Safe Durham Partnership

Better for everyone

# Cyber Crime Fact Sheet

## What is Cyber Crime?

Advances in technology and cyber related crime, impacts across virtually all areas of policing. It is an enabler of crime, such as fraud, harassment, child sexual abuse and exploitation or pure cyber-dependent crime and is also a source of significant amounts of data, in both an online and offline context.

Cyber criminals seek to exploit human or security vulnerabilities in order to steal passwords, data or money directly. The most common cyber threats include:

- Hacking - including of social media and email passwords
- Phishing - bogus emails asking for security information and personal details
- Malicious software – including ransomware through which criminals hijack files and hold them to ransom
- Distributed denial of service (DDOS) attacks against websites – often accompanied by extortion

## What is the issue?

The scale and complexity of cyber-attacks is wide ranging. 'Off the shelf' tools mean that less technically proficient criminals are now able to commit cybercrime and do so as awareness of the potential profits becomes more widespread.

The impact on policing is significant, particularly in terms of maximising capability to exploit investigatory opportunities and capture evidence as part of investigations that are proving more complex. In relation to fraud offences key concerns are around under reporting, particularly in relation to the business sector where there may be a reluctance to report crimes due to reputational damage.

## Why is it important?

The huge growth in technology and digital communications has enhanced society and quality of life for everyone. However, it comes with clear risks to homes and businesses, as cyber-fraud increases and there are new patterns of criminal activity all the time.

There have been increases in cybercrime and fraud due to the Covid-19 pandemic as many people are now working from home and using the internet more than ever.

National reports suggest increases in fraud especially targeting elderly vulnerable people (Action Fraud, 2020). There have also been a number of scams directly relating to Covid-19 as criminals exploit the vulnerabilities of people living in the pandemic.

The significant risks associated with cybercrime alongside the widely estimated understanding that the majority of cyber-attacks are preventable, make good practice critically important.

## How does it impact people?

Targeting of individual victims is increasing and particularly among vulnerable groups. This has increased dramatically during the Covid-19 pandemic.

Cybercrime continues to rise in scale and complexity, impacting on a greater number of victims, affecting essential services, businesses and private individuals alike. However, less complex means are also very successful such as phishing for personal information using bogus information.

It is costing the UK billions of pounds, causing untold damage, and threatens national security. According to the National Crime Agency home-grown cyber criminals are becoming more sophisticated and therefore a rising threat. Although young criminals are often driven by peer kudos rather than financial reward, organised UK cybercrime groups are motivated by profit.

## County Durham context (Covering the period Feb 2020 to Jan 2021)

- 14 reports were recorded by Action Fraud/Durham police by organisations reporting cyber dependant crime, specifically cyber security breaches or cyber-attacks in this 12-month period. These 14 reports relate to 12 organisations (some organisations have made multiple reports).

- As a proportion, a total of 21 cyber-dependant reports were made by organisations in this 12-month period, so the 14 that relate to cyber security breaches or attacks represents 66.7%. No figures are provided for any financial losses.

- All 14 reports (100%) are recorded as NFIB (National Fraud Intelligence Bureau) Frauds under the following subcategories:

- Hacking – social media and email.

- Hacking – personal, Computer virus/malware/spyware.

- Hacking – extortion and Hacking – PBX * (Private branch exchanges) dial through.

- Of the 14 reports referenced above:

- 9 (64%) are recorded as “hacking - social media and email”
- 2 (14%) are recorded as “computer virus/malware/spyware”
- 3 do not have a category.
- Of all 21 cyber-dependant reports made by organisations:
- 14 (66.7%) are recorded as “hacking - social media and email”
- 2 (9.4%) are recorded as “computer virus/malware/spyware”
- 2 (9.5%) are recorded as “hacking – extortion”
- 3 do not have a category.

*Private Branch Exchanges (PBX) are telephone systems used by small and medium businesses for internal and external communications. They are frequently targeted by criminals who exploit the technology by committing what is known as “dial-through fraud” – where the PBX is hacked into allowing calls to be routed through the system to high rate international/premium rate numbers.

## National context

- The Cyber Security Breaches Survey 2020 indicates that almost half of businesses (46%) and a quarter of charities (26%) report having cyber security breaches or attacks in the last 12 months, at an average cost of around £3,230.
- For the year ending June 2020 the Telephone-operated Crime Survey for England and Wales (TCSEW) estimated that there were 5.9 million cybercrimes, 73% were fraud offences and 27% were related to computer misuse.
- Estimates showed that there were 733,967 fraud offences and 29,138 computer misuse offences referred to National Fraud Intelligence Bureau in the year ending June 2020.
- Within plastic card frauds, there was a 58% increase in “remote banking” fraud which reflects the greater number of people now regularly using internet, telephone and mobile banking, and the attempts by fraudsters to take advantage of this. The two highest-volume computer misuse types were “Hacking – social media and email” and “computer viruses and malware”.
- The coronavirus (COVID-19) pandemic is likely to have had differential effects on trends in fraud and computer misuse offence, for example Action Fraud reported the increase in “online shopping and auctions” fraud could be accounted for by the increase in online shopping whilst the decrease in “other

advance fee" fraud could be attributed to reduction in holiday fraud figures as fewer holidays were booked. However, it is too early to say whether this is evidence of a change to longer-term patterns.

## Resources

General Advice

www.internetmatters.org

Apps

www.net-aware.org.uk/

Support directly for children

www.childline.org.uk/

Fraud / Cybercrime

www.getsafeonline.org/

www.ncsc.gov.uk/cyberaware/home

Local SCP

www.durham-scp.org.uk/parents-carers/online-safety/

Office of National Statistics

www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingjune2020#computer-misuse

-