STAFFORDSHIRE POLICE

Fraud & Cyber Crime – Covid-19 Update

30/03/2020

'Beware fraud and scams during Covid-19 pandemic fraud

Criminals are using the Covid-19 pandemic to scam the public – don't become a victim. 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. Criminals are experts at impersonating people, organisations and the police. They spend hours researching you for their scams, hoping you'll let your guard down for just a moment.

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*.

Your bank or the police will NEVER ask you to transfer money or move it to a safe account' *City of London Police, NCA, NECC*.

Phishing Emails

Action Fraud have already received over 200 reports of coronavirus-themed phishing emails containing links and attachments attempting to trick people into divulging personal information including financial information including banking details, email logins, passwords, etc.

TAKE FIVE TO STOP FRAUD

Some of the tactics being used in phishing emails which have been seen nationally and locally include:

HMRC:

Emails purporting to be from HMRC offering a tax refund and directing victims to a fake website to harvest their personal and financial details. The emails often display the HMRC logo making it look reasonably genuine and convincing.

Assistance with Funding in the Absence of School Meals:

Fraudsters are targeting families with phishing emails offering financial support to parents and carers:

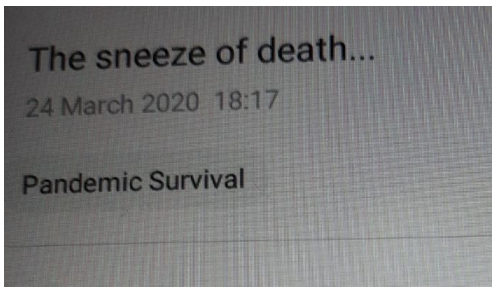
'if your child is entitled to free school meals send your bank details to the school and they will help with funding while the school is closed', there is a link in the email which takes anyone who clicks it to a fraudulent website.

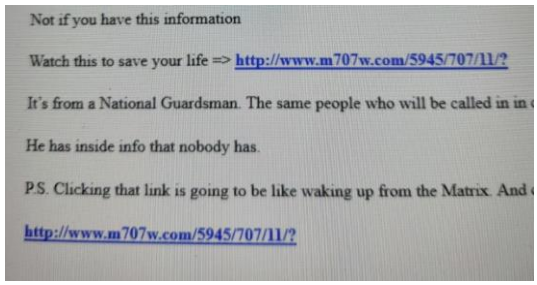
ASDA/Tesco – Sterile Delivery:

'We can offer ASDA/Tesco sterile delivery plus gift card if you click here to register your credit card'.

'The sneeze of death/Pandemic survival':

An unpleasant phishing email has been landing is some people's mailboxes, this email details unpleasantries about Coronavirus and makes for uncomfortable reading. It plays on people's fears and hopes, people who are searching for answers and information, encouraging to click dangerous links. Here is a sanitised clip of the email:





'Fraudulent News Letters and Updates:

Fraudsters providing articles about the virus outbreak with a link to a fake company website where victims are encouraged to click to subscribe to a daily newsletter for further updates (AF).

Trading Advice and Investment Opportunities:

Fraudsters sending investment scheme and trading advice encouraging people to take advantage of the coronavirus downturn (AF).

Graeme Biggar, Director General of the National Economic Crime Centre, said:

"We have already seen fraudsters using the COVID-19 pandemic to scam people looking to buy medical supplies online, sending emails offering fake medical support and targeting people who may be vulnerable or increasingly isolated at home.

"These frauds try to lure you in with offers that look too good to be true, such as high return investments and 'healthcare opportunities', or appeals for you to support those who are ill or bogus charities.

The advice is simple, think very carefully before you hand over your money, and don't give out your personal details unless you are sure who you are dealing with"' Action Fraud (AF).

Protect yourself

1) Watch out for scam messages - **Don't click on the links or attachments in suspicious emails**, and never respond to unsolicited messages and calls that ask for your personal or financial details.

2) Shopping online - If you're making a purchase from a company or person you don't know and trust, carry out some research first, and ask a friend or family member for advice before completing the purchase. If you decide to go ahead with the purchase, use a credit card if you have one, as most major credit card providers insure online purchases.

3) Protect your devices from the latest threats - Always install the latest software and app updates to protect your devices from the latest threats.

As always, please report Cybercrime and Fraud to 'Action Fraud' using their online reporting portal here:
https://www.actionfraud.police.uk/reporting-fraud-and-cyber-crime

Fraudulent Text Messages

We are also seeing an increase in fraudulent text messages, one in particular purporting to be from GOV.UK

Any **text message containing a link should be treated with upmost caution**. The best way to find information from GOV.UK, or any other agency, is to visit that particular website via a trusted source and **not clicking on links** in unsolicited texts or emails.

Further Information and Resources:

For more information on how to shop online safely, please visit: https://www.actionfraud.police.uk/shoponlinesafely

For resources and latest news visit Take Five visit: https://takefive-stopfraud.org.uk/news/scam-alert-coronavirus/

For information on how to update your devices, please visit: https://www.ncsc.gov.uk/guidance/securing-your-devices

For the most up-to-date guidance around Covid-19 visit: https://www.gov.uk/coronavirus

For the latest health information and advice about COVID-19 please visit the NHS website.

To report offers of financial assistance from HMRC contact phishing@hmrc.gov.uk