GREATER MANCHESTER
DOING DIGITAL DIFFERENTLY

**Covid-19 Cyber Safety Partner Communications Pack**

## BACKGROUND

In the UK, the National Cyber Security Centre (NCSC) has detected more UK government branded scams relating to COVID-19 than any other subject. The NCSC has seen a growing use of COVID-19 related themes by malicious cyber actors. Similarly, the increase in home working has increased the use of potentially vulnerable services, such as Virtual Private Networks (VPNs), amplifying the threat to individuals and organisations.

Law enforcement, government and private sectors partners are working together to encourage members of the public to be more vigilant against fraud, particularly about sharing their financial and personal information, as criminals seek to capitalise on the Covid-19 pandemic.

**Common threats identified by NCSC include:**

- Phishing using COVID-19 subject as a lure
    - Emails using heading such as 2020 Covid-19 Updates which include a call to action link
    - SMS which appear to be from COVID-19 or UKGOV which includes a link to phishing site
- Malware disruption using COVID-19 as a lure
- Registration of new domain names using COVID-19 related wording
- Attacks against newly created home working domain info structure E.g. emails with fake links to commonly used home working devices- Microsoft Teams and Zoom

## KEY MESSAGES

### GENERAL

- Across the UK we have seen a significant increase in Covid-19 related cyber-crime, it is now more important than ever to stay safe online.
- #Tell2 to protect many
- Remember to Stop, Challenge, Protect when being asked for your money or information.

    - **Stop**- Taking a moment to stop and think before parting with your money or information could keep you safe.
    - **Challenge**- Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
    - **Protect**- Contact your bank immediately if you think you've fallen for a scam and report it to Action Fraud.

### ADVICE
**General Online Safety**

- Make sure you download all software updates as they contain vital security updates to help protect your devices from cyber criminals.
- Turn on two-factor authentication on your email to make sure your data is secure.
- If you believe you've fallen for a scam, contact your bank immediately on a number you know to be correct
- Question claims that you're due money for goods or services that you haven't ordered or are unaware of, especially if you have to pay any fees upfront.
- Question uninvited approaches and contact companies directly using a known email or phone number.

**Passwords**

- Have different passwords for all your accounts/systems
- Use three random words in your passwords e.g. Redhousemonkey27
- NEVER include personal details in your passwords e.g. your partners name, pets name or date of birth

**Phishing**

- **If you are in doubt, call it out-** if you are uncertain about an email you receive report it or delete it
- To spot a phishing email look for urgent calls to action, generic address e.g. dear friend, poor quality images and spelling mistakes.

**Social media**

- Most websites, apps and social networks you can share information on have 'privacy settings'. Use these to help you control what and who you share it with
- Don't accept people you don't know on your social media accounts

**SMS**

- There has been an increase in criminals using text messages to scam consumers. Please always refrain from clicking on any links contained within text messages.
- If you suspect a spam text you can report it to your mobile network provider by forwarding it to 7726

## CAMPAIGN GRAPHICS

The GMCA have developed a series of Greater Manchester Doing Things Differently branded campaign graphics sized for social media and in A5 format for use in print publications.

These graphics have been developed for localities to use to target different audiences and vulnerable groups in their area.

## LINKS AND RESOURCES

**Take Five**

We are using Take Five campaign branding as it is a known campaign which already has brand recognition and some useful key messages.

Take Five is a national campaign that offers straight-forward and impartial advice to help everyone protect themselves from preventable financial fraud. This includes email deception and phone-based scams as well as online fraud – particularly where criminals impersonate trusted organisations.

The Take Five campaign is led by UK Finance and backed by the government and is being delivered with and through a range of partners.

- Covid-19 Fraud and Scams: https://takefive-stopfraud.org.uk/coronavirus-fraud-and-scams/

**National Cyber Security Centre**

NCSC have launched their Cyber Aware campaign to advice residents on how to stay secure online during coronavirus. The campaign includes a number of useful resources including support on video conferencing securely and advice on dealing with phishing emails.

They have also set up a Suspicious Email Reporting Service, they are urging people to email any suspect emails to: report@phishing.gov.uk

- Cyber Aware campaign: https://www.ncsc.gov.uk/cyberaware
- Home working- Managing the Cyber risks advice and infographic: https://www.ncsc.gov.uk/guidance/home-working
- Phishing- dealing with suspicious emails: https://www.ncsc.gov.uk/guidance/suspicious-email-actions

**Action Fraud**

Action Fraud is the UK's national reporting centre for fraud and cybercrime.

Victims of fraud or cybercrime can report it using their online reporting service or by calling 0300 123 2040.

- How to report fraud and cyber-crime: https://www.actionfraud.police.uk/reporting-fraud-and-cyber-crime

**SOCIAL MEDIA**

Example social media content

GREATER MANCHESTER
DOING DIGITAL DIFFERENTLY

| | |
|---|---|
| 🏠 As people continue to stay at home, we are are spending increasing amounts of time online.<br><br>📈 Which has meant a significant increase in cyber-crime. We will be regularly sharing tips to help you stay safe online.<br><br>More tips here 👉 https://www.ncsc.gov.uk/cyberaware<br><br>#StaySafeOnline | |
| 🚨 Did you know one of the most common online threats is phishing emails using COVID-19 in the subject as a lure.<br><br>📧 If you receive a suspicious email forward it to 👉 report@phishing.gov.uk<br><br>#StaySafeOnline #CyberSafety | |

Useful twitter pages:

- @GMCADigital
- @Takefive
- @NCSC
- @CyberCentreGM
- @Actionfrauduk
- @gmpfraud
- @GetSafeOnline

Useful hashtags:

- #StaySafeOnline
- #CyberSafety
- #Tell2
- #TakeFive