REPORT OF CICM EAST OF ENGLAND BRANCH LUNCH & LEARN WEBINAR ON CYBER CRIME BY CITY OF LONDON POLICE ON 28th OCTOBER 2025

Following his two previous insightful presentations Matthew Eccles of City of London Police's Cyber Griffin team was welcomed by host CICM East of England Branch committee member Steve Walsh of RSM Creditor Solutions.

Matt talked through a two year long case study based on real events (with names changed and redactions) which started with a post on X warning that a senior executive had been phished. Matt invited everyone to consider what they would do in this situation, e.g. respond to the X message, call the police, contact their IT department etc;

The company involved used open source intelligence and Google source to find that the organisation posting on X were reliable security researchers so the police were notified, who obtained the considerable detailed information held.

Using a sandbox the team looked at websites and several were identified as phishing. The email address being used showed in the browser as "dangerous", and a supposed SharePoint link was false.

Once the fraudsters had control of an executive's email account they sent a number payment diversion fraud emails to staff asking them to pay fake invoices, hoping that they would be paid without question - and sometimes they were. Replies to the executive who had been phished were diverted to their RSS folder rather than their inbox.

Reviewing the metadata the team coordinated with the Microsoft Digital Claims Unit who gave significant information about how the bulk phishing emails were being sent. The identities of both fraudsters was established by going through their ICQ chats after obtaining access to their iCloud accounts via a subpoena to Apple.

After answering many questions and being thanked by Steve, Matt closed by inviting all to contact his team for further information or advice, and with key takeaways:-

- check an incoming email address carefully, looking for anomalies e.g. full stops or additional letters
- look for a "dangerous" warning in the browser heading
- check any link by hovering over it for a few seconds to reveal the true originator's email,
- use official contact routes
- agree an "I will never" list with colleagues
- check your RSS folder regularly

- always "Stop, Think Fraud"

Richard Brown FCICM 6th November 2025

CICM East Of England Branch Vice Chairman, Secretary & Treasurer

(361 words)