



**NORTH WEST
REGIONAL
ORGANISED
CRIME UNIT**

Cyber Readiness for schools

Louisa Murphy
CISMP, TAQA, PGCE, BA(Hons)
Regional Cyber Protect Officer
Louisa.Murphy@nwrocu.police.uk



OFFICIAL

UK Law Enforcement Structure



Action Fraud

National Fraud & Cyber Crime Reporting Centre

actionfraud.police.uk



2020 Winners

THE NATIONAL CYBER AWARDS

'The Cyber Policing Team of the Year'



UK Cyber Policing



PREPARE

Ensure the necessary capabilities exist to tackle and respond to cyber crime.

PROTECT

Reduce the vulnerability amongst our communities from the threat of cyber crime.

PREVENT

Prevent people from becoming involved in cyber crime.

PURSUE

Relentless disruption and prosecution of those committing cyber crime.



What is Cyber Crime?



Cyber-Dependant

Cyber-Enabled



Ransomware



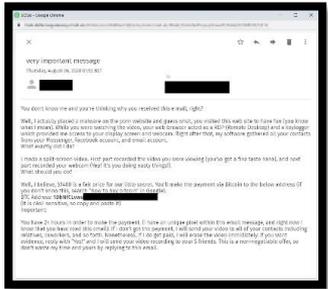
Business Email Compromise



Insider Threat



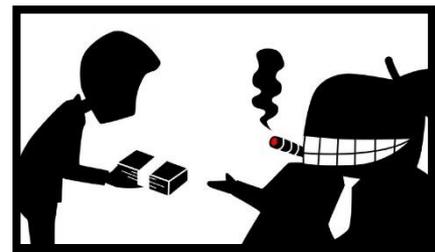
Drug Supply



Sextortion Phishing Email



Compromise



Blackmail



Harassment

Threat Actors



- *Script Kiddies*
- Hackavist Groups
- OCGs
- Advanced Persistent Threat (often state sponsored)
- State Actors



Main Cyber Crime Trends



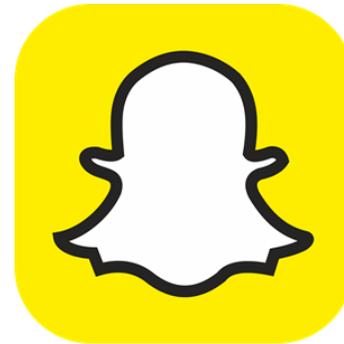
- Social Media account compromise for purposes of fraud
- Ransomware infections, often delivered via RDP
- Sextortion phishing
- SIM swapping

Social Media Account Compromise

OFFICIAL



- 5150 reports to Action Fraud in 2019/20
- Facebook most popular platform to takeover, followed by Instagram and Snapchat.
- Majority of reports from females ages 20 – 29 years old



Social Media Account Compromise

OFFICIAL



**NORTH WEST
REGIONAL
ORGANISED
CRIME UNIT**

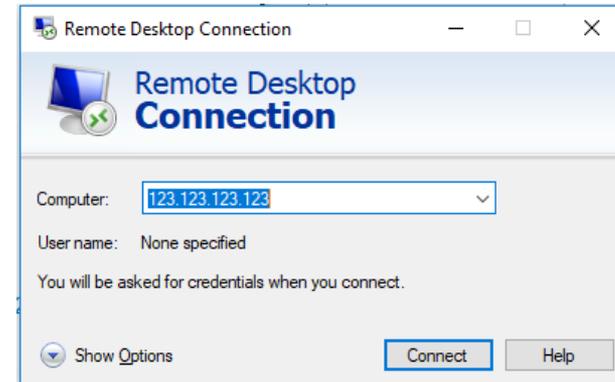
Various distinct suspect motivations:

- Personal amusement and challenge
- Financial gain and fraud
- Revenge
- Domestic Abuse (Coercive Controlling Behaviour)
- ID theft
- Facilitating sextortion (typically occurring on Snapchat)
- To promote extremist material
- To facilitate money muling

Ransomware Infections

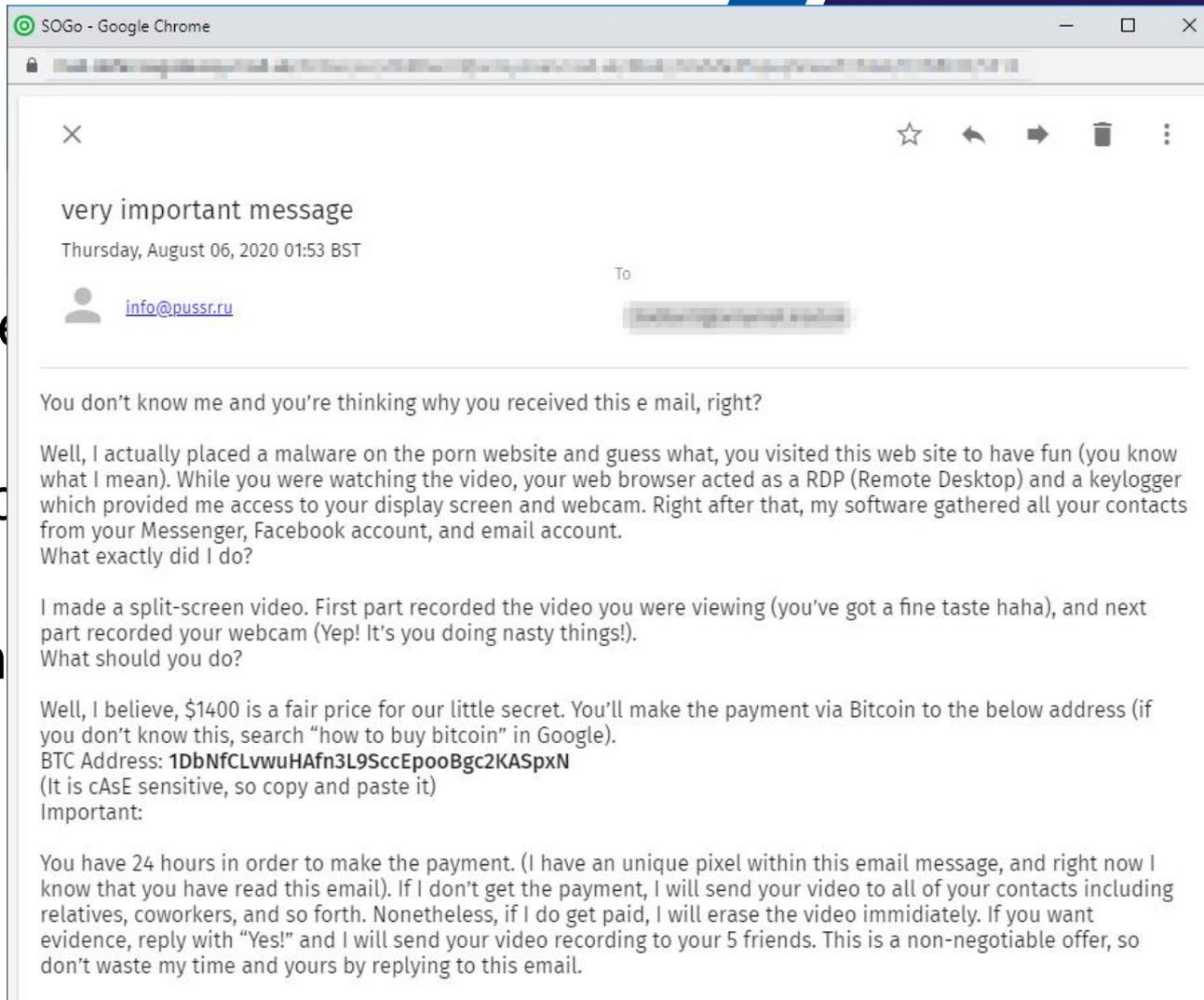


- Targeting businesses that are wholly reliant on networked infrastructure and have sufficient assets to pay ransoms
- Ransoms have been as large as £4.2 million
- Attackers now steal data before dropping ransomware and hold this to ransom as well



Sextortion

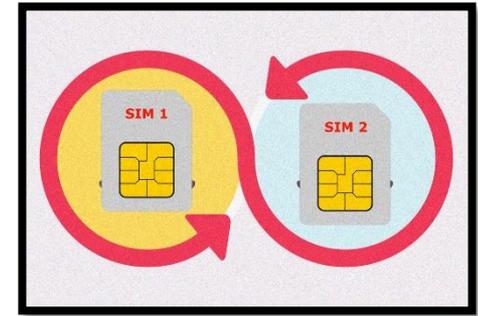
- 200 reports per week
- Ransoms between \$1000 and \$10000
- Contain pseudo-technical details
- Vary from webcam recordings and/or phishing emails



Sim Swapping



- Usually High Value targets
- Social Engineered for detailed information
- Convince phone company port the phone number onto a new phone/SIM
- Upsurge in cases, mostly for purposes of bypassing 2FA
- Or gain info to request OTT(P)



Password Spraying



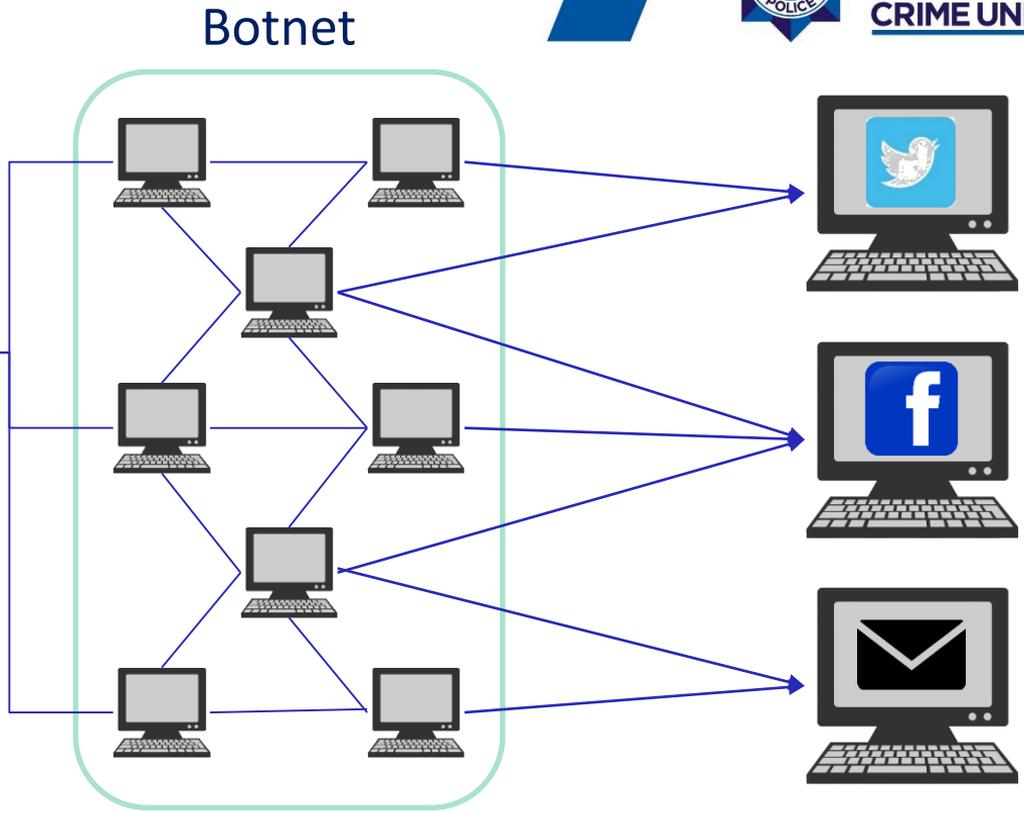
Most used in total	Names	Premier League football teams	Musicians	Fictional characters
123456 (23.2m)	ashley (432,276)	liverpool (280,723)	blink182 (285,706)	superman (333,139)
123456789 (7.7m)	michael (425,291)	chelsea (216,677)	50cent (191,153)	naruto (242,749)
qwerty (3.8m)	daniel (368,227)	arsenal (179,095)	eminem (167,983)	tigger (237,290)
password (3.6m)	jessica (324,125)	manutd (59,440)	metallica (140,841)	pokemon (226,947)
111111 (3.1m)	charlie (308,939)	everton (46,619)	slipknot (140,833)	batman (203,116)

Credential stuffing

Check if your Email & Password
have been leaked:
haveibeenpwned.com



Email	Password	Twitter	Facebook	Email
VickyS97	Password1	✓	X	✓
NCage44	abc123	✓	✓	✓
TCook14	ManUtd66	✓	X	X
JEdward47	Maroon5	X	X	✓





FREE STUFF for Schools

It's the simple things that make the difference

Planning & Exercising

OFFICIAL

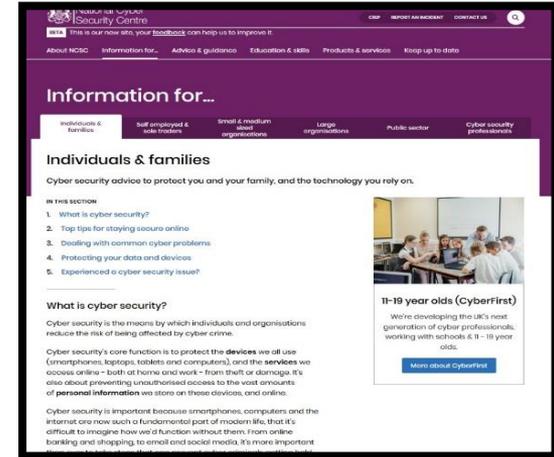


**NORTH WEST
REGIONAL
ORGANISED
CRIME UNIT**



**Decisions & Disruptions
Lego Based Cyber Exercise**

Exercise in a box



www.ncsc.gov.uk

Does your school have a Cyber Incident Response Plans?

NCSC Cyber Security for Schools

OFFICIAL



**NORTH WEST
REGIONAL
ORGANISED
CRIME UNIT**

1. Cyber security in schools: questions for governors and trustees
2. School Staff – resources for Schools
3. School IT: admin teams, procurers & providers
4. Other useful resources & advice
5. Reporting a school cyber incident

The screenshot shows the NCSC Cyber Security for Schools website. At the top, there is a green navigation bar with the NCSC logo and menu items: 'About NCSC', 'Information for...', 'Advice & guidance', 'Education & skills', and 'Pro...'. Below this is a sub-navigation bar with 'Home > Cyber Security for Schools' and the main heading 'Education & skills'. Further down, there are tabs for 'Schools', 'Higher education', 'Professional skills & training', and 'Working w/ NCSC'. The main content area is titled 'Cyber Security for Schools' with the subtitle 'Practical resources to help schools improve their cyber security.' Below the subtitle is a photograph of a desk with several blue pens and a stack of books. Underneath the photo is a section titled 'ON THIS PAGE' with a numbered list of five links: 1. Governing boards and senior leaders, 2. School staff, 3. School IT: admin teams, procurers & providers, 4. Other useful resources & advice, and 5. Reporting a school cyber incident. A paragraph follows, stating 'Cyber security should be high on the agenda for any school with a reliance on IT and online systems.' Below this is another paragraph: 'We have produced a number of downloadable resources for everyone working with schools, aimed at:'. At the bottom, there are two preview cards. The first is titled 'Governing boards and senior leaders' and contains a link to 'Cyber security in schools: questions for governors and trustees' with a small image of a desk. The second is titled 'Board Toolkit' and contains a link to 'Resources designed to encourage essential cyber security...' with a small image of people working at computers.

This small graphic features the NCSC logo on the left and the NEN logo on the right. Below the logos, the text reads: 'Cyber security in schools: Practical tips for everyone working in education'. At the bottom, there is a stylized graphic of a computer monitor with a padlock icon on the screen, set against a background of green and blue geometric shapes.

<https://www.ncsc.gov.uk/section/education-skills/cyber-security-schools>

Advice to keep you and your family safe online (and your workplace)

OFFICIAL



Create a separate password for your email account



Create a strong password using three random words



Save your passwords in your browser



Turn on two factor authentication for important accounts



Update your devices regularly (ideally set them to automatically update)



Back up important data

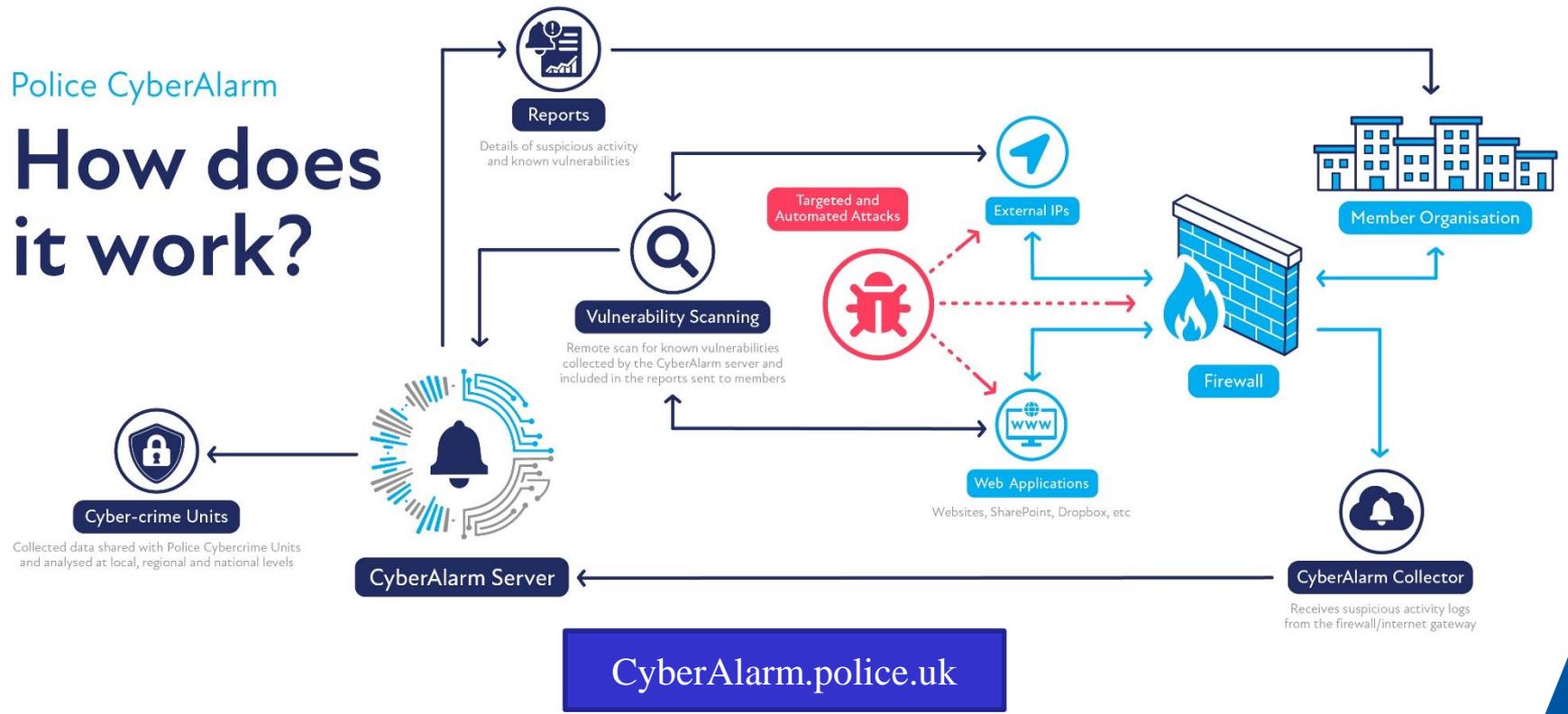


**NORTH WEST
REGIONAL
ORGANISED
CRIME UNIT**

Police CyberAlarm

Police CyberAlarm

How does it work?



CyberAlarm.police.uk

Reporting

OFFICIAL



Cyber Crime or Fraud

If you have been scammed, defrauded or experienced crime (computer based crime) report it immediately to Action Fraud.

ActionFraud

National Fraud & Cyber Crime Reporting Centre

■■■■ [actionfraud.police.uk](https://www.actionfraud.police.uk) ■■■■

0300 123 2040

Phishing or Vishing

Phishing

If you receive an email you are unsure about, forward it to the NCSC Suspicious Email Reporting Service (SERS)

report@phishing.gov.uk

Vishing

If you receive a suspicious text, forward it to **7726** (spells SPAM)

Useful Contacts



Louisa Murphy

Regional Cyber PROTECT Officer

0151 777 4393

Louisa.Murphy@nwrocu.police.uk

Keith Terrill

Regional Cyber PROTECT Officer

0151 777 8273

Keith.Terrill@nwrocu.police.uk

NWROCU PROTECT Inbox

Titan.Cyber.Protect@nwrocu.police.uk

ActionFraud

National Fraud & Cyber Crime Reporting Centre

❑❑❑ actionfraud.police.uk ❑❑❑

0300 123 2040