OPERATION REPEAT
Reinforcing Elderly Persons Education at All Times

COVID -19 Cyber Crime Advice

The National Cyber Security Centre (NCSC) a part of GCHQ, has launched a Cyber Aware campaign, promoting behaviours to try and reduce online threats.

Part of this project has been to establish a **Suspicious Email Reporting Service**, co-developed with the City of London Police. By forwarding any dubious emails – including those claiming to offer support related to COVID-19 to ***report@phishing.gov.uk*****,** the NCSC's automated programme will immediately test the validity of the site. Any sites found to be phishing scams will be removed immediately.

As well as taking down malicious sites it will support the police by providing live time analysis of reports and identifying new patterns in online offending - helping them stop even more offenders in their tracks.

If people have lost money, they **should tell their bank** and **report it as a crime to Action Fraud**, but the new ***Suspicious Email Reporting Service*** will offer an automated service to people who flag what they think to be a suspicious email.

This will build on the organisation's existing takedown services, which have already removed more than 2,000 online campaigns related to coronavirus in the last month, including;

- 471 fake online shops selling fraudulent coronavirus related items
- 555 malware distribution sites set up to cause significant damage to any visitors
- 200 phishing sites seeking personal information such as passwords or credit card details
- 832 advance-fee frauds where a large sum of money is promised in return for a set-up payment

NCSC Chief Executive Officer Ciaran Martin said:

"Technology is helping us cope with the coronavirus crisis and will play a role helping us out of it - but that means cyber security is more important than ever.

"With greater use of technology, there are different ways attackers can harm all of us. But everyone can help to stop them by following the guidance campaign we have launched today. But even with the best security in place, some attacks will still get through.

"That's why we have created a new national reporting service for suspicious emails – and if they link to malicious content, it will be taken down or blocked. By forwarding messages to us, you will be protecting the UK from email scams and cyber crime."

To help keep you safe from cyber crime NCSC have produced a 6 simple step guide for you to follow and share with anyone who you know uses a computer, tablet or mobile phone. Please take a few minutes to complete these steps – Doing so may not only save you hours of time in the future, but the heartache and worry getting caught up in cybercrime brings.

1. **<u>Create a separate password for your email</u>**

- Your personal email account contains lots of important information about you and is the gateway to all your other online accounts.
- If your email account is hacked all your other passwords can be reset, so use a strong password that is different to all your others.

2. **<u>Create a strong password using three random words</u>**

- Weak passwords can be hacked in seconds. The longer and more unusual your password is, the stronger it becomes and the harder it is to hack. The best way to make your password long and difficult to hack is by using a sequence of three random words you'll remember.
- You can make it even stronger with special characters.
- Starting with your most important accounts (such as email, banking and social media), replace your ***old passwords*** with new ones. Just connect three random - but memorable - words together.

3. **<u>Save your passwords in your browser</u>**

- Using the same passwords for all your accounts makes you vulnerable - if that one password is stolen all your accounts can be accessed.
- It's good practice to use different passwords for the accounts you care most about.
- Of course, remembering lots of passwords can be difficult, but if you save them in your browser then you don't have to.
- Online service providers are constantly updating their software to keep sensitive personal data secure, so store your passwords in your browser when prompted; it's quick, convenient and safer than re-using the same password.

-

4. **Turn on two-factor authentication**

- Two-factor authentication (2FA) is a free security feature that gives you an extra layer of protection online and stops cyber criminals getting into your accounts - even if they have your password.
- 2FA reduces the risk of being hacked by asking you to provide a second factor of information, such as getting a text or code when you log in, to check you are who you say you are.
- Check if the online services and apps you use offer 2FA – it's also called two-step verification or multi-factor authentication. If they do, turn it on. Start with the accounts you care most about such as your email and social media.
- Your bank automatically carries out an extra security check if you use online banking, so you don't need to turn this on yourself. However, you should check your bank has your correct phone number so they're able to text a code to your mobile or call your landline to confirm it's you.

-

5. **Update your devices**

- Cyber criminals exploit weaknesses in software and apps to access your sensitive personal data, but providers are continually working to keep you secure by releasing regular updates. These updates fix weaknesses, so criminals can't access your data.
- Using the latest versions of software, apps and operating system on your phone or tablet can immediately improve your security.
- Remember to update regularly, or set your phone or tablet to automatically update so you don't have to think about it.

6. **Turn on backup**

- If your phone, tablet or laptop is hacked, your sensitive personal data could be lost, damaged or stolen.
- Make sure you keep a copy of all your important information by backing it up.
- You can choose to back up all your data or only information that is important to you.