Chartered Institute of
Information Security

Pulse:

March 2023

CIISec Live 2023

This year's flagship event will be held in Manchester.

Criminal Creativity

See just how complex and widespread this issue is across the globe.

Educating the next generation

Organisations are struggling to recruit the necessary expertise to protect and defend themselves.

Criminal Creativity

Most criminal activity has an underlying motivation which has been rooted in the same foundations across time. Criminals will be motivated by financial or personal gain and have evolved tactics, techniques and procedures to meet with current and future trends.

Phil Chapman

The digital era has provided criminals with a wide platform to conduct their activities and with the evolution of technology has come an adaptation of new methods to profit from criminal activity.

The past few years has changed us. Our working habits, our social activities and for some, our overall view on life has been impacted by the pandemic and ensuring socio-economic situations.

Cyber criminals are creative in how they manipulate their victims in accordance with these life-changing events. Social engineering is not a new technique and criminals will use all the tactics from old and tweak them to suit the current situation.

The pandemic saw a rise in phishing and other social engineering attacks against vulnerable victims by using our initial lack of understanding of covid and other health related issues and criminals fed off the fear and ignorance of individuals. Phishing, watering hole attacks and cyber-fraud all tweaked with a covid-19 slant.

The current economic climate also feeds new tactics to target individuals who are looking to either increase funds or save money to survive the current situation they may find themselves in. Cyber criminals will use all social engineering tactics and modify their technologies to meet this. For several years phishing and mandate fraud techniques have become far more sophisticated and spread across all communication and social media platforms.

Meet creativity with creativity and make your training sessions current, interactive, relevant and memorable. Highlight new techniques whilst reminding of the underpinning motivations of the criminal threat actors.

Cyber criminals are creative in how they manipulate their victims in accordance with these life-changing events. Social engineering is not a new technique and criminals will use all the tactics from old and tweak them to suit the current situation.

We live in a 'smart' world. Nearly everything can be done via the Internet or with a QR code. Cyber criminals see all of this technology as an opportunity. A recent report has identified the fraudulent use of QR codes on parking meters which take the unsuspecting victim to a scam site rather than the official parking app. Simple idea using smart technology by creative perpetrators.

We can employ technical controls to protect us. However, defence of our networks, people and organisations must have a multi-tiered approach. We cannot simply rely on technology to protect us. Physical controls the protection of our sites and physical assets but procedural controls are probably the most important aspect. Policies, Planning and Procedures are by far the least 'sexy' part of cybersecurity but are the mainstay of everything.

User training and awareness is always the right answer and constitutes one of the biggest defence mechanisms we can use to combat criminal creativity.

Meet creativity with creativity and make your training sessions current, interactive, relevant and memorable. Highlight new techniques whilst reminding of the underpinning motivations of the criminal threat actors. Numerous examples exist of current techniques, tactics and procedures to use in sessions and online training from organisations such as the NCSC provide great resources. You may also call upon your local, friendly police cyber protect unit to give you advice and guidance or make a creative memory with Lego!