



# ROCU

REGIONAL ORGANISED CRIME UNIT  
FOR THE WEST MIDLANDS REGION

DC Patrick McBrearty

-

[rccu@west-  
midlands.pnn.police.uk](mailto:rccu@west-midlands.pnn.police.uk)

Twitter:- [@ROCUWMM](https://twitter.com/ROCUWMM)

To reduce the impact and increase  
the disruption of serious and  
organised crime across the  
region and beyond

# Why am I here?

- Threats and motivations
- The Police and the Policing structure
- Support available and general advice

# Cyber / Crime





# Why is Cybercrime important?

- The UK
- Business and Charities
- Because its Personal



# The Routine Activity Theory

- The Problem
- The Target
- The Prevention



# The Web



To reduce the impact and increase the disruption of serious and organised crime across the region and beyond

## **The 5 W - H of Cybercrime**

**(Lagazio, Sherif and Cushman, 2014)**

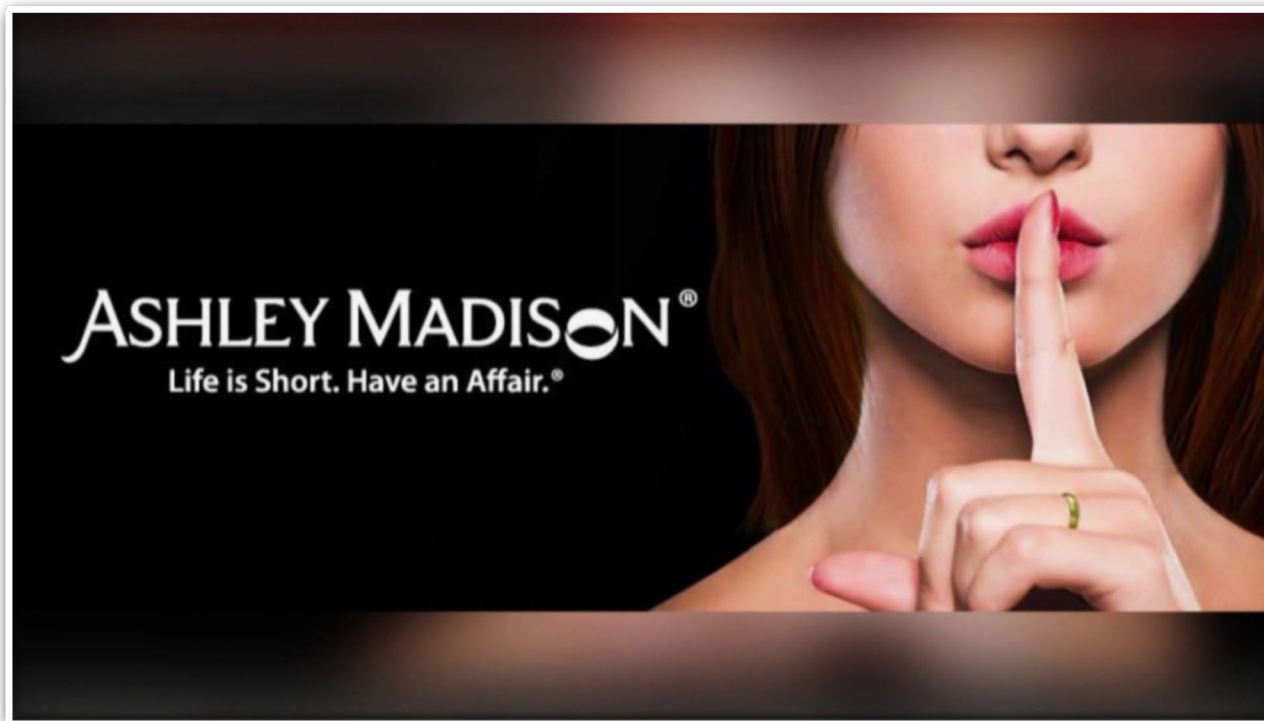


# Ransomware & DDOS



(NCSC, 2018)





**(NCSC, 2018)**

# Supply Chain

The infographic is titled "Supply Chain Insights" in the top left corner, accompanied by a logo of a green and blue cluster of dots. The central focus is a large circular diagram with a network of nodes and dashed lines, representing a digital supply chain. Surrounding this central hub are various icons and data visualizations: a document labeled "INFORMATION", a "GET THE REPORT" button, a globe, a bar chart labeled "DATA ANALYSIS", a computer monitor showing a line graph, a magnifying glass, a smartphone, a Wi-Fi symbol, a clock, a binary code "01011011", a person silhouette with a briefcase, and several smaller charts and graphs. The bottom of the infographic features a dark blue banner with the text "Building a Digital Supply Chain" in white. The entire graphic is framed by a green border.

To reduce the impact and increase the disruption of serious and organised crime across the region and beyond

# Fake News



# What?

- Ransomware and DDOS
- Data Breach
- Supply chain compromise
- Fake News

**(NCSC, 2018)**



- Cryptojacking
- Supply chain compromises
- Increased use of worms
- Internet of Things
- Cloud security

**(NCSC, 2018)**



# Why?

- Identity
- Financial
- Competitive Advantage
- Fame / Kudos
- Hacktivism

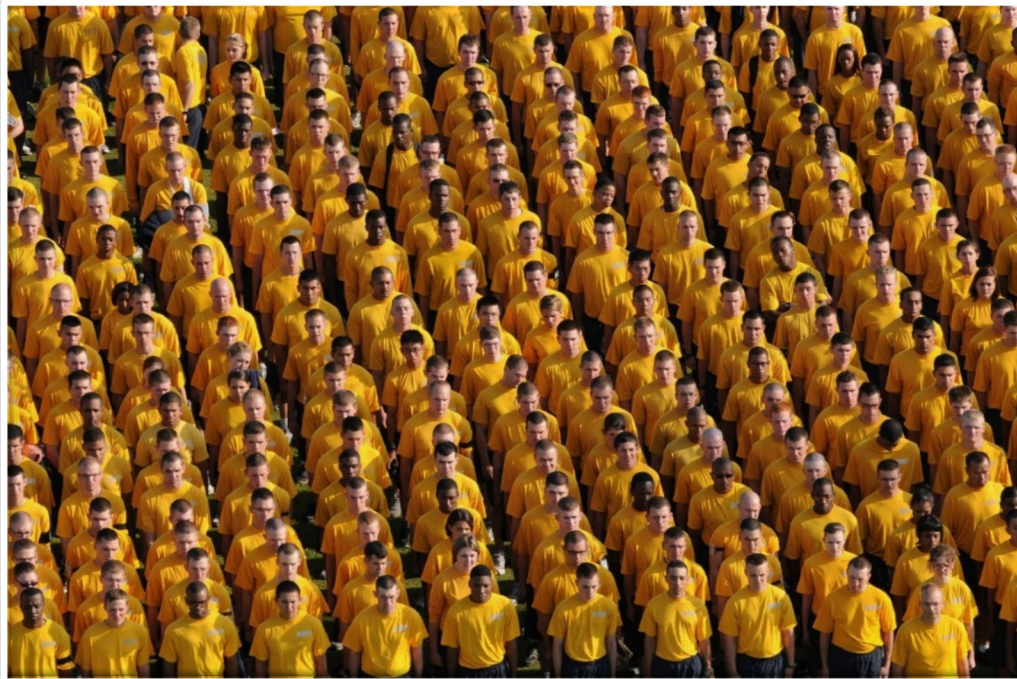
**(Yip, Webber and Shadbolt, 2013)**

# Who?

- Insider
- Experimenters and Gamers
- Hacktivist
- Businesses
- Nation States

**(Yip, Webber and Shadbolt, 2013)**

# The Target



- Organisation
  - Money
  - Data / Identification
  - Zombie
- Individual
  - Money
  - Data / Identification
  - Zombie

**(Wesley and Ndofor, 2013)**

# Organisational Target

**ROCU**  
REGIONAL ORGANISED CRIME UNIT  
FOR THE WEST MIDLANDS REGION



Two vulnerabilities

- Human
- Technical

**(Eisen, 2010)**

To reduce the impact and increase the disruption of serious and organised crime across the region and beyond





## Vulnerabilities

- Technical
- Emotionally

**(Bossler and Holt, 2010)**





**Joseph Edwards**

# Where?

- North Korea
- China
- Russia
- Others

**(Roche and Blaine, 2014)**

## Cheating student who hacked into university computer system to give himself a better degree is jailed

- Imran Uddin, 25, used a keyboard spying device to obtain staff passwords
- Final-year student hacked into exam system and upped his own marks
- He increased one of his bio-science grades from 57 per cent to 73 per cent
- Uddin admitted breaking Computer Misuse Act and was jailed for 4 months

By [EMILY KENT SMITH FOR THE DAILY MAIL](#)

**PUBLISHED:** 09:36, 24 April 2015 | **UPDATED:** 01:51, 25 April 2015

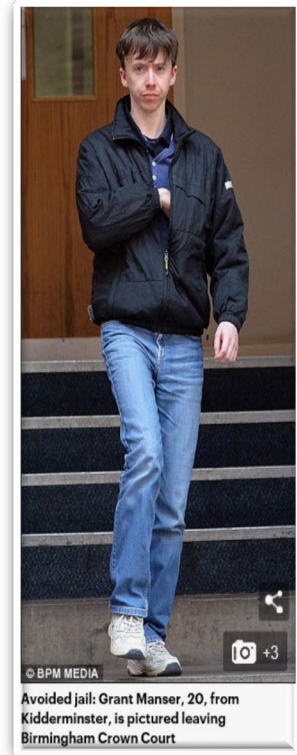


## Teenage boffin created damaging computer software used by cyber-hackers to crash 224,000 websites around the world from the bedroom of his £170,000 family home

- Grant Manser set up damaging software and sold it on 'dark web' aged 16
- The program bombarded websites with so much information they crashed
- Victims included firms, schools, colleges and government departments
- He pleaded guilty to ten charges but only received suspended sentence

By [MARK DUELL FOR MAILONLINE](#)

**PUBLISHED:** 09:47, 8 April 2016 | **UPDATED:** 02:06, 9 April 2016



© BPM MEDIA  
Avoided jail: Grant Manser, 20, from Kidderminster, is pictured leaving Birmingham Crown Court



## Solihull hacker Charlton Floate sentenced for FBI and Home Office hacks

16 October 2015 | Birmingham & Black Country

[f](#) [t](#) [d](#) [✉](#) [Share](#)



Charlton Floate said after the hearing he wanted to move on with his life

**A fame-hungry teenager has been given a suspended jail sentence for hacking FBI and Home office websites.**

Charlton Floate's 2013 attacks from his home in Solihull prevented the reporting of internet crime in the US for more than five hours and crashed the main Home Office for 83 minutes.

The 19-year-old already admitted three charges under the Computer Misuse Act.

To reduce the impact and increase the disruption of serious and organised crime across the region and beyond



# When?

- Disaster
- During Elections
- Financial upturns
- Seasonal
- Moments of Weakness

**(Stout, 2018)**

# How?

- Technologically
- **Human Interaction**


**(Cramer, Nobles, Amacker and Dovoedo,  
2013)**

# The Dark Web


Category Drugs

<http://lchudifyeqm4ldjj.onion/?cate...>


4g Incredible Bulk

 **£0.03919**  
hammerhome123 (5200)  
(4.91 ★)  
GB → GB, EU  
[Order](#)

1 x Red Devil Ecstasy PILLS. - 170mg MDMA  
- Ecstas

 **£0.0047**  
InsideTheWhale (2950)  
(4.93 ★)  
GB → EU, GB  
[Order](#)

Starter Pack 5x GTW Cartridges and 1  
Battery, Ch

 **£0.1143**  
GoodCatKilla (1750) (4.97 ★)  
US → US  
[Order](#)

To reduce the impact and increase the disruption of serious and organised crime across the region and beyond

# The Dark Web

Profile		Ratings				
Age	1 Stars	2 Stars	3 Stars	4 Stars	5 Stars	
Newer than 1 Month	2	2	6	6	455	
Newer than 3 Months	16	3	8	17	969	
Older	34	14	28	76	3663	

2d 7h	★★★★★	Enter your comments here	A.
12:28	★★★★★	2 blades hit the spot NDD	B.
2d 9h	★★★★★	FE - Great Vendor, always reliable	D.
08:51	★★★★★	Thx like always, NDD even easter top. Ty mate.	B.
10:32	★★★★★	Enter your comments here	s.
1d 9h	★★★★★	Got my order today everything seems to be fine smells good 2 and it was NDD	o.
00:39	★★★★★	Ndd decent smoke nice mellow buzz.10/10	m.
3d	★★★★★	the most reliable vendor around, NDD, top stealth and as always a fine smoke.	J.
1d 3h	★★★★★	Once again doesn't fail to disappoint! Very very fair and efficient vendor - NDD after order was accepted - perfect product again. The 90-95% pure cocaine really IS!!	s.
1d 23h	★★★★★		p.
1d 1h	★★★★★	NDD, great stealth and product gives a smooth, mellow daytime high	m.
1d 17h	★★★★★	Enter your comments here	u.
1d 5h	★★★★★	Enter your comments here	j.
4d	★★★★★	Enter your comments here	u.



# The Dark Web

Contact hammerhome123

<http://lchudifyeqm4ldjj.onion/conta...>

[Shop](#) Messages: 0 Account: £0.00 [wannabeamillionaire](#)

Contact vendor

**Username** hammerhome123 (5200) (4.91 ★)  
(@ 2097/37/18)

**Trusted seller** Yes ✓

**FE enabled** Yes

**Join date** 08/11/2015

**Last active** 14/04/2017 (today)

[Profile](#) [Ratings](#)

### Terms and conditions

This shop operates using escrow only. Messages and Addresses will only be accepted using PGP encryption or your order will be rejected. once you receive your order please finalize as soon as possible to avoid any unwanted disputes- we have had problems with non payers before and will not tolerate accusations of scamming or false advertisement. This shop will provide exactly what you order and nothing else.

Please leave a review of the shop and your experiences with us, and please don't leave negative feedback without first getting in touch as we are sure we can resolve any of our customers problems.

This shop and is also available on Alpha Bay Market so don't forget to keep a look out. If you found our service to be up to the exceptional standards we keep at the shop, please don't hesitate to recommend on forums.

Finally This shop ships using UK Royal mail exclusively, your package will be sent using 1st Class delivery and will not include any tracking numbers. Orders placed before 2.30pm UK time will be shipped the same day and orders placed after that time the next day.

Thank you and we hope you have a positive experience using our shop. Customers with good feedback whom do not receive their packages within 10 working days are entitled to a 50% refund or reship of product amount.

To reduce the impact and increase the disruption of serious and organised crime across the region and beyond

- Malicious Software
- Virus
- Worms
- **Phishing**

**(NCSC, 2018)**

# Phishing



- Phishing
- Spear Phishing
- Whale Phishing
- SMishing
- Vishing

**(NCSC, 2018)**

# Phishing



**Don't click on**  
**links within**  
**emails!**

This might be a phishing message and is potentially unsafe. Links and other functionality have been disabled. Click here to enable functionality (not recommended).

From: PayPal [service@paypal-australia.com.au] 24 AM  
To: [redacted]  
Cc: [redacted]  
Subject: Your account has been limited

**1. Fake sender domain.**  
(not service@paypal-australia.com.au)

**2. Suspicious Subject and content.**

**3. Bad grammar**

**4. Hovering over link reveals suspicious URL.**

**PayPal™**

**How to restore your PayPal account**

Dear PayPal member,  
To restore your PayPal account, you'll need to log in your account.

It's easy:

1. Click the link below to open a secure browser window.
2. Confirm <http://69.162.70.169/ppau/> the account, and then follow the instructions.

[Log in your account now](#)

PayPal Email ID PP32260008777636



# The aims of Phishing

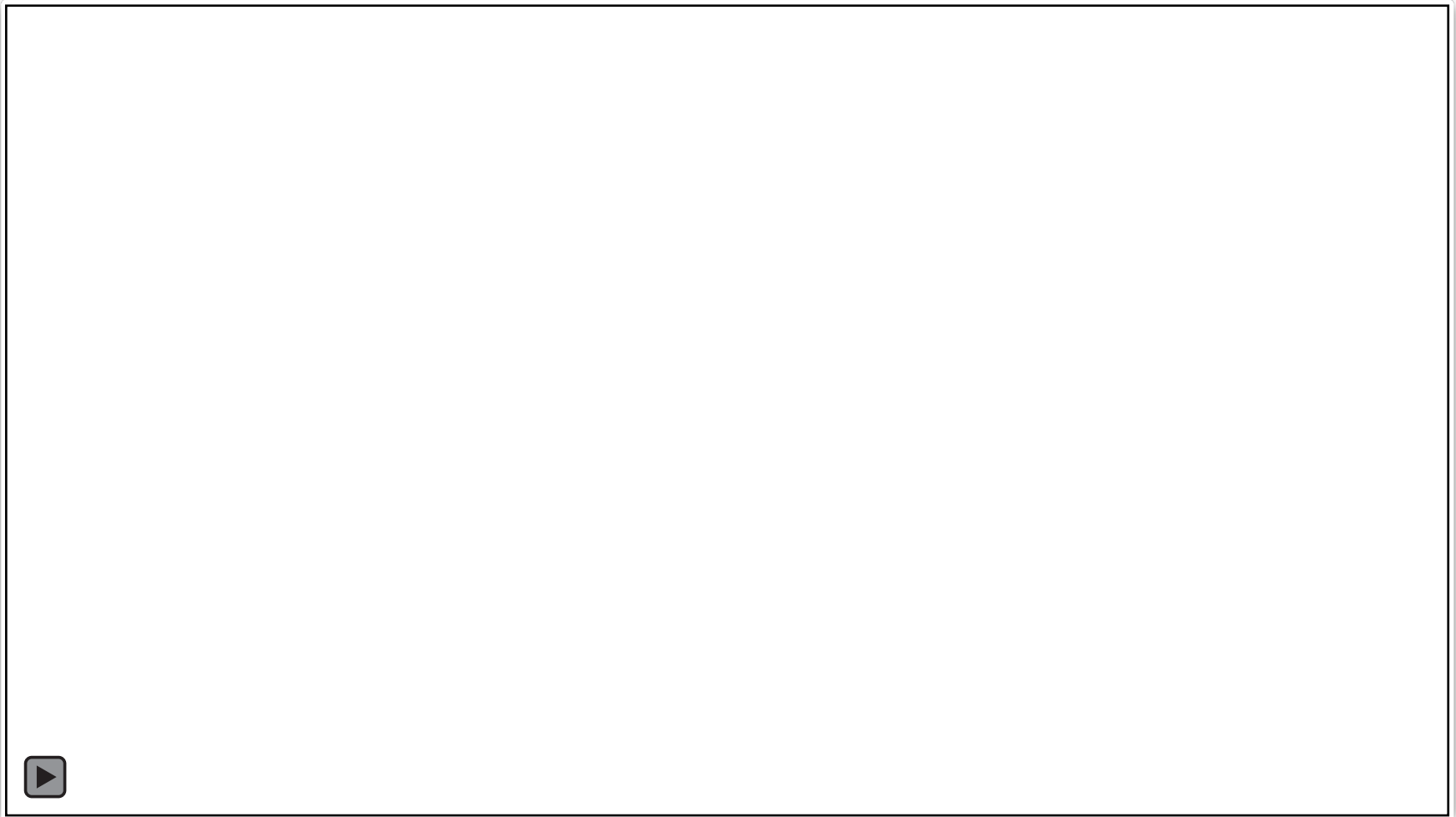


To reduce the impact and increase the disruption of serious and organised crime across the region and beyond

- Social Engineering
- Open Source Intelligence

**(Rader, and Rahman, 2015)**

# People Hacking



To reduce the impact and increase the disruption of serious and organised crime across the region and beyond

# The Policing Contribution .....

To reduce the impact and increase the disruption of serious and organised crime across the region and beyond



# Regional and National Policing Structures

**ROCU**  
REGIONAL ORGANISED CRIME UNIT  
FOR THE WEST MIDLANDS REGION



**Action Fraud**  
National Fraud & Cyber Crime Reporting Centre  
**0300 123 2040**

**National Fraud  
Intelligence Bureau**

 **SECURITY SERVICE**  
MI5

 **NPCC**  
National Police Chiefs' Council

 **GCHQ**

 **NCA**  
National Crime Agency

To reduce the impact and increase the disruption of serious and organised crime across the region and beyond

# ROCU

---

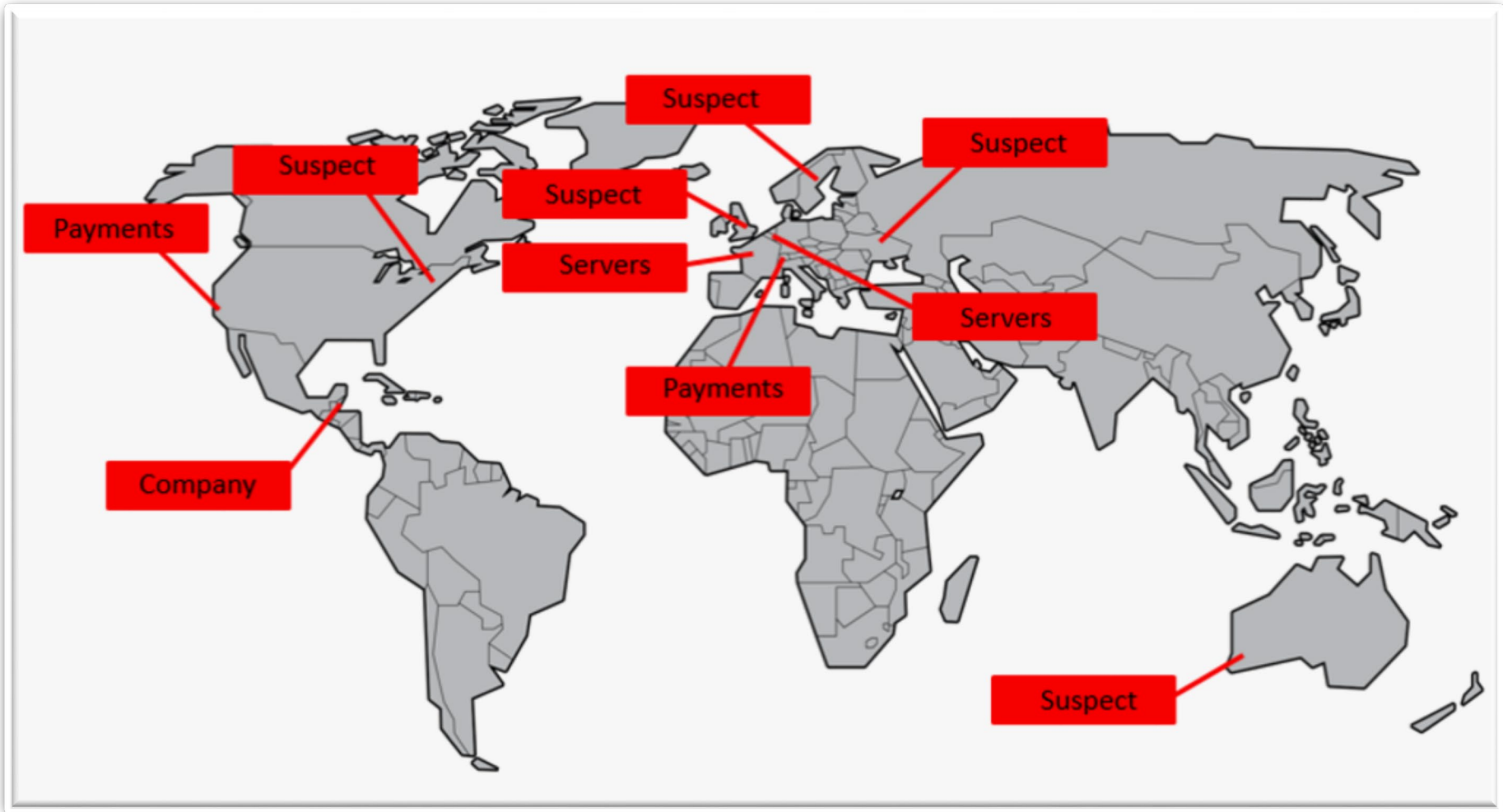
**REGIONAL ORGANISED CRIME UNIT  
FOR THE WEST MIDLANDS REGION**

To reduce the impact and increase the disruption of serious and organised crime across the region and beyond

# What would you do?

- **Disaster recovery plan?**
  - Key players to execute the plan?
- **Communication methods internally and externally?**
- **Do you know how and who to report to if attacked?**
- **Critical partners? (Data, infrastructure)**
  - Are they contractually obliged to assist and cooperate?
- **Data backup strategy?**

# Current Challenges



To reduce the impact and increase the disruption of serious and organised crime across the region and beyond

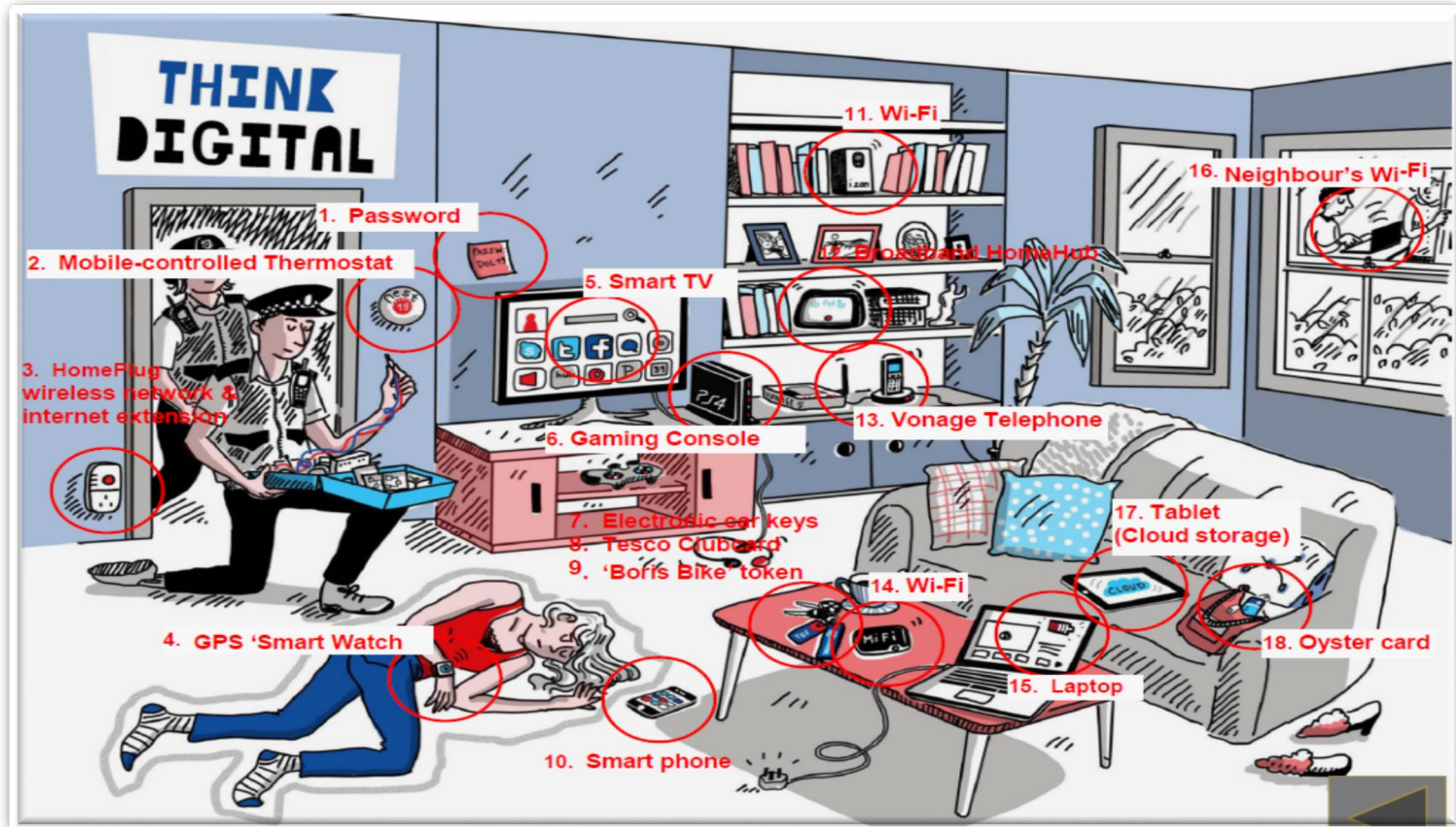


# Crime Scene



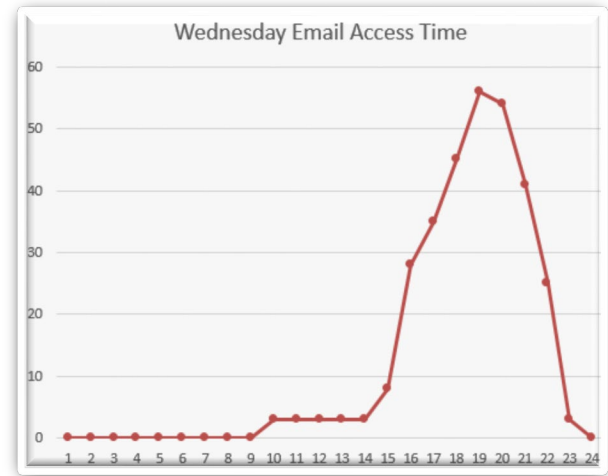
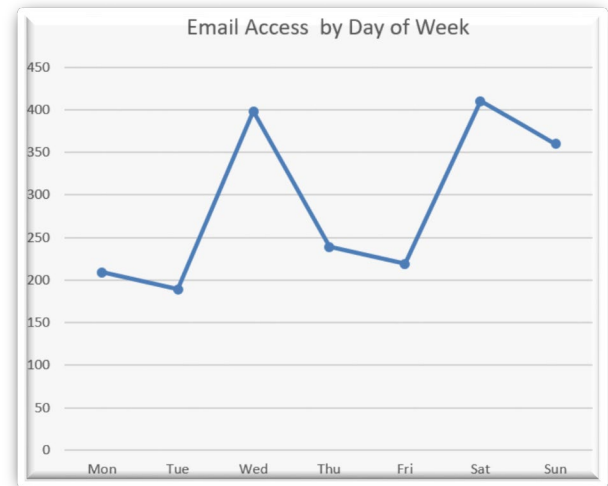
To reduce the impact and increase the disruption of serious and organised crime across the region and beyond

# The New Crime Scene



To reduce the impact and increase the disruption of serious and organised crime across the region and beyond





To reduce the impact and increase the disruption of serious and organised crime across the region and beyond



- Financial Institutes
- Internet Service Providers
- Facebook, Amazon, Netflix and Google (FANGs)

**(Wesley and Ndofor, 2013)**

# Societal Policing

**ROCU**  
REGIONAL ORGANISED CRIME UNIT  
FOR THE WEST MIDLANDS REGION



You

**(Wall, 2007)**



# Support .....

To reduce the impact and increase the disruption of serious and organised crime across the region and beyond

# Reporting

We encourage the reporting of Cyber Crime through the National Reporting mechanism [www.actionfraud.police.uk](http://www.actionfraud.police.uk) (24 hours)



## Cyber Security Information Sharing Partnership ([www.ncsc.gov.uk/cisp](http://www.ncsc.gov.uk/cisp))



To reduce the impact and increase the disruption of serious and organised crime across the region and beyond

## National Cyber Security Centre

([www.ncsc.gov.uk](http://www.ncsc.gov.uk))



To reduce the impact and increase the disruption of serious and organised crime across the region and beyond

# Resources

**ROCU**  
REGIONAL ORGANISED CRIME UNIT  
FOR THE WEST MIDLANDS REGION

**Get Safe Online ([www.getsafeonline.org](http://www.getsafeonline.org))**



**IT'S ALWAYS**

**PERS****NAL**

**DON'T BE A TARGET FOR AN ONLINE CRIMINAL**



# Resources

Cyber Aware ([www.cyberaware.gov.uk](http://www.cyberaware.gov.uk))



- **Password Hygiene**
- Anti Malware / Internet Security Software
- Firewall
- **Update** and Migrate
  
- Data Encryption
- Data Recovery (Backups)
  
- User Accounts and Privileges
- Photographs and Memes
- **Public Wi-Fi**



# Top Ten Passwords

- 1) 123456
- 2) 123456789
- 3) qwerty
- 4) 12345678
- 5) 111111
- 6) 1234567890
- 7) 1234567
- 8) password
- 9) 123123
- 10) 987654321

# Support

**ROCU**  
REGIONAL ORGANISED CRIME UNIT  
FOR THE WEST MIDLANDS REGION

## Cyber Essentials

([www.cyberessentials.ncsc.gov.uk](http://www.cyberessentials.ncsc.gov.uk))



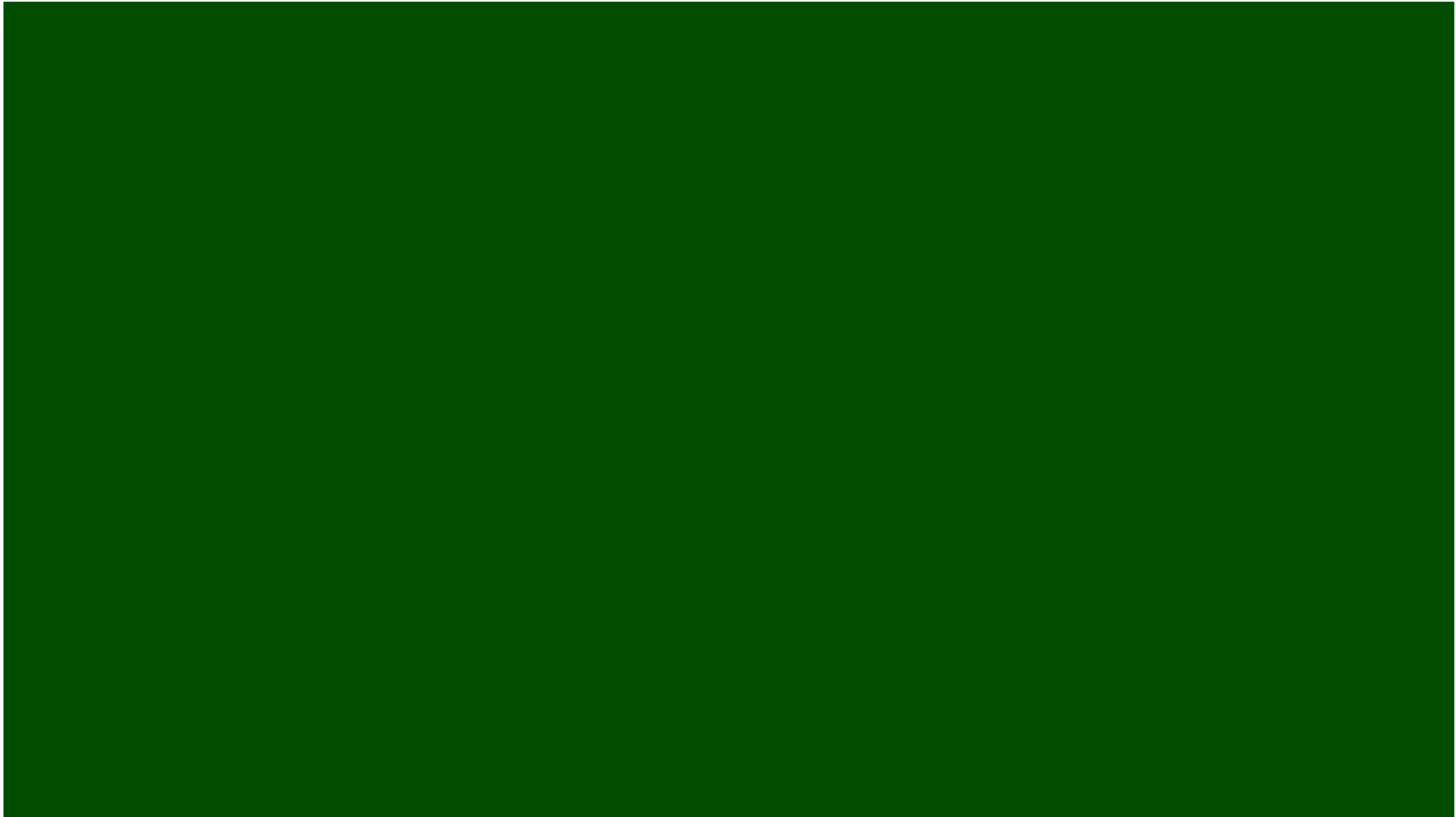
The screenshot shows the Cyber Essentials website homepage. At the top left is the Cyber Essentials logo, a blue circle with a white checkmark. To its right is the text "CYBER ESSENTIALS" in blue and green. Further right is a link "Cyber Essentials downloads" with a downward arrow. The main heading is "Protect your business against cyber threats". Below this is a paragraph: "Cyber Essentials is a new Government-backed and industry supported scheme to guide businesses in protecting themselves against cyber threats." Another paragraph states: "Cyber Essentials documents are FREE to download and any organisation can use the guidance to implement essential security controls." There are two green buttons: "Cyber Essentials downloads" and "Go to questionnaire", both with downward arrows. On the right side, there is an image of a laptop and a monitor displaying the Cyber Essentials logo and "CYBER ESSENTIALS PLUS".

To reduce the impact and increase the disruption of serious and organised crime across the region and beyond

- 1. Boundary controls**
- 2. Secure configuration**
- 3. Access Control**
- 4. Anti virus**
- 5. Patch Management**



# Real World Cyber attack



To reduce the impact and increase the disruption of serious and organised crime across the region and beyond

- Always consider the 5wh
- Strong Passwords
- Online Activity
- Email



# Please Surf Safely



## Questions?

To reduce the impact and increase the disruption of serious and organised crime across the region and beyond





# ROCU

REGIONAL ORGANISED CRIME UNIT  
FOR THE WEST MIDLANDS REGION

DC Patrick McBrearty

-

[rccu@west-  
midlands.pnn.police.uk](mailto:rccu@west-midlands.pnn.police.uk)

Twitter:- [@ROCUWMM](https://twitter.com/ROCUWMM)

To reduce the impact and increase  
the disruption of serious and  
organised crime across the  
region and beyond