Cybercrime Analysis Brief

Author: Helen Parker
Warwickshire Community Safety Partnership Analyst,
Warwickshire Observatory

August 2014

Summary

Although overall crime is reducing in Warwickshire, it is thought that cybercrime has been on the increase for years, as the public carry out their day to day transactions online and as more businesses use the internet to successfully run their business, and is still increasing nationally, however it remains under reported.

Action Fraud identified 2,037 reports from victims of cybercrime in Warwickshire in the period of January 2013 to March 2014. Furthermore the largest complaints received were from online shopping and auctions (374 reports), retail fraud (224) and advance fee frauds (234).

Definition - There is no clear set definition of cybercrime, however largely, it is a means of using the internet and technology to commit criminal offences.

Warwickshire Police's definition of a cybercrime suggests that "An offence should be flagged as cyber-enabled where the reporting 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."

Offenders - Unknown – Cybercrime offenders can be anywhere in the world, they are largely anonymous to the victim.

Victims - Anyone can be a victim of a cybercrime. According to the British Crime Survey in July 2013[1], victimisation of a cybercrime is significantly higher than for other types of crime.

Location – Anywhere - However Warwickshire has seen 2,037 reports of cybercrime in the period of January 2013 to March 2014.

This is the fourth in a series of local crime briefings, with the idea adapted from the Jill Dando institute (JDi) of Security and Crime Science briefings, sourced from www.ucl.ac.uk/jdibrief/homepage.

[1] House of Commons, E-Crime report - http://bit.ly/1hThmtF

What is cybercrime?

There is no clear set definition of cybercrime, however largely; it is a means of using the internet and technology to commit criminal offences. The most common offence types include:

- Theft of personal data
- Copyright infringement
- Fraud
- Child pornography
- Cyberstalking
- Bullying

It is thought that there are two types of cybercrime. Type 1 is where the victim could respond to a phishing email pretending to be from a bank which leads them to a bogus website enabling the offender to install a virus on their device. Or the victim unknowingly downloads a Trojan horse virus onto their device, enabling the offender to obtain the victims private information such as passwords and bank details.

Type 2 is the more extreme cybercrimes. Norton[2] defines these as “stalking and harassment through the internet via chat rooms and social media, child predation, extortion, blackmail, stock market manipulation, complex corporate espionage, and planning or carrying out terrorist activities.”

Warwickshire Police’s definition of a cybercrime suggests that “An offence should be flagged as cyber-enabled where the reporting 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.”

Cybercrime can also bring new ways of committing the more ‘conventional’ crime types such as domestic burglary and vehicle crime using social media such as Facebook and Twitter to identify potential vulnerable victims, for example knowing when a house is unoccupied due to the occupant stating they are currently on holiday on Facebook. Furthermore sexual offences, bullying and hate crimes can also be committed via the internet taking place in chat rooms or on Facebook.

Drugs can also be sold anonymously on the internet via the dark net (an anonymous or hidden internet, unable to trace your location) and the advert for this type of offence is increasing. According to the BBC News[3]: “The number of listings offering illegal drugs for sale on the dark net appears to have more than doubled in less than a year”.

[2] Norton - http://bit.ly/1rFwA6w
[3] BBC News - http://bbc.in/1oUB5v8

It is thought that paedophiles are also using the dark net to trade images of sexual abuse. BBC News[4] found that on one site on the dark net, as many as 500 users were viewing the page per second, and figures received from another website suggest that British people were responsible for producing and distributing obscene material on the website.

So who are the offenders?...

Cybercrimes can often be on a large scale and be anonymous to the victim. Offenders can be anyone across the world who have access to ways of uploading viruses via the internet and are able to hack into other people's computers, tablets and mobile phones. For example, an offender can upload a virus in America however it may only impact in Europe.

… And who are the Victims?

Anyone… Anyone can be a victim of a cybercrime, whether they are aware of it or not.

According to the British Crime Survey in July 2013[5], victimisation of a cybercrime is significantly higher than for other types of crime, with between one and 17% of the online population for 21 countries across the world becoming a victim of online credit card fraud, experiencing unauthorised access to an email account, responding to phishing scams and identity theft. This can be compared to 5% in the same countries becoming a victim of a domestic burglary, robbery and vehicle crime. It is also recognised that not many victims of a cybercrime will know that they have fallen victim to this type of offence.

Cybercrime does not only affect individuals, it can have a huge impact on the business world also, from small to large businesses. According to the British Retail Consortium's Retail Crime Survey in 2013[6] "the majority of retailers reported that cyber-attacks pose a critical threat to their business. Hacking and denial of service attacks were the most serious threat in the last 12 months."

The National Crime Agency[7] has stated that "as an indicator of the size of the problem, Symantec recently assessed the UK as the top target in Europe for financial Trojans. The UK is a developed country with a large population and comparatively wealthy residents, but limited in choice to a relatively small number of financial institutions; a combination of conditions generally conducive to such criminal targeting."

[4] BBC News - http://bbc.in/1pKZSmD
[5] House of Commons, E-Crime report - http://bit.ly/1hThmtF
[6] British Retail Consortium - http://bit.ly/1rO2Oh1
[7] National Crime Agency - http://bit.ly/1kRlBEO

RSA (Rivest-Shamir-Adleman, an Internet encryption and authentication system)[8] have identified that in 2013 the UK lost £300 million to phishing scams, making it the second highest country out of 13 identified countries where phishing scams have been analysed by RSA. The USA was the highest with $2.3 billion lost.

In December 2013, Action Fraud (the UKs national fraud reporting and internet crime reporting centre) received 96,669 crime and information reports of which 35% were cyber related (cyber enabled fraud and computer misuse offences).

Furthermore 34,155 internet related reports (internet enabled fraud and computer misuse crimes) were received between October and December 2013.

Online shopping and auctions continues to be the largest internet enabled fraud type, accounting for over one third (36%) of internet enabled reporting from October to December 2013.

So what's going on in Warwickshire?

Although overall crime is reducing in Warwickshire, it is thought that cybercrime has been on the increase for a number of years as growth in the use of the internet has taken place and is still increasing nationally, however it remains under reported. Upon opening a cybercrime conference held at Coventry university in May 2014, Ron Ball, the Warwickshire Police and Crime Commissioner highlighted[9]: "we are two and a half times more likely to become a victim of internet fraud than any other crime. The cost of internet-related criminality is estimated at between £18 and £27 billion, yet in truth, the figure is much higher. Traditional crime such as burglary and robbery have declined year on year but in contrast, cybercrime is growing at a rapid pace. There needs to be a coordinated approach to counter this trend with everyone showing greater awareness and taking action to step up online security."

Since 1st April 2014 it has been a requirement for Police forces to record cybercrimes by means of using a cybercrime flag against offences relating to these crimes. However it is worth noting that it will take a couple of years for figures to settle down and become more accurate, due to delays in recording and teething issues with new systems and new ways of recording. It is likely that this type of crime will be largely under reported also, and therefore it will be difficult to retrieve accurate information on how much cybercrime is taking place in the county.

Action Fraud identified 2,037 reports from victims of cybercrime in Warwickshire in the period of January 2013 to March 2014 with the largest complaints received from online shopping and auctions (374 reports), retail fraud (224) and advance fee frauds (234).

[8] RSA - World Wide Estimated Losses from Phishing (2013) - http://bit.ly/1kdy8Gb
[9] Warwickshire Police - http://bit.ly/UN1sHf

Both West Mercia and Warwickshire Police[10] recognise that cybercrime issues create huge challenges for law enforcement and in May 2014 identified that one in three adults suffered an online crime over the past twelve months compared to one in five adults suffering crime offline.

Warwickshire Police currently have a Cybercrime Task and Finish Group which meet every two to three months and discuss ways they can tackle cybercrime in the county and better protect individuals from cybercrime.

Nuneaton & Bedworth Neighbourhood Watch Association is currently using a member only Database and Intranet for Safer Communities (DISC) system and is the first in the country to use it. This enables Neighbourhood Watch to communicate messages on a weekly basis and on a variety of topics but particularly regarding cybercrime to the community via various partner agencies such as Action Fraud, Trading Standards, National Crime Agency, Fire and Rescue and the Police.

The table illustrates the number of 'online' and 'cyber' related offences reported in Warwickshire between January and June 2014.

Offence	No of offences
Online Shopping and Auction Related Offences	162
Other Advance Fee Frauds	95
Computer Software Service Fraud	51
Cheque, Plastic Card and Online Bank Accounts (not PSP)	49
Hacking - Social Media and Email	31
Computer Virus \ Malware \ Spyware	22
Hacking - Server	3
Total	**413**

Source, Action Fraud, UK

Offences relating to online shopping and auctions are the most reported cybercrime offence in Warwickshire, followed by other advance fee frauds (where victims make advance payments for goods, services and/or financial gains that do not materialise).

Warwickshire Trading Standards have found that between November 2013 and August 2014, a total 31 reports have been received (via a number of sources) where a cybercrime has been reported. Of these 31 reports, an estimated total of £5,333 has been lost due to victims reporting scams which have happened on the internet, such as purchasing goods that have never been received or through copycat websites along with various other scams. Online shopping and auction related offences are one of the highest recorded offences in the county (12 offences) followed by responding to phishing scams (5). Reports have come from all over Warwickshire where Warwick District has seen the highest levels of reports (9 offences) followed by Stratford District (8 offences), Nuneaton and

[10] Warwickshire Police - http://bit.ly/1kdAZyO

Bedworth Borough (5), North Warwickshire Borough (4) and Rugby Borough (3). Two were in unknown locations in Warwickshire.

So what can be done in order to prevent cybercrime affecting our lives?

It is important that cybercrime is reported to Action Fraud and the Police, as well as raising the awareness to individuals and businesses on how they can protect themselves against this cybercrime. Training and education could be put in place in schools and colleges as well as agencies and partnerships raising awareness to the public on how they can protect computer-based equipment and information from unintended or unauthorised access from outside parties. Essential advice could include:

- Familiarising yourself with information regarding the best anti-virus protection to use. Keeping virus scanners and malware protection tools installed and up to date as well as keeping them them on and not disabling them. This includes mobile and tablet devices as well as laptops and desktop computers.

- Be careful of opening emails that you were not expecting even if they appear to be from someone you know that you haven't heard from in a long time, or if the email subject raises suspicion. Never open unknown attachments. And check any suspicious links in the bar at the bottom of the screen to see where the link is really taking you.

- Keep data secure and ideally encrypted. Microsoft Windows comes with a tool called BitLocker that will keep hard drives, including USB drives secure.

- Rather than using the same password for multiple sites consider using free password managers such as LastPass[11] or Keepass[12].

- Do not divulge any personal information on social networking sites, checking bank statements regularly as well as promoting the awareness of software able to track stolen technology (such as "Find My iPhone" app or "Where's my Droid" app for smartphones that can track mobile phones) and other internet based technology, such as televisions, Blu-ray and DVD players. It is also important to raise the significance of reporting such crimes as this can improve detection rates and raise awareness within Police forces that cybercrime is increasing.

[11] LastPass - http://bit.ly/1eHKhv9

[12] Keepass - http://bit.ly/IzB7qC

- For businesses the government launched Cyber Essentials[13] in April 2014, which is the first recognised cyber security certification, as part of the National Cyber Security Strategy which guides businesses into protecting themselves from cybercrimes and threats. It is free to use and once completed and successfully independently assessed or tested through the schemes assurance framework, Cyber Essentials a certification badge will then be awarded to show customers of that business that they have taken measures to defend themselves against cyber-attacks.

- Crimestoppers launched 'The Game of Fraud'[14] in an attempt to assess their risk of encountering a fraud in their business. The quiz highlights ten fraud types which businesses are likely to be subjected to and once completed will assess the risk of the business and what it can do to reduce the risk of them becoming a victim of fraudulent activity.

What's going to happen in the future?

Presently it is difficult to measure the full extent of cybercrime both nationally and locally. The Office for National Statistics have said that they will be looking to develop some cybercrime questions to be included in the Crime Survey for England and Wales in the future which will give us more of an idea as to what is being reported.

Warwickshire Police have started to record cybercrime and this year will be the baseline, so data next year can be compared with this year's results and give us a feel of what is going on locally, with those who have reported a cybercrime to the Police.

Agencies such as county councils should be able to access data stored on the Police Area Knowledge Site (POLKA) where Action Fraud send their reports of cybercrimes to for analysis in the future. From here analysis could be carried out as to how many cybercrimes have been reported to Action Fraud from Warwickshire, and this can then be compared to the number of reports received in recent years.

Useful Links

! **To report a cybercrime** - http://www.actionfraud.police.uk/
- http://www.tradingstandardsecrime.org.uk/

! **Advice on how to be safe online** - https://www.getsafeonline.org/
- http://www.stop-idfraud.co.uk/

[13] Cyber Essentials - http://bit.ly/1p8RBWZ
[14] Crimestoppers - The Game of Fraud - http://bit.ly/1ulFl7D