

尊敬的客戶：

提防網絡詐騙及防騙貼士

為保障您使用浦發銀行香港分行（“本行”）網上銀行/手機銀行的安全，我們為您準備關於提防網絡詐騙及防騙貼士：

重點安全提示

1. 必須妥善保管密碼

密碼是保障您安全使用網上銀行/手機銀行交易渠道的第一道防線，請務必好好保管您的密碼，切勿與第三者共享。密碼應設定為高強度，並請定期更新，應避免使用相同密碼於多個賬戶。

2. 勿墮入網絡陷阱

本行提示您，為避免墮入網絡陷阱，請謹記：

- ◆ 切勿經電郵內連結、二維碼及非本行官方網絡渠道，去登錄網上銀行及下載手機銀行；
- ◆ 切勿於網絡平台，社交媒體、即時通信軟件等，透露個人信息；及
- ◆ 切勿在可疑網站指示操作或輸入登入賬號、密碼、一次性密碼、保安編碼、個人資料等重要信息

欺詐手法層出不窮，以下為近期常見詐騙手法：

1. 釣魚短訊騙案

這類釣魚短訊通常假冒如銀行、政府部門或速遞公司等送出釣魚短訊，內容包含誘導性連結，謊稱受害人賬戶異常或中獎，要求受害人點擊超連結進入虛假銀行網站或表格，並輸入銀行登入名稱/密碼/一次性認證/個人訊息等，實質是為了騙取網上銀行權限或盜取個人資料。

2. 網上購物騙案

網購騙徒假冒賣家於網上平台刊登虛假熱賣產品，以較低價格吸引買家，並以先付款後交易的方式，要求買家存款入指定賬戶。當買家入款後，便失去聯絡。另外，有騙徒假冒買家並通過提供超連結，要求賣家登入虛假網上銀行以接受款項，最後把賣家的銀行資金轉走。

3. 假冒官員或銀行職員電話騙案

冒充官員或銀行職員來電，利用受害人的信任或恐懼心理，謊稱受害人涉案或賬戶有問題，要求提供個人訊息或將資金轉至騙徒賬戶，實則騙取錢財。

4. 網絡投資騙案

騙徒假扮成理想對象通過社交平台或交友軟件，與受害人建立關係後，推薦虛假投資或要求巨額借款，以高回報作餌誘騙受害人投入資金，最終切斷聯繫，消失無蹤。

5. 刷單詐騙

以簡單工作賺取佣金，聲稱工作無需學歷或經驗並工時靈活，受害人則需墊付資金進行刷單任務。騙徒初期會兌現承諾，將購物任務金額及佣金轉回給受害人。獲取受害人信任及投入更多資金後，騙徒便會以不同藉口拖延，並再誘騙繼續墊付資金刷單或要求轉入巨款才能提取款項，更會要求受害人去借款達到要求，最終捲款消失。

如何提防被詐騙？

1. 提高警覺，切勿點擊不明連結

對不明來電、短信、郵件須保持警惕，切勿點擊不明連結，對於聲稱緊急、中獎或立即行動等訊息應謹慎處理，不應輕信未經核實身份發送人的信息。

按照香港金管局的監管要求，銀行不會透過短訊或電郵提供超連結，更不會透過連結要求客戶進行交易或提供任何個人資料（包括登入密碼和一次性密碼）。如需要瀏覽銀行網址或登入網上銀行，應透過輸入銀行網址或使用官方提供的手機銀行登入。

本行網銀的網址：
<https://ebankhk.spdb.com.cn/hkbank/>
<https://ebankhkpdb.spdb.com.cn/>

2. 保護個人訊息

不要隨意透露個人訊息，如身份證號碼、銀行賬戶資料及密碼等。網上銀行服務的個人登入資料（包括賬戶名稱、登入密碼和一次性密碼等）必須妥善保管，並切勿與第三者共享。

3. 核實身份

對於收到任何要求提供個人訊息或付款的要求，應先通過官方渠道核實，並可通過警方提供的「防騙視伏App」評估詐騙及網絡安全風險。如您對電郵或短訊的真偽存疑，請致電相關機構 / 本行的客戶服務熱線，作進一步確認。

4. 通知及報警

如曾經向不明網站或騙徒透露網上銀行登入資料或發現賬戶錄得未經授權交易，應盡快通知銀行，並向警方報案。如發現涉及詐騙行為，立即停止與騙徒的聯繫，馬上向警方報案。如懷疑受騙，可致電警方反詐騙協調中心「防騙易18222」熱線查詢。

如您對上述信息和安排有任何查詢，請致電本行客戶服務熱線（852）2169 5528或聯絡閣下的客戶經理。

上海浦東發展銀行股份有限公司 香港分行謹啟
（於中華人民共和國註冊成立的股份有限公司）
2026年1月30日

尊敬的客户：

提防网络诈骗及防骗贴士

为保障您使用浦发银行香港分行（“本行”）网上银行/手机银行的安全，我们为您准备关于提防网络诈骗及防骗贴士：

重点安全提示

1. 必须妥善保管密码

密码是保障您安全使用网上银行/手机银行交易渠道的第一道防线，请务必好好保管您的密码，切勿与第三者共享。密码应设定为高强度，并请定期更新，应避免使用相同密码于多个账户。

2. 勿堕入网络陷阱

本行提示您，为避免堕入网络陷阱，请谨记：

- ◆ 切勿经电邮内连结、二维码及非本行官方网络渠道，去登录网上银行及下载手机银行；
- ◆ 切勿于网络平台，社交媒体、实时通信软件等，透露个人信息；及
- ◆ 切勿在可疑网站指示操作或输入登入账号、密码、一次性密码、保安编码、个人资料等重要信息。

欺诈手法层出不穷，以下为近期常见诈骗手法：

1. 钓鱼短讯骗案

这类钓鱼短讯通常假冒银行、政府部门或速递公司等送出钓鱼短讯，内容包含诱导性连结，谎称受害人账户异常或中奖，要求受害人点击超链接进入虚假银行网站或表格，并输入银行登入名称/密码/一次性认证/个人讯息等，实质是为了骗取网上银行权限或盗取个人资料。

2. 网上购物骗案

网购骗徒假冒卖家于网上平台刊登虚假热卖产品，以较低价格吸引买家，并以先付款后交易的方式，要求买家存款入指定账户。当买家入款后，便失去联络。另外，有骗徒假冒买家并通过提供超链接，要求卖家登入虚假网上银行以接受款项，最后把卖家的银行资金转走。

3. 假冒官员或银行职员电话骗案

冒充官员或银行职员来电，利用受害人的信任或恐惧心理，谎称受害人涉案或账户有问题，要求提供个人讯息或将资金转至骗徒账户，实则骗取钱财。

4. 网络投资骗案

骗徒假扮成理想对象通过社交平台或交友软件，与受害人建立关系后，推荐虚假投资或要求巨额借款，以高回报作饵诱骗受害人投入资金，最终切断联系，消失无踪。

5. 刷单诈骗

以简单工作赚取佣金，声称工作无需学历或经验并工时灵活，受害人则需垫付资金进行刷单任务。骗徒初期会兑现承诺，将购物任务金额及佣金转回给受害人。获取受害人信任及投入更多资金后，骗徒便会以不同借口拖延，并再诱骗继续垫付资金刷单或要求转入巨款才能提取款项，更会要求受害人去借款达到要求，最终卷款消失。

如何提防被诈骗？

1. 提高警觉，切勿点击不明连结

对不明来电、短信、邮件须保持警惕，切勿点击不明连结，对于声称紧急、中奖或立即行动等讯息应谨慎处理，不应轻信未经核实身份发送人的信息。

按照香港金管局的监管要求，银行不会透过短讯或电邮提供超链接，更不会透过链接要求客户进行交易或提供任何个人资料（包括登入密码和一次性密码）。如需要浏览银行网址或登入网上银行，应透过输入银行网址或使用官方提供的手机银行登入。

本行网银的网址：
<https://ebankhk.spdb.com.cn/hkbank/>
<https://ebankhkpdb.spdb.com.cn/>

2. 保护个人讯息

不要随意透露个人讯息，如身份证号码、银行账户数据及密码等。网上银行服务的个人登入资料（包括账户名称、登入密码和一次性密码等）必须妥善保管，并切勿与第三者共享。

3. 核实身份

对于收到任何要求提供个人讯息或付款的要求，应先通过官方渠道核实，并可通过警方提供的「防骗视伙App」评估诈骗及网络安全风险。如您对电邮或短讯的真伪存疑，请致电相关机构 / 本行的客户服务热线，作进一步确认。

4. 通知及报警

如曾经向不明网站或骗徒透露网上银行登入资料或发现账户录得未经授权交易，应尽快通知银行，并向警方报案。如发现涉及诈骗行为，立即停止与骗徒的联紧，马上向警方报案。

如怀疑受骗，可致电警方反诈骗协调中心「防骗易18222」热线查询。

如您对上述信息和安排有任何查询，请致电本行客户服务热线（852）2169 5528或联络阁下的客户经理。

上海浦东发展银行股份有限公司 香港分行谨启

（于中华人民共和国注册成立的股份有限公司）

2026年1月30日

Dear Customer,

Beware of online scams and anti-fraud tips

To ensure the security of your transactions using the online banking/mobile banking services of Shanghai Pudong Development Bank. Co. Ltd. Hong Kong Branch (“the Bank”), we provide you with the following information on online scams and anti-fraud tips:

Key Online Safety Tips:

Protect your password carefully

Your password is the first line of defense for your online banking/mobile banking services. Please keep your password safe and do not share it with anyone. Set a strong password and update it regularly. Avoid using the same password for multiple accounts.

Beware of online scams

To avoid falling victim to online scams, please remember the following:

- ◆ Do not log in to your online banking or download the mobile banking app through links in emails, QR codes, or non-official Bank websites.
- ◆ Do not disclose any personal information on online platforms, social media, or instant messaging apps.
- ◆ Do not follow instructions from suspicious websites or enter important information such as login credentials, passwords, one-time passwords, security codes, or personal details.

Some recent common types of scams

Phishing SMS Scams:

These types of phishing messages often pretend to be from banks, government departments, or courier companies. The message content contain hyperlink that claim the victim’s account is abnormal or that they have won a prize. They trick the victim into clicking on a link that leads to a fake bank website or form. By having the victim enter their login credentials, one-time passwords, personal information, etc., the fraudsters could gain access to their online banking accounts or steal their personal data.

Online Shopping Scams:

Fraudsters create fake listings for popular products on online platforms at lower prices to attract buyers. They ask the buyers to make payments in advance and then disappear without delivering the goods. In other cases, fraudsters pretend to be buyers and provide fake hyperlinks, asking the sellers to log into a

fake e-banking account to receive the payment for transferring the seller's funds.

Scams Impersonating Officials or Bank Employees:

Fraudsters call and pretend to be officials or bank employees, exploiting the victim's trust or fear. They claim that the victim is involved in illegal activities or that there is a problem with their account, and then request victims' personal information or the transfer of funds to the scammer's accounts.

Online Investment Scams:

Fraudsters establish contact with victims through social media or dating apps, pretending to be trustworthy individuals. They offer fake investment opportunities or request loans, promising high returns to get the victims to invest. Once the victims deposit money, the fraudsters cut off all communication and disappear.

Fake Order Placement Scams:

These scams promise easy jobs with no educational requirements or experience with flexible working hours. Victims are asked to pay in advance to place fake orders. Initially, the fraudsters fulfill their promises by returning the amount of the order and any commission. Once they gain the victim's trust, they delay payment, use various excuses to continue asking for more funds, and may even demand loans to withdraw the money, eventually disappear with the stolen money.

How to guard against fraud?

Stay alert and never click on any unknown hyperlinks

Be cautious of unsolicited calls, texts, and emails. Do not click on unknown hyperlinks, and be skeptical of messages claiming to be urgent, about winning prizes, or requiring immediate action. Do not trust information from senders whose identities have not been verified.

According to the regulatory requirements of the Hong Kong Monetary Authority, banks will not provide hyperlinks via text messages or emails, nor will they request customers to conduct transactions or provide any personal information (including login passwords and one-time passwords) through links. If you need to visit the bank's website or log in to online banking, do so by entering the bank's official URL or using the mobile banking service provided by the bank.

The URLs for our online banking services are: <https://ebankhk.spdb.com.cn/hkbank/>
<https://ebankhkpb.spdb.com.cn/>

Protect Your Personal Information

Do not casually disclose personal information such as your ID number, bank account details, and passwords. Personal login information for online banking services (including account names, login passwords, and one-time passwords) must be kept secure and should not be shared with third parties.

Verify Identities

Before providing any personal information or making payments from request, please verify the request through official channels. You can also use the “Scameter+” App provided by the Hong Kong Police Force to assess the risk of fraud and online security threats. If you doubt the authenticity of an email or text message, please contact the relevant institution or our bank’s customer service hotline for further confirmation.

Notify and Report Incidents

If you have disclosed your online banking login information to an unknown website or scammer, or if you notice unauthorized transactions on your account, please notify the bank immediately and report the incident to the police. If you suspect fraud, stop all communication with the scammer and report it to the police as soon as possible. If you think you have been scammed, you can call the police’s Anti-Deception Coordination Centre (ADCC) at the hotline “Anti-Scam Helpline 18222” for assistance.

If you have any questions about the above information, please contact our bank’s customer service hotline at (852) 2169 5528 or your relationship manager.

Shanghai Pudong Development Bank Co., Ltd., Hong Kong Branch
(incorporated in the PRC with limited liability)
30-Jan-2026