

Be a Fraud Fighter – The Changing Face of Fraud

Fraudsters are using Digital Technology and AI as opportunities to carry out fraudulent attacks on individuals and organisations by harnessing new AI advances for their own gain.

INCREASING TRENDS



❖ **Scam clickbait:** Clickbait ad scams may include counterfeit products, campaigns impersonating brands or businesses by referencing or modifying the brand content in the ads, URL, destinations or misrepresenting themselves as the brand or business. If it seems too good to be true, it probably is!

❖ **Fraudulent Documents:** AI can be used to create convincingly realistic documents and data such as invoices, contracts, reports, spreadsheets, and bank statements to support a fraud scheme.

❖ **Email Phishing:** Phishing e-mails often closely resemble a legitimate source, requesting the recipient provide security data either directly or via clicking a link to a fraudulent website. Attackers deceive people into revealing sensitive information or installing malware such as ransomware



❖ **Fake Identities:** Generative AI can be used by fraudsters to create fake images and videos in order to create fake accounts and identities. Realistic looking photos can trick victims into thinking they are interacting with a real human to exchange money, goods and services.

❖ **ChatGPT – Friend or Foe?**

ChatGPT can be used by fraudsters to create phishing emails or messages that appear to be from legitimate sources.



These messages can be used to trick individuals into providing personal information or transferring money. ChatGPT can also be used to generate phone scripts, which can be used by fraudsters to impersonate others and trick individuals into providing sensitive information.

❖ **Synthetic identity fraud:** This includes the use of stolen data to create identity theft in which criminals combine both real and fake personal information to create a new, fictitious identity that can then be used for various identity-related schemes, such as obtaining credit or goods.

Stay alert and report any suspected Technology Fraud to ICS

Fraud Awareness Week

17 – 23 November 2024

**We're seeking fraud fighters.
Will you answer the call?**

