Generative Artificial Intelligence (AI) & Fraud Awareness Guide

HSBC UK

Contents

Generative AI & Fraud **3**

What's AI? 3

What's the difference between traditional and generative AI? 3

How could generative AI help fraudsters? 3

How can you protect yourself against these threats? **4**

Maintain fraud controls 4

Consider using daily security codes 4

Human oversight and training 5

Spotting a deepfake - additional guidance **6**

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.

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 in a similar way to a human. This helps scammers try to impersonate people or businesses.

What's the difference between traditional and generative AI?

The difference lies in what it can do:

- **Traditional AI** – analyses data to make predictions.
- **Generative AI** – analyses data to create new content like text, images, and audio. An example of a generative AI tool is Chat-GPT.

How could generative AI help fraudsters?

- **Enhanced email phishing** - while most scam 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. Like voice spoofing, deepfake scams are rare. You're more likely to see a deepfake of a celebrity than someone you know personally.

How can you protect yourself against these threats?

Maintain 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, contact the company on a phone number from their official website.
- Be mindful of emails, phone calls, and videos that want you to act quickly – this is often a sign of a scam.
- Where practical conduct your business in person, especially if instructing large payments.
- Caution against requests for personal information, account information, and financial information; HSBC will not request this information from you.
- Make sure 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.
- Don't open unexpected attachments or links on emails and text messages. Never input sensitive information after clicking on a link, and if you need to open attachments use an up-to-date antivirus software to scan the files before downloading them.
- Don't be put off seeking a second opinion, make sure staff are comfortable to escalate concerns to a colleague or a manager.
- Check you have the latest security updates and patches, apply them as soon as they are available as weakness in systems can be exploited by criminals.
- Make sure employees are aware of their digital footprint and not oversharing personal information online. Criminals may use this to launch a personalised and sophisticated fraud attack using Generative AI.

Consider using 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 an additional 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.
- **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 and 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. Training should cover how to recognise potential deepfake attempts and the importance of adhering to security protocols.

  Here's a few things to look out for to spot a deepfake:

  — **Blinking** – a deepfake might not blink normally.

  — **Poor lip synching** – deepfake lip synching might be poor.

  — **Poor rendering** – a deepfake might have strangely lit teeth and jewellery.

  — **Blurred edges –** a deepfake may have flickering edges around their face.

  These tips are useful when looking at deepfakes in lab conditions, but spotting a deepfake online may be harder.

- **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

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.

Accessibility

If you need any of this information in a different format, please let us know. **This includes large print, braille, or audio.** You can speak to us using the live chat on our website, by visiting one of our branches, or by giving us a call.

There are also lots of other options available to help you communicate with us. Some of these are provided by third parties who are responsible for the service. These include a Text Relay Service and a British Sign Language (BSL) Video Relay Service. To find out more please get in touch. You can also visit: business.hsbc.uk/accessibility or business.hsbc.uk/contact-us.

business.hsbc.uk

HSBC UK Bank plc. Registered in England and Wales (company number: 09928412)**.** Registered Office: 1 Centenary Square, Birmingham, B1 1HQ, United Kingdom. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. Our Financial Services Register number is 765112.

Customer information: Customer Service Centre, BX8 1HB.