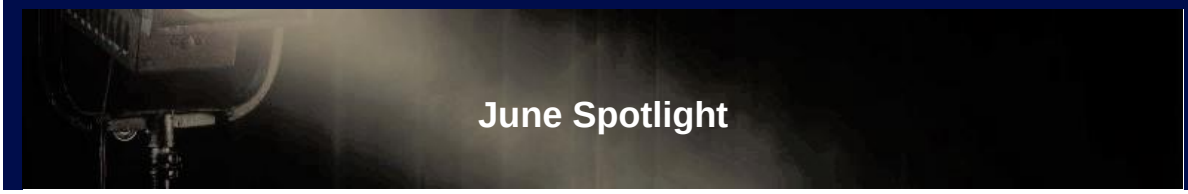
National Cyber Security Centre

Small Organisations Newsletter

Coffee Break Cyber

Edition 4 June 2021



Training for small organisations and charities now available

Most small organisations do not have an IT department, or technical staff responsible for cyber security. And with so much cyber security advice out there, it can be difficult for small organisations to know where to start.
This is where the NCSC's new training for small organisations and charities can help. It guides you through all the actions you need to take to reduce the likelihood of you becoming a victim of the most common cyber attacks.

The training demonstrates how you can improve your organisation's resilience, and covers five key areas:

1. Backing up your organisation's data correctly
2. Protecting your organisation against malware
3. Keeping the devices used by your employees secure
4. The importance of creating strong password
5. Defending your organisation against phishing

The training will put your staff in the driving seat. They will be answering questions, identifying possible issues, and making suggestions for how to prevent, and tackle common cyber security challenges.

Threat Reports

Hoax COVID-19 vaccine website taken down

The Cyber Breaches Survey 2021

Over 25,000 servers in the UK still running vulnerable Exim versions

NCSC News

Cyber Action Plan

Diversity & Inclusion Survey 2021

CYBERUK21 ONLINE video highlights

The training is primarily aimed at SMEs, charities and the voluntary sector, but can be applied to any organisation, regardless of size or sector. It's been deliberately designed for a non-technical audience (who may have little or no knowledge of cyber security), with tips that complement any existing policies and procedures.

To find out more, click here

New tool launched to organisations achieve Cyber Essentials certification

The Cyber Essentials Readiness Tool is a free, online resource that guides organisations through a series of questions related to the Cyber Essentials criteria to help prepare them for certification.
The tool asks questions about an organisation's use of hardware, software, and boundary devices such as firewalls, as well as use of passwords and protections against malware and provides clear, non-technical advice for the user. Upon completion of the tool the user receives a tailored action plan that outlines the steps they need to take to achieve Cyber Essentials certification.

This tool, developed by IASME on behalf of the NCSC – a part of GCHQ - was launched at the NCSC's flagship conference CYBERUK 2021.

Sarah Lyons, NCSC Deputy Director for Economy and Society, said:
"The Cyber Essentials Readiness Tool is a fantastic starting point for organisations who are unsure about where to start their preparation for Cyber Essentials certification. Not only does the tool highlight areas where more cyber security controls need to be put in place, it also provides guidance on how to implement them. From catering to

Cyber Essentials Readiness Tool Available

Future Look

What you are most excited about in the next 12months as

As of 30th April the number of reports received stand at more than 5,800,000 with the removal of more than 43,000 scams and 84,000 URLs.

Forward suspicious or phishing emails to:
Report@phishing.gov.uk

Glossary of Terms

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

construction, everyone should care about their businesses' online security and I'd encourage people to take advantage of the new tool."

Cyber attackers often use relatively simple methods to exploit basic vulnerabilities, which are the equivalent of a burglar checking a front door to see if it is locked. But through the Cyber Essentials scheme, businesses can learn how to defend themselves by securing internet connections and devices, controlling access to data, and understanding how to protect against malware.

Since the scheme launched in 2014, the NCSC has helped to protect over 60,000 UK businesses from the most common cyber threats. Achieving Cyber Essentials certification allows businesses to:

- reassure customers that they have put measures in place to secure their IT against cyber attacks
- attract new business with the promise they have independently verified cyber security measures in place
- have a clear picture of their cyber security level, and
- apply for some government contracts which require Cyber Essentials certification

Cyber Incident -

- A breach of the security rules for a system or service - most commonly; Attempts to gain unauthorised access to a system and/or to data.
- Unauthorised use of systems for the processing or storing of data.
- Changes to a systems firmware, software or hardware without the system owners consent.
- Malicious disruption and/or denial of service.

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Report a Cyber Incident

If you think you have been a victim of cyber crime or a cyber incident including social media account cloning, report it to Action Fraud.

Action Fraud Website

University of Portsmouth Cybercrime Awareness Clinic

The University of Portsmouth Cybercrime Awareness Clinic are currently recruiting interviewees for their study into SME cyber awareness, which is funded by the National Cyber Security Centre (NCSC). To participate you must either be a sole trader or a manager/owner of a micro, small or medium business. Unfortunately, employees/owners of cybersecurity businesses are excluded as their knowledge of cybersecurity may interfere with the results. Eligible participants will be invited to take part in 1-hour interviews conducted in a mode most convenient to them, usually via zoom or other online platforms.
Your participation will help shape NCSC cybersecurity policy and guidance in relation to small-medium enterprises (SMEs). It will also offer you the opportunity to gain some knowledge of the free NCSC resources available and gain relevant advice from the Clinic research team. If you're interested in participating, please contact the clinic director, Dr Vasileios Karagiannopoulos, via email (vk@port.ac.uk). Thank you.