

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 types of scams and what to look out for.

How could generative AI help fraudsters?

- **Enhanced email phishing** - While most phishing emails are still basic, fraudsters could use generative AI to create more sophisticated emails that are perfectly written, and even copy the tone of voice of trusted people or businesses. This could make phishing emails harder to spot.
- **Voice spoofing** - Voice spoofing (or voice cloning) uses generative AI to copy a person's voice. The copied voice can then say certain phrases or act as a chatbot. Compared to other scams, voice spoofing is rare. However, this technology could help fraudsters to enhance the effectiveness of their scams.
- **Deepfakes** - A deepfake uses generative AI to copy the appearance and voice of a person. Deepfake videos can be convincing, usually showing the copied person saying things they've never said.

What's 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, helping scammers to impersonate people or businesses.

How can you protect yourself against fraud facilitated by Generative AI?

Deepfakes enhance a fraudster's ability to social engineer their victims. That said, lots of existing controls remain effective for mitigating against this risk. Some key controls are noted below.

Maintain and review fraud controls

- 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.
- 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.
- 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 WhatsApp, as they are unable to access approved company channels.
- Perform call back to the number that is in your business' records, speak with your usual business counterparty and verify the information prior to executing transactions. Email confirmation may not be as effective, especially if the counterparty's IT or email systems are compromised.

Security Codes

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

- **Unique Codes:** Generate a unique code to be used by employees.
- **Secure Distribution:** Distribute these codes via secure channels such as encrypted emails, or through internal secure platforms.
- **Verification Processes:** Require the 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. Consider having meetings / negotiations for significant transactions in person.
- **Deepfake Awareness:** Educate employees about the risks of deepfakes and how they can be used in fraud schemes. Training should cover how to recognize potential deepfake attempts and the importance of adhering to security protocols.
- **Phishing Awareness:** Provide ongoing training to help employees identify and respond appropriately to phishing attempts, which are often the precursor to more sophisticated attacks.

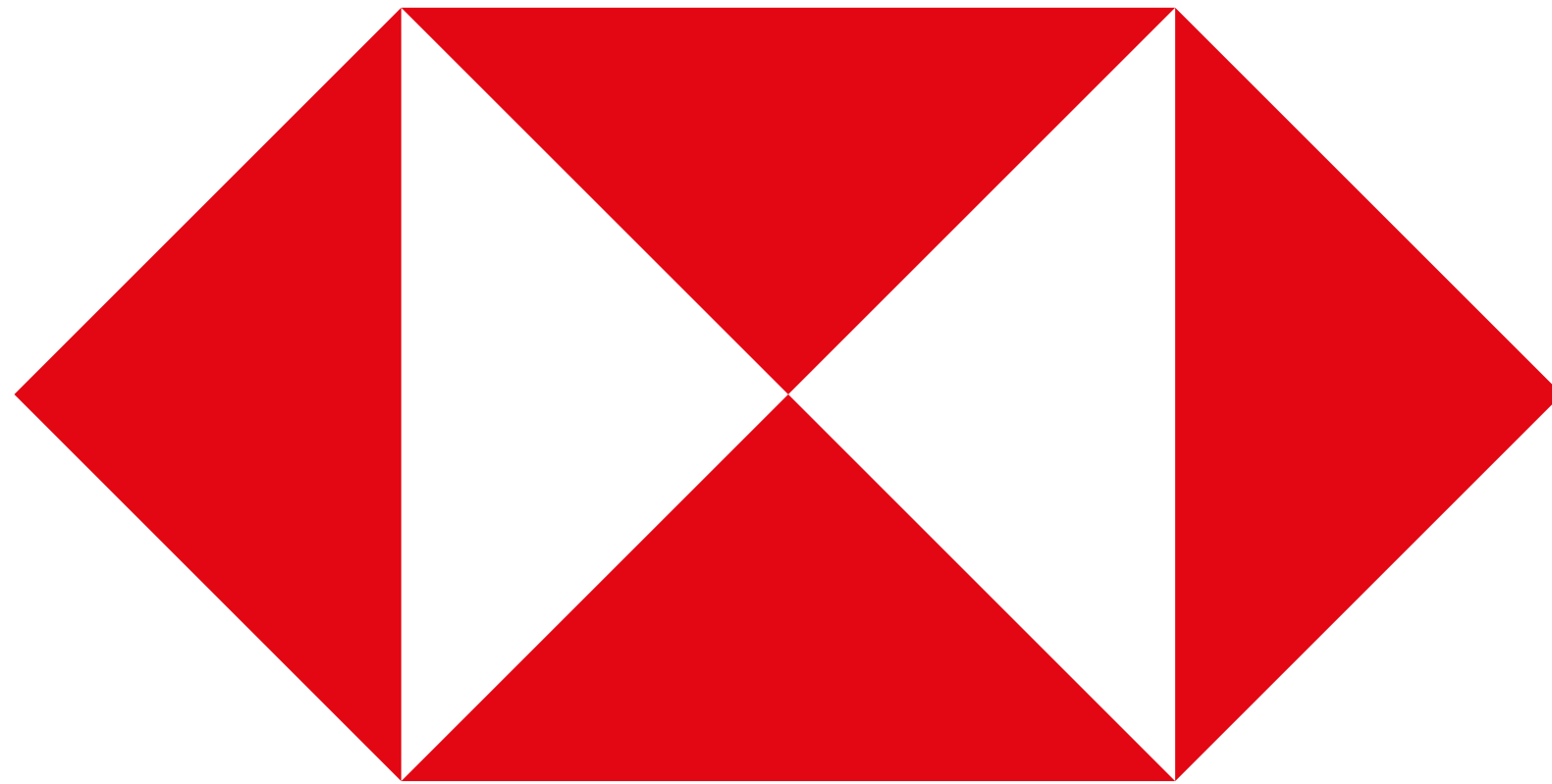
Spotting A Deepfake – Some Key Points



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



- 1 Glasses may appear odd, reflect differently or even disappear.
- 2 The persons features may be positioned incorrectly or move unnaturally.
- 3 The persons 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.



The Hongkong and Shanghai Banking Corporation Limited, Singapore Branch is sharing this guide (the "Guide") for information purposes only. The contents of this Guide are shared with you without any warranty of any kind and to the fullest extent permitted by law we do not give or make any warranty or representation of any kind, whether express or implied in respect of such information, for example we do not represent or warrant the Guide is sufficient for your purposes or requirements. Your use of this Guide is at your sole risk.

In no event shall we be liable for any damages, losses or liabilities, in connection with your use of this Guide or your reliance on any information in this Guide.

Issued by The Hongkong and Shanghai Banking Corporation Limited, Singapore Branch (UEN S16FC0010A). The Hongkong and Shanghai Banking Corporation Limited is incorporated in the Hong Kong SAR with limited liability.