Case Study Digest

THE CYBER RESILIENCE CENTRE FOR WALES

NORTH WEST REGIONAL ORGANISED CRIME UNIT

TARIAN ROCU

HEDDLU GOGLEDD CYMRU · NORTH WALES POLICE

HEDDLU DE CYMRU · SOUTH WALES POLICE

HEDDLU GWENT POLICE

Heddlu Police DYFED POWYS

TABLE OF CONTENTS

Foreword

The Cyber Resilience Centre for Wales (WCRC) is a not-for-profit company that has been set up by policing in partnership with academia and the private sector to raise cyber resilience across Wales. The WCRC is focused on supporting SMEs, micro-businesses and third sector organisations to improve their cyber security. As part of the WCRC community we have spoken to businesses, organisations, police cyber investigative units, as well as taking our own experiences as an SME to better understand some of the common attacks across Wales and the UK.

This is the first case study digest produced by the WCRC and the purpose of this publication is to inform partners and members as to the types of attacks being seen by businesses and to help raise awareness of how to identify these.

We would encourage our members and partners to share your experiences with us, so we can in turn inform the wider WCRC community. The more experiences we are able to share, the more likely others will be able to recognise cyber-attacks and avoid becoming victims themselves

Detective Superintendent Paul Peters, The Wales Cyber Resilience Centre

As Detective Chief Inspector at the North West Regional Organised Crime Unit, I am charged with investigation and reduction of cyber crime in the North West region. The North West Regional Organised Crime Unit (NWROCU) is a collaboration of officers from all the North West Police services – North Wales, Cheshire, Merseyside, Greater Manchester, Cumbria and Lancashire.

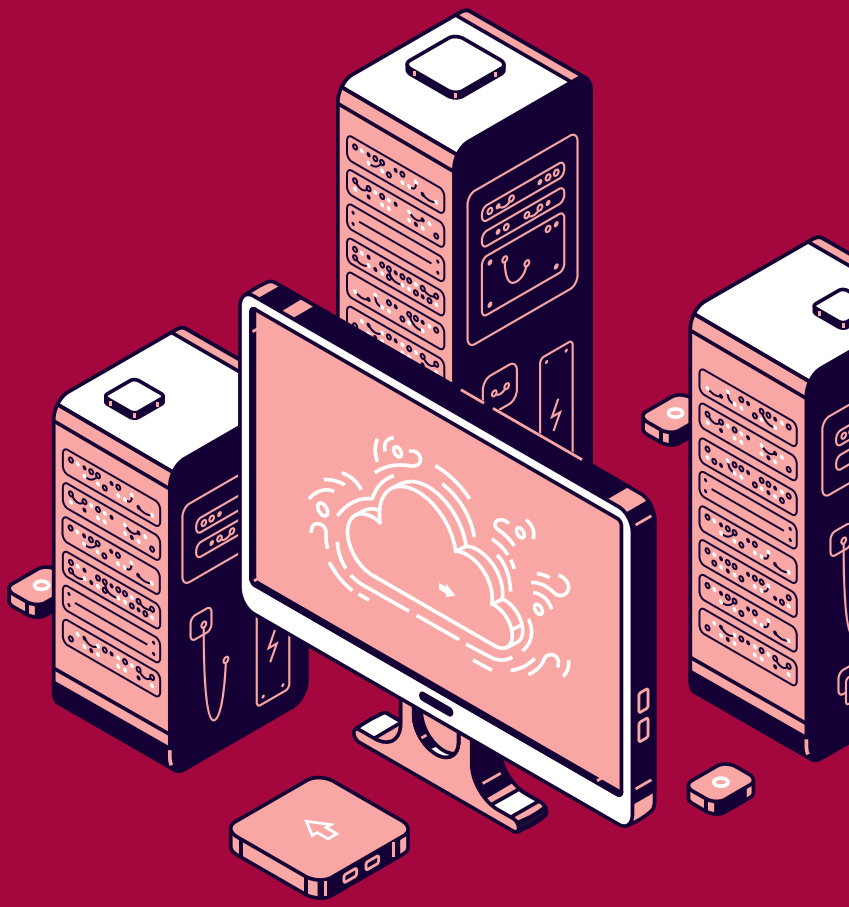
Cybercrime is one of our key strategic priorities and presents a significant threat both here in the northwest and nationally. Fraud offences account for nearly half of all reported crime in the England and Wales and 80% of these have a cyber element.

Together with our partners from the public and private sector, there is a global and whole system approach to tackling the harm caused by cybercrime, with substantial investment to equipping law enforcement agencies with the latest capabilities and technology needed to counter this evolving threat.

As you explore the pages of this booklet, you will discover a wealth of knowledge, insights, and practical advice to help strengthen resilience against cybercrime

Detective Chief Inspector Chris Maddocks, The North West Regional Organised Crime Unit

Repeat victim of Ransomware



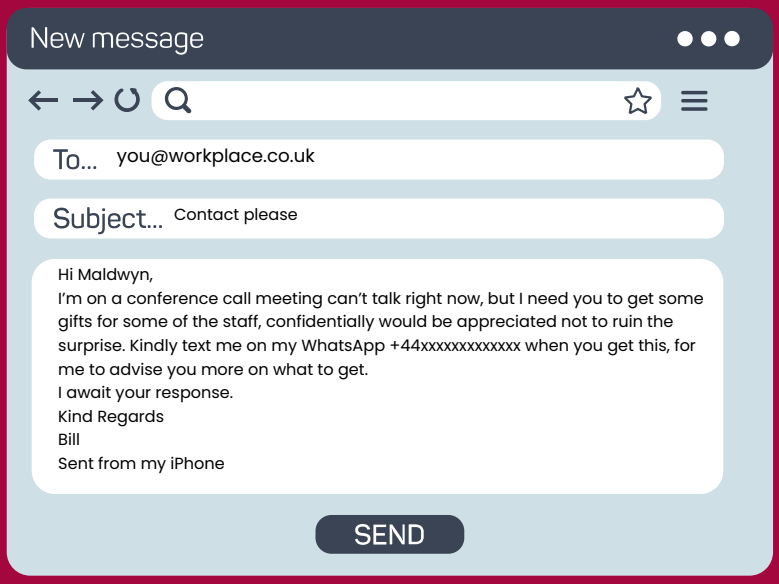
A small business in Wales was the victim of ransomware on three separate occasions. The business used an IT support company to ensure its data was backed up, and after the first case had received guidance on recognising phishing emails, and how to avoid falling victim to ransomware.

The IT support company was able to establish after the third attack, that despite the guidance given, the managing director of the business had instructed the administrative staff to open any attachments, even if from an unknown source, where there was a request for payment as he did not want the business to have unpaid debts.

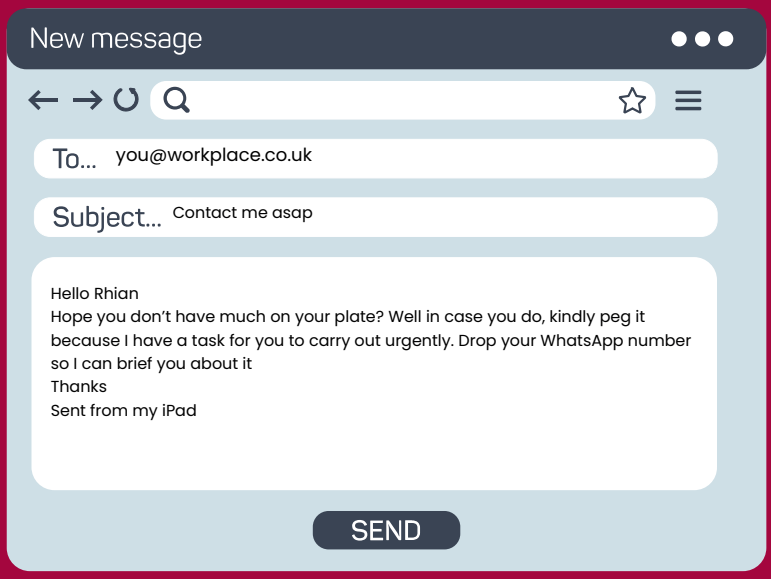
This meant that administrative staff had repeatedly opened attachments within emails despite them being from an unknown source. The attachments had contained ransomware which led to the encryption of its data.

Cyber security needs to be adhered to by all members of an organisation. It is not acceptable for members of management to over-rule basic cyber security measures.

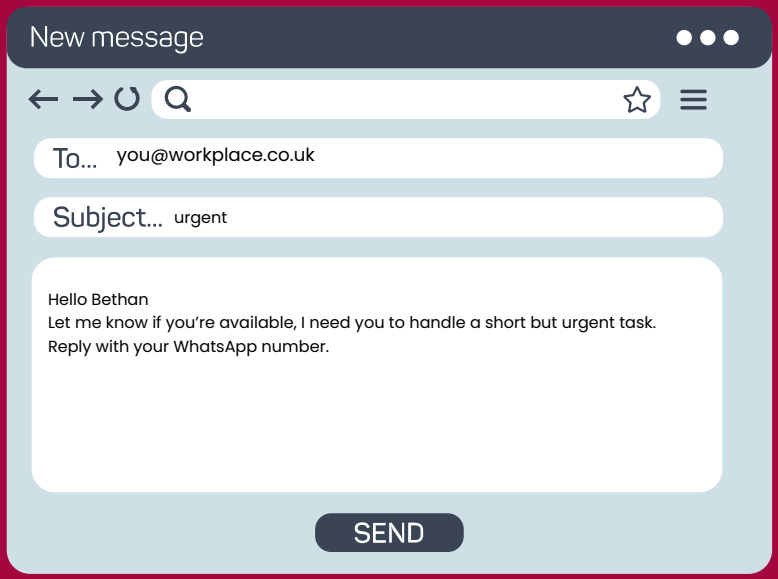
Spear phishing campaign



This is a common phishing attack, which in this case was identified and did not result in any loss. The incident has been passed to police and an investigation commenced.



Of note, each email sent was from a different sender, and different email supplier. These were easily identifiable as not from the company/boss unless the recipient was just reading the email content and not noting the sender details (common in phishing campaigns).



They appeared to have been designed from social engineering using details of the company and staff on LinkedIn to make them appear legitimate.

Phishing attack on guesthouse

The manager received an email purporting to be from Airbnb. They ignored the first email but responded to a follow-up email with a question. They had previously declined to use Channel manager. The email that confirmed was quickly followed by a phone call.

A Teams invitation followed, and the manager recognised that the email was from @outerreachair.bnb.

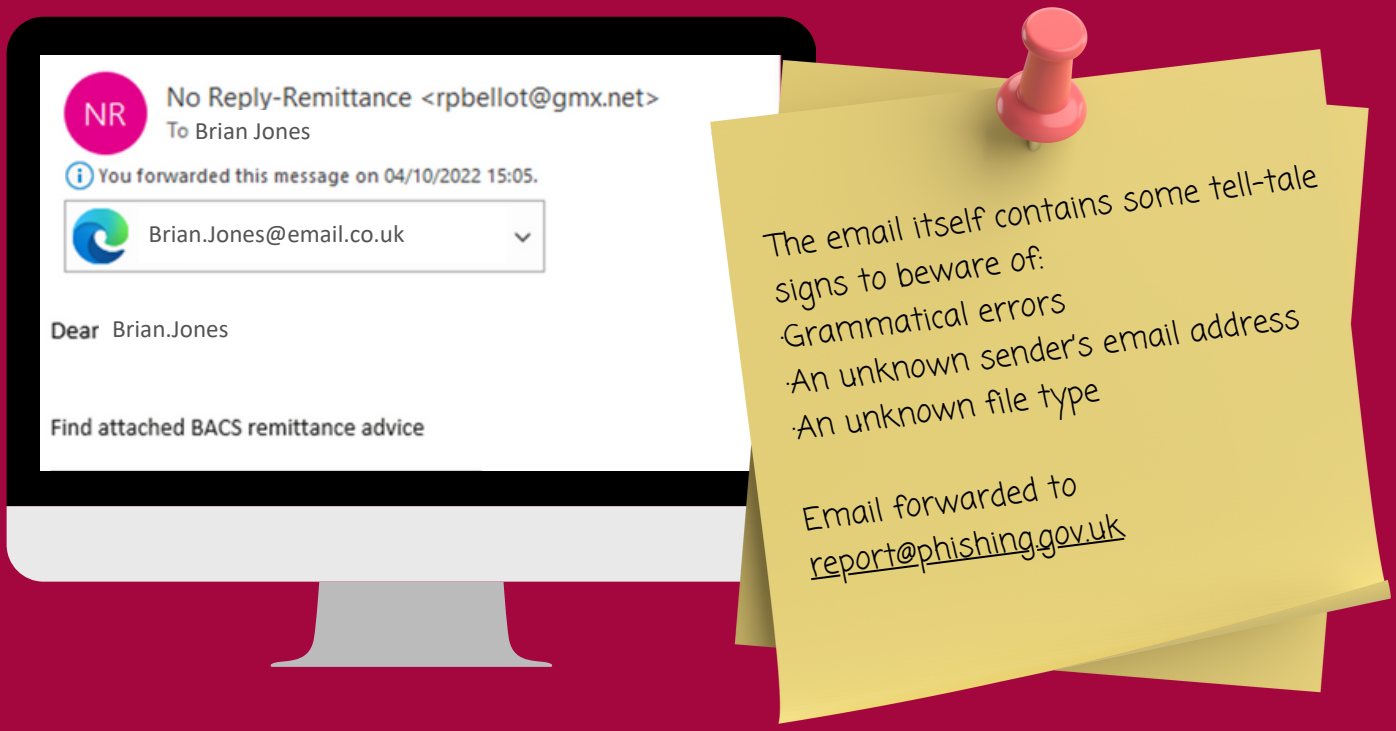
The manager contacted Airbnb on a publicly available number and was able to confirm name of person was not an employee of Airbnb, and that this was not its email, and it did not have a channel manager in use.

The business forwarded the emails on to phishing@gov.uk which is the National Cyber Security Centre (NCSC) portal for reporting phishing emails.

The National Cyber Security Centre (NCSC) analyses the suspect emails and any websites it links to. If it is believed to be malicious, then the NCSC can seek to block the address the email came from, so it can no longer send emails. It also works with hosting companies to remove links to malicious websites.

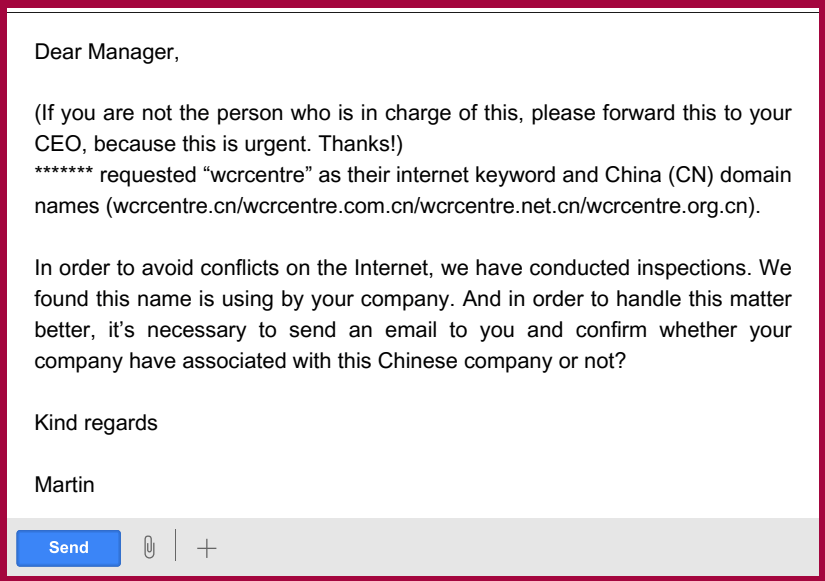
Phishing attack on the WCRC

A phishing email was received on a Friday afternoon alleging to relate to a BACS remittance. The attached file, if opened created an Office 365 login page in an attempt to harvest usernames and passwords. These would have then been sent to the criminal server.



A phishing email was received from an organisation posing as a Chinese domain name registry, claiming that a Chinese company was seeking to register domain names using wcrcentre as the internet keyword.

This is known as the 'Chinese domain name registration scam', this is an attempt to scare us into registering the other versions of our website's address. If the centre had responded, then there would have been further emails which would have led to the conclusion that we would need to pay to register a number of domains on a yearly basis to protect the brand.



Phishing attack email attack

This case study relates to an attack on a larger organisation (Company A), where the attackers were able to get the victim organisation to change account details which then resulted in significant financial losses.

The attacker contacted the finance officer, claiming to be from a company within its supply chain (Company X), highlighting that a payment through its portal had the incorrect date and needed to be brought forward. A revised invoice was provided along with 'updated' bank account information.

The date was changed as per the request and the attacker asked for confirmation that the bank details had also been updated. The finance officer responded that this could be done through the portal themselves and directed them to another employee within Company A for support if needed. This person provided details of the admin user (who was an employee of Company X) to complete this update, but the attacker confused this thinking this was someone else in Company A. When it was pointed out that the admin user was a Company X employee, the attacker responded that they were off sick and would not be back in time to make the changes before the payment.

Company A made the changes to Company X account details resulting in payment being made to the attacker.

There were multiple opportunities to identify that this was an attack. The simple step of making direct contact with the client company would have revealed that this was fraudulent. This led to significant losses for the victim organisation.

Having a policy in place to ensure that account details are not changed unless confirmed through at least two methods i.e. phone contact with supplier using known number following email request may have identified this was fraudulent.

This digest has been created in order to share case studies of cyber-attacks across Wales and the UK. The examples are anonymised and focus on the methodology used in the attack. The case studies have been provided by members of the Cyber Resilience Centre for Wales, police forces and regional units across Wales.

Contributors:
The Cyber Resilience Centre for Wales
The North West Regional Organised Crime Unit
Tarian
North Wales Police
South Wales Police
Gwent Police
Dyfed-Powys Police

WCRC Membership packages

Free Core Membership

This is for SMEs or micro-business that are under-resourced when it comes to improving cyber resilience or there's uncertainty of what the requirements are. Businesses already with a good grasp of cyber security will also benefit from joining, as we help keep the community up to date with the latest guidance and local alerts.

Community Ambassador Membership (£500 annually)

This membership has been specifically created for all businesses interested in being a part of the WCRC cyber community made up of Welsh organisations that are committed to supporting businesses across Wales to develop their cyber resilience.

For more information on the Cyber Resilience Centre for Wales and all the services and support it provides, go to www.wcrcentre.co.uk

To keep up to date on the latest WCRC news, the centre can be found on LinkedIn under Cyber Resilience Centre for Wales, on Facebook using @WalesCRC and @CRCWales on X.