Thames Valley Police.

Cyber Protect - COVID-19 specific Newsletter

April 2020

Hello and welcome to this COVID-19 Newsletter aimed at bringing the key National Cyber Protect messages to SME's / Charities across the Thames Valley area.

As you all well know the COVID-19 situation has been forefront in everyone's daily life both at home and at work.

In this edition, we will be covering the current guidance and information being provided by our colleagues at the **National Cyber Security Centre** (NCSC)

At the time this item was being written, we are looking to focus our National Cyber Protect Network toward four main threat areas, namely, **Ransomware, Phishing, Remote / Home working and online Fraud.**

Notwithstanding the links we normally provided at the end of our newsletter, the below should be seen at your first point of call for the above areas.

The National Cyber Sexurity Centre(NCSC) has published a range advice and guidance for business:

https://www.ncsc.gov.uk/blog-post/updating-malware-ransomware-guidance

The NCSC have tried to make things easier by providing a single piece of guidance, with all the most up-to-date advice in one place.

https://www.ncsc.gov.uk/news/home-working-increases-in-response-to-covid-19

Working from home is new for a lot of organisations and employees. Even if home working has been supported for some time, there may suddenly be more people working from home than usual, some of whom may not have done it before.

Mobile devices come in many different shapes and sizes: smartphones, tablets, laptops and even desktop PCs. When thinking about how to secure these devices, a number of questions come to mind, such as:

- Which devices should I buy?
- How should I configure these devices?
- What security software should I load onto them?

The NCSC has answered these questions, and more. These pages form a comprehensive guide to the protection of mobile devices.

https://www.ncsc.gov.uk/collection/mobile-device-guidance

Experts from the National Cyber Security Centre have revealed a range of attacks being perpetrated online as cyber criminals seek to exploit COVID-19.

https://www.ncsc.gov.uk/news/cyber-experts-step-criminals-exploit-coronavirus

Other NCSC guidance and information

Advisory: COVID-19 exploited by malicious cyber actors: Practical advice for individuals and organisations on how to deal with COVID-19 related malicious cyber activity.

https://www.ncsc.gov.uk/news/covid-19-exploited-by-cyber-actors-advisory

Online Staff Training guidance and support provided by the NCSC

https://www.ncsc.gov.uk/blog-post/ncsc-cyber-security-training-for-staff-now-available

https://www.ncsc.gov.uk/information/exercise-in-a-box

https://www.ncsc.gov.uk/collection/board-toolkit

We have provided at the end of this Newsletter a series of Infographics.

The NCSC provide a weekly resume of the current key issues that the NCSC wish to make the wider population and business communities aware of: **NCSC Keep-up-to-date/threat-reports**

Action Fraud: Guidance and information awareness

As of the 9th of April, Action Fraud have reported "A total of £1,820,731 has been reported lost by 641 victims of coronavirus-related scams. We have received 2,643 reports of coronavirus-related phishing emails.

Criminals continue to exploit the coronavirus pandemic to defraud innocent members of the public. Currently, coronavirus-related frauds make up 3-5% of all fraud reports we receive.

To keep this number as low as possible, we want people to be aware of the very simple steps they can take to protect themselves from handing over their money, or personal details, to criminals.

Please continue to visit this page for information on the latest scams we are seeing and advice on how to protect yourself"

https://www.actionfraud.police.uk/covid19

What scams are Action Fraud seeing?

The majority of reports are related to online shopping scams where people have ordered protective face masks, hand sanitiser, and other products, which have never arrived.

Other frauds being reported include ticket fraud, romance fraud, charity fraud and lender loan fraud.

Phishing emails: We have also received reports of coronavirus-themed phishing emails. These attempt to trick people into opening malicious attachments which could lead to fraudsters stealing people's personal information, email logins and passwords, and banking details"

Sign up for **Action Fraud Alerts** or visit their News page: **https://www.actionfraud.police.uk/news**

CiSP (Cyber Security Information Sharing Partnership) is a joint industry and government initiative set up to exchange cyber threat information in real time, in a secure, confidential and dynamic environment, increasing situational awareness and reducing the impact on UK business.

Benefits of the CiSP
Engagement with industry and government counterparts in a secure environment
Early warning of cyber threats
Ability to learn from experiences, mistakes, successes of other users and seek advice Access to free network monitoring reports tailored to your organisations' requirements.

How?
Organisations: Sponsors must be a government department, existing CiSP member or a regional Cyber PROTECT police officer or industry champion.
Individuals: Their Organisation must already have a CiSP account. **NCSC CISP**

If you wish to be provided with more specific information or guidance, please email**: cyber.protect@thamesvalley.pnn.police.uk**

Regional information
If your business is worried about the effects of cyber-crime, please see this link to our Regional Organised Crime Unit (SEROCU) external facing site, where additional information is provided. **https://serocu.police.uk/cyber-protect** (Our apologies, but external presentations are now suspended for the duration of the current COVID-19 situation.

Vulnerability Assessments
SEROCU are offering public sector, small & medium-sized enterprises & charities the opportunity for a free vulnerability assessment / IT health check in the Thames Valley Police area. Search VULNERABILITY ASSESSMENTS **https://serocu.police.uk/cyber-protect/**

You can also follow us on Twitter: @TVPCyber_Fraud

Report Internet & Fraud to Action Fraud via the 24/7 online reporting tool for business and charities **https://www.actionfraud.police.uk/**

Content correct as of the 15th April 2020