East Midlands Special Operations Unit

COVID-19 CYBER AND FRAUD PROTECT MESSAGES

Tuesday 26 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 – Business Email Compromise (BEC)

Business Email Compromise (BEC) is a form of phishing attack. BEC attacks are crafted to appeal to specific individuals and can be even harder to detect than typical phishing emails. The attackers attempt to defraud the company, its customers, partners, and/or employees into sending money or sensitive data to the attacker's account.

Examples of BEC

- **The Bogus Invoice Scheme**: An attacker pretends to be the supplier and requests a funds transfer to an account the attacker controls. Companies with foreign suppliers are often targeted with this tactic.
- **CEO Fraud:** Attackers pose as an executive and send an email to employees in finance, requesting that they transfer money to a bogus account. Often requested as a matter of urgency and when the CEO may be otherwise engaged.
- **Account Compromise**: An executive's or employee's email account is hacked and used to request invoice payments to vendors listed in their email contacts.
- **Impersonation:** When a legal representative's e-mail address is used to contact clients, asking that they pay money to an account controlled by the attacker.
- **Data Theft**: Employees are targeted to obtain Personally Identifiable Information (PII) of employees and executives. Such data can then be used for future attacks.

Why BEC scams work

- An attacker will conduct research when targeting a company executive or employee (social media, LinkedIn, Companies House, accounts and website). This research makes the email more convincing to the recipient.
- The email contains no hyperlinks or malware attachments, which is usually identified and removed by traditional IT security systems.
- An attacker will spoof an organisation's name. For example, instead of using **johnsmith@trident.com**, they will use **johnsmith@tridant.com** – it can be hard to spot the difference.
- An attacker may monitor corporate communications to identify the best tactics and timing to employ for a successful attack.

Top tips

- **Training:** Train staff to identify fake emails. Always be sceptical of urgent and hurried requests to transfer money. Verify those requests either by phone or in person.
- **2-Step Factor Authentication (2FA):** 2FA will protect user accounts from being hijacked by an attacker. Usernames and passwords require us to 'know something' and we can prove who we are by 'having something', such as a pin sent to our phone.
- **DMARC:** This enables an organisation to verify that an email they receive aligns with what they know about the sender. The technology is extremely effective in eliminating spoofed emails. See here for more information
- **Secure Email Gateway:** This is your email ‘firewall’. It will stop spam, malware and viruses, but it can also be configured to hunt for key words such as ‘payment’, ‘urgent’, ‘sensitive’ and ‘secret’.
- **Add Warning Banners:** Most email systems can be configured to place warning banners on emails from new or unusual contacts, helping to mitigate the risk of lookalike domain spoofing.

Further information and infographic from the NCSC available here.

Courier fraud alert

There have been increasing reports of fraudsters contacting victims in the East Midlands area. The fraudsters claim to be a police officer using the names ; DC Andrews from Hammersmith Police Station or Paddington Fraud Prevention Team and DC Hunt of Paddington Police Station. Victims have been asked to purchase expensive goods (watches, jewellery etc) or withdraw cash or move funds to an account controlled by the fraudsters.

Webinar – Thursday 28st May 2020 @ 1400 – 1500 hrs

Join East Midlands Special Operations Unit, for a free Webinar on how to identify, respond and recover from cyber-attacks.

About this Event

The faster your organisation can detect and respond to a security incident, the less likely to have a significant impact on your data, reputation and finances. This presentation will help Business leaders and IT managers prepare for 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).