stalking—

(a) following a person,
(b) contacting, or attempting to contact, a person by any means,
(c) publishing any statement or other material—
(i) relating or purporting to relate to a person, or
(ii) purporting to originate from a person,
(d) monitoring the use by a person of the internet, email or any other form of electronic communication,
(e) loitering in any place (whether public or private),
(f) interfering with any property in the possession of a person,
(g) watching or spying on a person.

(4) A person guilty of an offence under this section is liable on summary conviction to imprisonment for a term not exceeding 51 weeks, or a fine not exceeding level 5 on the standard scale, or both.

Based on Nathan's account, the offence committed is attempted burglary, contrary to section 1, Criminal Attempts Act 1981.

Section 1 states:

(1) If, with intent to commit an offence to which this section applies, a person does an act which is more than merely preparatory to the commission of the offence, he is guilty of attempting to commit this offence

Section 9 of the Theft Act 1968 states:

(1) A person is guilty of burglary if—

(a) he enters any building or part of a building as a trespasser and with intent to commit any such offence as is mentioned in subsection (2) below; or

(b) having entered any building or part of a building as a trespasser he steals or attempts to steal anything in the building or that part of it or inflicts or attempts to inflict on any person therein any grievous bodily harm.

(2) The offences referred to in subsection (1)(a) above are offences of stealing anything in the building or part of a building in question, of inflicting on any person therein any grievous bodily harm therein, and of doing unlawful damage to the building or anything therein.

(3) A person guilty of burglary shall on conviction on indictment be liable to imprisonment for a term not exceeding—

(a) where the offence was committed in respect of a building or part of a building which is a dwelling, fourteen years.

Based on Simon's account, the offence committed is fraud by false representation, contrary to section 2(a), Fraud Act 2006.

Section 2 states:

1) A person is in breach of this section if he—

(a) dishonestly makes a false representation, and

(b) intends, by making the representation—

(i) to make a gain for himself or another, or

(ii) to cause loss to another or to expose another to a risk of loss.

(2) A representation is false if—

(a) it is untrue or misleading, and

(b) the person making it knows that it is, or might be, untrue or misleading.

(3) "Representation" means any representation as to fact or law, including a representation as to the state of mind of—

(a) the person making the representation, or

(b) any other person.

(4) A representation may be express or implied.

(5) For the purposes of this section a representation may be regarded as made if it (or anything implying it) is submitted in any form to any system or device designed to receive, convey or respond to communications (with or without human intervention).

Section 1(3) states:

(3) A person who is guilty of fraud is liable—

(a) on summary conviction, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum (or to both);

(b) on conviction on indictment, to imprisonment for a term not exceeding 10 years or to a fine (or to both).