East Midlands Special Operations Unit

COVID-19 CYBER AND FRAUD PROTECT MESSAGES

Friday 01 May 2020

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 Protect Team or your local Force protect team.

Today's cyber topic is Bring Your Own Device (BYOD)

BOYD, refers to an employee accessing company data from a personal device and has grown in popularity over the past few years. Many employees have devices of their own, such as a mobile phone or laptop and want use them rather than using a device issued by the organisation.

With the rise in cloud computing employees, using a web browser or a piece of client software, can access an organisation's sensitive data.

BOYD can be a real problem for any organisation that permits their use and the expression "Bring Your Own Disaster" is often heard.

How can an organisation be sure that a personal device is;

- Password protected
- Has anti-virus installed
- Updated & uses secure online connections
- Encrypted, tracked & can be remotely wiped if lost
- That organisation data is not being auto-synced to the employee's own cloud storage
- That organisation data is removed when the device is disposed with

Other potential problems arise if an employee leaves, will they agree to allow their device to be checked to ensure that no organisation data is on the device and in the event of an organisation reporting data loss.

Solving the problem:

A complete ban on the use of personal devices is one solution. However, this will involve issuing everyone who wants to work remotely with a company issued device and strict technical enforcement of system and data access.

Investing in Mobile Device Management software is another possible solution. MDM can enforce the use of passwords, encryption and push security updates. It can block certain apps, separate your data from the employees and even remove data if the device is lost. Employees will need to consent to the installation of an MDM app on their personal device.

MDM software can be a cost effective solution for some organisations. By allowing employees to use their own device, on their own plans and provider, organisations will not need to buy or maintain devices or force employees onto a specific platform or ecosystem.

East Midlands Special Operations Unit

One of the key factors when deciding on the approach is to review an organisations data policies. Classifying data and identifying whether it is protected by legislation or industry regulation is a first step. For business continuity an organisation should also identify the data that is most vital to running its business and train employees how to:

- Use anti-virus software and keep devices up to date
- Use a VPN to safely access an organisation's network
- Protect and handle information
- Mark data as sensitive before sharing
- Use two factor authentication 2FA
- Password protect files

Hot Topics

- COVID-19 themed phishing attacks are impersonating delivery services such as FedEx, UPS, and DHL claiming that packages are held due to lockdowns. The recipient is asked to either open an attachment or click a link, which deliver malware.
- Bogus texts from HMRC claiming the taxman has been forced to issue refunds due to coronavirus, and providing a link for recipients to 'calculate their refund'.
- Fake messages purporting to be from the government, requesting people pay a fine for breaching the coronavirus lockdown rules.
- Emails encouraging people to invest in bitcoin.
- Unsolicited calls from fraudsters offering to enrol vulnerable people on to coronavirus vaccine trials for a fee.
- Bogus texts purporting to be from TV licensing.
- Free or cheaper access to streaming sites is being offered, often via WhatsApp, only to find that victims are giving bank and personal details to fraudsters.

Webinar - Monday 4th May 2020 @ 1400 – 1500 hrs

This week's topic: **The Internet of Things – Protecting your devices, data, and home.**

Internet of Things (IoT) devices feature in many homes, but are also increasingly integrated into industry infrastructures. This session, and the themes covered are applicable to both individuals and businesses.

SW Regional Cyber Crime Unit will take you through a real life cybercrime investigation involving internet connected devices and the challenges that law enforcement faced to bring an offender to justice

To register for this event click on the following link - places are limited.

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.