



CYBERCRIME

Leicestershire Safer Communities Strategy Board 26th June 2020

Detective Inspector Peter Flynn
Detective Chief Inspector Reme Gibson
Leicestershire Police Cybercrime Strategic Lead

Cyber Crime - Why such a fuss?



**POLICE & CRIME
COMMISSIONER
for Leicestershire**
Prevention | Partnership | Protection



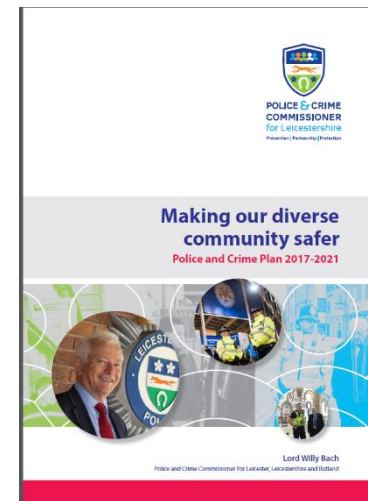
**Leicestershire
Police**
Protecting our communities



Hostile attacks
upon UK cyber
space by other
states and large scale
cyber crime.



- Tier 1 Government Risk
- Strategic Priority of Leicestershire Police
 - Police and Crime Plan 2017-201
- Now more crimes online than offline
- **WHEN ... not IF it affects us all**



2

Cybercrime

ANYONE can be a victim ranging from individuals, to targeted attacks on key businesses but often the most damage is caused by those which use a vulnerability across a range of softwares.

For example Wannacry and the NHS.

And many many more...

How do we deal with Cybercrime?

PREPARE
R
PROTECT
V
PursuE
N
T

- Protect
 - Raise awareness
 - Simple advice
- Prevent – Identify those at risk of offending
 - Identification
 - Diversion
 - Development
 - De-escalation
- Prepare
 - When.. not if.. affected
 - Further understanding of impact
- Pursue
 - Lock up those offending - ***issue***

4

How we Keep Ahead of the Game ..

NATIONAL FRAUD INTELLIGENCE BUREAU

ANNUAL ASSESSMENT

2018 - 2019

Assessment of the threat posed to the UK from Cyber Crime

CITY OF LONDON POLICE

OFFICIAL - LAW ENFORCEMENT

FOREWORD

In early 2018, the National Fraud Intelligence Bureau (NFIB) reviewed and enhanced its structure and processes to offer a more proactive service to address fraud and cyber crime, with the aim of providing a more integrated response. As part of this review, the NFIB has advanced its intelligence development capability for serious and organised crime networks, cyber-enabled and the highest level fraud threats.

This foreword has been crafted from various sources to properly inform this work, and cannot represent what they add most value. This took the form of a survey last year, a conference call with interested forces and with such those coordinated within the new National Co-ordinated Office in City of London Police. One of the resulting changes has been to move away from the production of separate intelligence profiles, previously created before paper, in the interest of developing an interactive dashboard which all forces will be able to access later this year. Subsequent each quarter events, the data and statistics contained within this dashboard will be more timely, and more flexible, enabling forces to better understand the crime reported by victims residing in their force area.

Whilst the dashboard is being finalised, an individual intelligence indicating the key fraud statistics and trends is provided for each of police force which will also be available on the active fraud website in June 2019. Further feedback from forces is invited to help refine the prototype and we would encourage those interested to contact us at info@nationalfraudintelligencebureau.org.uk if you're interested.

In addition to the dashboard, two new annual assessments for fraud and cyber crime will provide an intelligence assessment of strategic trends and threats as reported to the NFIB each financial year.

This report is the first edition of the annual fraud assessment, focusing on fraud reported to Action Fraud (the UK's national reporting centre for fraud and other crime), and relevant intelligence on fraud affecting victims to police.

The expenditure in this document also provides a breakdown of reporting victims by crime type, reported losses, and customer data to police force for those that wish to seek individual contacts or compare against national or regional levels and by crime or neighbouring force.

The expenditure in this document also provides a breakdown of reporting victims by crime type, reported losses, and customer data to police force for those that wish to seek individual contacts or compare against national or regional levels and by crime or neighbouring force.

The expenditure in this document also provides a breakdown of reporting victims by crime type, reported losses, and customer data to police force for those that wish to seek individual contacts or compare against national or regional levels and by crime or neighbouring force.

The expenditure in this document also provides a breakdown of reporting victims by crime type, reported losses, and customer data to police force for those that wish to seek individual contacts or compare against national or regional levels and by crime or neighbouring force.

The expenditure in this document also provides a breakdown of reporting victims by crime type, reported losses, and customer data to police force for those that wish to seek individual contacts or compare against national or regional levels and by crime or neighbouring force.

The expenditure in this document also provides a breakdown of reporting victims by crime type, reported losses, and customer data to police force for those that wish to seek individual contacts or compare against national or regional levels and by crime or neighbouring force.

The expenditure in this document also provides a breakdown of reporting victims by crime type, reported losses, and customer data to police force for those that wish to seek individual contacts or compare against national or regional levels and by crime or neighbouring force.

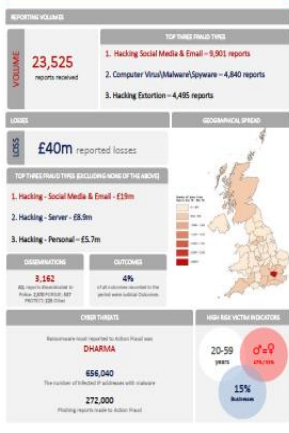
The expenditure in this document also provides a breakdown of reporting victims by crime type, reported losses, and customer data to police force for those that wish to seek individual contacts or compare against national or regional levels and by crime or neighbouring force.

The expenditure in this document also provides a breakdown of reporting victims by crime type, reported losses, and customer data to police force for those that wish to seek individual contacts or compare against national or regional levels and by crime or neighbouring force.

CONTENTS

- Cyber Crime Trends 3
- 2018/19 Overview 4
- Victim Reporting 4
- Distributions and Outcomes 5
- Trends and Outlook 5
- Malware Incidents 6
- Malware - Banking Trojans 7
- Malware - Ransomware 7
- Malware - Denial of Service 8
- Malware - Phishing 8
- Malware - Future Threats 10
- Key Intelligence Requirements 10
- Summary 10
- Appendix 10
- Distribution List 10
- Feedback 10

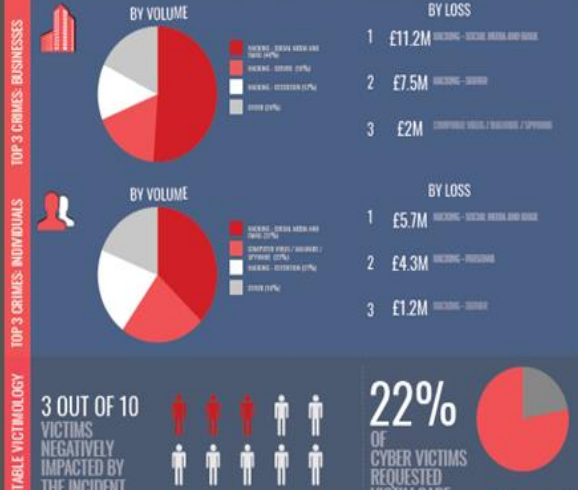
CYBER CRIME TRENDS



NFIB CYBER CRIME ASSESSMENT 2018/19 | Page 4 of 22

CYBER PROFILE

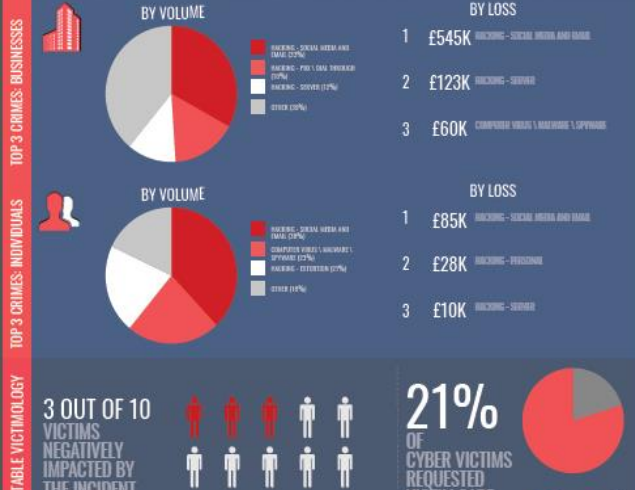
CITY OF LONDON POLICE



NFIB CYBER CRIME ASSESSMENT 2018/19 | Page 5 of 22

CYBER PROFILE

Leicestershire Police



NFIB CYBER CRIME ASSESSMENT 2018/19 | Page 6 of 22

Things we are Proud of:

- Expansion and maturation of Cyber dependent crime unit:
 - 3 Detectives plus a Detective Sergeant
 - 1 Cyber PCSO
 - 1 Cyber Protect officer
- Prevent role created and linked to regional and national issues.
- Two Cybercrime conferences run locally targeting hard to reach groups which were well attended and under budget to spread the messages of how to keep yourself safe online.
- National funding KPI's reached with 100% Cybercrime victims gaining investigative support, 100% of victims receiving support to mitigate repeat.
- National recognition for being at the forefront of investigative capability leading on several incidents with international reach.

Things to do:

- Create and develop Prevent referral scheme for organisations to help them identify someone at risk of becoming an offender and feed the information through the right channels.
- Empower and enable key staff members to share their knowledge/experience others and provide advice.
- Create a toolbox of scenarios and considerations to make it as simple to follow for organisations.
- Develop and deliver a baseline assessment for key small/medium enterprises to identify recurring themes and how we can deal.

7

What do we need:

- Points of contact within key stakeholders to discuss changes in our system.
- Support and encourage training of staff across organisations to minimise risk of most issues.
- Review of intelligence gaps across Cybercrime and identify associated opportunities to improve understanding. ∞
- Ensure advertising within organisations is completed around core messages to both keep self safe but also to identify threats.

Questions?



DCI Reme Gibson – Strategic lead
DI Peter Flynn

For questions, advice or contact:

[Email: Cybercrime@Leicestershire.pnn.police.uk](mailto:Cybercrime@Leicestershire.pnn.police.uk)

Twitter: @Leicscyberaware / @LeicsCybercrime

This page is intentionally left blank