NERCCU
North East Regional Cyber Crime Unit

Boosting Specialist Cyber Crime Capabilities through Regional Special Operations Units

North East Cyber Protect

nerccuprotect@durham.police.uk
www.nerccu.police.uk

Boosting Specialist Cyber Crime Capabilities through Regional Special Operations Units

NERCCU
North East Regional Cyber Crime Unit

North East Cyber Protect Network

- Claire Vandenbroecke – Force Specialist Cyber Protect and Prepare Officer, Northumbria Police
- Jon Hudson – Regional Cyber Protect & Prepare Officer, NERSOU
- Jonathan Green - Regional Cyber Protect & Prepare Officer, NERSOU
- Claire Turnbull – Force Specialist Cyber Prevent and Protect Supervisor, Durham Constabulary
- Kelly Close – Force Specialist Cyber Protect & Prepare Officer, Cleveland Police

Boosting Specialist Cyber Crime Capabilities through Regional Special Operations Units

NERCCU
North East Regional Cyber Crime Unit

Contents

- ❑ Overview of the NPCC National Cyber Security Strategy & Team Cyber UK
- ❑ Regional Strategy
- ❑ Case Study - Improving Incident Response
- ❑ Case Study - Developing Threat Intelligence

nerccuprotect@durham.police.uk
www.nerccu.police.uk

Boosting Specialist Cyber Crime Capabilities through Regional Special Operations Units

NERCCU
North East Regional Cyber Crime Unit

Overview

nerccuprotect@durham.police.uk
www.nerccu.police.uk

Boosting Specialist Cyber Crime Capabilities through Regional Special Operations Units

Overview

National Cyber Security Centre
a part of GCHQ

NERCCU
North East Regional Cyber Crime Unit

PURSUE
PREVENT
PROTECT
PREPARE

https://www.ncsc.gov.uk/information/regional-organised-crime-units-rocus

NERSOU North East Regional Special Operations Unit | Protecting communities from organised crime

nerccuprotect@durham.police.uk
www.nerccu.police.uk

If you have been a victim of fraud or cyber crime, report it to Action Fraud

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

Boosting Specialist Cyber Crime Capabilities through Regional Special Operations Units

NERCCU
North East Regional Cyber Crime Unit

Overview

2014	**P**URSUE	3 x Detectives, 1 x Investigator
2016	**P**ROTECT/**P**REPARE	2 x Protect/Prepare
2017	**P**REVENT	3 x P.Cs
2019	**RMLD**	Protect Officers in All Forces

nerccuprotect@durham.police.uk
www.nerccu.police.uk

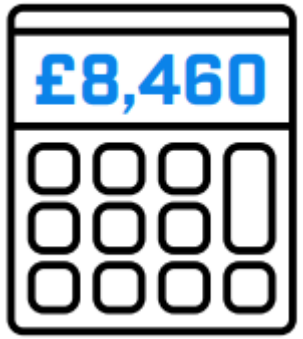
Boosting Specialist Cyber Crime Capabilities through Regional Special Operations Units

NERCCU
North East Regional Cyber Crime Unit

Overview

Untargeted  **Targeted**

of businesses identified cyber security breaches or attacks in the last 12 months



is the average annual cost for businesses that lost data or assets after breaches

Office for National Statistics

Total	71,460
Micro	62,595
Small	7,230
Medium	1,285
Large	350

27,869

£235,775,124

NERSOU North East Regional Special Operations Unit | Protecting communities from organised crime

nerccuprotect@durham.police.uk
www.nerccu.police.uk

If you have been a victim of fraud or cyber crime, report it to Action Fraud

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

Boosting Specialist Cyber Crime Capabilities through Regional Special Operations Units

NERCCU
North East Regional Cyber Crime Unit

Overview

Who Are We Defending Against?

Hackers

Status and technical challenge

- Can be good or bad depending on their actions

Insiders

Privileged access to data

- Can be malicious or, more commonly, accidental

Criminals

Often driven by financial gain

- Theft of data
- Ransomware
- Cyber enabled or dependant

What Are We Defending Against?

Remote Desktop Protocol (RDP)

Phishing

Vulnerable software or hardware

Ransomware

nerccuprotect@durham.police.uk
www.nerccu.police.uk

If you have been a victim of fraud or cyber crime, report it to Action Fraud

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

Boosting Specialist Cyber Crime Capabilities through Regional Special Operations Units

NERCCU
North East Regional Cyber Crime Unit

Overview

RMLD

Reactive support to victims of cyber dependant crime

Disseminated to local forces from regional supervision

CITY OF LONDON POLICE

National Cyber Security Centre
a part of GCHQ

Reactive support to victims of cyber dependant crime

Proactive engagement aimed at empowering the public to change their cyber security behaviour

Enhancing Intelligence Picture

Capability Development

nerccuprotect@durham.police.uk
www.nerccu.police.uk

If you have been a victim of fraud or cyber crime, report it to Action Fraud

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

Boosting Specialist Cyber Crime Capabilities through Regional Special Operations Units

NERCCU
North East Regional Cyber Crime Unit

Regional Strategy

nerccuprotect@durham.police.uk
www.nerccu.police.uk

Boosting Specialist Cyber Crime Capabilities through Regional Special Operations Units

NERCCU
North East Regional Cyber Crime Unit

Regional Strategy

Engagements with sole traders, charities, individuals and communities

Engagement with victims of crime through RMLD/Action Fraud Referrals

Upskilling/Training of front line policing

Delivery of National Strategy

NERCCU
North East Regional Cyber Crime Unit

Co-ordinate Proactive and Reactive Engagement with SMEs, large businesses, business clusters, WARPS LRFs & Banks

Influence Network & establish/share best practice through the national working group

Increase the provision of products and services across the region/network through capability/project development

nerccuprotect@durham.police.uk
www.nerccu.police.uk

If you have been a victim of fraud or cyber crime, report it to Action Fraud

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

Boosting Specialist Cyber Crime Capabilities through Regional Special Operations Units

NERCCU
North East Regional Cyber Crime Unit

Regional Strategy

Protect Products

- **Cyber Basic Review**
- **Vulnerability Assessment**
- **Police Cyber Alarm**

- **Staff Training**
- **Cyber Inputs, Meetings and Webinars**

- **Decisions & Disruptions**
- (aka Cyber Lego)

- **Cyber Exercising**
- Cyber Incident Response Plan

nerccuprotect@durham.police.uk
www.nerccu.police.uk

Boosting Specialist Cyber Crime Capabilities through Regional Special Operations Units

NERCCU
North East Regional Cyber Crime Unit

Regional Strategy

Benefits to being part of the North East Cyber Protect Network

Support, guidance and effective communication

Increased reach of engagements

Increased capability

nerccuprotect@durham.police.uk
www.nerccu.police.uk

If you have been a victim of fraud or cyber crime, report it to Action Fraud

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

Boosting Specialist Cyber Crime Capabilities through Regional Special Operations Units

NERCCU
North East Regional Cyber Crime Unit

Reactive Support

Case Study - Improving Incident Response

nerccuprotect@durham.police.uk
www.nerccu.police.uk

Boosting Specialist Cyber Crime Capabilities through Regional Special Operations Units

NERCCU
North East Regional Cyber Crime Unit

Reactive Support

August 2020

2 Universities fall victim to individual strains of ransomware
NERCCU attended daily gold group meetings to provide victim care and co-ordinate IOC/TTPs for dissemination.

January 2021

Increase in Ransomware Threat to Education Sector
Core Protect Messaging pushed out by NERCCU to Directors of Education in Local Authorities as well as via SLOs

February 2021

RYUK Seen as attack method against Education.
Indicators of Compromise Disseminated to Directors of Education in Local Authorities as well as via SLOs. Further Intelligence from Industry Partners (Cijax) obtained to enhance the picture.

nerccuprotect@durham.police.uk
www.nerccu.police.uk

Boosting Specialist Cyber Crime Capabilities through Regional Special Operations Units

NERCCU
North East Regional Cyber Crime Unit

Reactive Support

March 2021

Zero Day Vulnerability Found in Microsoft Exchange Server
Case Study

April 2021

School in Northumbria falls victim to Phobos Ransomware Attack
NERCCU co-ordinate Protect response: IOC's/TTPs obtained from threat intelligence partners and disseminated to stakeholders across the region

Operational Strategy obtained from lead ROCU for Phobos ransomware and shared with Northumbria Pursue Detectives for ongoing investigative support

Victim care provided by Northumbria Cyber Officers

May 2021

NCSC release their 'Cyber Aware For Schools' training package
In partnership with other ROCUs, NERCCU deliver the training across the country to address the increased threat from ransomware within the education sector

Boosting Specialist Cyber Crime Capabilities through Regional Special Operations Units

NERCCU
North East Regional Cyber Crime Unit

Regional Strategy

Benefits to being part of the North East Cyber Protect Network

A coordinated approach

Improved investigations

Efficient and effective communication

nerccuprotect@durham.police.uk
www.nerccu.police.uk

Boosting Specialist Cyber Crime Capabilities through Regional Special Operations Units

NERCCU
North East Regional Cyber Crime Unit

Proactive Support

Case Study - Developing Threat Intelligence

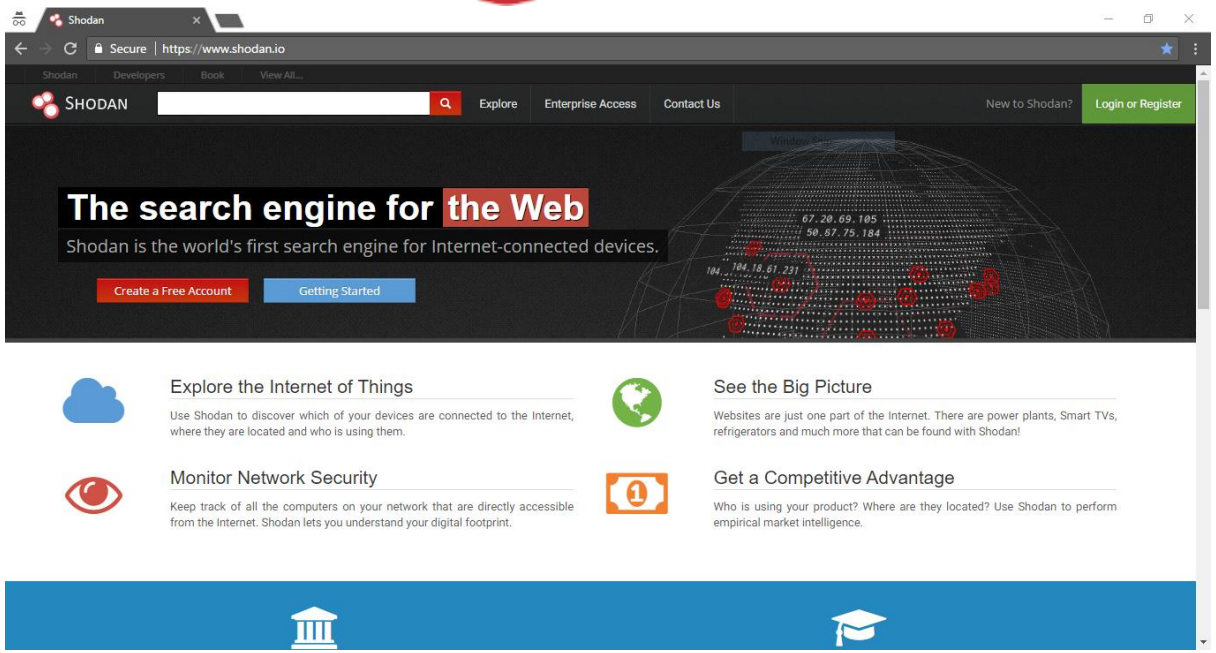
nerccuprotect@durham.police.uk
www.nerccu.police.uk

Boosting Specialist Cyber Crime Capabilities through Regional Special Operations Units

NERCCU
North East Regional Cyber Crime Unit

Proactive Support

SHODAN



NORTH EAST:

Unique:	All	Has Vuln	
isp	148	79	53%
domain	1775	542	31%
org	1179	301	26%
os	41	4	10%
port	723	67	9%
product	364	23	6%

1096 unique vulnerabilities identified

nerccuprotect@durham.police.uk
www.nerccu.police.uk

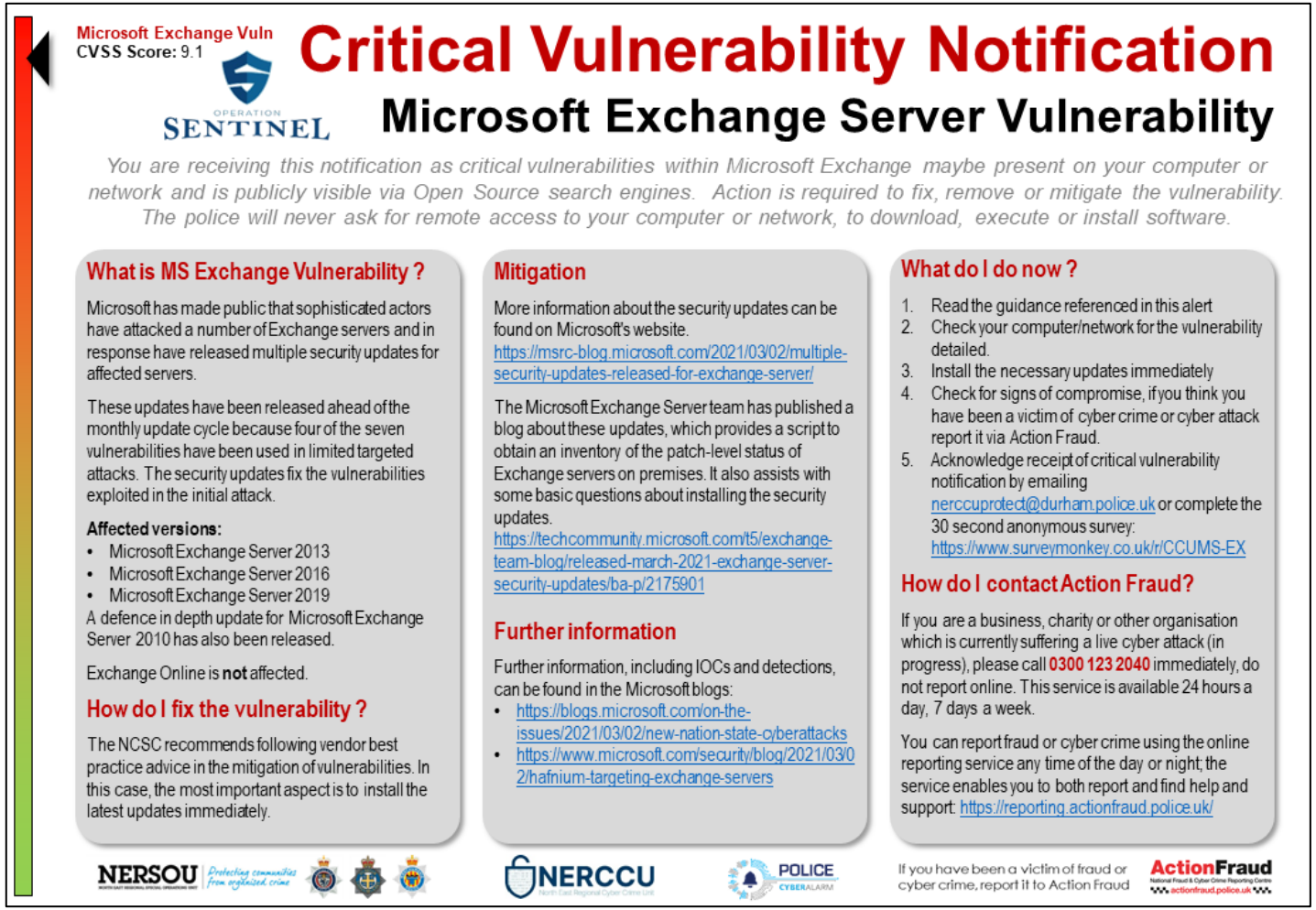
If you have been a victim of fraud or cyber crime, report it to Action Fraud

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

Boosting Specialist Cyber Crime Capabilities through Regional Special Operations Units

NERCCU North East Regional Cyber Crime Unit

Proactive Support



Microsoft Exchange Vuln
CVSS Score: 9.1

OPERATION SENTINEL

Critical Vulnerability Notification

Microsoft Exchange Server Vulnerability

You are receiving this notification as critical vulnerabilities within Microsoft Exchange maybe present on your computer or network and is publicly visible via Open Source search engines. Action is required to fix, remove or mitigate the vulnerability. The police will never ask for remote access to your computer or network, to download, execute or install software.

What is MS Exchange Vulnerability ?

Microsoft has made public that sophisticated actors have attacked a number of Exchange servers and in response have released multiple security updates for affected servers.

These updates have been released ahead of the monthly update cycle because four of the seven vulnerabilities have been used in limited targeted attacks. The security updates fix the vulnerabilities exploited in the initial attack.

Affected versions:

- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019

A defence in depth update for Microsoft Exchange Server 2010 has also been released.

Exchange Online is **not** affected.

How do I fix the vulnerability ?

The NCSC recommends following vendor best practice advice in the mitigation of vulnerabilities. In this case, the most important aspect is to install the latest updates immediately.

Mitigation

More information about the security updates can be found on Microsoft's website.
https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/

The Microsoft Exchange Server team has published a blog about these updates, which provides a script to obtain an inventory of the patch-level status of Exchange servers on premises. It also assists with some basic questions about installing the security updates.
https://techcommunity.microsoft.com/t5/exchange-team-blog/released-march-2021-exchange-server-security-updates/ba-p/2175901

Further information

Further information, including IOCs and detections, can be found in the Microsoft blogs:

- https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks
- https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers

What do I do now ?

1. Read the guidance referenced in this alert
2. Check your computer/network for the vulnerability detailed.
3. Install the necessary updates immediately
4. Check for signs of compromise, if you think you have been a victim of cyber crime or cyber attack report it via Action Fraud.
5. Acknowledge receipt of critical vulnerability notification by emailing nerccuprotect@durham.police.uk or complete the 30 second anonymous survey: https://www.surveymonkey.co.uk/r/CCUMS-EX

How do I contact Action Fraud?

If you are a business, charity or other organisation which is currently suffering a live cyber attack (in progress), please call **0300 123 2040** immediately, do not report online. This service is available 24 hours a day, 7 days a week.

You can report fraud or cyber crime using the online reporting service any time of the day or night; the service enables you to both report and find help and support: https://reporting.actionfraud.police.uk/

NERSOU Protecting communities from organised crime

NERCCU

POLICE CYBERALARM

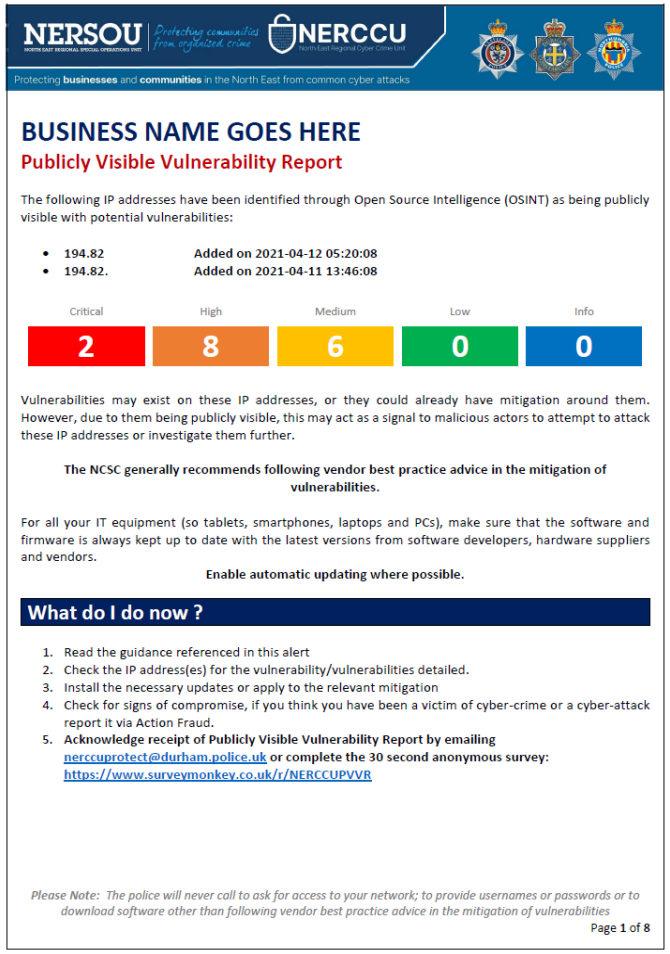
If you have been a victim of fraud or cyber crime, report it to Action Fraud

ActionFraud National Fraud & Cyber Crime Reporting Centre actionfraud.police.uk

Boosting Specialist Cyber Crime Capabilities through Regional Special Operations Units

NERCCU
North East Regional Cyber Crime Unit

Proactive Support



NERSOU | Protecting communities from organised crime | NERCCU

Protecting **businesses** and **communities** in the North East from common cyber attacks

BUSINESS NAME GOES HERE

Publicly Visible Vulnerability Report

The following IP addresses have been identified through Open Source Intelligence (OSINT) as being publicly visible with potential vulnerabilities:

- 194.82 **Added on 2021-04-12 05:20:08**
- 194.82. **Added on 2021-04-11 13:46:08**

Critical	High	Medium	Low	Info
2	8	6	0	0

Vulnerabilities may exist on these IP addresses, or they could already have mitigation around them. However, due to them being publicly visible, this may act as a signal to malicious actors to attempt to attack these IP addresses or investigate them further.

The NCSC generally recommends following vendor best practice advice in the mitigation of vulnerabilities.

For all your IT equipment (so tablets, smartphones, laptops and PCs), make sure that the software and firmware is always kept up to date with the latest versions from software developers, hardware suppliers and vendors.

Enable automatic updating where possible.

What do I do now ?

1. Read the guidance referenced in this alert
2. Check the IP address(es) for the vulnerability/vulnerabilities detailed.
3. Install the necessary updates or apply to the relevant mitigation
4. Check for signs of compromise, if you think you have been a victim of cyber-crime or a cyber-attack report it via Action Fraud.
5. **Acknowledge receipt of Publicly Visible Vulnerability Report by emailing nerccuprotect@durham.police.uk or complete the 30 second anonymous survey: https://www.surveymonkey.co.uk/r/NERCCUPVVR**

Please Note: The police will never call to ask for access to your network; to provide usernames or passwords or to download software other than following vendor best practice advice in the mitigation of vulnerabilities

Page 1 of 8

BUSINESS NAME GOES HERE

Publicly Visible Vulnerability Report

The following IP addresses have been identified through Open Source Intelligence (OSINT) as being publicly visible with potential vulnerabilities:

- 194.82 **Added on 2021-04-12 05:20:08**
- 194.82. **Added on 2021-04-11 13:46:08**

Critical	High	Medium	Low	Info
2	8	6	0	0

Vulnerabilities may exist on these IP addresses, or they could already have mitigation around them. However, due to them being publicly visible, this may act as a signal to malicious actors to attempt to attack these IP addresses or investigate them further.

Boosting Specialist Cyber Crime Capabilities through Regional Special Operations Units

NERCCU
North East Regional Cyber Crime Unit

Regional Strategy

Benefits to being part of the North East Cyber Protect Network

Overcame lockdown challenges

Improved local visibility

Mitigated lockdown impact

nerccuprotect@durham.police.uk
www.nerccu.police.uk

Boosting Specialist Cyber Crime Capabilities through Regional Special Operations Units

NERCCU
North East Regional Cyber Crime Unit

Proactive Support

Conclusion

nerccuprotect@durham.police.uk
www.nerccu.police.uk