STAFFORDSHIRE POLICE

Cyber Champion Tips October 2020

Welcome to October's Top Tips. This month we are going to highlight fraudulent phone calls, emails and text messages, which are all methods of **phishing**. Last month we highlighted **Courier Fraud** due to emerging trends of this type of criminality and we continue to see this type of cyber enabled fraud circulating locally. This kind of crime generally begins with an unsolicited phone call to unsuspecting individuals, some current examples being received by local people are as follows:

Fraudulent calls:

Call from male purporting to be a police officer, caller asked individual for confirmation of name and address (which fraudster already knew). He stated he was ringing because credentials had been used to purchase goods earlier that day.

Call from Visa Fraud team regarding suspicious transaction on account, alleged police officer purportedly conducting a worldwide investigation suggesting someone was attempting to withdraw significant funds from account. Further call received, spoofed number used masquerading as the bank, asked individual to go to the bank and draw out funds for safe keeping. Told not to disrupt the police investigation by telling anyone.

Call from a withheld number, caller purporting to be a police officer. Claimed criminals had been arrested who were involved in fraudulent bank card activities on the individuals account.

In the examples given above, the callers attempted to gain financial and personal information from individuals, masquerading as trusted professionals and using the fear that money was at risk to trick people into taking action. Only with vigilance of this type of criminality and having the confidence to **Take Five and stay in control** can people better protect themselves from this threat. It is OKAY not to engage with an unsolicited caller, no matter who they claim to be - STOP, CHALLENGE, PROTECT. Please continue to share awareness of these particular scams. **Advice:**

- Remain in **control** of the conversation
- Do not be rushed
- End the call and **verify** any request/instruction via a trusted, reliable source
- Phone numbers and menus can be spoofed (fake)
- Use a different phone to verify call (if this is not possible, wait at least five minutes before dialling out)

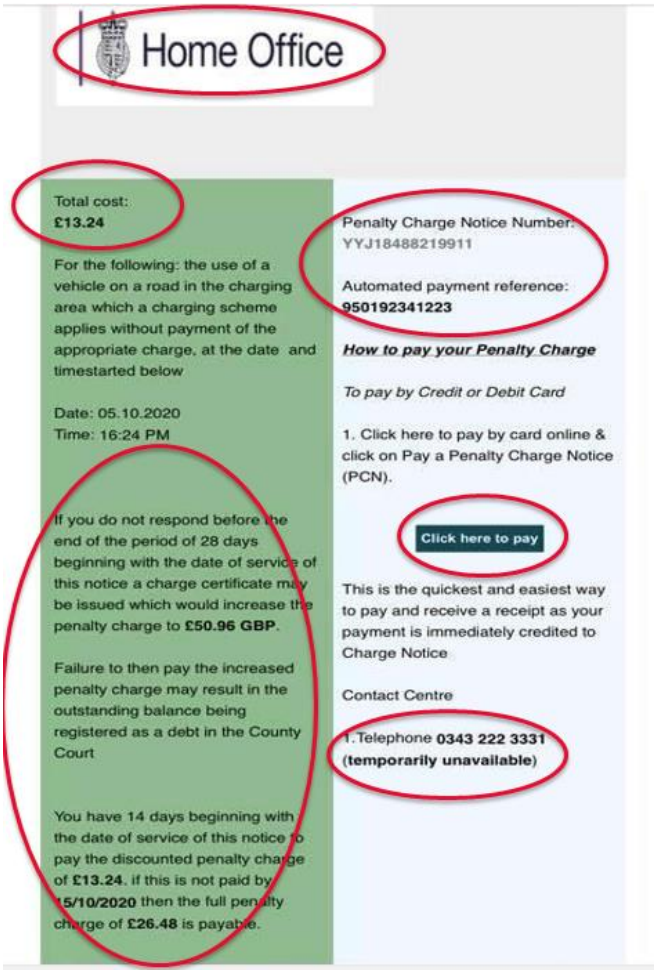
Phishing emails are an ongoing concern, we are seeing reports of spear phishing amongst businesses, these are targeted campaigns against individuals or businesses and these particular emails can be difficult to spot. Encourage staff to **be vigilant**, raise awareness of phishing emails, reiterate and reinforce education amongst staff and members of the public.

Generic phishing email scams which are currently circulating, are under the guise of:

- Home Office (penalty charge)
- Microsoft
- Amazon
- Facebook
- Netflix
- TV licencing
- Various purporting to be from banking

Here are a couple of examples, one, a phishing email and the second, a fraudulent text, which have been recently received by colleagues:

Penalty Charge Phishing Email:



The Detail

Purporting to be government organisation

The 'Ask'. Not too much to ask for? But what else will you give away if you click the link and respond?

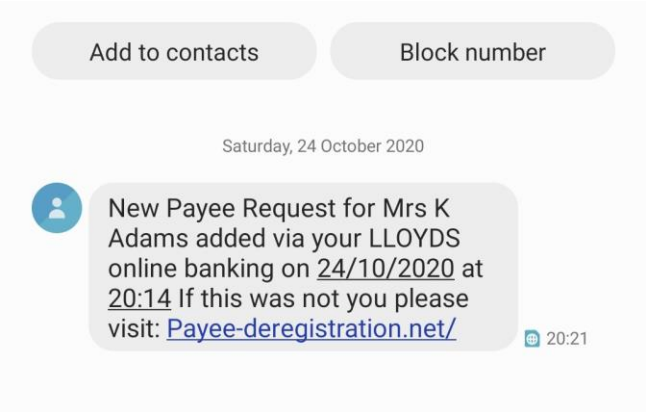
Reference number to add credibility?

Added **time pressure**, **threats** and **poor grammar**

Instruction to pay, it's easy, simply 'click here' **- dangerous link**

Telephone unavailable – Subconscious ploy to detract you from making enquiries by phone, shifting focus to encourage *'I'll just pay'* thinking

Banking Smishing Text:



The Detail

Purporting to be from the bank

Suggestive of suspicious activity on account to encourage response

The 'Ask'. 'If this was not you please visit'

And there it is, **the dangerous link**

It is worth noting that smishing texts can slip into the same feed as a genuine message, so treat any message containing a link with caution. If suspicious, verify content via a trusted source.

The purpose of phishing emails and texts is to try to obtain credentials, to gain access into systems, gain personal and financial information and/or distribute malware (malicious software).

Advice:

Never respond to any unsolicited phone calls, emails or text messages:

Stop – Think about what is being asked of you, or offered to you

Challenge – have the confidence to challenge both yourself and the delivery – Caller? Email? Text? Social media message? Challenge the detail

Protect - It is important to Stop and Challenge to ensure data is protected

You can now forward suspicious texts to: **7726**. Forward suspicious emails to: report@phishing.gov.uk

Next month there will be some useful tips for social media and how to keep accounts better secured.

In the News:

The Banking Protocol: We start with some great news, 'Bank branch staff worked with the police to stop £19 million of fraud in the first half of 2020 through the Banking Protocol. A system that alerts local police to suspected scams, the scheme has prevented victims from losing £116 million of fraud and led to 744 arrests since it was introduced three years ago. A range of scams that trick elderly and vulnerable customers into withdrawing cash from their branch have been prevented, including courier scams, romance fraud and rogue traders. The Banking Protocol scheme is now being expanded to telephone and online banking' *Action Fraud*. Read full article here: https://www.actionfraud.police.uk/news/bank-branch-staff-and-police-team-up-to-stop-19-million-of-fraud-in-first-half-of-2020

National Cyber Security Centre (NCSC) Alert: Risk of **SharePoint vulnerability** to UK organisations:

The NCSC is raising awareness of a new remote code execution vulnerability (CVE-2020-16952) affecting Microsoft SharePoint. Successful exploitation of this vulnerability would allow an attacker to run arbitrary code and carry out security actions in the context of the local administrator on affected installations of SharePoint server. The NCSC is issuing this alert to ensure that system owners are aware of this vulnerability and to ensure remediation actions are taken' *NCSC*, to find out more visit here: https://www.ncsc.gov.uk/news/sharepoint-vulnerability-uk-organisations

October NCSC threat reports here:

2nd October 2020: https://www.ncsc.gov.uk/report/weekly-threat-report-2nd-october-2020

- QNAP issues new ransomware warning to network-attached storage device users
- Cloud Security: The way forward?
- Vulnerabilities Affecting MobileIron Products (CVE-2020-15505)

9th October 2020: https://www.ncsc.gov.uk/report/weekly-threat-report-9th-october-2020

- Ransomware attacks not being reported
- Endpoint security pain point for cyber professionals
- Annual list of most "dangerous" celebrities topped by familiar chat show host

16th October 2020: https://www.ncsc.gov.uk/report/weekly-threat-report-16th-october-2020

- Call for caution during online shopping events
- Passenger data compromise confirmed by Carnival
- Microsoft security updates now available
- Threat actors chaining vulnerabilities

23rd October 2020: https://www.ncsc.gov.uk/report/weekly-threat-report-23rd-october-2020

- US warns of Chinese actors exploiting public vulnerabilities
- Marks & Spencer CEO spoofed

Staying Informed:

To help you keep informed, West Midland Regional Cyber Crime Unit are providing **'Cyber Threat Weekly'** podcasts with cyber updates and current information which you can access here: https://cyberthreatweekly.buzzsprout.com/

Reporting

Suspicious Email Reporting Service – Please forward suspicious emails to:

report@phishing.gov.uk

Forward suspicious texts to: 7726

Report cybercrime and fraud to Action Fraud:

0300 123 2040

www.actionfraud.police.uk

Further information and advice can be found by visiting:

cyberaware.gov.uk

www.ncsc.gov.uk/

actionfraud.police.uk/

takefive-stopfraud.org.uk/