Generative Artificial Intelligence (AI) & Fraud

Generative AI & Fraud

Fraudsters may use generative AI to scam people and businesses

To help protect yourself, it's important that you understand the different ways that fraudsters can use the technology.

Generative AI is yet another tool that fraudsters can use to make their deception tactics more sophisticated. Given that this technology allows communication styles and likeness (video and audio) to be cloned – fraudsters can more easily impersonate people or business that you know and trust. **Some examples are below:**

- **Voice spoofing** – fraudster calls a member of a business pretending to be the CEO of the firm. They instruct the employee to make a 'secret' payment to a suspense account. Because the employee believes they are speaking to the CEO, they authorise the payment.
- **Deepfakes** – a fraudster may clone the full likeness of a member of a supplier company. Whilst pretending to be from the known supplier company, the fraudster may set up a call with the company paying for services and ask for a change in bank account details. Given that the colleague in accounts payable believes to have seen their colleague in the supplier company, they authorise the change in bank account details.

Do not assume a phone call or video call is genuine. Pay extra care if the individual is requesting sensitive information, requests you to make a payment to a new beneficiary or is making high-pressure demands.

Always have well understood procedures for paying new beneficiaries. These procedures should not be bypassed regardless of how much an employee 'trusts' the beneficiary.

What's Generative AI?

- Artificial Intelligence (AI) is technology that allows computers to perform tasks and make decisions like a human. AI tools make these decisions by learning, they do this by analysing large amounts of data and looking for patterns.
- These decisions improve as the AI tool takes in more data. With enough data, an AI tool can make decisions similar to how a human would.
- Generative AI uses similar technology to generate content. This content could be text, images, video and/or audio.

How can you protect yourself against these threats?

Generative AI enhances a fraudsters ability deceive their victims. That said, lots of existing controls remain effective for mitigating this risk. Some key controls are noted below.

Maintain usual fraud controls

- Be mindful of emails, phone calls, and videos that want you to act quickly – this is often a sign of a scam.
- Caution against requests for personal information, account information, and financial information. HSBC will not request this information from you.
- Ensure that, wherever possible, you only take payment instructions from approved company communication channels. Fraudsters will often have to contact victims via open communication channels like messaging apps, as they are unable to access approved company channels.
- Always check and validate information you receive in emails and/or online, especially in forums or open-source websites. If you're unsure, check with a line manager or a genuine HSBC employee.

Daily Security Codes

Daily security codes are unique, time-sensitive codes generated each day and distributed to authorised personnel. These codes can be used to authenticate communications and transactions, adding a layer of security that is difficult for fraudsters to replicate. Here's how they can be implemented effectively:

- **Unique Daily Codes:** Generate a unique code each day to be used by employees.
- **Secure Distribution:** Distribute these codes via secure channels such as encrypted emails, or through internal secure platforms. Do not share codes with anyone outside of the organisation.
- **Verification Processes:** Require the daily code to be presented during sensitive transactions, high-value communications, or any situation where identity verification is critical.

Human Oversight & Training

- **Human Oversight:** Maintain a level of human oversight for approving large or unusual transactions. Conducting business in person is not always possible but, for significant transactions, can act as a key control.
- **Deepfake Awareness:** Educate employees about the risks of deepfakes and how they can be used in fraud schemes.
- **Phishing Awareness:** Provide ongoing training to help employees identify and respond appropriately to phishing attempts, which are often the precursor to more sophisticated attacks.

Spotting A Deepfake - Additional Guidance

The rapid innovation in AI is likely to mean that deepfakes will become nearly indistinguishable from reality. Whilst these tips can help you to detect less sophisticated attacks, additional controls should be considered.

REMEMBER: Even if it looks & sounds like someone within your organisation, be sceptical if the request is unusual. It's always good to maintain a level of human oversight for approving large or unusual transactions.

1. Glasses may appear odd, reflect differently or even disappear.
2. The person's features may be positioned incorrectly or move unnaturally.
3. The person's skin or hair may appear blurry or move.
4. The audio might not sync or match the video. Listen out for changes in tone and volume.
5. The background might not fit the context of the call. It may show strange reflections or anomalies.
6. The lighting may seem off. There may be strange shadows.