Thames Valley Police

Cyber Protect – Newsletter (Twitter: @TVPCyber_Fraud)

For: November-December 2020
Hello and welcome to this our latest Newsletter and last for 2020, aimed at bringing the key National Cyber Protect guidance to the Public, Private and Charity sectors across the Thames Valley area.

The COVID-19 situation continues to be forefront in everyone's daily life both at home and at work and we covered a wide range of guidance and support in the previously distributed May 2020 Newsletter and we have provided additional guidance as and when it has been released, throughout the emerging year.

In this edition: We will be covering, Business Email Compromise a refreshed National Cyber Security Centre (NCSC) Small Business Guide, the joint British Retail Consortium and National Cyber Security Centre Retail Tool Kit refresh and the emerging Police lead South East Cyber Resilience Centre.

In addition: Our Forces continuing offer, to deliver a one hour webinar for "Staff Awareness" of Current Cyber threats, risk, harm, their mitigation guidance, with signposting to additional support and advice.

The continuing offer to provide free Vulnerability Assessments for the Public Sector, defined SME's and the Charity sector across the TVP delivered by our colleagues in the South East Regional Crime Unit * Closes on the 19th of November 2020, so any requests for such must have been submitted by the 18th of November 2020

1 Business Email Compromise (BEC)

Criminals hack into email systems or use social engineering tactics to gain information about corporate payments systems, then deceive company employees into transferring money into their bank account.

A recent BEC investigation led by us has resulted in a man who defrauded a Bristol-based company out of nearly half a million pounds being sentenced to three years and two months in prison. BEC attacks are a major threat to all organisations of all sizes, and across all sectors. Organisations need to be aware that criminal groups have become much more sophisticated in this space, and there are a number of steps that companies should take to become more resilient to this type of crime.

BEC Mitigation
Agree secure processes between employees internally and externally around financial transactions this might include verifying through other trusted channels, and segregating duties.

Defend against phishing

Avoid clicking on attachments or links in emails you aren't expecting, these can contain malware which give access to monitor accounts/steal information.

In general, it's also good practice to be suspicious of any correspondence asking you to act urgently with a veiled threat e.g. "send these details **within 24 hours**" or "you've been a victim of crime, click here **immediately**". More information can be found via the NCSC. https://www.ncsc.gov.uk/

Prevent malicious software (malware) infections

Using antivirus, firewalls, and other tools to scan computers and devices regularly can prevent malware from giving attackers unauthorised access to your systems.

The importance of updates

Keep your personal and business computers updated with the latest security fixes. Guidance on vulnerability management can be found via the NCSC. https://www.ncsc.gov.uk/

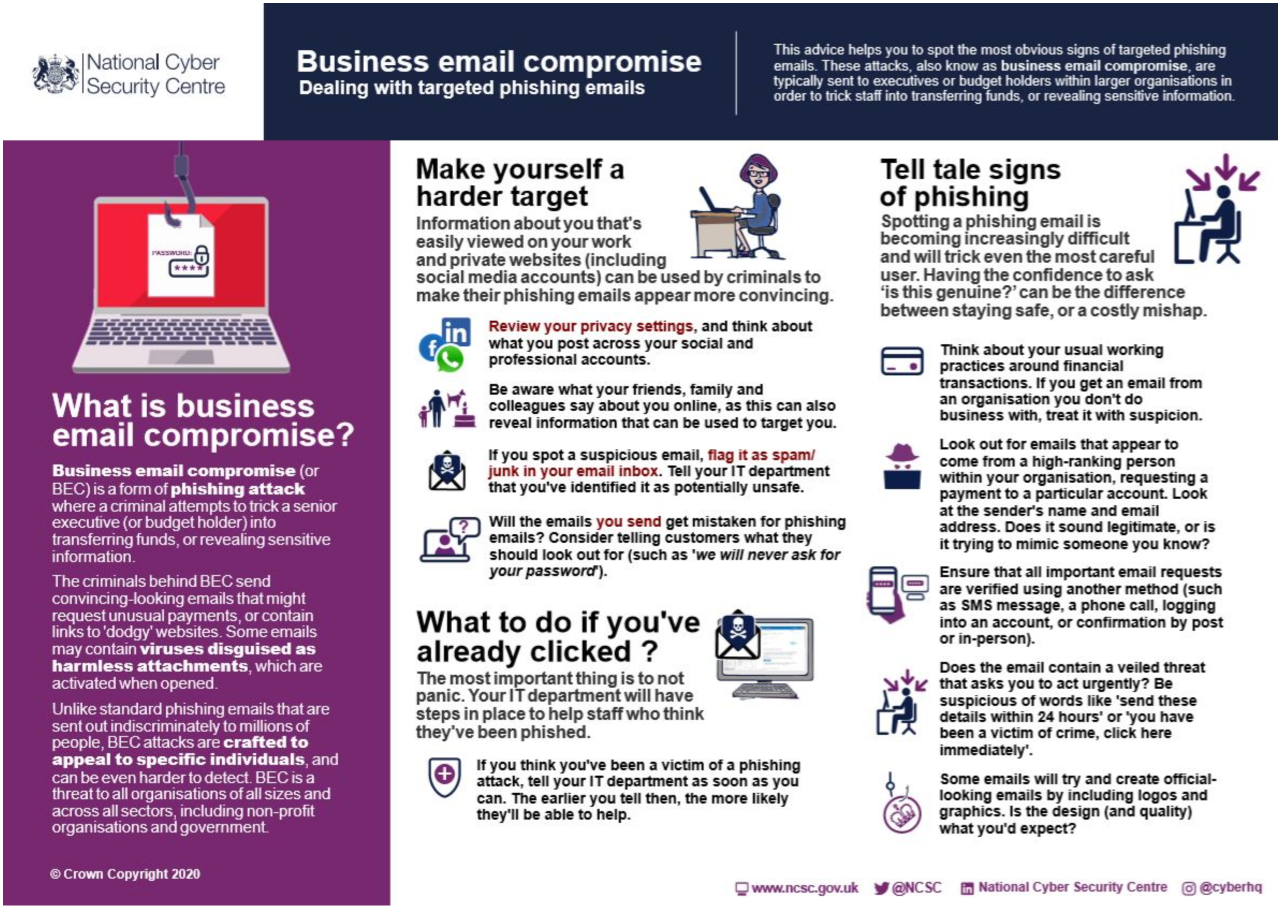
Spread the word

Staff awareness and experience is key to increasing your resilience to BEC. Regular training and communications about the issue should be an organisational priority. Although email is a major attack vector, also be aware of other communication methods as they can all be abused for fraudulent purposes.

Source SWROCU

Further Resources

For more information, we recommend the phishing advice link https://www.ncsc.gov.uk/blog-post/small-business-guide-2020 as well as below produced by the NCSC.



National Cyber Security Centre

Business email compromise

Dealing with targeted phishing emails

This advice helps you to spot the most obvious signs of targeted phishing emails. These attacks, also know as **business email compromise**, are typically sent to executives or budget holders within larger organisations in order to trick staff into transferring funds, or revealing sensitive information.

What is business email compromise?

Business email compromise (or BEC) is a form of **phishing attack** where a criminal attempts to trick a senior executive (or budget holder) into transferring funds, or revealing sensitive information.

The criminals behind BEC send convincing-looking emails that might request unusual payments, or contain links to 'dodgy' websites. Some emails may contain **viruses disguised as harmless attachments**, which are activated when opened.

Unlike standard phishing emails that are sent out indiscriminately to millions of people, BEC attacks are **crafted to appeal to specific individuals**, and can be even harder to detect. BEC is a threat to all organisations of all sizes and across all sectors, including non-profit organisations and government.

Make yourself a harder target

Information about you that's easily viewed on your work and private websites (including social media accounts) can be used by criminals to make their phishing emails appear more convincing.

Review your privacy settings, and think about what you post across your social and professional accounts.

Be aware what your friends, family and colleagues say about you online, as this can also reveal information that can be used to target you.

If you spot a suspicious email, flag it as spam/ junk in your email inbox. Tell your IT department that you've identified it as potentially unsafe.

Will the emails you send get mistaken for phishing emails? Consider telling customers what they should look out for (such as '*we will never ask for your password*').

What to do if you've already clicked ?

The most important thing is to not panic. Your IT department will have steps in place to help staff who think they've been phished.

If you think you've been a victim of a phishing attack, tell your IT department as soon as you can. The earlier you tell then, the more likely they'll be able to help.

Tell tale signs of phishing

Spotting a phishing email is becoming increasingly difficult and will trick even the most careful user. Having the confidence to ask 'is this genuine?' can be the difference between staying safe, or a costly mishap.

Think about your usual working practices around financial transactions. If you get an email from an organisation you don't do business with, treat it with suspicion.

Look out for emails that appear to come from a high-ranking person within your organisation, requesting a payment to a particular account. Look at the sender's name and email address. Does it sound legitimate, or is it trying to mimic someone you know?

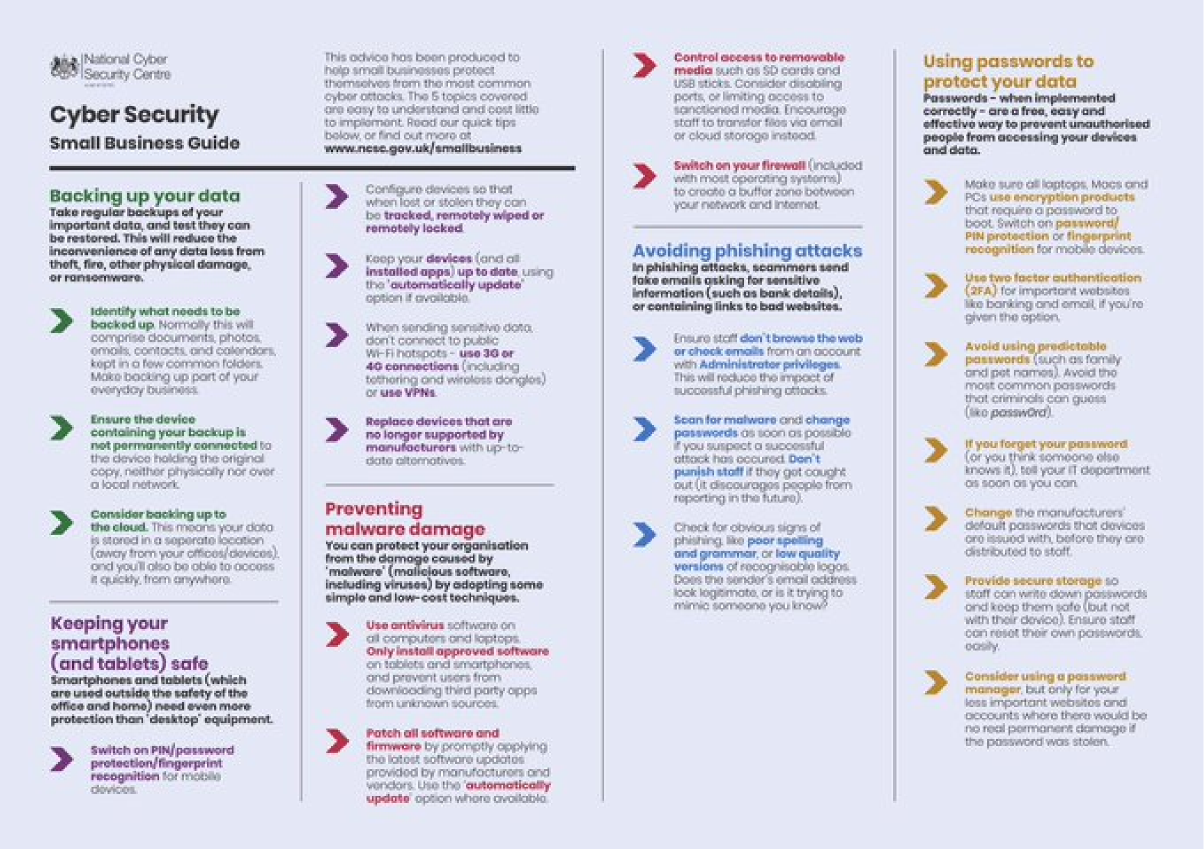
Ensure that all important email requests are verified using another method (such as SMS message, a phone call, logging into an account, or confirmation by post or in-person).

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'.

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

www.ncsc.gov.uk @NCSC National Cyber Security Centre @cyberhq

2 NCSC Small Business Guide – refreshed (Source material from the NCSC)



National Cyber Security Centre

Cyber Security

Small Business Guide

This advice has been produced to help small businesses protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at **www.ncsc.gov.uk/smallbusiness**

Backing up your data

Take regular backups of your important data, and test they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.

- **Identify what needs to be backed up.** Normally this will comprise documents, photos, emails, contacts, and calendars, kept in a few common folders. Make backing up part of your everyday business.
- **Ensure the device containing your backup is not permanently connected** to the device holding the original copy, neither physically nor over a local network.
- **Consider backing up to the cloud.** This means your data is stored in a seperate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.

- **Switch on PIN/password protection/fingerprint recognition** for mobile devices.
- Configure devices so that when lost or stolen they can be **tracked, remotely wiped or remotely locked**.
- Keep your **devices** (and all **installed apps**) **up to date**, using the '**automatically update**' option if available.
- When sending sensitive data, don't connect to public Wi-Fi hotspots - **use 3G or 4G connections** (including tethering and wireless dongles) or **use VPNs**.
- **Replace devices that are no longer supported by manufacturers** with up-to-date alternatives.

Preventing malware damage

You can protect your organisation from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.

- **Use antivirus** software on all computers and laptops. **Only install approved software** on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.
- **Patch all software and firmware** by promptly applying the latest software updates provided by manufacturers and vendors. Use the '**automatically update**' option where available.
- **Control access to removable media** such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.
- **Switch on your firewall** (included with most operating systems) to create a buffer zone between your network and Internet.

Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.

- Ensure staff **don't browse the web or check emails** from an account with **Administrator privileges**. This will reduce the impact of successful phishing attacks.
- **Scan for malware** and **change passwords** as soon as possible if you suspect a successful attack has occured. **Don't punish staff** if they get caught out (it discourages people from reporting in the future).
- Check for obvious signs of phishing, like **poor spelling and grammar**, or **low quality versions** of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

Using passwords to protect your data

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.

- Make sure all laptops, Macs and PCs **use encryption products** that require a password to boot. Switch on **password/PIN protection** or **fingerprint recognition** for mobile devices.
- **Use two factor authentication (2FA)** for important websites like banking and email, if you're given the option.
- **Avoid using predictable passwords** (such as family and pet names). Avoid the most common passwords that criminals can guess (like *passw0rd*).
- **If you forget your password** (or you think someone else knows it), tell your IT department as soon as you can.
- **Change** the manufacturers' default passwords that devices are issued with, before they are distributed to staff.
- **Provide secure storage** so staff can write down passwords and keep them safe (but not with their device). Ensure staff can reset their own passwords, easily.
- **Consider using a password manager**, but only for your less important websites and accounts where there would be no real permanent damage if the password was stolen.

It's been a challenging year for the UK economy, with many small businesses having to react quickly to the constraints imposed by COVID-19 to keep their business active. In many cases, this has meant placing greater reliance on digital technology, including home working.

Whilst this can have many positive outcomes for your business, the idea of formal 'cyber security' is new to many business owners. Even hearing the expression may sound intimidating. But it does not have to be.

In 2017 the NCSC's published its **Small Business Guide**, guidance specifically designed to help small businesses - many of whom won't have dedicated IT staff - protect themselves from cyber crime. In response to businesses and partners, the NCSC have this updated version, with a new design and up-to-date advice about how you can protect yourself from the most common cyber-attacks.

Also updated:

- the **Small Business Guide Actions** (a list of actions to carry in accordance with the Small Business Guide)
- the **Response & Recovery Guide** (to help small businesses prepare their response to and plan their recovery from a cyber incident)

If you're new to cyber security, we hope this guidance gets you started. More experienced readers may want to check their existing cyber security measures against it, to ensure their devices and data are suitably protected. (Source NCSC) https://www.ncsc.gov.uk/news/revamped-small-business-guide

3 Revamped cyber toolkit launched to support retailers improve defences
The British Retail Consortium's (BRC) refreshed toolkit, developed alongside experts at the NCSC, will help retailers boost cyber defences. (Source material from the BRC)

Retailers will benefit from fresh advice and guidance published today which aims to help them reduce the threat of a successful cyber-attack.

Working alongside the National Cyber Security Centre, which is a part of GCHQ, the British Retail Consortium has launched the Cyber Resilience Toolkit for Retail, an actionable guide specifically designed for non-cyber experts, such as Board members, those in senior strategic roles, and start-up businesses.

It highlights the threats faced by retailers, key questions to consider when developing cyber resilience strategies, and guidance on the types of protections retailers should implement. The toolkit outlines recommended actions for retailers in:

- Preventing breaches through stronger protections
- Preparation to mitigate the impact of a successful breach
- Recovering after a cyber attack
- Developing and embedding a positive cyber resilience culture at Board level

Link to the full tool kit: https://brc.org.uk/media/676134/cyber-resilience-toolkit-for-retail.pdf

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

DEVELOPING THE CYBER RESILIENCE OF SOUTH EAST BUSINESS
"The Cyber Resilience Centre for the South East supports and helps protect SMEs and supply chain businesses and third sector organisations in the region against cyber crime.

Working with local Universities and the Police forces in Thames Valley, Sussex, Surrey and Hampshire, provides us with access to the latest local as well as national information on emerging cyber threats, criminal trends, best practice for cyber resilience and new technology to provide you with timely advice to prepare and protect your business, staff and clients from cyber criminals.

We also provide affordable testing and training services, with the opportunity to learn how to procure private sector cyber services where needed.
A trusted resource, we are also a straightforward place to find IASME approved Cyber Essentials and Cyber Essentials + Certifiers in the South East. The full website is available here" https://www.secrc.co.uk

Other topics

TVP Cyber Protects continuing offer of the delivery of 1hr 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*

Nationally, we are seeing, as a result of this crisis, 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
3 Home working
4 Wider online fraud

Therefore and for the foreseeable future, this 1hr online presentation, will be delivered via **Microsoft Teams or Zoom** as a **webinar** (At the moment the TVP Force system only permits audio and content sharing, but we are awaiting authorisation to have video enabled as the default) we have already delivered similar sessions to that outlined above and have existing plans to deliver to business representative organisations, who have already made an approach.

Or if 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 our **@TVPCyber_Fraud** Twitter account. If you have already received session in 2020, you will not need to revisit the above, unless it is critical to your organisation.

If you would like this TVP delivered 1hr online session either in its current audio and content presentation of the slides or when video is enabled, please come to us via our email address of cyber.protect@thamesvalley.pnn.police.uk , 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 connection log-in 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

To manage supply and demand expectations, due to capacity to deliver we would not be able to deliver the webinar for a sole businesses, so our suggestion would be for Sole Traders or smaller SME’s to collaborate and put forward dates or with arrangement.
We are happy to deliver the session of an evening, Tuesday or Thursday, especially leading in to the late autumn, winter of 2020 should this be more beneficial. In any event, please allow at least 10 working days’ notice to arrange.

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, till at least the 17th of January 2021)

Vulnerability Assessment – (*Closes for applications 18th November 2020)
The South East Regional Organised Crime Unit is a Police unit responsible for delivering specialist and niche capabilities in the South East of the United Kingdom.
We have produced this crime prevention initiative which offers a free vulnerability assessment for the public sector, selected small to medium sized companies and charities based in Thames Valley Police, Hampshire Constabulary, Surrey Police and Sussex Police areas.

What is the assessment?
The vulnerability assessment uses an industry recognised software package. It's not a penetration test but a basic assessment of your network (i.e. internet facing systems like firewalls, mail servers, etc… not user workstations or internal systems) – it doesn't give protection against complex or persistent attacks, but does give an overview of the network security weaknesses that could be exploited by criminals on the internet. To obtain such a scan from the private sector could incur a cost.

Why are we offering this service?
Cyber criminals are constantly scanning the internet looking for vulnerabilities.
A large percentage of crimes occur when the attacker has found a well-known, easily exploitable vulnerability in an organisation's network. If you believe your organisation may benefit from this prevention service, please get in touch and a member of the team will contact you to discuss the assessment in more detail.

These are all crimes which could have been prevented if the organisation had known about the vulnerability and taken the appropriate action. The aim of this service is to identify these common vulnerabilities before the criminals do. Falling victim to cyber crime can cause significant financial loss, reputational damage and emotional distress for those involved.

How will the assessment be conducted?
By providing some technical information to us, this assessment can be conducted, remotely – meaning nobody needs to be physically present on your premises and the assessment can occur at any time of the day.

What you will receive?
A report which outlines your vulnerabilities, not all of them, but it's a good way of establishing if you have high risks, easy to exploit gaps, which attackers could use. The report will help you understand where you need to start to improve your security and an assessment can help you comply with regulations and certifications such as Cyber Essentials, GDPR, ISO27001 and PCI Compliance."

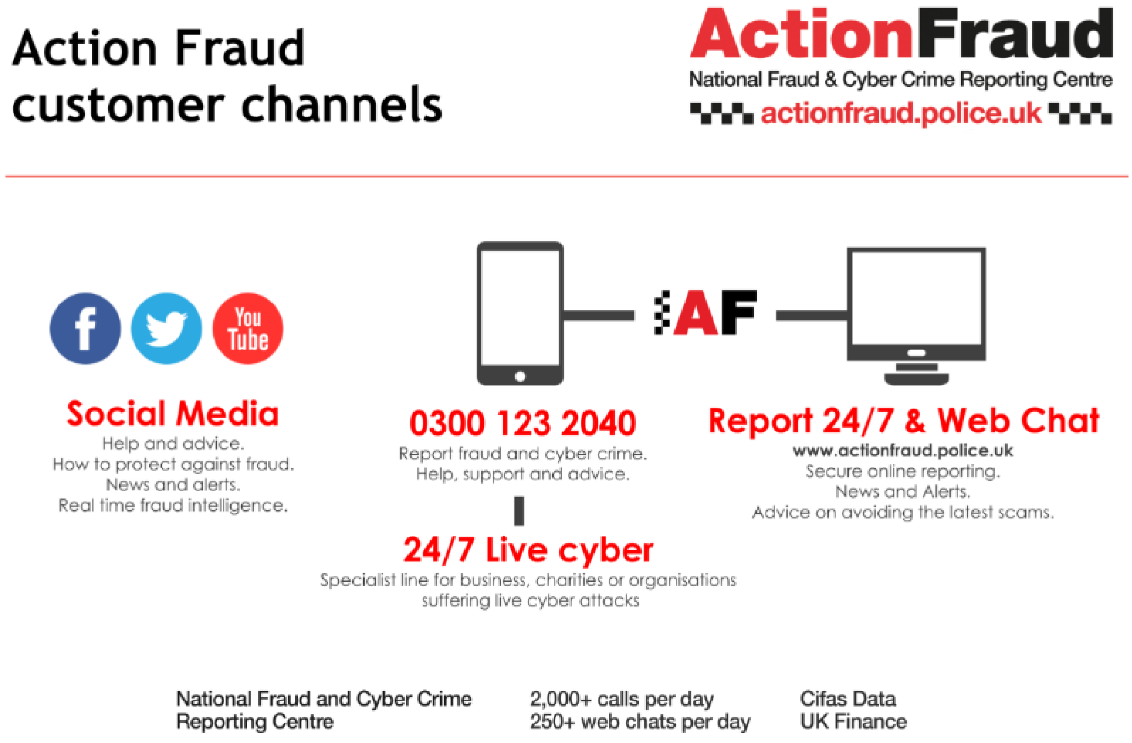
If your organisation would like this facility, please email: cyber.protect@thamesvalley.pnn.police.uk , quoting Vulnerability Assessment, following which we will send over the contract letter to be completed and signed, from which the requester returns and we forward to our Regional colleagues for their action.

(**LEA Schools in the TV area, have been(140 to date) or will be offered the above via a direct contact from the Cyber Protect team here in TVP, so please do not communicate the Vulnerability Assessment offering as above* to such*)

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

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: 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 can be found here: https://www.actionfraud.police.uk/reporting-fraud-and-cyber-crime



Action Fraud customer channels

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

Social Media
Help and advice.
How to protect against fraud.
News and alerts.
Real time fraud intelligence.

0300 123 2040
Report fraud and cyber crime.
Help, support and advice.

24/7 Live cyber
Specialist line for business, charities or organisations suffering live cyber attacks

Report 24/7 & Web Chat
www.actionfraud.police.uk
Secure online reporting.
News and Alerts.
Advice on avoiding the latest scams.

National Fraud and Cyber Crime Reporting Centre

2,000+ calls per day
250+ web chats per day

Cifas Data
UK Finance

Keep up to date with NCSC reports and advisories
https://www.ncsc.gov.uk/section/keep-up-to-date/reports-advisories
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 suspended for the duration of the current COVID-19 situation)

And finally
In the lead up to the end of 2020, we would like to thank all who have encouraged and given recognition of the work we deliver to better support and inform yourselves in the Public, Private and Charity sectors of emerging and ongoing Cyber / Fraud crime both in the Thames Valley area and which marks two years of providing these Newsletters.

Best wishes, TVP Cyber Protect