Eastern Region Special Operations Unit

Regional Organised Crime Unit

COVID-19 CYBER & FRAUD PROTECT MESSAGES

This advice has been collated by the East Midlands Regional Organised Crime Unit (ROCU) and is intended for wider distribution to raise awareness among businesses and the public. Advice and information is changing daily as we navigate our way through the COVID-19 pandemic, so please ensure you only take information from reputable sources.

If you require any further information, assistance or guidance please contact the ERSOU Protect Team CyberProtect@ERSOU.pnn.police.uk or your local Force protect team.

Thursday 9th April 2020

Today's topic is 'How to keep in touch and stay safe online'.

Working from home is new for a lot of organisations and employees, even if home working has been supported for some time, there may suddenly be more people working from home than usual, some of whom may not have done it before.

If organisations need to set up new accounts or access so staff can work from home, they need to set strong passwords for user accounts, so today's 'Hot Topic' is passwords.

How to create a strong memorable password - use three random words.
Numbers, symbols and capital letters can still be added, e.g. **3RedHouseMonkeys27!**

Be creative and use words memorable to you, so that people can't guess your password. Your social media accounts can give away vital clues about yourself so don't use words such as your child's name or favorite sports team which are easy to guess.

Cyber criminals are very smart and know many of the simple substitutions we use such as 'Pa55word!" which utilises symbols to replace letters.

Two-factor authentication (often shortened to 2FA) provides a way of 'double checking' that you really **are** the person you are claiming to be when you're using online services, such as banking, email or social media.

Consider using a password manager and avoid the following;

- Sharing your password with other people
- Using the same password on multiple platforms

Further information available at the NCSC website

Eastern Region Special Operations Unit

Regional Organised Crime Unit

Trending

ZOOM video security

The video conferencing application ZOOM has rapidly gained popularity during the current situation. It's easy and free - it is a popular way to stay in touch.

There are several reports in the media, both mainstream and Cyber, raising doubts about the security of ZOOM.

In the current unprecedented circumstances the need for effective channels of communication are vital. NCSC guidance shows there is no security reason for Zoom not to be used for conversations below a certain classification. The NCSC recommends following vendor best practice advice in the mitigation of vulnerabilities. In this case, the most important aspect is to use the latest version of the application and follow vendor security advice. More information can be found at: https://zoom.us/security

Top tips for video users:

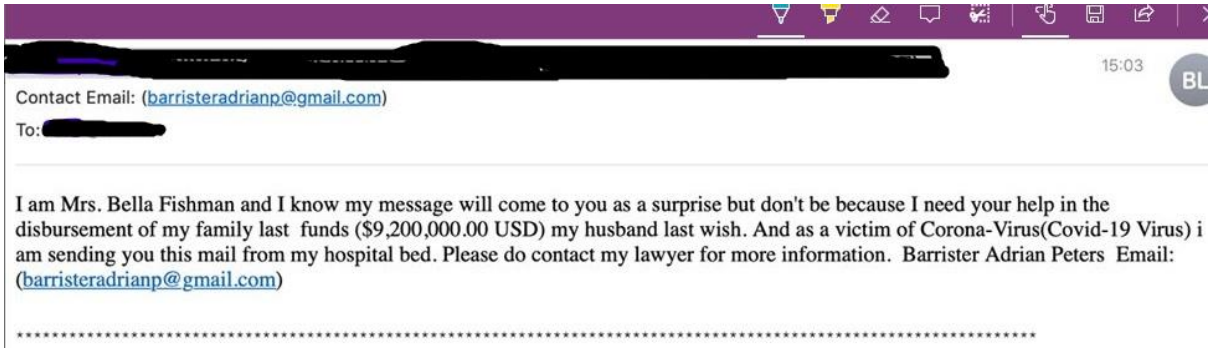
- Think about location - what can be seen in the background?
- Do you have Alexa, Siri or Google Assistant listening in the background?
- Sharing your screen – think about what else can be seen when you "share"

NHS England

Emails have been sent purporting to be from NHS England, asking the recipients to pay into a bank account to support the NHS.

Hackers are sending a new COVID 19 email titled "You are infected". Recipients are asked to download an infected Excel document attached to the email and proceed to the nearest emergency health clinic for testing.

Locally we have been made aware of the below email that shows that even the least sophisticated of the scammers are jumping on the Covid19 bandwagon.


[redacted]

15:03

Contact Email: (barristeradrianp@gmail.com)

To: [redacted]

I am Mrs. Bella Fishman and I know my message will come to you as a surprise but don't be because I need your help in the disbursement of my family last funds ($9,200,000.00 USD) my husband last wish. And as a victim of Corona-Virus(Covid-19 Virus) i am sending you this mail from my hospital bed. Please do contact my lawyer for more information. Barrister Adrian Peters Email: (barristeradrianp@gmail.com)

Reporting

Reporting is CRUCIAL. If you think you've been a victim of fraud report this to Action Fraud either online at or by calling 0300 123 2040.