

# CYBER CRIME SENTINEL

ISSUE 12, 14TH AUGUST 2020

[WMCYBER@WEST-MIDLANDS.PNN.POLICE.UK](mailto:WMCYBER@WEST-MIDLANDS.PNN.POLICE.UK)

[WWW.WMCYBER.ORG](http://WWW.WMCYBER.ORG)



IN THE NEWS

TOP CYBER HEADLINES

THE LATEST NEWS ON CYBERCRIME FROM THE REGIONAL CYBER CRIME UNIT

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 WMRCU has become aware of reports of SIM swapping scams taking place within the West Midlands. SIM swapping (also known as 'SIM splitting') emerged several years ago but is on the increase as mobile phone numbers become more widely used as part of security checks. The scam sees attackers access victims' texts, calls and other sensitive information, including security codes used as part of two-factor authentication (2FA).

To be successful, attackers first need personal information, gleaned through various forms of phishing, purchasing victims' details from organised crime networks, or by conducting open source research. Social media sites can also contain sufficient information for attackers, including important dates, names, and hobbies that can be easily obtained through profile information or user posts.

Next, the attacker contacts the victim's mobile phone provider, answers basic security questions and convinces the provider to transfer the phone number to a new SIM. The attacker (who has the new SIM) then has access, while the genuine account owner is blocked.

The attacker may then contact the victim's bank, posing as the victim and claiming to have forgotten a PIN number or other details. The bank will usually send a text message containing a new activation code, allowing the attacker to take funds directly from the bank account.

Most victims will not discover they have been compromised until they are unable to make a call or send a text message. According to a 2019 Telegraph [article](#), bank customers have lost £9.1million in 'SIM swapping' scams over the last five years. UK banks are aware of SIM swapping and have taken steps to improve security, but there are a number of ways to protect yourself including setting up two factor authentication, establishing secure passwords and being very conscious about what information your putting in the public domain.

For mitigation advice, Action Fraud's, the UK's National Fraud and Cyber Crime Reporting Centre, has previously issued SIM swap fraud warnings and advice on their website - <https://www.actionfraud.police.uk/alert/fraudsters-are-emptying-bank-accounts-by-diverting-calls-and-text-messages>

### Please also follow the below advice:

NCSC's 2FA guidance for individuals - <https://www.ncsc.gov.uk/guidance/setting-two-factor-authentication-2fa>  
NCSC's Cyber Aware - <https://www.ncsc.gov.uk/cyberaware/home>

[Camera giant Canon hit by Maze ransomware attack](#)

[Is cyber insurance right for you?](#)

[Security training body Sans Institute hit by data breach](#)

[NHS hit by thousands of malicious emails at height of pandemic](#)

[164 Instagram users report losing over £350,000 to investment scams](#)

[UN Reports Sharp Increase in Cybercrime During Pandemic](#)

[Hacking Medical Devices to Hijack Secure Facilities](#)

[Under Half of Teachers Think Schools Have "Done Enough" to Tackle Cybersecurity Issues](#)

[Traveler Forced into Administration After Ransomware Attack](#)

[Have I Been Pwned to release code base to the open source community](#)

[Ransomware Threatens Production of 300 Ventilators Per Day](#)

[The Weaponization of Zero-day Exploits Becoming a New Favourite of Attackers](#)

[Ransomware: These warning signs could mean you are already under attack](#)

[Google Awards \\$10,000 for Remote Code Execution Vulnerability in Chrome](#)

[TikTok reportedly violated Google's data collection policies by tracking the individual identifiers of Android users' smartphones](#)

[Israel says it thwarted foreign cyber attack on defence industry](#)

## TECH TALK

### NCSC Weekly Threat Report Topics

- Hundreds targeted by TV License scam
- Surge in online viewing figures
- Punishing users for cyber security mishaps increases anxiety and reduces productivity
- British Dental Association reveals cyber attack on network
- US warns of attacks on Critical National Infrastructure

<https://www.ncsc.gov.uk/report/weekly-threat-report-7th-august-2020>

Over 30 Vulnerabilities Discovered Across 20 CMS Products

[https://www.securityweek.com/over-30-vulnerabilities-discovered-across-20-cms-products?&web\\_view=true](https://www.securityweek.com/over-30-vulnerabilities-discovered-across-20-cms-products?&web_view=true)

Microsoft Patch Tuesday, August 2020 Edition

<https://krebsonsecurity.com/2020/08/microsoft-patch-tuesday-august-2020-edition/>

Critical Intel Flaw Afflicts Several Motherboards, Server Systems, Compute Modules

<https://threatpost.com/critical-intel-flaw-motherboards-server-compute-modules/158270/>

Critical Adobe Acrobat and Reader Bugs Allow RCE

<https://threatpost.com/critical-adobe-acrobat-reader-bugs-rce/158261/>

# EVENTS & ENGAGEMENTS



**Got a question about cyber security?**

Ask us on our live Q&A

**slido**

10:00 am - Wednesdays

If you received an email which you're not quite sure about, forward it to the Suspicious Email Reporting Service (SERS)

[report@phishing.gov.uk](mailto: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.

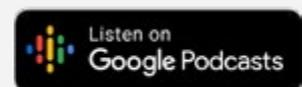
E-news – regular digestible updates relevant to West Midlands organisations about cyber resilience

<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/>



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