# CYBER CRIME SENTINEL

**ISSUE** 18 25-Sep-2020

WMCYBER@WEST-MIDLANDS.PNN.POLICE.UK
WWW.WMCYBER.ORG

This newsletter has been collated by West Midlands Regional Cyber Crime Unit and is intended for wider distribution within the West Midlands Region to raise awareness among businesses and members of the public.

## CYBER PROTECT WEEKLY TIP

This week, the NHS has launched the NHS COVID-19 app whereby venues are being instructed to download and display QR codes for visitors to scan when they arrive, using the new app. This is to help trace and stop the spread of coronavirus (COVID-19). It is important to note that users are advised to only scan venue QR codes through the NHS COVID-19 app to ensure that the user is accessing the correct website rather than a malicious one. Cyber criminals use a practice called QR Spoofing or "Attagging" which is where a real QR code is replaced by a cloned one, which then redirects the person scanning that code to a similar, potentially malicious, website where personal data can be intercepted and breached.

Protecting yourself from QR Spoofing when `checking in' to places, as is now required, is as simple as avoiding scanning QR codes with your camera and instead downloading the free NHS COVID-19 (Test and Trace) app from the Google Play Store or Apple App Store. When using the NHS COVID-19 app the QR code is scanned using an in-app camera and only official NHS QR codes are accepted. The app also does not require its users to open a separate webpage eliminating the risk of malicious links nor does it require the user to enter any personal information other than the first three letters of the users postcode as it relies mainly on venue check ins and Bluetooth location.

### QR Spoofing or Attagging

QR codes, particularly printed to signs or posters, are static and available to exploitation by cyber criminals by putting a fake QR code over a genuine QR code. For example, a QR code, on scanning, would link to the genuine website www.wmcyber.org but a fake QR code can be made up, printed off and placed over the genuine code to redirect to www.wm-cyber.org. At this point, the member of the public may be tricked into entering their personal and private data and financial information. Often, the spoofed website looks the exact same as the genuine one to make the users think they are legitimate and trustworthy. To protect yourself, we ask that members of the public always stay vigilant of spotting malicious URLS and, if possible, ensure that they preview the actual URL when scanning QR codes via phone QR readers. Also, take advantage of the free QR code readers available that function as a typical reader but also provides the added benefit of security to the scan.

## IN THE NEWS

## TOP CYBER HEADLINES

THE LATEST NEWS ON CYBERCRIME FROM THE REGIONAL CYBER CRIME UNIT

**Northamptonshire `Dark Overload' hacker jailed for 5 years in US.**
A British hacker, Nathan Wyatt, involved Dark Overload hacking group has was caught after a telephone number used for demanding a ransom off cyber victims linked back to him. Though this is not the first run in with the police, in 2017 he was arrested on suspicion of hacking the iCloud of Pippa Middleton but was released with no further action taken.
https://bbc.in/3hTJQ76

**The First Documented Death caused by a Cyber Attack**
A Ransomware attack on the University Hospital Düsseldor has been linked to the death of a German woman. The attack affected 30 servers, crashing systems and forcing the Hospital to turn away patients. The victim suffered a life threatening condition but was sent to a hospital over 20 miles away and died as a result of the delay.
https://nyti.ms/306GmYZ
https://bit.ly/3kOI7lH

**Funding Boost to Help Healthcare Suppliers Improve Cyber Security**
https://bit.ly/3cqe1C3

**Webinar Event Opportunity: How cyber-safe are our public services?**
https://bit.ly/32WnspF

**Shopify breach: Help Center Employees are a Unique Breed of Insider Threat**
https://bit.ly/3cEncyZ

## TECH TALK

**Weekly Threat Report 18th September 2020**
NCSC warns UK academia of rise in number of cyber attacks
Remote workers access company data on personal devices
Vulnerabilities discovered across multiple travel company websites
https://bit.ly/360ifz7

**Chinese Antivirus Firm Was Part of APT41 `Supply Chain' Attack**
https://bit.ly/33ZIenL

**Multiple vulnerabilities disclosed in Philips, Advantech, and Wibu-Systems ICS products**
https://us-cert.cisa.gov/ics/advisories

**Vulnerability Disclosure Toolkit**
Making it easier for you to create a vulnerability disclosure process
https://bit.ly/2RVtvV3

# EVENTS & ENGAGEMENTS

RCCU
West Midlands | Regional Cyber Crime Unit
Got a question about cyber security?
Ask us on our live Q&A
sli.do
10:00 am - Wednesdays
If your received an email which you're not quite sure about, forward it to the Suspicious Email Reporting Service (SERS)
report@phishing.gov.uk

https://app.sli.do/event/jvodjdcu/

THE CYBER RESILIENCE CENTRE FOR THE WEST MIDLANDS

**CORE MEMBER - FREE**

**Includes:**
NCSC Guidance - How organisations can protect themselves in cyberspace, including the 10 steps to cyber security from the Government NCSC division.

**NCSCs Exercise In A Box** – a tool to give your organisation a 'dummy' run of a cyber attack. Similar to testing your fire drill. Tailored for different sized organisations.

**NCSC Board Toolkit** - Resources designed to encourage essential cyber security discussions between the Board and their technical experts.

E-news – regular digestible updates relevant to West Midlands organisations about cyber resilience

https://www.wmcrc.co.uk/

Our lives are relying on technology more every day. Join us each Friday for your bitesize cybersecurity podcast. In this increasingly technical world we deliver non-technical cyber news, and identify the current threats we're facing.

https://cyberthreatweekly.buzzsprout.com/

Listen on Google Podcasts

Listen on Spotify

Listen on Apple Podcasts

**APPEAL:** *PLEASE GET IN TOUCH FOR FREE CYBER AWARENESS INPUTS FOR YOUR OWN BUSINESS, ORGANISATION OR GROUPS.*