East Midlands Special Operations Unit

COVID-19 CYBER AND FRAUD PROTECT MESSAGES

Thursday 28 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 topic is 'Cyber Essentials'

What is it and who is it for?

Cyber Essentials is a simple but effective government-backed scheme that will help protect organisations, whatever the size, against a whole range of the most common cyber-attacks.

Attacks come in many shapes and sizes, but the vast majority are very basic in nature and are carried out by relatively unskilled individuals. Think of them as the digital equivalent of a thief trying the front door to see if it's unlocked. There are two levels of certification offered:

Cyber Essentials self-assessment

This option gives protection against a wide variety of the most common cyber-attacks by addressing procedures and cyber security measures. Vulnerability to simple attacks can mark organisations out as a target for more in-depth and unwanted attention from cyber criminals and others.

Certification gives peace of mind that an organisations' defences will protect against the majority of common cyber-attacks. These attacks are looking for targets which do not have the Cyber Essentials technical controls in place.

Cyber Essentials Plus

Cyber Essentials Plus offers additional hands-on technical verification and certification of the procedures and security measures implemented in Cyber Essentials. Questions and answers about the scheme and certification can be found here.

What are the advantages of Cyber Essentials?

- Reassure customers that you are working to secure your IT against cyber-attacks.
- Attract new customers with the confidence that cyber security measures are in place.
- A clear picture of the organisation's cyber security level.
- Some government contracts require Cyber Essentials certification.

To bid for central government contracts, which involve handling sensitive and personal information, or the provision of certain technical products and services, organisations will require Cyber Essentials Certification. More information is available on the Gov.UK website.

East Midlands Special Operations Unit

Contact NCSC Cyber Essentials Partner the IASME consortium to get certified.

Hot topics

Reports have been received of emails purportedly from BMW in which recipients are told they have won a brand new BMW 5 Series and cash prize in a BMW COVID-19 lottery. Recipients are told to contact the claims department and send in their personal details.

Attempts by fraudsters to acquire information, which would support fraudulent applications for COVID-19 retail, hospitality and leisure grants have targeted organisations such as Lloyds Pharmacy, Greggs (bakery), Boots and Marston's Brewery. Each attempt uses the closure of premises or homeworking to justify the enquiry for information relating to; premises, reference numbers and/or extended retail discount. On closer examination the email addresses are not formatted correctly and website details and telephone numbers are incorrect. Always verify unexpected requests by other means.

Users of the QTS operating system (used in file sharing, storage, back up etc.) have been urged to update to the latest version as devices running older versions of the QTS operating system. These may be attacked through a number of vulnerabilities which, when chained together, would allow an attacker to gain remote access.

Webinar – Monday 1st June 2020 @ 1400 – 1500 hrs

Join West Midlands and Tarian Regional Cyber Crime Teams, as they host a free webinar on how to plan and prepare for a cyber incident.

About this Event

Despite best-efforts, data-breach incidents and cyber-attacks are always going to occur. The good news is that businesses and organisations have the power to control how they prepare themselves to deal with these events. Cyber incident response plans are essential in protecting business assets and reputation, whilst restoring critical services and capabilities. This presentation considers concepts when writing plans, testing and exercising. Identifying common gaps and learning outcomes from cyber incident exercises.

This presentation will help businesses owners and business continuity specialists prepare for a cyber-attack and respond effectively in a crisis.

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.

Report SMS scams by forwarding the original message to 7726 (spells SPAM on the keypad).