STAFFORDSHIRE POLICE

Cyber Champion Tips – March 2021

NCSC Alert for Organisations - Microsoft Exchange Server Vulnerabilities

If you are running an out-of-support version of Exchange Server you should update to a supported version without delay. 'On 2 March 2021 Microsoft made public that sophisticated actors had attacked a number of Exchange servers. In response to this they released multiple security updates for affected servers. This does not affect Exchange Online. The updates were released ahead of the monthly update cycle because four of the seven vulnerabilities have been used in ongoing attacks. The security updates fix the vulnerabilities exploited in the attack.

A wide variety of threat actors are using automated tools to scan for Exchange servers where updates are not installed. The actors then install malicious software to servers identified as vulnerable. On 11 March it was reported that ransomware actors have also exploited these vulnerabilities, or made use of the installed malicious software, to install ransomware on a network.

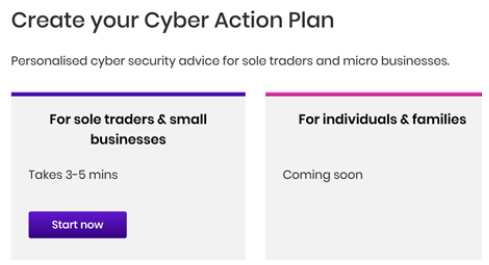
Affected versions:

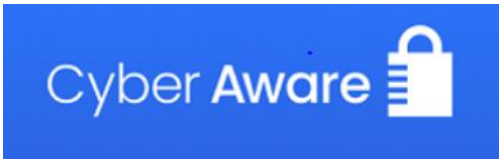
The vulnerabilities affect Microsoft Exchange Server. The affected versions are:

- 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. Organisations running an out-of-support version of Exchange Server should update to a supported version without delay. Exchange Online (as part of Microsoft 365) is not affected' *National Cyber Security Centre (NCSC)*. Full alert and NCSC advice on actions to take found here: https://www.ncsc.gov.uk/news/advice-following-microsoft-vulnerabilities-exploitation

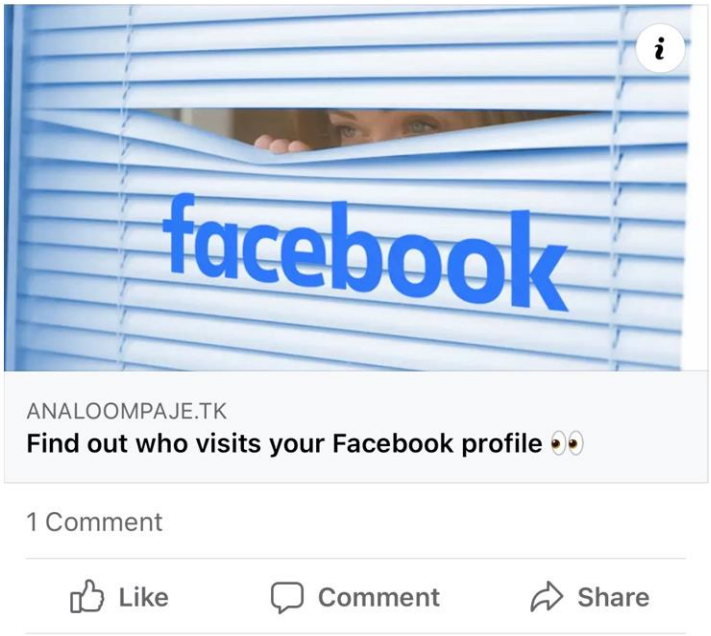
NCSC Sole Traders and Micro Businesses Support - Newly launched Cyber Action Plan to help small businesses - Over the last twelve months, many businesses have resorted to more opportunities for the usage of digital and online platforms, but it's important to ensure cyber security considerations be an integral part of this shift when adopting new technology and online ways of working. As part of the Cyber Aware campaign, a self-assessment tool for sole traders and micro businesses has now been developed to help smaller businesses with their cyber security. The self-assessment tool is an easy to navigate framework which helps to identify areas of risk and areas for improvement, it gives a personalised list of actions which can help your cyber security, so why not give it a try, access can be gained visiting here: https://www.ncsc.gov.uk/news/cyber-aware-action-plan





Social Media Continuing Threats and Advice - #SecureYourAccounts

Action Fraud received '15,214 reports of email and social media hacking between February 2020 and February 2021 – 88 per cent of which were from individuals who had their personal accounts compromised by criminals' *Action Fraud*. Social media accounts can be compromised by clicking on links forwarded from contacts such as photos, videos and posts in which you may have been tagged, such as this one which is currently circulating on Facebook:



If you think your account has been compromised, it is important to act fast:

- **change passwords** straight away using three random words
- Add **two factor authentication**
- **Update** apps and devices
- review **privacy settings**

Find out more tips on keeping safe with Action Fraud and the NCSC here: https://www.actionfraud.police.uk/news/city-of-london-police-warns-public-to-keep-online-accounts-safe-from-hackers

Privacy Settings - It is always a good idea to keep regular reviews of privacy settings, especially after device and software updates to ensure settings have not reverted to default. Further guidance for safer usage of social media accounts can be found here: https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

March NCSC threat reports here:

5th March 2021 - https://www.ncsc.gov.uk/report/weekly-threat-report-5th-march-2021

- Urgent patches released following MS Exchange vulnerabilities exploitation
- Leaky AWS S3 bucket leaves 114,000 files exposed

12th March 2021 - https://www.ncsc.gov.uk/report/weekly-threat-report-12th-march-2021

- Report finds vulnerability reporting is on the rise
- Premier League club leaks supporter details

19th March 2021 - https://www.ncsc.gov.uk/report/weekly-threat-report-19th-march-2021

- Client data stolen in attack on courier company
- Trading standards issues warning over popular telephone scams
- F5 BIG-IP Vulnerabilities

West Midlands Regional Cyber Crime Unit (WMRCCU):

The WMRCCU website has a host of information to help boost your cyber awareness and help keep you informed, take a visit where you will find tips, information, advice, podcasts and subscription to the Cyber Crime Sentinel, check it out here: https://www.wmcyber.org/

Reporting

Report cyber-crime and fraud to Action Fraud: actionfraud.police.uk

Businesses suffering a live cyber-attack can call: 0300 123 2040

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Received a phishing email?

Forward suspicious emails to: report@phishing.gov.uk

Received a suspicious text message?

You can report fraudulent texts by forwarding to: **7726**

If a scam text claims to be from your bank, you should also report it to them

Further advice can be found by visiting:

cyberaware.gov.uk

ncsc.gov.uk

actionfraud.police.uk

takefive-stopfraud.org.uk

ukfinance.org.uk

staffordshire.police.uk

TAKE FIVE TO STOP FRAUD