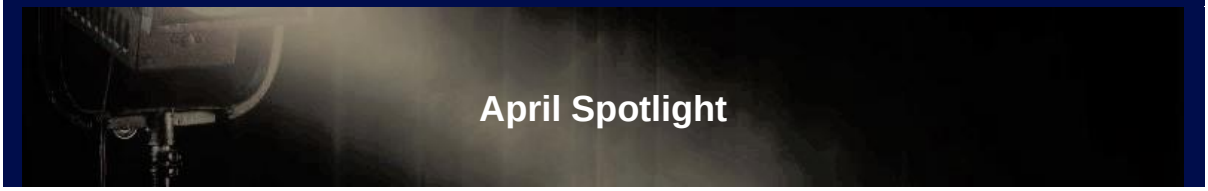
National Cyber Security Centre

Small Organisations Newsletter

Coffee Break Cyber

Edition 2 April 2021



Urgent updates and actions following Exchange server vulnerabilities

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.

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 pat of Microsoft 365) is **not** affected.

Reporting a compromise

Threat Reports

The Cyber Breaches Survey 2021

Trading standards issues warning over popular telephone scams

Premier League Club leaks supporter details

NCSC News

MyNCSC

Affected UK organisations should report any suspected compromises to the **NCSC via the website.**

Ransomware

What is ransomware?

Ransomware is a type of malware that prevents you from accessing your computer (or the data that is stored on it). The computer itself may become locked, or the data on it might be stolen, deleted or encrypted. Normally you're then asked to make a payment by the attackers in order to unlock your computer or release your data.

What's new?

The good news is that at the NCSC, we have just updated our ransomware guidance to ensure it remains current with the types of attacks we are seeing and how best to defend against them.

In the review, we have added a new element to the guidance by emphasising offline backups as a defence against ransomware. NCSC have seen a number of ransomware incidents lately where the victims had backed up their essential data (which is great), but all the backups were online at the time of the incident (not so great). It meant the backups were also encrypted and ransomed together with the rest of the victim's data. Ultimately meaning that they had no clean backup from which to restore from.

Should I pay the ransom?

We often get asked, "should I pay the ransom?" – The NCSC supports the National Crime Agency (NCA) recommendations who generally advise not to pay the ransom, as there is no guarantee that you will get access to your device (or data).

Secure Home Learning

Cyber Action Plan

Future Look

Practical help for SME's in the Legal Sector
21st April 2021 - 12.45 – 16.00

The National Cyber Security Centre (NCSC) are hosting an afternoon for SME's in the legal sector covering the following topics:
Understanding the environment – Hear from NCSC and SRA about current cyber threats to your business.

Securing the landscape – Learn how to protect yourself from cyber threats and hear from a partner of a law firm about how they manage risk.

Dealing with incidents
- Hear from the victim of a ransomware attack

Helping you and your clients be more cyber secure – Learn more about NCSC's Cyber aware campaign for small

You are also encouraged to report cyber crime and fraud to Action Fraud

Help! I am experiencing a ransomware attack now…

If your organisation is already infected, NCSC have produced a list of actions you should take as soon as possible.

Exercise in a Box

Exercise in a Box is an online tool which helps organisations find out how resilient they are to cyber attacks and practise their response in a safe environment.

The NCSC has recently added a number of 15minute micro exercises suitable for organisations:

Responding to a ransomware attack -
short and sharp exercise focussed on ransomware, exploring this topic using a combination of interactive activities covering the definition of ransomware, the impact, and responding to a ransomware attack.

Using Passwords
A short and sharp exercise focussed on passwords, exploring this topic using a combination of interactive activities covering the common use of passwords, how attackers find your passwords, and what you can do to limit the risk of your passwords being discovered.

businesses, easy ways to protect yourself, and ask questions to experts.

Click here to sign up

Coming Soon...Cyber Essentials Readiness Tool

Sometimes, organisations are unsure how to prepare for Cyber Essentials.

The Cyber Essentials Readiness Tool is a series of questions developed to explain the Cyber Essentials requirements and give targeted guidance on how to implement them.

This readiness tool is the step that comes before taking the Cyber Essentials self- assessment. It is the start of the journey to becoming Cyber Essentials certified.

Glossary of Terms

Ransomware - A type of malware that makes data or systems unusable under the victim makes a payment.

Identifying and reporting a suspected phishing email

A short and sharp exercise focussed on phishing, exploring this topic using a combination of interactive activities covering the definition of phishing, the impact, and identifying a phishing email.

To find out more, click here

Have your say

Ransomware can seriously disrupt or even damage a business.

The NCSC wants to hear your opinion on what services a business victim would seek from a government assured supplier service if it existed. Help us to build such a service by providing some of your time to complete the questionnaire via the button below.

Click here to take part

Encryption - A mathematical function that protects information by making it unreadable by everyone except those with the key to decode it.

Phishing Explained

Phishing is untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.

Phishing can be conducted via a text message, social media, or by phone, but the term 'phishing' is mainly used to describe attacks that arrive by email.

Next month... How to notice and protect yourself from Phishing

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown Copyright ©