East Midlands Special Operations Unit

COVID-19 CYBER AND FRAUD PROTECT MESSAGES

Thursday 14 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 'Cloud Computing'

At a time when remote working is a key component for the survival of an organisation, cloud computing becomes an even more compelling proposition. The benefits of flexibility, mobility, disaster recovery and accessibility are just some of the potential gains that organisations may exploit. We have previously discussed the challenges organisations face when considering the cloud provider and we now focus on how to evaluate your business needs in the face of cloud computing.

Know your business requirements: Understand the intended use of the service. Consider issues such as availability and connectivity. Identify those risks which would be unacceptable to the organisation and those that would not.

Understand your information: Identify the information that will be processed, stored or transported by the cloud service. Understand the legal and regulatory implications.

Determine relevant security principles: Knowing the business requirements and identifying the risks you are/aren't willing to take will give a clear picture of the information exposed to the service.

With this information, determine which of the Cloud Security Principles are most relevant to your planned use of the service.

Understand:

- **How the principles are implemented:** Find out how the service claims to implement the relevant security principles. Different approaches result in different risks to consider. NCSC's detailed guide to implementing cloud security principles will help with this.
- **The level of assurance offered:** Can the service provider demonstrate that the principles have been implemented correctly?

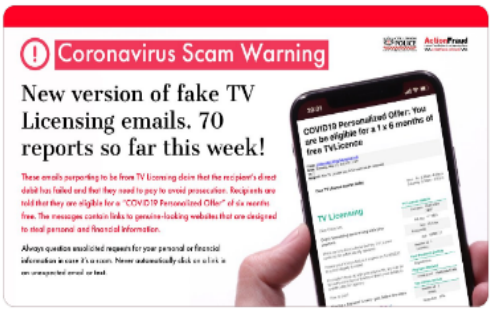
Some suppliers offer little more than promises, others provide contracts, and some engage certified, independent assessors to validate their claims. Reputable suppliers will generally be happy to provide you with information on how their products interact with internet-based services outside of your direct control, and any third party services they make use of.

Consider any additional measures the organisation can apply to help reduce risk to data and applications and decide whether any remaining risks are acceptable.

East Midlands Special Operations Unit

Monitor and manage the risks: Periodically review whether the service still meets the business and security needs. Continued vigilance in an ever changing environment is necessary to maintain the integrity of the systems and data.

Hot Topics



A new version of the fake TV Licensing emails has emerged, claiming the recipient's direct debit has failed and they need to pay, to avoid prosecution. These emails display the header ***"We couldn't process the latest payment from your Debit Card - COVID19 Personalized Offer: You are be eligible for a 1 x 6 months of free TV Licence"***. There is a link to set up a new direct debit on a website designed to steal logins, passwords and personal details.

Fake emails stating the government are offering "emergency COVID-19 tax relief" are still being sent. Recipients are asked to click on a malicious link to get a free evaluation.

Phishing attempts purporting to be from the World Health Organisation (WHO) offering cash grants to selected individuals, of $450,000. The recipient is asked to email the sender for more information on how to receive the funds, quoting reference W.H.O-511.

Even before it has been rolled out nationally, Phishing scams, have been seen that reference the government's new contact tracing app. Members of the public received texts informing them that they have come into contact with someone who has tested positive for COVID-19. The text contains a link to a bogus website which asks for the personal details of the user.

Webinar – Monday 18th May 2020 @ 1400 – 1500 hrs

Topic: The not-so Anonymous hacker - A perspective from the other side

In this one hour Webinar, Mike Jones, a former member of the Anonymous hacking group, will be answering your questions as he talks about his life before, during and after Anonymous.

- What makes someone turn to cybercrime?
- What life is like inside the world's most notorious hacking group?
- How can that experience help us now?

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).