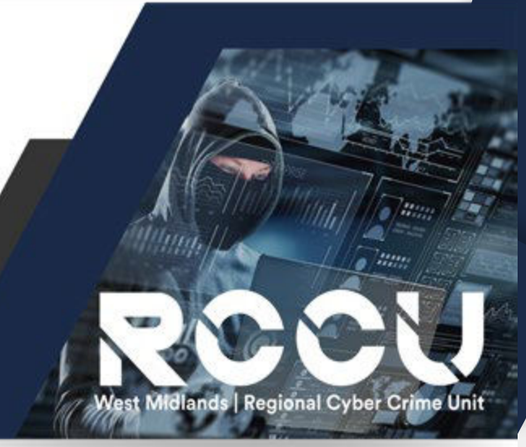
CYBER CRIME SENTINEL

ISSUE 19 02-Oct-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

Stay Safe When Working from Home

With the uncertainty of the COVID pandemic continuously looming, working from home has become the new norm and may continue to be into the foreseeable future. In a recent survey carried out by Marsh Commercials, 38% of employees claimed to have not received information about the security risks of working at home from their employer. Working without the systems and security implements that workplaces provide, like secure networks and firewalls, we open ourselves and our data up to criminals and scammers.

Protecting Data and Devices

- The first step to creating a safe home-work environment is to be aware of the risks, thus **educating yourself and others** of the cyber risks that may arise when with working from home.
- **Stay up to date with software updates and patches.** As tempting as it might be to postpone updates, especially when you are busy, don't wait.
- **Secure you home network.** Making your network more secure can be as easy as changing you route password. If your router is breached, attackers can gain access to your devices and the information you send via your router. Default or weak passwords may be a vulnerability.
- **Take advantage of VPN's (Virtual Private Networks).** VPN's can secure your network and protect you data. VPN's are especially important if you are working from a personal device or using public Wi-Fi. For more information on VPN's go to: https://www.ncsc.gov.uk/collection/mobile-device-guidance/virtual-private-networks
- **Use antivirus software.** Antivirus software is vital to computer safety whether you use your laptop for personal or work reason, take advantage of the many free antivirus software available online.
- **Be wary of phishing emails**. Phishing emails take many forms so it is important to be aware that even innocent seeming emails or emails that are have been sent by an individual within your organisation could potentially be malicious. If in doubt, reach out to the individual directly before following any links or forwarding the email on.
- **Lock your device.** If you work in a public space or live with individuals who you cannot share work data with then it is important to password-lock your device.

IN THE NEWS — TOP CYBER HEADLINES

THE LATEST NEWS ON CYBERCRIME FROM THE REGIONAL CYBER CRIME UNIT

Top General lifts lid on Britain's Cyber-Attack Capability
According to General Sir Patrick Sanders (head of Strategic Command), the UK has developed an offensive cyber capacity that can "degrade, disrupt and even destroy critical capabilities and infrastructure of those who would do us harm, ranging from strategic to tactical targets." - **https://bit.ly/2GfF1s5**

Facebook Grant Scams
Social media giant Facebook is offering $100 million in grants to businesses that have been affected by the COVID-19 pandemic. Unfortunately, scammers and cybercriminals where quick to exploit individuals hoping for a grant by pushing fake URLS and phishing links - **https://bit.ly/33gTSLz**

Who's Behind Monday's 14-State 911 Outage?
Emergency 911 systems were down for more than an hour on Monday in towns and cities across 14 U.S. states. The outages led many news outlets to speculate the problem was related to Microsoft's Azure web services platform, which also was struggling with a widespread outage at the time. However, multiple sources tell KrebsOnSecurity the 911 issues stemmed from some kind of technical snafu involving Intrado and Lumen, two companies that together handle 911 calls for a broad swath of the United States. **https://bit.ly/30n5cUD**

Hackers Arrested in Poland in Nation-Wide Action against Cybercrime - https://bit.ly/2S9bl2p

Louis Vuitton fixes data leak and account takeover vulnerability - https://bit.ly/36lv3jE

Cyber-attacks against energy sector industrial control systems are on the rise -https://bit.ly/3jnxDti

TECH TALK

NCSC Weekly Threat Alert
Gamers urged to secure online accounts
Firm caught offside in Ransomware attack
https://bit.ly/30iI1Lm

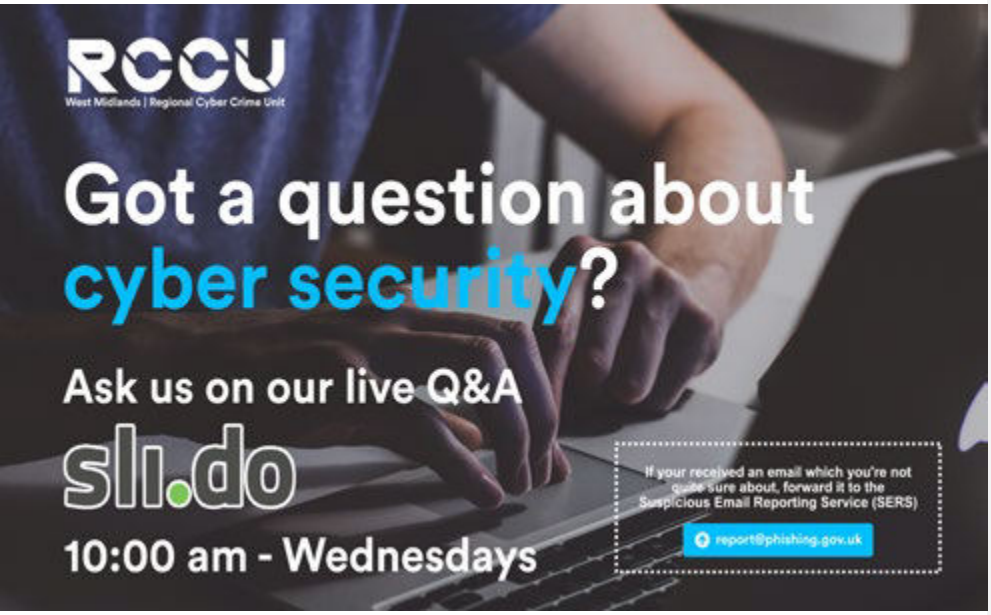
Enterprise patching in a post-Flash world - https://bit.ly/34ivV6a

NCSC's new cyber security training for staff now available - https://bit.ly/2HCMp12

New Phishing Message Harvest Credentials with GDPR Lure - https://bit.ly/2ScBIV8

Alert: UK organisations should patch Netlogon vulnerability
Microsoft Windows `Netlogon' vulnerability, also known as Zerologon, is being exploited and organisations should install necessary updates as soon as possible. A vulnerability in the Netlogon Remote Protocol permits an attacker with network access to a Domain Controller to imitate any domain user and change their account password, this can lead to huge data compromise. **https://bit.ly/2SaOpQ2**

EVENTS & ENGAGEMENTS



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.*