East Midlands Special Operations Unit

COVID-19 PROTECT MESSAGES

This advice has been collated by EMSOU and is intended for wider distribution within the East Midlands Region 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 EMSOU Protect Team E: EMSOU2@leicestershire.pnn.police.uk or your local Force protect team.

Ransomware

Ransomware can be devastating for any organisation to suddenly find its systems compromised. This malicious software will stop you accessing your computer by locking it and encrypting the data on it.

Some ransomware will try to spread to other machines too. Typically, it is spread by downloading malicious software and applications or by opening attachments in unsolicited or spoof emails. It may also be used by cyber criminals to hide evidence and cover the theft of data.

Back yourself up

Regular back-ups are the answer for all, whether as an individual on your home PC, using your work device or as an organisation.

Organisations

- Have a backup schedule that suits the needs of your company.
- Maintain multiple copies of backups.
- Protect backups from infection by ungrouping them from the network or by using an antivirus solution.
- Test your backups on a regular basis.

Individuals

- Make regular backups.
- You need multiple copies such as cloud storage **and** USB or external hard drive. If you rely on the cloud and this automatically syncs, you could infect your back up too.

How to protect from Ransomware

Organisations

- Train employees to identify malicious email attachments and the dangers of downloading from disreputable sources.
- Encourage staff to report problems as soon as they occur without fear of sanctions.
- Invest in firewalls which will block access to malicious websites and reduce the likelihood of malicious traffic entering your network.
- Use an email service that enables mail filtering.

East Midlands Special Operations Unit

- Restrict the use of plug-in device (such as USBs) where possible.
- Ensure that devices can only run applications from trusted locations.
- Invest in antivirus or anti-malware products and update this software.
- Use up-to-date operating systems and applications with the latest security features.
- Enable automatic updates for operating systems and applications where possible.
- Segregate the network virtually or physically to limit the spread of malware.
- **Develop** a business continuity plan – so that the organisation can continue to operate without IT services and recover as quickly as possible.

Individuals

- Be wary of emails that contain attachments and hyperlinks. Be very careful of any attachment that ends in **.exe.** This means it's a program and could be ransomware.
- Get anti-virus and keep it up-to-date.
- Install updates as soon they are available (turn on automatic updates). Updates fix security problems with your devices.

Hot topic

There have been a number of concerns raised about recent text messages.

"The Government has only sent one text message to the public regarding new rules about staying at home to prevent the spread of COVID-19. Any others claiming to be from UK Government are false."

"Criminals are able to use spoofing technology to send texts and emails impersonating organisations that you know and trust. We would remind anyone who receives an unexpected text or email asking for personal or financial details not click on the links or attachments, and don't respond to any messages that ask for your personal or financial details."

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.

Received a bogus email offering financial assistance from HMRC? Contact phishing@hmrc.gov.uk.