East Midlands Special Operations Unit

COVID-19 CYBER 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: EMSOU-Cyset@leicestershire.pnn.police.uk or your local Force protect team.

Today's topic is Safer Internet Day (SID)

Cybercrime knows no borders and criminals take advantage of the borderless nature of the internet to commit crimes globally. In an effort to combat this the SafeBorders project was initiated, resulting in the first global safer internet day in February 2004, it was celebrated in 14 countries.

Safer Internet Day (SID) has become a landmark event in the online safety calendar, on the second Tuesday of February each year. It is now celebrated in more than 170 countries across all continents, and reaches millions of people worldwide.

The Internet is a powerful tool with enormous opportunities for learning, enhancing skills and acquiring new knowledge, as highlighted especially during the COVID-19 pandemic. However, with opportunities come risks and the goal of SID is to raise awareness of the risks.

The pandemic has introduced new challenges to maintain a strong security posture. The reliance on technology is a double edge sword. On the one hand, it has made the storage, retrieval and manipulation of information remarkably simple opening vast opportunities to provide customer services and exploit market opportunities. On the other hand, it has introduced unparalleled threats to business operations. Here are some of our top tips for end users and organisations:

EMAIL

- ✓ Require strong, unique passphrases on email accounts.
- ✓ Turn on two-factor authentication on sensitive accounts.
- ✓ Encrypt sensitive emails and use digital signatures.
- ✓ Do not use personal email accounts for company business.
- ✓ Recognise phishing emails and avoid suspicious links or attachments.

East Midlands Special Operations Unit

USB's

- ✓ Scan USB's and other external devices for viruses and malware.
- ✓ Disable auto-run.
- ✓ Ensure USB's benefit from encryption.

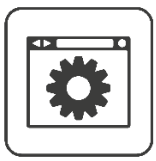
MOBILES

- ✓ Delete unnecessary apps and update the rest regularly.
- ✓ Only download apps from trusted sources and check reviews.
- ✓ Secure with passcodes/biometrics, such as fingerprint recognition.
- ✓ Turn off Bluetooth, GPS and Wi-Fi whilst not in use.
- ✓ Turn on remote wipe in case device is lost.
- ✓ Configure app permissions after downloading.
- ✓ Do not connect to unknown public networks - use a VPN or mobile data.

Wi-Fi

- ✓ Keep home Wi-Fi equipment out of sight from outside the property.
- ✓ Change default admin password, SSID name and SSID passwords.
- ✓ Restrict remote administrative management.
- ✓ Be mindful of signal radius.
- ✓ Keep firmware updated.
- ✓ Use separate Wi-Fi for guests, customers and business operations.

SOFTWARE /RESILIENCE



- ✓ Automatically update the operating system, browser and applications.
- ✓ Get rid of unused software.
- ✓ Review software that can be installed.
- ✓ Equip all machines with regularly updated antivirus software.
- ✓ Ensure regular backups are tested, encrypted and stored offline.

Reporting

Please report all Fraud and Cybercrime to Action Fraud by calling 0300 123 2040 or online.
Forward suspicious emails to report@phishing.gov.uk
Report SMS scams by forwarding the original message to 7726 (spells SPAM on the keypad).