HSBC Anti-Fraud Handbook

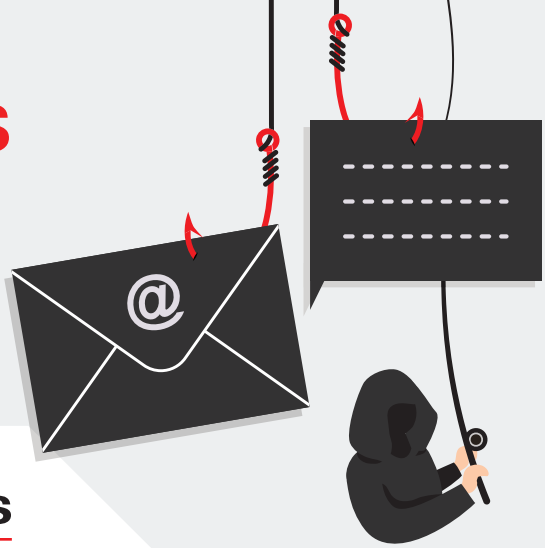
Stay Informed, Stay Protected

Make use of Scameter+ App for verification

滙豐
HSBC

Phishing SMS and Emails

These are some of the most common ways used by scammers to trick you.



Common Tactics

❶ Impersonating Reputable Organisations

Scammers often pose as government agencies, banks, payment platforms, or insurance companies, using excuses like “expiring reward points,” “failed auto-payment,” “insurance policy expiry” or even claim that you’re eligible for a tax refund, urging you to enter fake websites to steal your sensitive personal information.

❷ Fake Account Verification via Messaging Apps

They may claim that your account isn’t verified and prompt you to input personal details - including a verification code. This allows them to hijack your messaging account and request money transfers from your friends and family.

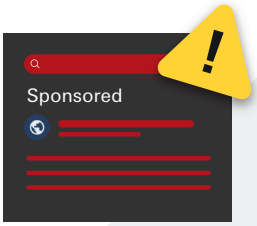
Anti-Scam Tips

- Your bank will never send you hyperlinks where you’re required to enter any sensitive personal information or log into your account. Always open your own banking app or enter the Bank’s website yourself when using online banking service.
- Pay attention to SMS Sender names; registered SMS sender IDs start with “#” (not applicable to 2-way SMS).
- If a friend or family member requests a transfer, call to confirm before taking action.
- Never share sensitive information such as verification codes, one-time passwords (OTP), or bank account details.

Phishing Websites

Learn to differentiate between a real website and a convincing fake.

Common Tactics



❶ Fake Websites Placed Through Paid Ads

Scammers pay to advertise fake websites as top results at online search engine. Victims may mistake the authenticity and unknowingly provide sensitive personal information.

❷ Impersonating HSBC Websites

Fraudsters create fake HSBC websites, offering banking services like investments or time deposits. They trick users into making transfers, stealing critical information such as bank account details and credit card numbers.

Anti-Scam Tips

- Never transfer money to unknown individuals or organisations.
- If you see an offer from the bank that appears to be ‘too good’ you can check with us via our customer hotline, chat with us on mobile / online banking or visit our branch.
- When using HSBC online services, ensure the domain is correct. It’s best to manually enter: https://www.hsbc.com.hk

Online Shopping Scams

Shopping online should be enjoyable, but chasing bargains can quickly turn excitement into regret.

Common Tactics

1 Shopping Scams

Fraudsters use fake social media pages and trading platforms with various excuses to lure victims into downloading apps with malicious software. This allows them to infiltrate your phone, steal data, and could even give them access to your apps to make unauthorised transfers from your account.

2 Travel Booking Scams

Scammers may pose as major travel agencies, offering fake deals on flights or hotels. They use fake customer service officers or photos to trick victims into making payments.

3 Online Marketplace Scams

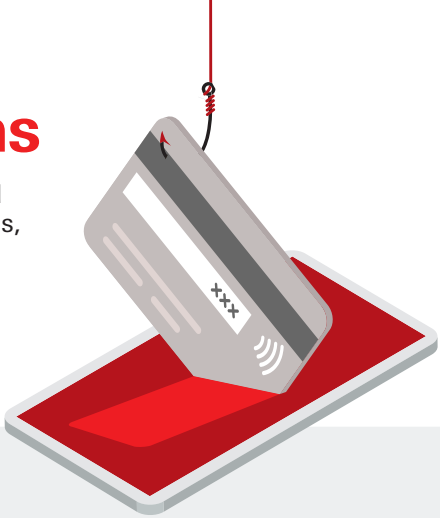
Scammers post enticing offers, demand upfront payments but vanish after receiving money. Others act as fake buyers, sending counterfeit payment confirmation emails which lead you to a fake website to steal personal details or even take over your digital banking access.

Anti-Scam Tips

- Be cautious of deals that seem too good to be true.
- When buying off a marketplace, try to not pay upfront for goods. If the seller is unnecessarily demanding, then consider cancelling the purchase.
- Avoid paying on unofficial websites – always check if you're using the authentic site.
- Verify merchants' identities and profiles (such as registration history, positive reviews, contact information).
- When selling items online, always use reliable payment channels like cash and Faster Payment System (FPS).

Credit Card Scams

If your credit card number, expiry date, and security code fall into the hands of criminals, the information can be misappropriated, potentially leading to financial loss.



Common Tactics

❶ Fake Online Deals

Scammers lure victims with enticing deals on packages or tickets, redirecting them to fake websites to steal credit card details.

❷ Beware of Specific Courier Companies

Scammers impersonate "buyers", insisting on using specific courier services. They send fake notifications claiming payment has been made, instructing victims to enter critical details such as bank account information, passwords, and OTPs on fraudulent websites to complete the "transaction."

Anti-Scam Tips

- Block your card immediately via the HSBC HK App if you suspect fraud on your credit card.
- Temporarily disable online transactions on your credit / debit cards when not in use.
- Set a monthly limit for online spending to prevent unauthorised large transactions.
- If you spot a suspicious transaction, raise a dispute immediately through the HSBC HK App.
- Safeguard your physical credit card and avoid entering OTPs casually. Enable HSBC HK App Online Transaction Authentication Service to authenticate online transactions.
- If you get a notification for a transaction that you didn't authorise, contact the bank immediately.

Impersonation Scams: Law Enforcement

Scammers may pretend to be police officers, judges, or prosecutors, using elaborate tactics to exploit emotional vulnerabilities and manipulate victims with excuses and psychological tricks.

Common Tactics

❶ Impersonating Mainland Law Enforcement Agencies

Beware of scammers alleging that you're involved in money laundering, spreading misinformation, or have violated mainland laws. They will ask for your account details and huge amount of guaranteed money, otherwise you (or family members) will be prosecuted or restricted from returning to the mainland. They may even use internet telephone (VoIP) spoofing to fake official caller IDs, luring you into their trap.

Anti-Scam Tips

- Be wary of suspicious calls, and never disclose your banking or personal information to strangers.
- Mainland law enforcement officials will never request personal information or transfers via phone calls.
- Scammers may have your personal details via unlawful means. Even if scammers know your details, it doesn't imply their identity is authentic.

Impersonation Scams: Fake Customer Service

Customer service is available to help you when you contact them—but what if they proactively reach out? Scammers posing as customer service officers can quickly turn from being "helpful" into “harmful”.

Common Tactics

❶ Fake Online Shopping / Payment Platform Customer Service

Scammers claim that you’ve subscribed to a paid service or VIP membership, and you’ll need to provide banking details for cancellation to avoid autopay. Victims will be redirected to fake "bank staff," who request sensitive information and demand fund transfers.

❷ Fake Bank Customer Service

Fraudsters impersonate bank staff, falsely claiming there are issues with the account, or it may be frozen, tricking victims to share online banking passwords or click on password reset links, ultimately taking over their accounts.

Anti-Scam Tips

- Never tap on links from suspicious messages, emails, or websites, and download unknown software.
- If your password or sensitive personal information has been compromised, contact us immediately, check for suspicious transaction records, and update your password.
- Use the details provided on the official bank website, app or the hotline details available on the back of your banking cards.

Impersonation Scams: Tech Support & Deepfake

For scammers, helping others is just a guise for fraud. Don't let their kindness fool you—stay vigilant against fake support schemes!

Common Tactics

1 Fake Tech Support Personnel

Scammers use pop-up messages, bogus calls, or phishing emails claiming service interruptions or detection of illegal activities. They urge victims to call hotlines or install a specific software, which grants remote access to devices, allowing them to steal sensitive personal data or take control of online banking.

2 Fake Corporate Executives or Government Officials

Fraudsters leverage Deepfake technology to create convincing videos, impersonating senior executives or government officials. They use these videos to pressure victims via email or instant messages to transfer funds.

Anti-Scam Tips

- Never tap on links in pop-up messages or call numbers provided.
- Avoid transferring funds to unknown accounts or sharing personal details and remote access permissions with strangers.
- Never download apps outside of the official app store.
- Run regular malware and virus scans on your device to identify potential security gaps.
- Do not open or download or install any files or attachments unless you are confident that they are from a safe and reliable source.
- Even if you think you know the sender, keep an eye out for deepfakes - pay close attention to the person's voice, tone, expressions, and any signs of editing or blurriness.

Cryptocurrency Investment Scams

Haste makes waste! Rushing to invest may result in financial loss.

Common Tactics

1 "Low-Risk, High-Return" Investment Platforms

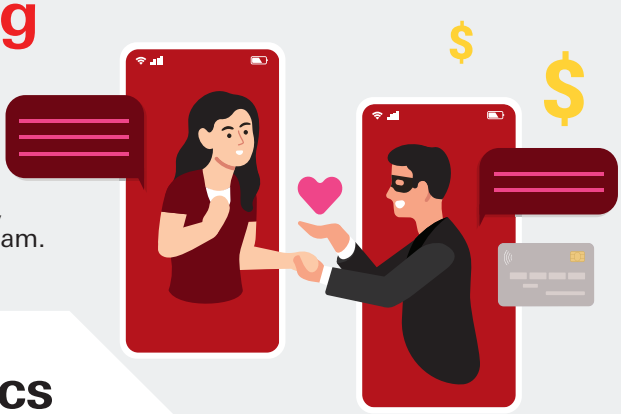
Scammers impersonate celebrities on social media or in chat groups, sharing "insider tips" or pose as "romantic prospects" to lure victims into opening accounts and transferring funds on fake investment platforms. They may even fabricate transaction records to make up profits, eventually stealing funds, personal information, and access to online banking.

Anti-Scam Tips

- Only invest through registered or trusted institutions.
- Consult professionals and thoroughly understand investment products before committing.
- Only download apps from your devices' official stores.
- Avoid downloading suspicious apps or sharing sensitive personal information on dubious investment platforms.

Online Dating Scams

Online dating can be a trap where nothing is as it seems—fake identities, false affections, and all too real intentions to scam.



Common Tactics

❶ Urgent Need for Cash

Scammers flaunt their background or profession on social or dating platforms or join an online fraternity to get familiar with emotionally vulnerable people, aiming to establish a romantic relationship online with the victims.

Once trust is established, they ask for help with business liquidity and living expenses, and request financial assistance.

❷ Sextortion Scams

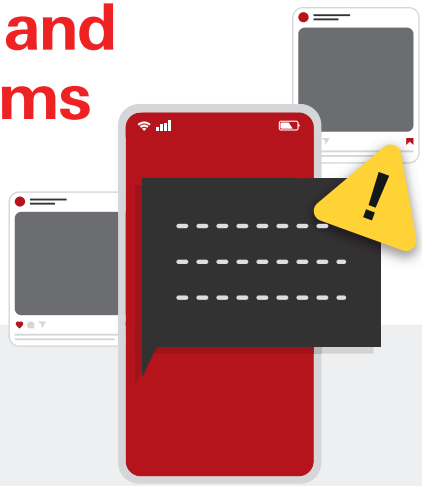
Scammers may persuade victims to engage in video calls, even do it naked. They then use this material to blackmail the victim.

Anti-Scam Tips

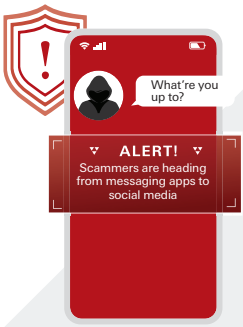
- Maintain an appropriate distance with online acquaintances and cross check their identities via search engines.
- Avoid sharing personal information and never share banking details on social platforms.
- Be extra cautious of what seem like perfect matches—they could be too good to be true.

Messaging Apps and Social Media Scams

In today's world, messaging and social media apps are indispensable in our daily life, but they've also become an essential means for quick wins for scammers.



Common Tactics



❶ Impersonating Friends or Family to Borrow Money

A simple "Are you busy?" may seem like a friendly check-in, but there may be hidden agenda. Scammers use illegal methods to hack messaging or social media accounts and then impersonate the account owner to request money from their friends or family under various excuses.

Anti-Scam Tips

- Enable two-factor authentication on messaging apps to enhance account security.
- If you receive a message from friends or family requesting a bank transfer or payment, always call to verify before taking any action.
- Never disclose sensitive information such as verification codes, OTPs, or bank account details without proper verification.

Cheque Scams

Online shopping often involves direct transfers, but some scammers, known as rubber cheque artists, use invalid cheques to deceive sellers.

Common Tactics

❶ Cheque Deposit Before Shipment

Scammers typically impersonate schools, elderly homes, charity staffs, or marketplace buyers, settling payment with invalid cheques. They claim to have settled their payment as reflected in the increased ledger balance in your account. Believing that the seller has already paid, the seller arranges for the shipment only to discover later that the cheque is void.

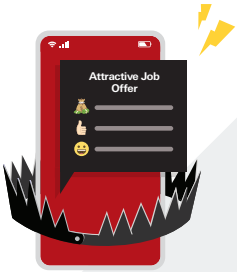
Anti-Scam Tips

- “Ledger balance” may include cheques that have been deposited but have not yet been cleared for withdrawal. It's for reference only.
- “Available balance” is the amount of money you have in your account that can be withdrawn.
- Cheque deposit takes 1 to 2 working days for clearance. Check your “available balance” instead of relying on the “ledger balance” when receiving payments.

Job Scams

Opportunities are meant to be earned, but sometimes, when a great job opportunity comes knocking, it might just be a carefully crafted scam!

Common Tactics



❶ Fake Job Offers

Scammers post job ads on social media, highlighting high pay, great benefits, with low prerequisites. During the recruitment process, they request personal and bank account details, creating urgency to pressure victims into making hasty decisions.

❷ Fake Online / Remote Jobs

Scammers invite people to fake messaging groups, offering easy money for simple tasks. They try to steal personal information or ask for upfront payments or deposits—then disappear when they receive the money.

Anti-Scam Tips

- Be cautious if a recruiter asks for sensitive personal information immediately during the job application process.
- Never disclose your banking login credentials, OTPs, or agree to apply for loans under your name.
- Stay extra vigilant of overseas job opportunities.
- Never allow others to use your account.
- You should never be required to make payments to a potential employer or a recruiter.

The information provided is for reference purposes only. If you have any questions about our services, feel free to call our hotline at 2233 3000 or visit any branch to speak with our staff.

If you suspect a scam, call the Hong Kong Police Force's Anti-Scam Hotline 18222 or download the upgraded Scameter+ App for verification.

Issued by The Hongkong and Shanghai Banking Corporation Limited