青少年理财教育

提防网络安全隐患

汇丰 HSBC
汇见新可能
Opening up a world of opportunity

目录

点击可浏览各个章节

提防骗子，由你开始

我们往往会认为诈骗只会发生在别人身上，直到自己被骗。

识别诈骗就像解密魔术一样，如果不知道其中的关键，它就会让你感到十分困惑。当知道它是如何运作时，你就可以立刻识别骗术。如果我们了解这些伎俩，就不会轻易上当。

诈骗的种类

电邮诈骗“网络钓鱼”

“网路钓鱼”是骗徒试图通过电子邮件取得用户名称和密码等敏感资料的一种手段。这些电邮看起来像是来自你信任的人，例如银行。

需要注意：

这类电邮会要求你提供个人资料，或者引导你到一个和真实网站极度相似的假网站，要求你输入个人资料。电邮的开头可能只是用一个普通的称谓（一般都不会用你的名称），电邮内容也可能出现拼写和语法问题。

如何防骗：

每次都要检查发件人的电邮地址。不要轻易点击任何链接，或打开任何附件。千万不要透露你的敏感资料。如果你是汇丰客户，你可以将电邮转寄到 phishing@hsbc.com，我们会跟进调查。

小测验：如何识别“网络钓鱼”

短信诈骗“短信钓鱼”

骗徒可能向你发出诈骗短信，假扮成你信任的人，例如银行或者电话服务供应商。

需要注意：

骗徒会试图让你点击链接或回复你的个人或银行资料给他。

如何防骗：

如果你不确定是否是诈骗短信，请不要点击任何链接，也不要回复。可以先对比平时来自该机构的短信内容。

电话诈骗“电话钓鱼”

骗徒可能会打电话给你，声称自己是银行或者警察等你通常会信任的身份，但其实他们想骗钱或获取你的个人资料，以便日后再向你行骗。

需要注意：

他们会尝试说服你将钱存入一个“安全的地方”。他们还会要求你提供个人资料，例如你的账户密码、个人身份识别码或者安全钥匙密码。

如何防骗：

正常挂断电话，然后等待 15 秒，直到电话完全断线。继续等待 15 秒后，再致电骗徒声称的公司热线核实。如果对方声称是银行，那就致电你银行卡背面的电话号码。

盗用身份

骗徒可能会试图取得你重要的个人资料，然后以你的名义开立新账户或接管你的账户。

需要注意：

一些心理或性格测试网站看似没问题，但是他们可能会泄露你的个人资料给盗用身份的人。这些测验的条款和细则通常要求你允许将输入的资料被出售给其他人。

如何防骗：

不要点击任何出现在社交媒体上看起来很有趣的简单测试，同时将你的个人版面设为隐私状态。确保在看完你的银行月结单和其它包含个人资料的文件后将其销毁。

购物诈骗

在社交媒体上购买二手物品或特价货品通常是省钱的好方法。但要小心许多虚假账户和骗子都活跃在这些购物平台。

需要注意：

遇到以下情况，你都应该格外小心，例如：卖家账户最近才创建，却在销售大量的商品，或使用一些通用的产品图片。

如何防骗：

当买家要求一笔定金或者要你转账到一个毫不相关的账户或公司时，请务必提高警觉。

了解如何避免这些类型的诈骗是很重要，因为如果不幸成为受害者，你所损失的金钱通常难以获得赔偿。

防骗：保护自己

诈骗和骗局是指罪犯为了钱欺骗你的行为。

诈骗可能在你毫不知情的情况下发生，而骗局则是有人怂恿你以他们的名义完成某件事情。

我们总认为诈骗和骗局只会发生在其他人身上，但实际上所有人都有机会上当受骗。骗徒掌握向我们施压的技巧，让我们堕入陷阱。

当你觉得不对劲时，可以问自己以下问题：

- 他是否催促我采取紧急行动，或者威胁我如果不迅速采取行动就会冻结我的账户？
- 他是否告诉我我的银行账户在我不知情的情况下存入了一笔钱？
- 他是否让我点击来历不明的信息或电邮中的连接？
- 他是否要求我提供个人资料？
- 他是否要我回复或者验证我的账户？
- 他发送的信息是否有拼写、格式或语法错误？
- 他是否要求我验证新的收款人、交易或电子设备？
- 它是否看起来像是真的，但当我仔细研究时却发现有些地方不太对劲？
- 他是否要求我将钱转移至“安全账户”或提取现金并交予“警方”进行调查？
- 他是否提供给我好得难以置信的优惠？
- 他是否用不同的理由要求我更改付款资料？

保护你的财产

恭喜你终于存到第一笔钱！而现在你需要学习如何确保你的财产安全。

你可以通过日常小习惯来确保资金安全，例如经常检查银行月结单是否有可疑交易。你也可以采取进一步的措施，例如在付款前检查收款人或公司是否真实存在。

你可以用以下情境，测试一下你识别诈骗的能力。

情景	答案
1 你的一位朋友在社交媒体上发信息给你，说他有**急事**，急需一笔现金。 **你会怎么做，为什么？** 	不要转账给他们。打电话或发信息给你的朋友，确认他们是否真的需要借钱。不要在社交媒体上联系他们。如果你朋友的账户被黑客入侵或被人冒充账户，你可能会成为下一个受害者。
2  你逛街购物时，将手机连接至购物中心的公共无线网络。然后，你看到一双特别喜欢的鞋，但需要**检查卡上的余额**，以查看是否买得起。 **你会怎么做，为什么？**	连接至公共无线网络时，请不要使用手机检查银行余额。公共无线网络并不安全，骗徒可能利用它获取你的银行资料。最好使用正常的手机移动数据上网，或到自动柜员机查看余额。
3 你和朋友外出用餐。你在上厕所时把卡交给他们付费，他们要求你提供**密码**，以防感应式支付无法使用。 **你会怎么做，为什么？** 	请勿将卡交由他人保管，也不要告诉任何人你的密码，即使是最好的朋友，尤其不要在可能被人偷听到的公共场合说出你的密码。你是唯一知道密码并且可以使用这张卡的人。

如何安全地在网上理财和付款

通过网页或手机应用程序购物和理财，既快速又方便。

但要注意保护自己，就如同其他消费或理财方式一样。以下小贴士可有效确保你的安全：

确保你电子设备的安全性

经常更新你的手机、平板电脑或者笔记本的操作系统到最新版本，确保安全。

只要将笔记本电脑和桌上电脑设定为自动安装更新系统，每当有软件更新就会自动下载安装，其它应用程序也一样。你可以选择将电子设备连接到无线网络时或在晚上充电时自动升级到最新版本。这样你的电子设备就会有为防止黑客入侵而设的最新安全功能。

你还应该安装声誉良好且值得信赖的防毒软件，以保护电子设备免受任何恶意攻击。请前往我们的网络安全及防诈骗资讯中心了解更多。

设置不易破解的密码

复杂的密码可能会令人感到很麻烦，但它们确实可以保护你的个人资料。

密码越长就越安全。使用大写字母、小写字母、数字和符号的组合能让密码难以破解。另一种强化密码的方法是将不相关的词串连起来。

使用网上或手机理财服务时，你可以设定一些安全措施。例如，你可以使用指纹或人脸识别等生物辨识，令手机理财服务更加安全，这也称作双重认证。当你进行网上付款时，汇丰还会用行为生物认证技术来验证你的身份。

安全连接

请检查你的网络连接是否安全，看一看网址列上是否有锁形图示。但请记住，拥有锁形图示并不能保证网站是真实的。

例如，如果你正在浏览 hsbc.com.hk，并且看到绿色的锁形图示，这表明你在安全的情况下与汇丰互动。但如果你访问的是 hs8c.com.hk，你仍然可以看到绿色挂锁，虽然这表示联机安全，但你互动的对象不是汇丰。骗徒专门设置了这个假网站，让你以为你访问的是汇丰网站。

因此，你要再三确认网站的真实性，检查网址是否有轻微的拼写错误、多出的字符或其他存在异常的地方。守网者等网站可以帮助你判断网站是否正规。

网上购物和银行转账

购物时，输入你的个人或付款资料之前，请再次检查网址列中的锁形图示，并且不要提供非交易相关的资料。例如，只填写必填栏。

通常不需要你建立账户就可以购买东西 – 所以如果不是必要，就不要建立账户。尽量不要让卖家储存你的付款资料。

如果你不认识卖家，切勿以银行转账方式付款。请使用信用卡、借记卡、PayPal 或可提供防骗保护的其它付款方式。

如果你发现账户有任何可疑情况，请立即致电 +852 2233 3000 联系我们。

防范骗局

即使你已采取这些安全措施，你仍需注意一些常见的骗局。以下是两个值得注意的警示信号。

要求你转移资金：真正的银行不会要求你将钱转移到另一个账户，也不会无缘无故要求你提供个人识别码、密码或其他个人资料。

不明发件人：切勿点击来历不明的链接或附件。

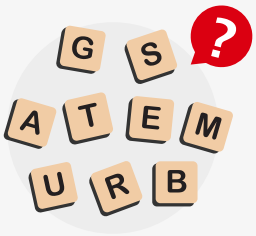
如何识别“网络钓鱼”

认清虚假邮件和网站

骗徒会试图设下陷阱获取你的密码和银行资料，这种骗局俗称“网络钓鱼”。
他们会设置看起来很真实的电子邮件和网站。但你其实可以从细节上分辨真假：

伪装或修改过的链接

仔细检查链接处显示的网址，例如：你是否进入“H5BC.com”网站

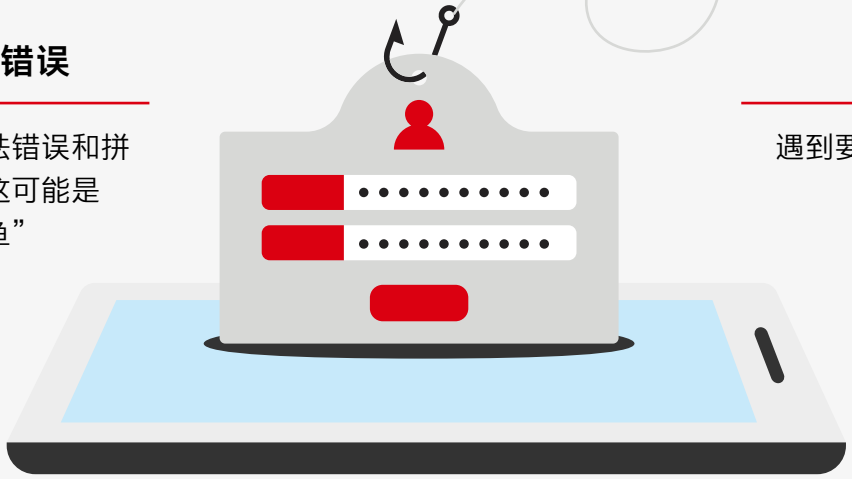


语法和拼写错误

句子不流畅、语法错误和拼写错误都表示这可能是“网络钓鱼”

个人资料

遇到要求提供个人资料的讯息要小心



紧急情况和账户威胁

警告你的账户有紧急变更，需要立即进行验证

公司标志或署名

不要因为电邮里有看起来像官方的标志或署名，就认为这是真的官方邮件

电邮挑战1：
发现骗局中的蛛丝马迹

在一些骗局里，骗徒会尝试通过电邮盗取受害人的银行账户或金钱。虽然有时要分辨电邮真伪并不容易，但你仍然可以通过一些蛛丝马迹识别伪冒电邮。你能从以下示例中找出端倪吗？

在这里输入...

答案：

提示 1：“亲爱的客户”：你的银行知道你的姓名，并会在电邮内附上你的姓名。

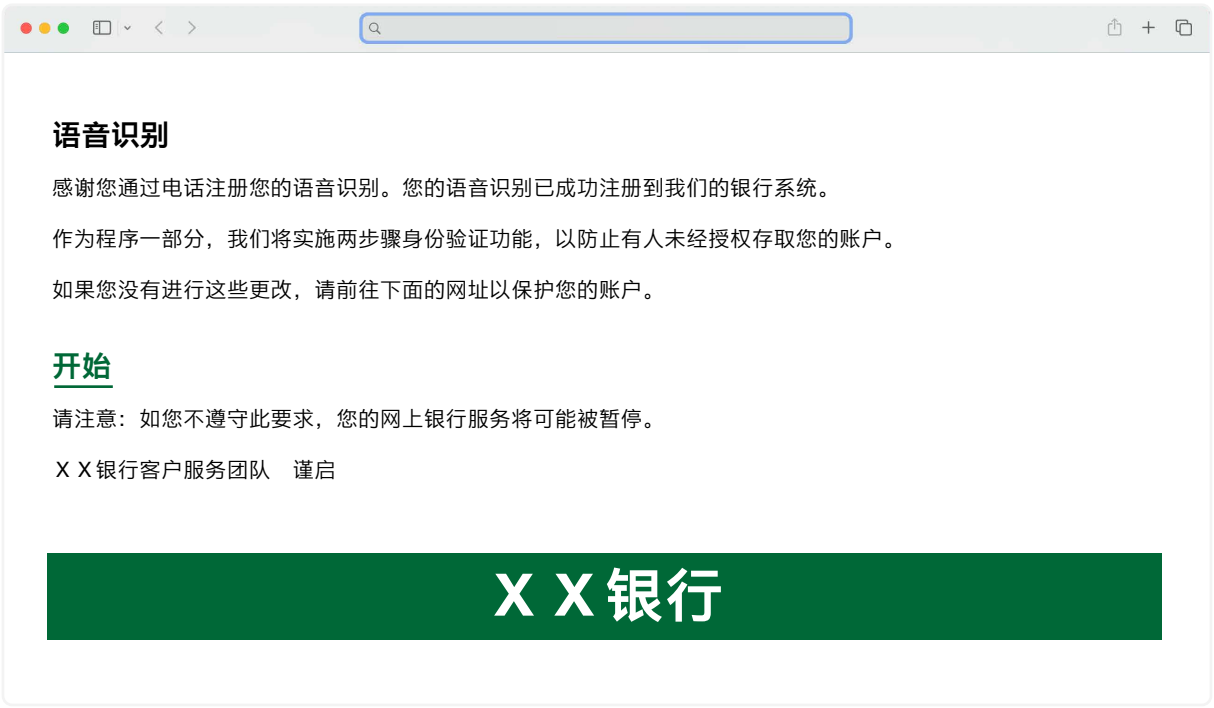
提示 2：检查寄件人的电邮地址 – 此处通常会显示寄件人的真正电邮地址，有可能是一个看起来很可疑的电邮地址。

提示 3：检查语法错误和错别字。你的银行不会说你的资料“有轻微错误” – 如有问题，银行会直接要求你经安全途径更新资料。

提示 4：你认识这个网站链接吗？不要点击任何你不认识的网站链接。

电邮挑战2:
察觉骗局中的蛛丝马迹

有些电邮看起来非常专业，让你以为他们是真实的。但其中仍然有可疑的地方 – 你能发现它们吗?



语音识别

感谢您通过电话注册您的语音识别。您的语音识别已成功注册到我们的银行系统。

作为程序一部分，我们将实施两步骤身份验证功能，以防止有人未经授权存取您的账户。

如果您没有进行这些更改，请前往下面的网址以保护您的账户。

开始

请注意：如您不遵守此要求，您的网上银行服务将可能被暂停。

ＸＸ银行客户服务团队　谨启

ＸＸ银行

答案:

提示 1：点击链接可能带来风险 – 例如，它可能会将你引导至诈骗网站，或让骗徒窃取你电脑中的信息。在点击之前，将鼠标移至链接上方，查看链接的去向。

提示 2：电邮内容写得不专业，使用不同的字体大小和颜色并威胁你立刻行动，让人生疑。

提示 3：没有写客户姓名。

提示 4：你注册语音认证了吗？如果收到这封邮件的人没有注册，收到信息时记得想一想此信息是否符合你的真实情况。

短信挑战1：识别伪造信息

收到短信时，你能看出诈骗短信的端倪吗？

答案：

要分辨短信内容是真的还是诈骗就更难了。

停下来思考几分钟。

你有没有买过短信提及过的东西？不要拨打短信中的号码。这类诈骗现在很常见。请打给银行的电话号码（例如你银行卡背面的号码），而不是打给短信中的号码。

短信挑战2:
识别伪造信息

1

☐ 官方短信 ☐ 诈骗短信

2

☐ 官方短信 ☐ 诈骗短信

答案:

1. 诈骗短信　2. 诈骗短信

短信挑战3:
识别伪造信息

3

☐ 官方短信 ☐ 诈骗短信

4

☐ 官方短信 ☐ 诈骗短信

答案:

3. 诈骗短信 4. 诈骗短信

快问快答：
最后考考你

1. **学校里的朋友要你告诉他们你的密码。**
   你会告诉他们吗？
   A. 会 / B. 不会

2. **你在社交媒体上看到一则信息，请你将他的钱保管在你的账户，然后付给你报酬。**
   你会接受吗？
   A. 会 / B. 不会

3. **你在社交媒体上收到陌生人的好友请求。**
   你会接受吗？
   A. 会 / B. 不会

4. **你的朋友在社交媒体 (WhatsApp、Facebook、Instagram、Snapchat)上向你借钱。**
   你会答应吗？
   A. 会 / B. 不会

5. **当你使用自动柜员机时，有人试图分散你的注意力。**
   你会转身回应吗？
   A. 会 / B. 不会

6. **你遗失了银行卡。**
   接下来你会怎么做？
   A. 什么都不做 / B. 尽快向银行挂失

答案：

1.B - 永远不要告诉任何人你的密码。

2.B - 这叫“钱骡”，在香港是非法的。

3.B - 如果接受，骗徒可能会获取你的个人资料。

4.B - 可能不是你的朋友提出请求 - 先与他们当面确认。

5.B - 请确保遮盖你的 PIN 码。如果你觉得不安全，直接取走你的卡，并离开自动柜员机。银行分行内部的自动柜员机可能是更好的选择。

6.B - 确保你将遗失或被盗卡背面的号码记录在手机内。