

HASE Fraud Prevention Guide

Protect your business against fraud & cybercrime

Fraud: protect your business

Fraud is one of the most common threats to businesses today.

Unfortunately, fraud can result in significant financial losses. Businesses of every size are at risk. This guide is designed to equip you and your staff to spot and prevent scams, and to take the right steps if you do fall victim.

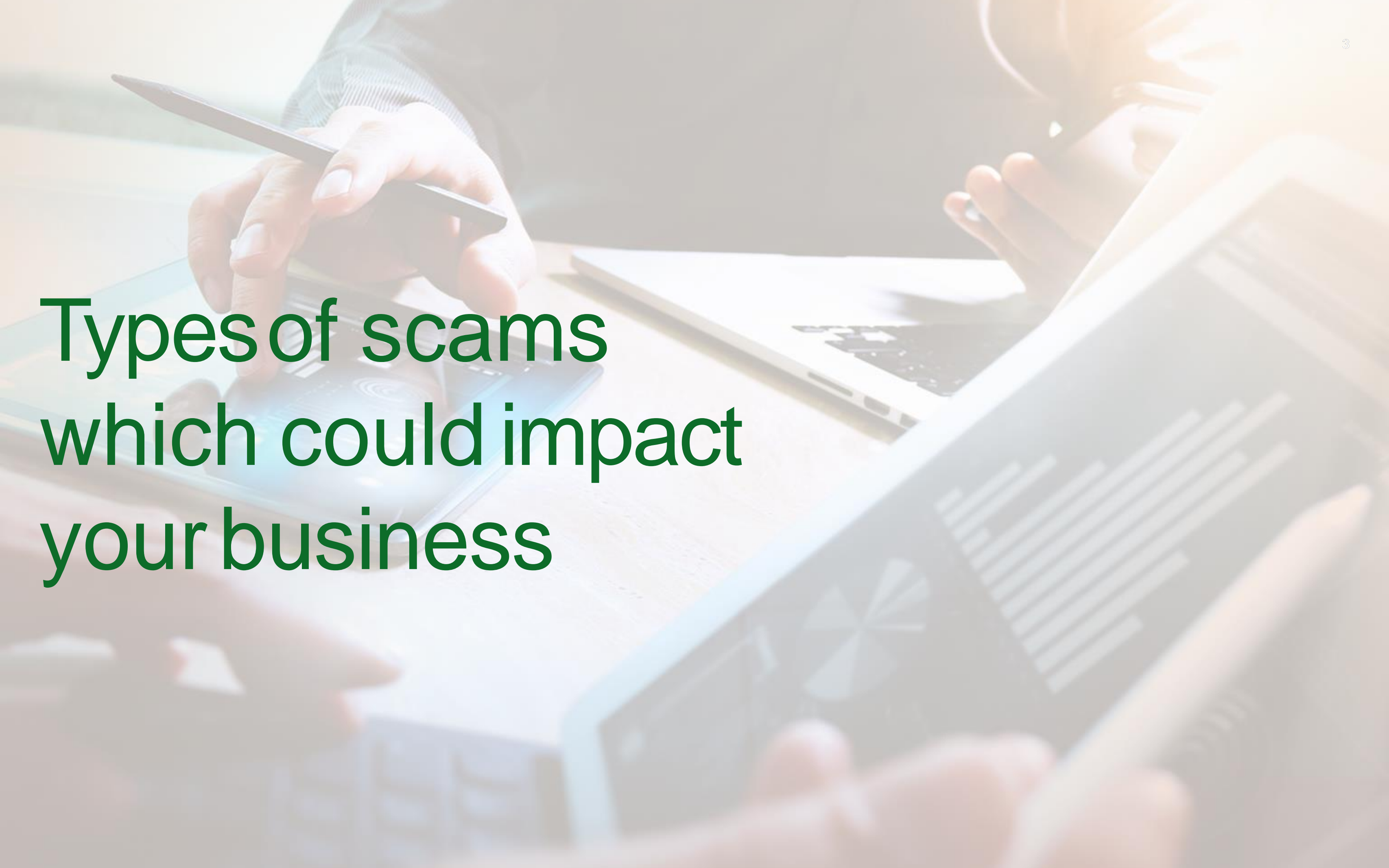


HKD2.69bn

The number of reported fraud case in Hong Kong increased by 65% in the first quarter of 2023 and by 42% in the second quarter of 2023 when compared to the same quarter of 2022. The total pecuniary loss amounted to HKD2.69 billion in the first half of 2023, which represents a 28% increase.

Source: Hong Kong Police Force

This guide will help you learn about common scams that could impact your business and outline some practical steps you can take to support with fraud prevention. Education on this topic across an organisation makes for a better protected business, and this guide provides a number of tips and checklists which can be shared across management and payment teams.



Types of scams
which could impact
your business

Fraud is a particular risk when making payments

- **Authorised Push Payment (APP)** scams happen when a business is tricked into sending money to a fraudster posing as a genuine payee.
- **Phishing** is a common theme in many APP scams. This describes attackers' attempts to trick users into clicking on a link that will download malware, for example, or direct them to a fake website.
- Phishing attacks may also seek to obtain sensitive information such as usernames, passwords and account details, by pretending to be a trusted contact or even your bank.



Business Email Compromise

Fake emails are a common tool used in scams.

When payments are due, criminals send an email designed to look and read like a genuine message from a supplier. They tell you the bank details for your payment have changed, provide new details and request payment.

These can be hard to spot:

- The attackers often use the vendor's regular email address, or a spoofed email address which looks just like the legitimate address.
- They will make invoices look authentic.
- There may be no perceptible difference in the vendor employee's email signature or communication style.
- In some circumstances, the attacker may have gained access to the inbox, so it will be coming from an authentic email address. They attacker will have access to the email chain and will be able to reply using similar language & tone.
- Perhaps most importantly – often the payment they are requesting is actually due.
- Often the only difference is that the business's bank details have changed.



How does email compromise happen?

Email account takeover

- The attacker uses hacking, or stolen account credentials, to gain access to a corporate email account.
- Account details may have been gained through a phishing attack or a data breach.
- The criminal may gather information about the user's contacts, email style and personal data to make their messages more convincing.

Email impersonation

- The criminal sets up an account with a very similar address to the real one.
- Or they may use a spoof email envelope and header, hoping the recipient will not notice and engage with it as with a legitimate message.

CEO fraud

Criminals impersonate a senior manager in the company.

- They send an email to the accounts department, requesting that a large payment be made urgently. This could even be for an acquisition or other important transaction.
- They often time this so that the manager they are impersonating is away, and the details difficult to verify.
- Again, the email account may have been compromised through phishing or data breach, and information gathered through company websites or social media.

Other Common Attack Types

Vishing, Telephone Scams

Phone scams, or vishing, are when a fraudster calls pretending to be your bank or another trusted organization. Nowadays with Artificial intelligence (“AI”) technology (e.g. Deepfake), image can be synthesized to create falsified videos. Besides, Deepfake has extended its application to sounds in which your voice can be mimicked by deep fake technique to create different conversations by capturing your voice of 5 seconds. With deepfake images and sound, one can fabricate videos that never exist. Fraudsters can even make their call appear to come from a number you know and trust or impersonate the voice of someone you know to direct your company to transfer money to a third person bank account. This is known as Phone Number Spoofing.

They can sound very convincing and may already know some of your personal information, such as your account number or address. If you feel uncomfortable, or sense something is wrong, don't be afraid to end the call.

You can always call the organisation on a number that you know, such as the number on the back of your bank card.

Fraudsters can keep the line open and even spoof a dial tone, so try to use a different phone, or wait at least 30 seconds before making your call.

Typical examples include:

- ‘Your bank’ advise you that your account is at risk, and you need to move your money to another account to keep it safe.
- ‘Your bank’ needs your help to investigate a fraud.
- Your internet or mobile provider calls you to fix a problem you haven't reported.

A bank can already transfer funds at your request and would never ask for your passwords, PIN, any One Time Passcodes or secure key code.

Other Common Attack Types

Deepfake Technology

Deepfake utilizes advanced deep learning techniques, specifically generative AI, to imitate the appearance and voice of individuals, creating synthetic media. This technology can be used to deceive others, particularly by impersonating the high-level executives, such as the CEO, CFO or senior management within your organization or business partners. Deepfake can be disseminated through various channels, including voice message, phone calls or video calls.

Deepfake voice and video can be convincing, usually showing the copied person saying things they've never said. The messages are often urgent in tone, asking for sensitive information, and or requesting that action be taken outside of normal protocols.

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

- Blinking- a deepfake might not blink normally.
- Glare- a deepfake might not reflect the natural physics of light perfectly from glasses.
- Unnatural facial movement– a deepfake may have jerky or mechanical facial movement.
- Poor lip synching- deepfake lip synching might be poor.
- Poor rendering- a deepfake might have strangely lit teeth and jewelry.
- Blurred edges- a deepfake may have flickering edges around their face.
- Ask questions- Test the participants' identity when encountering a suspicious video calls.

Account takeover fraud

Fraudsters may contact you via telephone, often from “spoofed” telephone numbers displaying the HASE telephone banking number or that of the company they are purporting to be. Fraudsters know company practices inside out and will take you through the process you would expect in order to gain trust. For example, a verification process.

They will then use various methods to trick you into providing them with security details such as usernames, passwords, secure key codes. Fraudsters can then use this information to successfully take over your account and pay funds away.

Remember:

- HASE will never ask you for card PIN numbers, passwords or secure key codes.
- Never disclose secure codes to anyone.
- HASE will never ask you to move money into a secure account.

Preventing fraud



Minimise fraud risk

There are steps every business can take to minimise fraud risk that do not need to be complicated or expensive.

- Foster a sense of vigilance in the parts of your business that could be vulnerable.
- Educate employees about how to identify and avoid scams, and make sure they are aware of the company's security policies and procedures.
- Critically, **any new payee or account details need to be verified.**
- Query any request that is unusual or out of context.
- The next few slides provide more detailed guidance to support individuals responsible for payments.



Check the email address

Fraudsters will pose as reputable individuals.

- If the name attached to the email is familiar (someone you know or regularly correspond with), check to be sure the email address matches.
- If it's a co-worker, the email address should be listed in the company email directory (if you have one).
- Be sure the domain name is spelt correctly. Often, fraudsters will create fake domains that closely resemble the real one, but will alter a letter or two hoping that recipients don't notice. For example, J@rnbusiness.com vs J@mbusiness.com.
- Be aware that the displayed name can be hiding the actual sender's email address.

Check the email thoroughly

Urgency is a red flag.

- Treat any email relating to payments as suspicious if it uses urgent language or provides excuses for the lack of a call back option.
- Some phishing emails are poorly written. Even if the spelling is correct, they often contain poor grammar. Treat external emails with extreme caution, especially those containing links or attachments. Be aware that Generative AI is making it easier for attackers to create convincing malicious emails.
- If you are not expecting the communication and/or do not recognise the sender, **do not click links or open attachments.**

Verify new payee or change of account details

Check with the instructing party using known contact details.

- Where possible, try to speak to someone you know. For example, if the change request is coming from someone within the business, try to confirm it directly with that individual by telephone. If it is from a supplier, speak to your normal contact by telephone.
- **Don't reply to the email or use contact details within the email.**
- Often, cybercriminals are sending phishing emails to individuals in the contact lists of the account to which they've gained access. That means you may recognise the sender because the email address is accurate, though the message itself is suspicious. Calling your contact verifies the request in the email. It may also alert them that their email account has been compromised.
- When you encounter suspicious calls, email or online sellers, etc, you can enter the platform name or number, payment account, phone number, email address and URL, etc via an anti-fraud search engine mobile APP "Scameter" launched by the Hong Kong Police. It could instantly check if the input information is related to any scam report and to assess the risk of fraud and cyber security.

Preventing fraud

Fraud can happen to any type of business and in many different ways. Luckily there are steps you can take to help protect your business against fraud and cybercrime. Here's a round up of some top tips and useful checklists you can utilise to help mitigate fraud risk within your business.

Top tips



Create and embed clear security procedures for payment teams

Ensuring all payments are properly validated is the most important action in fraud prevention. Create a procedure to prevent payment teams authorising new or amended payments without proper validation. Following this procedure should mean that payment teams never move money based solely on unverified email or telephone instructions, even when they appear trustworthy. Best practice is to encourage staff to contact payees directly to confirm new or amended payment requests.



Raise employee awareness

Provide employees with adequate training. Fraud awareness is everybody's responsibility within an organisation. Create a risk-based culture and have a procedure for staff to escalate concerns to management. Staff should feel able to challenge and query instructions.



Encourage all staff to think before they click

It's fine to click on links when you're on trusted websites. However, avoid clicking on links that appear in unverified emails and instant messages. If you hover over a link, you will be able to see the hidden URL and verify its legitimacy. Double check email addresses, and look out for poor spelling and grammar before clicking on any links or downloading any attachments.



Strengthen your passwords

Consider password managers or using a passphrase – a string of words that is typically longer than a traditional password. Passphrases are easy to remember but very difficult to crack. Encourage employees to choose three random words and to select a mixture of alpha-numeric characters and symbols.



Know what do in an event of a fraud/cyber-attack

If you or your company fall victim, it's important to act quickly. Reporting known or suspected security incidents helps protect the workplace. Contact your financial institution

Checklist: Senior Management

The most cost-effective way to limit the impact of fraud is to prevent it from occurring in the first place. This checklist is designed to help provide some key tips for keeping your business safe.

- Does your business have procedures that require validation of new or amended payment instructions? Do staff know where they can source known contact details?
- Have you got protocols around how, who and by what means staff can request payments to be made and how these can be verified if there are concerns?
- Are passwords of a suitable strength (e.g., minimum character lengths, use of alphanumeric and symbols). Have you considered using a password manager or mandate the use of passphrases?
- Has two-factor authentication been considered and applied where possible?
- Do your staff know what to do in the event of a fraudulent payment being sent?
- Do you have an incident response plan for cyber incidents, i.e., a compromised email address?
- Do you regularly discuss the potential risks of fraud with individuals submitting payments?



Checklist Two: Processing Payments

It is important to adopt a general mindset of awareness and action in the parts of your business that could be vulnerable. The checklist below has been created to support individuals responsible for making payments and to harbour a culture of fraud awareness.



Check that the email address is legitimate

If the name attached to the email is familiar (someone you know or regularly correspond with), check to **be sure the email address matches**. Fraudsters will pretend to be reputable individuals. If it's a co-worker, the email address should be listed in the company email directory (if you have one). Also, be sure the domain name is spelt correctly. Often, fraudsters will create fake domains that closely resemble the real one but will alter a letter or two so that the recipients don't notice. E.g., J@rnbusiness.com vs J@mbusiness.com. Be aware that the displayed name can be hiding the actual sender's email address.



Check the email thoroughly

Any email relating to payments or accounts that uses urgent language or provides excuses for the lack of a call back option should be treated as extremely suspicious. Some phishing emails are poorly written. Even if the spelling is correct, they often contain poor grammar. External emails should be treated with extreme caution, especially those that contain links or attachments. If you are not expecting the communication and/or do not recognise the sender, **do not click any links or open any attachments**.



Verify all new payees and all requests to change account details

Check with the instructing party using known contact details. Where possible, try to speak to someone you know. For example, if the change request is coming from someone within the business, try and confirm it directly with that individual by telephone. If it is from a supplier, speak to your normal contact by telephone. Don't reply to the email or use contact details within the email. Often, cybercriminals have gained access to someone else's account and are sending phishing emails to individuals in their contact lists. As such, you may recognise the sender because the email address is accurate, though the message itself is suspicious. Calling your contact verifies the request in the email and may also alert them that their email account has been compromised.



Check the risk of fraud and cyber security via "Scameter"

When you encounter the suspicious calls, emails or online sellers, etc., you may enter the platform account name or number, payment account, phone number, email address, URL, etc at mobile APP "Scameter" to instantly check if the input information is related to any scam report and assess the risk of fraud and cyber security.



Is the request unusual or out of context?
Does it make sense?

What to do if you fall victim





If you fall victim to fraud

Act immediately to minimise the damage from fraud and to ensure the best chance of recovering funds.

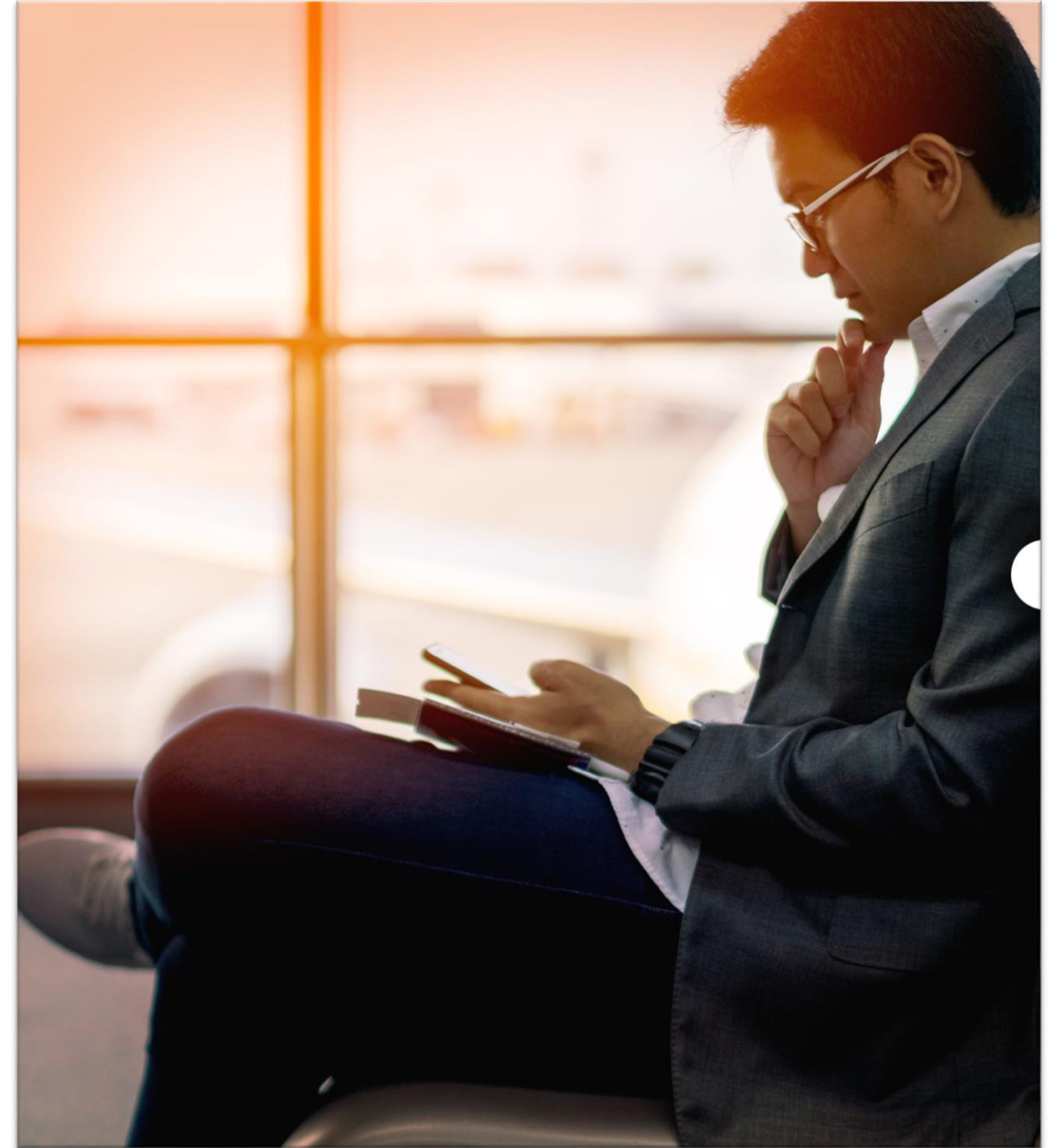
- **Stop all communication** with the scammer.
- **Alert any relevant parties** (employees, customers, and financial institutions). It is extremely important to contact the bank with a view to initiating a payment recall as soon as possible. Funds move very quickly and it can be very difficult to get funds returned once they have gone.
- **Report the scam** to the appropriate authorities.
- **Review your financial records** to identify any unauthorised transactions or suspicious activity.
- **Keep all documentation** related to the scam, including emails, invoices and any other correspondence.
- **Review and update your security policies** and procedures.

Reporting fraud to HASE

If you believe there is a fraudulent bank transfer or bill that you didn't authorize OR if you've authorized a bank transfer or bill payment and now believe you've been the victim of a scam, you can contact us 24 hours a day, 7 days a week via:-

- (852) 2198 8000 if you're calling from Hong Kong
- 4001 20 8288 if you're calling from the Mainland China

We recommend you also report the fraud case at the nearest police station or online at [police.gov.hk](https://www.police.gov.hk). or dial 999 for emergency, keep the local police force case reporting number and notify us by calling the above numbers.



If you suffer a cyber attack

- **Disconnect the affected devices** from the internet to prevent the spread of malware or further unauthorised access.
- **Change the passwords** for all affected accounts, including email, network, and any other accounts that may have been compromised.
- Use a reputable security firm to **conduct a full audit** of your systems to identify any other vulnerabilities or breaches.
- **Alert any relevant parties**, such as employees, customers, and regulatory authorities, and provide them with any necessary information.
- **Determine the source** of the attack and take steps to prevent similar attacks in the future.



Jargon buster



Fraud and cyber terms you need to know

- **Anti-Virus** – a computer program used to prevent, detect and sometimes remove malicious software.
- **Bring Your Own Device (BYOD)** – a policy implemented by businesses that allows an employee to use their own personal electronic devices for work purposes.
- **Common Vulnerabilities and Exposures (CVE)** – a publicly available list of known security vulnerabilities, indexed with unique ID numbers, descriptions and references.
- **Cryptocurrency** – peer-to-peer decentralised, digital currencies that are traded like a commodity.
- **Cyber-attack** – malicious targeting of computer systems, networks, infrastructures or devices.
- **Cyber incident** – defined by the National Cyber Security Centre (NCSC) as a ‘breach of a system’s security policy in order to affect its integrity or availability and/or the unauthorised access or attempted access to a system or systems; in line with the Computer Misuse Act (1990)’.
- **Dark web** – the portion of the internet that isn’t indexed by a search engine and is only accessed with special permissions or software.
- **Digital footprint** – a trail of data left behind after internet use. This can include passive information such as stored cookies, or information that’s been actively placed on the internet, such as social media posts.
- **Encryption** – the process of mathematically scrambling data. This data can be encrypted at rest, like data saved to a hard drive, or in transit, like data sent via HTTPS between your web browser and your bank’s server. Encrypting data doesn’t make it invisible to malicious cyber actors; it simply converts it into useless, unintelligible gibberish.
- **Firewall** – a network security system that monitors and controls incoming and outgoing network traffic based on a set of rules.
- **Hacker** – a person engaged in a wide range of computer network exploitation (CNE). ‘Black hat’ hackers generally conduct malicious CNE, whereas ‘white hat’ hackers conduct CNE for the benefit of cyber defences.
- **Malware** – an umbrella term for a wide variety of malicious code designed to accomplish nefarious goals such as providing remote access, loading or dropping additional malware, stealing bank information, encrypting and denying access to data, or hijacking a device’s computing power.
- **Patching** – process of updating an existing software or hardware to fix known bugs and vulnerabilities.
- **Penetration testing (pen testing)** – a process used by organisations to probe their own security with tactics used by cyber threat actors, usually conducted by ‘red teams’ or teams of professional white hat hackers.

- **Phishing** – usually conducted via email, this is a message designed to trick the recipient in to disclosing sensitive information, click a malicious link and/or open a malicious attachment. Phishing is often used to establish initial access on a device or network.
- **Ransomware** – a type of malicious software that blocks or otherwise restricts access to data under the promise that the restriction will be removed once a ransom has been paid.
- **Smishing** – a phishing message via SMS/text message.
- **Social engineering** – the manipulation of people to perform an action, usually to disclose personal information.
- **Spear phishing** – a phishing message that has been directed to a specific person or select group of people.
- **Trojan** – malware disguised as a seemingly innocent file or program in an effort to convince a potential victim that it can be opened safely. Trojans are very common and are frequently delivered via phishing emails or loaded by other malware called 'loaders'.
- **Two-factor authentication (2FA)** – a process of authentication where a user is required to have two factors, such as a known password and a one-time passcode (OTP). Generally, these factors are categorised as something you know (a password), something you are (a fingerprint), or something you have (a key card).
- **Virtual Private Networks (VPN)** – allow for secure private connections over public infrastructure, originally developed for use by organisations to authenticate the employee to internal network resources like email servers or shared folders. Today, consumer VPNs are increasingly used by individuals to create encrypted connections to a VPN server of their choice and use that server to connect to other internet resources.

- **Vishing** – a phishing attempt via phone call with a heavy use of social engineering.
- **Zero-day vulnerability** – a vulnerability identified prior to a patch or update being issued. Malware that exploits such a vulnerability is commonly referred to as a zero-day exploit.





恒生銀行
HANG SENG BANK

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 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.

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. This helps scammers try to impersonate people or businesses.

How can you protect yourself against these threats?

Deepfakes enhance a fraudsters 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 usual fraud controls

- Always check and validate information you receive in SMS, emails and/or online, especially in forums or open-source websites. If you're unsure, check with a line manager or a genuine HASE employee.
- Be mindful of SMS, 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, HASE 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 WhatsApp, as they are unable to access approved company channels."

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 protected:

- Never disclose any of your authentication methods to unauthorized persons including passwords, one-time security codes and one-time passwords (OTPs) sent to your registered mobile or security devices.
- Secure Distribution: Distribute these codes via secure channels such as encrypted emails, or through internal secure platforms to authorized person where necessary.

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. 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.
- **Simulated Attacks:** Use simulated phishing attack to help employee recognise and respond to fraudulent communication.

Spotting A Deepfake - Additional Guidance



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.



恒生銀行

HANG SENG BANK