East Midlands Special Operations Unit

COVID-19 CYBER AND FRAUD PROTECT MESSAGES

Wednesday 03 June 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 'Incident Response'

According to soldier and British military historian, Sir Michael Howard, "in preparing an army for war, you can be clear that you will not get it precisely right, but the important thing is not to be too far wrong, so that you can put it right quickly."

In the battle against cybercrime, an organisation can deploy as many preventive controls as planning and finance permits, and attackers will still slip through the net. It is the ability to detect and respond that determines how badly the business is impacted and why incident response (IR) preparation is so important.

1. **Develop policy:** To outline the authority and responsibilities of the IR team. This might include; the revocation of access rights, taking systems offline, reconfiguring them, purchasing equipment and services, accessing sensitive information and conducting forensic investigations. Ultimately, any delays will hinder recovery so outline responsibilities and the means to settle disputes well in advance.

2. **Communication Plan:** Who should the IR team contact in the event of a problem? When is contact appropriate and how should it be made? How will messages be communicated vertically and horizontally across the organisation or to external agencies? How will you be contacted by customers and suppliers? A good communication plan facilitates a realistic appraisal of the ongoing situation and avoids unhelpful speculation during difficult times.

3. **Define critical functions:** Which systems have the highest impact if compromised and how quickly should they be restored? What data would be the most damaging to lose and where is it located? Once you know what the critical functions are, you can prioritise money, time and IR effort protecting them.

4. **Define roles:** To maximise efficiency! Who can lead the IR team, or facilitate purchases? Who will liaise with HR when there's an insider threat or an internal breach of policy? Who has the expertise to deal with applicable laws, regulations and contracts, or the skill and diplomacy to communicate across the organisation and to external entities?

5. **Rate the incident:** To understand the gravity of the situation and elicit the appropriate response across the organisation.

6. **IT hygiene:** Network diagrams, build documentation, recovery procedures, up-to-date inventories and change control documents should be in order to efficiently sanitise, recover or rebuild infected system and operations.

7. **Ensure network visibility:** Logs must be collated, synthesised and evaluated to identify and track problems across the network. Check - Windows event and security logs, anti-

virus and firewall logs, as well as rogue accounts on the network. Alternatively, consider holistic solutions such as SIEM technologies.

8. **Business continuity:** Failing to prepare is preparing to fail. Develop work arounds for when there is a complete or partial loss of IT services. How will critical operations continue in the face of such difficulties?
9. **Train:** The identification and resolution of a problem needs an organised response. The IR team need to react to different situations calmly and with confidence which is why it is so important to practice IR by exercising or simulation.

Further advice on incident response, from the NCSC, can be found here

Hot topic

Cybercriminals have been busy establishing dozens of fake websites that impersonate the domains of popular UK supermarket chains. Thirty lookalike domains impersonating Tesco, 11 illegitimate domains impersonating Asda, and 10 recent spoofed websites impersonating Amazon have been uncovered. These fake domains can enable hackers to obtain names, addresses, email addresses, and payment card information of hundreds of thousands of shoppers in a very short time.

NHS Test and Trace phishing emails are being sent by scammers, the fake email refers to the service as 'track and trace'. The recipient is told they have been exposed to someone who tested positive for coronavirus. They are instructed to click a link to find out who it is, within 24 hours. If they fail to do so legal action may be taken and their benefits suspended.

Remember: Contact tracers will never ask you to:

- Dial a premium rate number to speak to us (for example, those starting 09 or 087)
- Make any form of payment
- Give any details about your bank account
- Give your social media identities or login details, or those of your contacts
- Disclose passwords or pins
- Create any passwords or pins
- Purchase a product
- Download any software to your device
- Hand over control of your pc, smartphone or tablet
- Access any website that does not belong to the government or NHS

Webinar – Thursday 4th June 2020 @ 1400 – 1500 hrs

Join Tarian Regional Cyber Crime Team, as they host a free webinar.

The most common cyber-attack vector for small and medium sized businesses is the Phishing email, during the COVID-19 pandemic Phishing emails have spiked by over 600%. Join us for a live demo of the Tarian Not2Phish training platform and learn how it has helped to reduce successful Phishing attempts in Welsh SMEs.

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).