Thames Valley Police: Cyber Protect – Newsletter

(Find us on Twitter: @TVPCyber_Fraud)

For: September-October 2021

Hello and welcome to this our latest Newsletter for 2021, aimed at bringing the key National Cyber Protect guidance to the Public, Private and Charity sectors across the Thames Valley area. As always the key source for advice, guidance is the UK's National Cyber Security Centre (NCSC)

The COVID-19 situation continues to be forefront in everyone's daily life both at home and at work despite recent changes and as we have previously covered a wide range of guidance and support in the distributed content since the April 2020 Newsletter, it is our intention to continue in this vein as required during the Pandemic.

As previously noted in our last newsletter, the Thames Valley Police Cyber Crime Unit, although still located and delivering its enforcement responsibilities in the TVP Force area, now comes under the line management of the South East Regional Crime Unit (SEROCU) that will enable closer collaboration with our colleagues in South East Region. To see the SEROCU Cyber Protect web page: Cyber Security for Organisations – South East Regional Organised Crime Unit (serocu.police.uk)

In this latest edition:

NCSC updated 'Cyber Security Tool kit For Boards'

"We're really pleased to launch our new Cyber Security Toolkit for Boards Hub. We hope the hub will make it easier for you to find and use the toolkit resources.

Our customers told us it would be helpful to focus on certain cyber security topics - tailored specifically for board members - using different media, adding the following to the toolkit:

- A new Audio & Video tab, where we will collate all our multimedia content. This includes a new, fascinating interview with Jacqueline de Rojas, President of techUK and President of Digital Leaders, on how to get cyber security on the board's agenda.
- A new series of 'spotlight topics', the first of which addresses Ransomware: What board members should know and what they should be asking their technical experts.
- PowerPoint decks that you can download and use within your own organisation. The presentations explain what the Board toolkit is, and how to use it.

On our Resources tab – you can still find:

- Board toolkit: questions for the Board to ask. A brief summary of each module in the toolkit with questions for the Boards to ask about cyber security.
- A pdf of the full Cyber Security Toolkit for Boards guidance.

Do please give due consideration to sharing this information with your respective 'Board of Directors / Chief Executives" and on this point we would really recommend that they all listen to the audio clip and watch at least the second vide provided in this link. Especially if those board members have little or no knowledge about the integral importance that cyber security must play in any organisations business plans, resilience and operating processes" Audio & Video - NCSC.GOV.UK

If you have any questions regarding this, please make direct contact with the NCSC: let us know

NCSC: Configuring Office 365's 'Report Phishing' add-in for Outlook to use SERS (Suspicious Email Reporting Service)

This guidance describes how to configure the Office 365 'Report Phishing' add-in for Outlook, so that users can report suspicious emails to the NCSC's Suspicious Email Reporting Service (SERS).

This guidance is aimed at system owners responsible for administering Office 365 within organisations. Once configured, users can quickly report emails that they suspect to be phishing attempts, using a single mouse-click.

Note: The Report Phishing add-in is only available to corporate or business versions of O365. The add-in is not currently available to Office 365 users with home or student licences.

Configure O365's Phishing report add-in for SERS - NCSC.GOV.UK

Public and Businesses can now report Scam websites direct to the NCSC

A new reporting tool is now available for the public who come across scam websites

The National Cyber Security Centre's new website reporting tool allows people to send them a link from websites, which they think are trying to scam the public, regardless of how they got to the site.

The NCSC – which is a part of GCHQ – then analyses the site, and if found to be malicious a notice may be issued to the hosting provider for the site to be removed, preventing members of the public falling victim in future.

The NCSC has previously highlighted the problem of scam websites, including fake news pages where celebrities such as Sir Richard Branson appear to be endorsing investment schemes. Links to these pages were subsequently removed by the NCSC. Public can now report scam websites direct to the NCSC - NCSC.GOV.UK

Reminders

NCSC Toolkit
The National Cyber Security Centre (NCSC) has developed a digital tool to help businesses and individuals improve their cyber security. As part of the cross-government Cyber Aware campaign, the NCSC has launched the free use of Cyber Action Plan.

There are two versions of the tool: one for businesses and the other for individuals / families.
By answering a few questions on topics like passwords and two-factor authentication, users will receive a free personalised list of actions that will help them improve their cyber security.

The survey takes 3-5 minutes to complete and can be found here.

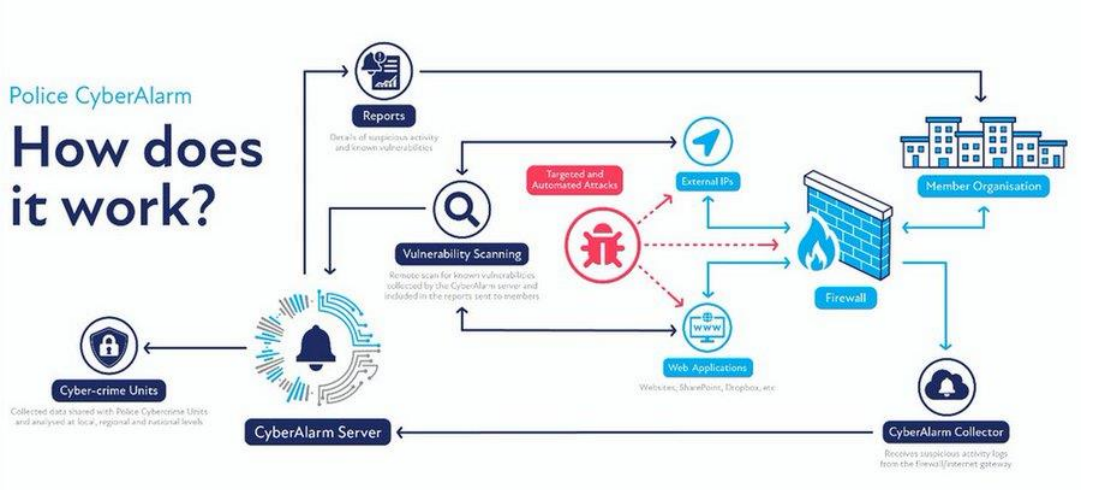
South East Regional Cyber Resilience Centre (Source material from SECRC)

"The intention of The Cyber Resilience Centre for the South East is to encourage cyber resilience by raising issues and disseminating information on the experiences and initiatives of others.
Articles on the website cannot by their nature be comprehensive and may not reflect most recent legislation, practice, or application to your circumstances.
The Cyber Resilience Centre for the South East provides affordable services and Trusted Partners if you need specific support. For specific questions, please Contact Us | Cyber Resilience Centre for the South East (secrc.co.uk)

As a trusted resource, they are also a straightforward place to find IASME approved Cyber Essentials and Cyber Essentials + Certifiers in the South East."
The full website is available via https://www.secrc.co.uk

Police CyberAlarm.
Police CyberAlarm helps business understand and monitor malicious cyber activity.

"Every business in the South East can now access a free digital tool designed to help understand and monitor incoming threats from hackers. Police CyberAlarm, was introduced to a number of organisations across the country who took part in a pilot roll out. Following its success, the government-funded initiative is now being rolled out across the country"



To read the full press release (As below) to see an online vide on how the process works and to know more please visit this link posted on the South East Cyber Resilience Centre web site.

'Cyber CCTV' on offer to all businesses in the South East (secrc.co.uk)

The Police CyberAlarm site is accessible here: https://cyberalarm.police.uk where you will find more detailed information and guides as to how to apply or ask questions direct to this service provider: support@cyberalarm.police.uk

Other ongoing topics
Nationally, we are continuing to see, because of Coronavirus increasing Cyber threats against a variety of targets, including Critical National Infrastructure and the health sector.

The existing wider, high volume of sophisticated ransomware attacks, which can cripple an organisation and put it out of business, is also a growing threat.

The current "business as usual" level of attacks may have more impact in this period as businesses themselves, their IT companies and wider cyber security industry may have less capacity to respond, through sickness and self-isolation.

*** The following are high-risk areas:**

1 Ransomware
2 Phishing / Business Email Compromise
3 Home working
4 Wider online fraud

Previously, the NCSC has also published guidance for organisations on increasing remote working and shared top tips for individuals working from home; small businesses have been supported with advice on how to move their physical operations online, and secure video conferencing guidance has been produced for organisations and individuals.

National Cyber Security Centre newsletter

The National Cyber Security Centre now publish specifically for Small to Medium Enterprises a monthly newsletter, which can be signed up to here: NCSC Small Organisations Newsletter Registration Tickets | Eventbrite

Locally delivered online Cyber Protect Presentations –Organisations in Thames Valley

We TVP Cyber Protect will continue in 2021 to offer of the delivery of our 90min (Includes time for Q&A) "high level" overview of Cyber Protect guidance for Small Businesses.

Being pragmatic, COVID-19 and its associated work place and societal restrictions will be with us for some time to come, which will prevent our traditional in-person sessions. Therefore and locally for the TVP area, we have developed a 1hr online presentation (An adaptation of the previously delivered face to face session) that is for all staff, which looks at the current Cyber and Fraud related threats and trends.

Therefore and for the foreseeable future, this online presentation, will be delivered via **Microsoft Teams or Zoom** as a **webinar which** we have already delivered similar sessions to that outlined above and have existing plans to deliver to business representative organisations.

However should you prefer you can look out for National Cyber Security Centre (NCSC) or other Police lead Cyber / Fraud online webinar events, which we promote via **@TVPCyber_Fraud** If your organisation received session from April 2020 onward, you will not need to revisit the above, unless it is critical to your organisation.

If you would like this TVP delivered online session please come to us via our email address of cyber.protect@thamesvalley.police.uk for the attention of M''listing your organisations purpose for the event, expected number of participants and when / timings.

Our expectation would be for your organisation to set up and run said event, providing us the secure connection login details. If you are new to online meetings, may we suggest you review and follow NCSC guidance: https://www.ncsc.gov.uk/guidance/video-conferencing-services-using-them-securely

The can be delivered subject to availability on a Tuesday to Thursday, between 0900-1230 or 1330-1530 (This offering will be kept on a rolling end of month review so as to be agile to COVID-19 restriction changes)

Locally delivered in-person Cyber Protect Presentations –Organisations in Thames Valley

Subject to ongoing COVID best practice; these can now be facilitated if required, to discuss arranging such please email cyber.potect@thamesvalley.police.uk for the attention of 'M'

Reporting of Internet & Fraud crime to Action Fraud
Via the 24/7 online reporting tool for business and charities https://www.actionfraud.police.uk/
Information on the 24/7 live reporting tool for businesses: https://www.actionfraud.police.uk/campaign/24-7-live-cyber-reporting-for-businesses

Please note that not all reported incidents will lead to an investigation. However, the reporting of such ensures to build a more accurate picture of where and how cyber and fraud crime is being committed, which helps build intelligence as well as to assist national teams to devise appropriate guidance and mitigation. More about the reporting process here:
https://www.actionfraud.police.uk/reporting-fraud-and-cyber-crime

Keep up to date with NCSC reports and advisories
https://www.ncsc.gov.uk/section/keep-up-to-date/reports-advisories
https://www.ncsc.gov.uk/section/keep-up-to-date/ncsc-news

If your business is worried about the effects of cyber-crime, please see this link to our colleagues in the Regional Organised Crime Unit (SEROCU) external facing site. Additional information:
https://serocu.police.uk/cyber-protect

Best wishes, TVP Cyber Protect.
Twitter: https://twitter.com/TVPCyber_Fraud

Email: cyber.protect@thamesvalley.police.uk