

## 最佳安全实践

星展银行将严格保密您向银行提供的个人信息。安全对我们而言至关重要，我们致力于为您提供安全放心的网络环境，满足您的银行业务需求。

星展银行关注安全实践，采用以下措施保护您的网上交易。

### 星展银行如何保护您

- 使用 128 位扩展验证安全套接层协议（SSL）。星展银行使用扩展验证 VeriSign SSL 证书和显示在星展银行/储蓄银行网银页面上的 VeriSign 标识。印章将向客户显示有效的 SSL 证书以及星展银行/储蓄银行网银页面的合法性。这将确保银行网站在星展银行的管理下合法运营。SSL 将保护进出银行的所有机密信息，防止盗用或擅自获取。
- 个人身份识别号码（PIN）和唯一用户识别号码（UID）。我们目前已采用双重认证登录流程，客户获取账户信息和/或在线交易时，需输入和其唯一用户识别号码匹配的网银个人身份识别号码（PIN）。需使用唯一用户识别号码进入星展银行网银系统，系统中的其他用户无法对此复制，PIN 号码和用户 ID 相关联。我们系统要求文字数字型用户 ID（5 至 20 个字符）和数字型 PIN（6 至 9 个字符）。星展银行从未以电子邮件或电话的形式要求您提供任何个人信息。
- 多因素认证。星展银行使用多因素认证，由用户 PIN、二因素（2FA）电子令牌和短消息确保您的在线交易安全。进行登录和在线交易时使用用户 PIN 和 2FA 电子令牌，进行添加第三方收款人等高风险交易时将激活 SMS。
- 交易提醒。当您的账户发生交易时，星展银行将予以提醒。您可以对提醒功能进行定制化处理。针对高风险交易，星展银行将授权使用短消息提醒，确保您安全无忧。
- 自动退出特点。当我们的系统检测到登录后的一段时间内未发生任何活动，您在网银的活动将被自动终止。如您希望使用服务，需使用用户 ID 和 PIN 再次登录。
- 设定交易额度。星展银行可让您设置针对星展银行/储蓄银行账户或其他银行账户的第三方资金交易额度。

### 您在使用星展银行/储蓄银行网银服务时的职责

- 确保星展银行/储蓄银行网银页面上显示 Verisign 标识。
- 妥善保管您的 PIN 和 ID 信息。妥善保管“电子令牌”——确保安全。
- 登录使用期间务必小心照管，使用后需退出在线网络。
- 丢失电子令牌后，请通知星展银行。
- 联系方式变更后，请及时通知我们。
- 如有任何可疑登录，请检查最近一次网银登录记录并通知我们。
- 切勿故意向可疑网站披露您的个人信息。
- 使用防病毒软件，保护您的电脑免受恶意程序攻击。
- 确保您使用 SMS OTP 前仔细阅读并遵守了操作说明。
- 定期检查您的账户余额和交易记录。

重要——如果怀疑您的网银用户识别信息、PIN 或电子令牌被损害或账户发生任何可疑行为，请立即拨打电话 800-999-3327 联系星展银行客服中心，重设您星展银行/储蓄银行的网银用户 ID 和 PIN。我们经验丰富的星展银行员工将竭诚为您服务。再次提醒，星展银行从未以电子邮件的形式要求您验证任何个人信息。如需帮助或了解详情，请拨打电话 800-999-3327 联系我们的客服中心。

### 网上交易的其他最佳安全实践

- 每日自动更新防病毒和防间谍软件。
- 每日自动更新运营系统。
- 为电子邮件、网上购物或订阅等网络服务设置不同的 pin 码或密码。
- 不要点击电子邮件中的链接或安装来自可疑网站的任何程序。
- 如您怀疑个人电脑遭受侵害，请不要用此进行网上交易。

## 了解安全措施的主要内容

- 预付款诈骗
- 间谍软件
- 身份盗用
- 网钓和鲸钓

### 预付款诈骗

预付款诈骗通常也称为“尼日尼亚诈骗”或“419 诈骗”，是一种信任骗局，收件人收到主动发送、据称来自政府或银行的正式电子邮件、信函或传真，劝服接收者预付一笔款额用于“行政”或“法律”目的，以协助获得一笔巨额钱款（据称是已故储户的无主财产或银行账户的“多余”资金）。按照承诺，收件人将获得在其帮助下取得的上述金额的 10%至 40%作为佣金。应注意的是，大多数情况下要求收件人采取的行为都可能违法。承诺佣金绝不会兑现，诈骗人也会逃之夭夭。

最近，诈骗人经常冒充星展银行高级管理人员，在很多信函或电子邮件中附上星展银行管理人员的介绍。此类介绍皆从星展银行网站上下载所得，用以增强骗局的真实性。使受害人“上钩”的主动发送电子邮件通常采用以下格式：

“尊敬的先生/女士，

“我是 X 先生，在星展银行资本投资公司担任高级投资顾问。我了解到 A 先生在银行内有 XXX 美元的存款。不幸的是，他去世时未留下任何遗嘱或指定任何家属继承此笔款项……我希望邀请您假作已故 XYZ 先生的亲戚索取此笔款项……请用我的私人邮箱 XYZ@email.com 和我联系。”

或者

“尊敬的先生/女士，

“我是 XYZ 小姐，担任星展（香港）银行主席的秘书和私人助理。应我的老板要求，在网上搜索时得到您的电子邮件账户。现需要您假扮该笔款项的受益人和所有者近亲，协助将 XXX 百万美元转账至海外账户……如您对此项交易感兴趣，请使用他的私人邮件账户与其取得联系并了解详细信息。”

我们已告知客户星展银行集团或其员工不会向公众或银行客户发送此类邮件，要求取回无主款项并通过私人电子邮件地址进行通信。此类电子邮件、邮寄信函或传真系诈骗活动，客户对此应不予理睬。

[星展银行使用的所有正式邮件只以@dbs.com 后缀结尾。](#)

DBS Bank (China) Limited  
18<sup>th</sup> Floor, DBS Bank Tower  
1318 Lujiazui Ring Road, Pudong  
Shanghai 200120 P. R. China

星展银行(中国)有限公司  
中国上海市浦东  
陆家嘴环路 1318 号  
星展银行大厦 18 楼  
邮编: 200120

电话 Tel: 86 21 38968888  
传真 Fax: 86 21 38968989  
网银热线: 8009993327  
[www.dbs.com](http://www.dbs.com)

若您收到此类电子邮件、传真或信函，我们建议您将相关内容转发至 [investigations@dbs.com](mailto:investigations@dbs.com) 或警察局。如需任何帮助，请拨打联系中心电话 800-999-3327。

## “间谍软件”也许正在监视着您

我们强烈建议您谨慎使用任何声称能加快网络连接速度的第三方软件。

此类软件或服务会通过其服务器篡改您的网络操作。

他们可藉此存储并分析您的网络活动，此类活动将有可能包括您在和星展银行或其他网上服务进行安全交易时的行为。

此类软件统称为“间谍软件”。间谍软件有多种形式。一些看上去和专业软件包或服务类似，其他则明显为恶意软件。

如稍有不慎，间谍软件和篡改器服务将会获得您的用户名、密码、信用卡号、PIN 码、银行使用交易信息、网络浏览记录等。

此类间谍软件或篡改器服务可能会有隐私政策。任何情况下，星展银行无权管理任何第三方的隐私政策。如第三方滥用或共享您的信息，您将无法得到有效的法律保护。

## 您如何进行自我保护

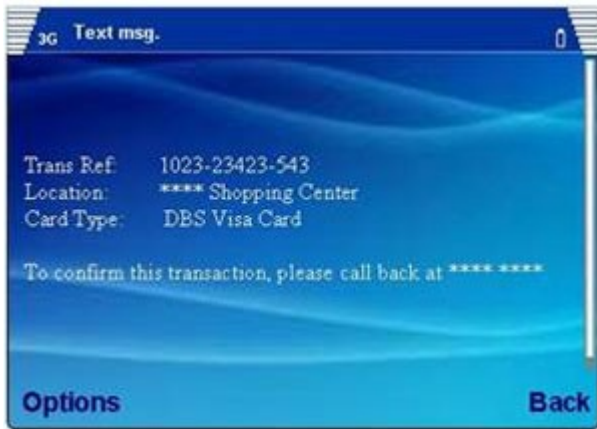
- 我们强烈建议，如您的电脑中有任何软件监督或篡改您的网上使用信息，切勿浏览星展银行网站。
- 如您记得安装过任何声称能加快网络连接速度的软件，或您的浏览器中有额外的第三方工具条，您可能正在有意或无意使用能够追踪您网络使用情况的软件。我们建议您**卸载**此类软件。
- 您通常可进入**控制面板**安全卸载此类软件，选择**添加/删除程序**，找到指定应用软件并选择**删除**。但是，我们了解一些软件很难通过正常的卸载程序进行删除，您需要寻求专业人士帮助将其删除。
- **自我学习**“间谍软件”。警惕电脑上的任何疑似间谍软件行为。如跳出众多对话框或收到主动发送的邮件，似乎“对您非常了解”时，请保持警惕。

## 我们如何保护您的利益

- 我们谨慎行事，确保万一，积极阻止通过篡改器/间谍软件服务对 db.com 进行的网络访问，并会一如既往。
- 不管何时，如果您被我们的网站拒绝进入，您可能有意或无意的在电脑中运行了篡改器/间谍软件。
- 如发生此类情况，我们敦促您**卸载**此类软件。

## 身份盗用

您是否曾受到过以下类似的短消息？



短消息文本

交易参考号 1023-23423-543  
地点: \*\*\*\* 购物中心  
银行卡类型: 星展银行维萨卡

确认该交易，请拨打电话 \*\*\*\*  
\*\*\*\*

是否考虑过给与回复或拨打电话予以确认？

这是身份盗用的典型案例，诈骗人企图通过此种方法获得您的信息。除了此类手机骗局，还有钓鱼电子邮件、电话或传统的垃圾收取，获得敏感的个人和/或财务信息用于诈骗活动。诈骗人伪装成您的银行或网络服务供应商等合法组织代表发送信息。当用户拨打电话时，他们会询问一些问题，引诱用户透露机密信息。

### 您应保持警惕，采取以下措施

- **妥善保管您的银行结单。**妥善保管您的银行结单并锁好确保安全。丢掷前最好先粉碎处理。
- **结单丢失。**关注未如期收到的账户或账单结单。结单丢失表明诈骗人已设法成功篡改了您在银行的登记地址。
- **您账户上的不明交易。**如您发现账户上发生不明交易，应立即提醒银行注意。
- **意外收到账户或账单结单。**如收到不属于您的账户或账单结单，请保持警惕。
- **收到涉及您并未发生的交易的短消息、电话或电子邮件。**对此类短消息、电话或电子邮件切勿回复。
- **切勿点击主动发送邮件中的 URL 链接。**始终在浏览器地址栏中直接输入网站地址。
- **使用复杂密码。**切勿使用简单或容易猜中的密码，例如您的个人信息（例如，生日、妻子或子女的姓名）。
- **保护您的个人信息。**不可向零售商等商业组织提供您的 NRIC 等个人信息，除非确实需要。

**谨记，星展银行不会询问您的 PIN 码。若您收到此类要求，请拨打热线电话 800-999-3327 向星展银行客服中心进行汇报。**

身份盗用会浪费您的时间和金钱。请采取保护措施。

### 网钓和鲸钓

假冒银行或商户向众人群发垃圾邮件，旨在引诱顾客前往貌似合法的银行或零售商店网站，输入姓名、身份证号、信用卡号和账户号码等个人或财务信息。此为网络钓鱼，邮件针对那些容易咬饵上钩的人士，就像传统的钓鱼行为。此类诈骗活动已存续多年。

后来还发展出了鲸钓。电子邮件来自收件人熟识的人士，通常是体面或更高级别的人士。然后要求收件人提供一些信息或下载带有特洛伊木马病毒的文件，以便让黑客从收件人处获取信息。

这些方法之所以起作用，是因为他们瞄准了人性特征，诸如尊重上司或公众人物以及贪婪的本性。

新行话称为鲸钓，工作原理类似，但是目标是大鱼——公司高管或巨富。调查显示收入超过 130,000 的人士将会收到多过 50% 的垃圾邮件，上当后将会失去 3.8 倍的金钱损失。

MAS 近期指出亚洲银行将很快成为钓鱼攻击的主要目标，虽然到目前为止，欧洲市场仍为关注重点。

**一些防范措施将保护您免受网钓和鲸钓的侵扰：**

- 不确定时，不可提供任何私人或财务信息。您不知道谁能看到您的信息。
- 切勿点击电子邮件中的网站链接——在您的网站浏览器中输入地址，尤其当它们看上去需要个人信息时。
- 实时更新您的桌面保护软件。包括防病毒软件、防间谍软件、防火墙和其他软件。