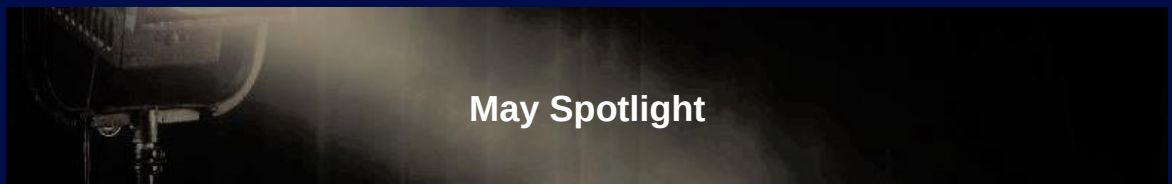
National Cyber Security Centre

Small Organisations Newsletter

Coffee Break Cyber

Edition 3 May 2021



Critical risk to unpatched Fortinet VPN devices

April 2021 update

APT actors are still actively scanning for CVE-2018-13379 and attempting to exploit it.

In addition, CISA and the FBI have evidence that APTs are actively scanning for and exploiting two other Fortinet vulnerabilities CVE-2020-12812 and CVE-2019-5591, and have published a joint CISA/FBI report.

The NCSC's advice to organisations remains to ensure the latest security updates are installed as soon as is practicable for all vulnerabilities.

Reporting a compromise

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

Seeking help following a cyber-attack – Questionnaire

Threat Reports

FluBot "package delivery" scam targeting Android devices

The Cyber Breaches Survey 2021

Spoof job offer for LinkedIn users

NCSC News

Cyber Action Plan

Advice on Pulse Connect Secure RCE Vulnerability

NCSC CEO's First Speech

Any form of cyber-attack such as phishing or ransomware can seriously disrupt or even damage a business. If you need to engage the services of a company to help you resolve a cyber attack (incident), how would you get help?

The NCSC want to look at this from your perspective and by filling in the questionnaire below you will help the NCSC form a view across varying business sizes of the things that you would currently associate with a good service when you seek help to respond to a cyber-attack and also whether you would look to undertake Cyber Exercising to help improve the cyber resilience of your company. We want to hear your opinion on what services a business 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. Thank you!

Click here to take part

Phishing

What is phishing?

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 also be in the form of mass text messages sent to users asking for sensitive information (eg bank details) or encouraging them to visit a fake website this is known as Smishing.

Or via phone calls often referred to as voice phishing or Vishing, where cybercriminals use savvy social engineering tactics to convince victims to giving up private information and access to bank accounts.

How can I spot Phishing?

Name

Is the email addressed to you by name, or does it refer to 'valued

Risk to unpatched Fortinet VPN devices

Future Look

CYBERUK ONLINE 2021

11-12 May 2021

CYBERUK conference will be fully virtual this year, meaning a wider audience than ever before can access the event.

Event updates, including joining detail, will be published *on our website* **in** the coming weeks.

For more info click here

CYBER ESSENTIALS

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

customer', or 'friend' or 'colleague'? This can be a sign that the sender does not actually know you, and that it is part of a phishing scam.

Logos & Graphics

Others will try and create official looking emails by including logos and graphics. Is the design (and quality) what you'd expect?

Sense of Urgency

Does the email contain a veiled threat that asks you to act urgently? Be suspicious of words like 'send these details within 24 hours' or 'you have been a victim of crime, click here immediately'.

Senders Details

Look at the sender's name and email address. Does it sound legitimate, or is it trying to mimic someone you know?

Bank or Personal Details

Your bank (or any other official source) should never ask you to supply personal information in an email. **If you need to check, call them directly.**

Winner

If it sounds too good to be true, it probably is. It's most unlikely that someone will offer you designer trainers for £10, or codes to access films for free.

Are there any exercises I could share with my staff?

Exercise in a Box provides exercises, based around the main cyber threats. They have just launched a 15minute micro exercise
- **Identifying and reporting a suspected phishing email**

This exercise is 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 you spotted a suspicious email or text?

If you have received an email which you're not quite sure about, forward it to the Suspicious Email Reporting Service (SERS): **report@phishing.gov.uk**

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

Breach - An incident in which data, computer systems or networks are accessed or affected in a non-authorised way.

Whaling- Highly targeted phishing attacks (masquerading as a legitimate emails) that are aimed at senior executives.

APT (Advance Persistent Threats) - A targeted cyber attack where a hacker accesses a system and remains undetected for a long time.

VPN (Virtual Private Network) - An encrypted network often created to allow secure connections for remote users, for example in an organisation with offices in multiple locations.

Suspicious text messages should be forwarded to **7726**. This free-of-charge short code enables your provider to investigate the origin of the text and take action, if found to be malicious.

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

*As of 31st March 2021 the number of reports submitted to the SERS service stand at more than **5,500,000** with the removal of more than **41,000** scams and **81,000** URLs*