OCBC Bank
65 Chulia Street OCBC Centre
Singapore 049513

恶意软件威胁

学习如何保护您的财务数据免受恶意软件攻击

什么是恶意软件？

恶意软件是一种恶意程式，网络犯罪分子利用这种软件感染目标电脑和移动设备，从而实施犯罪活动。

一旦设备受到感染，网络犯罪分子可能会窃取登录信息（包括网上银行登录账号、PIN 码和一次性密码（验证码）或公司编号、用户 ID 和密码）等机密数据，并利用这些详细信息从受害者的账户中进行欺诈性转账。其他恶意软件可能会在受害者不知情或未经同意的情况下，远程控制被入侵的设备和数据、监视用户的线上活动和/或实施其他犯罪活动，如货币交易和欺诈。

恶意软件类型

了解不同类型的恶意软件及其工作原理有助于保护您的设备免受威胁。

病毒

计算机病毒能够感染计算机系统或网络，通过在整个网络中复制自己来进行传播 - 就像生物病毒。它附着在现有程序上，当用户执行该程序时就会被强行植入其他程序和文件。病毒能够窃取敏感信息、删除或修改文件，甚至对其他系统发起攻击。

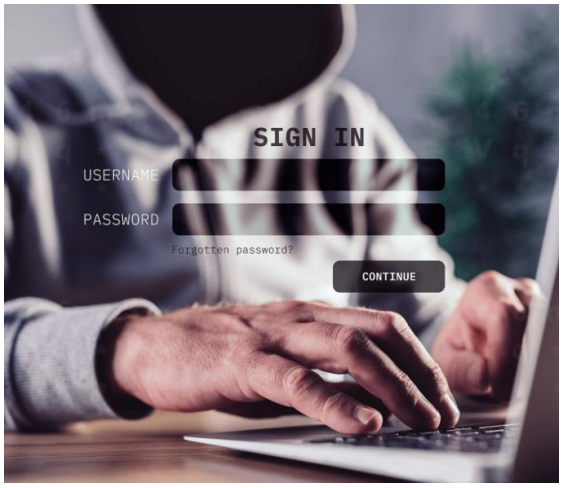
勒索软件

勒索软件是恶意软件的一种，用于对设备或设备操作系统上的个人文件进行加密，从而锁定用户的文件或设备。这将导致受害者无法对重要且通常是机密的数据进行访问，或被中断商业运作。然后，攻击者会威胁称将公布受害者的数据或永久禁止受害者的访问权限，除非支付赎金（通常为加密货币）才会恢复访问权限。

恐吓软件

恐吓软件通常通过弹出式广告传播，目的是诱使用户相信其设备已感染恶意软件，然后哄骗其下载或购买恶意（但毫无用处）的软件来解决所谓的“问题”。

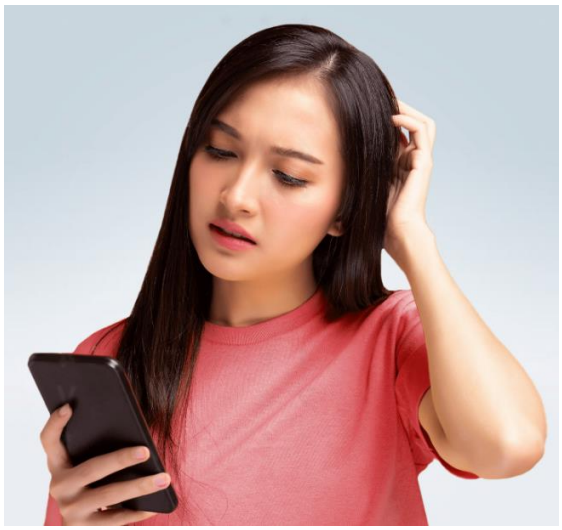
在某些情况下，受害者在下载假冒软件时会需要输入其信用卡信息或其他敏感信息，之后犯罪分子便会利用该等信息进行诈骗。其他情况下，诱使受害者使用假冒软件仅仅是犯罪分子向其设备安装其他类型恶意软件的一种方式。



广告软件/恶意广告

广告软件会在用户设备上展示广告，通常采用弹出式广告、横幅广告等形式。它可以跟踪用户的浏览行为，并收集用户线上活动的个人数据，以便有针对性地投放广告。

另一方面，恶意广告是指通过线上广告平台传播恶意软件的行为。其通常看起来像合法广告，但会将用户引向钓鱼网站或其他恶意网站。



木马

木马是特洛伊木马的简称，是恶意软件的一种，通常伪装成合法程序或文件，并且可能通过钓鱼邮件或软件下载的方式传播。木马一旦被下载，便会进行各种恶意活动，如窃取财务信息或安装其他恶意软件。

间谍软件

间谍软件是在用户不知情或未经用户同意的情况下从用户设备上收集信息，并可用于监控用户的线上活动并窃取敏感信息，如登录信息和信用卡信息。

间谍软件可以通过各种方法安装到设备上，如点击恶意链接或电子邮件附件、安装受感染的软件或访问受威胁的网站。

恶意软件是如何传播的？

钓鱼电子邮件

一种常见的方法是发送带有附件的电子邮件，而这些电子邮件看似来自可靠来源或您可能认识的人。如果您打开附件，则最终可能会在您的计算机上安装恶意软件。

可疑网站

访问恶意网站可能会导致有危害的软件在未经您允许的情况下被安装到您的设备上。这些欺骗性网站往往看似与知名公司的可信网站相似，但其存在的唯一目的就是植入恶意软件和窃取数据。

受感染的下载来源

恶意软件可以通过下载受感染的文件进行传播，这些文件通过短信、WhatsApp 和 Telegram 等消息服务业务或程序发送。恶意软件还可以通过从非官方来源下载假冒软件和移动应用程序、或通过连接到计算机的移动硬盘轻松传播。

恶意广告

网络犯罪分子可以通过在线上广告中植入破坏性的代码来传播恶意软件；他们将这些广告通过合法的广告网络进行传播，并将其展现在各种可靠网站上，从而最终实现传播恶意软件的目的。您甚至不需要点击广告——只要访问主网站，恶意软件便会自动进行安装。

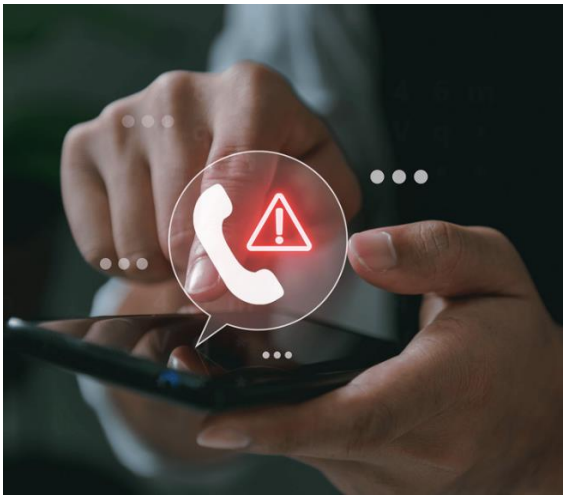
需要警惕的最新骗局

以下列举了从欺骗性特价商品到虚假二维码的一些需要引起重视的恶意软件相关骗局。

安卓系统上的可疑下载

受害者可能会看到特惠活动信息，并被诱骗通过社交媒体或消息平台（如 WhatsApp）与该等虚假企业联系。随后，受害者会收到一个网址，用于下载包含恶意软件的安卓软件包工具包 (APK) 文件，从而让诈骗分子能够远程访问其设备并窃取其个人信息和银行凭证。

请勿随意相信夸大其词、令人难以置信的广告，并避免在设备上下载任何可疑的应用程序。



假冒朋友来电的骗局

诈骗分子会假装朋友或熟人，试图通过电话或短信联系受害者。他们可能不会直接索要钱财，而是借口为各种差事（如预订餐厅或购买家具）寻求帮助而向受害者发送恶意链接。恶意链接会引导受害者下载 APK 文件和/或进入钓鱼网站，诱骗受害者输入其银行信息。之后，诈骗分子会进入受害者的银行账户执行未经授权的交易。

当收到自称是您“朋友”的人打来的异常电话或发送的短信时，需保持谨慎。在进行任何重大交易或透露敏感信息之前，一定要通过其他方式核实对方身份，如与对方见面或通过以往既定的联系方式与对方联系。

恶意二维码

随着商家越来越多地使用二维码，诈骗分子也找到了利用这项技术的新伎俩，他们在商店和餐馆等公共场所的授权扫码支付标志附近粘贴经过篡改的二维码。受害者随即被诱导扫描该二维码，并在不知情的情况下下载植入恶意软件的应用程序，而该等应用程序会窃取机密和敏感数据。

尤其需警惕看似可疑或被篡改过的二维码，并在扫描前向店员确认二维码是否安全。

如何检测恶意软件？

如果您认为自己的计算机或移动设备可能被植入了恶意软件，请留意以下警告信号：

在您的设备上

- 注意设备上出现的您未安装的陌生应用程序与图标、设备屏幕在外观和感觉上的异常变化，或提示您安装未知应用程序或向特定应用程序授予特殊权限的可疑屏幕弹窗。
- 性能问题，包括加载时间过长的应用程序、文件和网站、电池异常耗电情况，以及由于恶意软件在后台运行而导致的设备关机或启动问题。
- 设备突然关机或被锁定，并且屏幕上显示"系统更新中"信息，甚至在强行重启后也是如此。
- 通话过程中出现掉线或异常中断的情况，可能是移动恶意软件造成的干扰。
- 由于恶意软件向贵宾号码发送短信，导致电话/数据账单异常。

在浏览器中

- 重定向至第三方网站，这类网站会显示类似华侨银行登录页面的虚假覆盖页面，并可能提示您输入登录信息、安全令牌中的一次性密码（验证码）或您的自动取款机卡、借记卡或信用卡信息。该网站还可能提供虚假的热线电话号码（非华侨银行官方网站上的联系电话号码）。
- 假冒网站登录页面上显示的网址与华侨银行的官方网页不同。
    - Personal Banking（个人银行业务）：https://internet.ocbc.com/internet-banking
    - Business Banking（企业银行业务）：https://velocity.ocbc.com/login.html

- 即使输入了正确的登录信息，系统还是反复提示您输入登录信息，或者延迟弹出一个窗口显示系统不可用，并反复要求您输入一次性密码（验证码）或使用安全令牌生成一次性密码。
- 您会收到有关并非您生成的一次性密码的短信，或者提示您授权并非由您发起的交易。

如何防范恶意软件

为确保您的网络安全以及账户信息不会通过您的设备泄露，请采取以下华侨银行网上银行安全措施：

确保您的设备安全

使用可靠的安全解决方案，以确保设备的安全性以及始终为最新版本。

- 安装防病毒程序，对其保持更新并定期扫描，以帮助检测未经授权的软件
- 确保将操作系统更新至最新版本
- 切勿使用已越狱及已破解最高权限（已刷机）的手机访问华侨银行移动银行服务
- 采用生物识别技术、强密码或其他相关方法确保您的设备安全
- 检查您的设备是否有随机出现的未知应用程序
- 如果您的移动设备丢失/被盗，以及/或者您怀疑有人未经授权访问您的账户，请立即通知华侨银行
- 切勿在公共场所将您的设备置于无人看管的状态

保障您的网上浏览体验

养成通过安全方式浏览的习惯，减少设备受恶意软件侵害的可能性。

- 亲自在浏览器中输入域名以登录华侨银行网上银行
- 确保您访问的网站属于华侨银行个人银行业务或企业银行业务
- 请勿让您的网络浏览器或设备存储您的登录信息
- 会话结束后，当不再使用电脑时，请立即注销并锁定电脑屏幕
- 请勿使用公共设备或连接不安全/公共 Wi-Fi 来访问网上银行
- 删除计算机中的文件和打印机共享设置
- 浏览互联网时，切勿点击弹窗中的链接

谨慎下载

从未知来源下载任何文件或附件时务必谨慎。

- 请勿安装来历不明的软件或运行来历不明的程序
- 仅从官方应用程序商店（Apple App Store、Google Play Store 或 Huawei AppGallery）下载移动应用程序（包括 OCBC Digital、OCBC Business 和 OCBC Pay Anyone™）
- 请勿打开、运行或安装可疑或来路不明的电子邮件及信息中的任何附件或点击其中的任何链接

查看应用程序权限

了解应用程序在设备上可以访问哪些内容。

- 在安装应用程序之前，阅读并了解其所需权限
- 查看应用程序的预期功能是否有必要获得其所需权限
- 避免对可能泄露您隐私的危险权限进行授权，尤其是请求访问您的摄像头、麦克风、位置、联系人和类似敏感信息的应用程序

检测并处理恶意软件

如果您怀疑您的设备感染了病毒，被植入恶意软件，建议您采取以下步骤：

- 打开“飞行模式”，防止数据传入或传出您的设备
- 检查 Wi-Fi 是否已关闭，并且请勿将其打开

- 查找并立即卸载设备中发现的任何可疑应用程序
- 使用可靠的反病毒或反恶意软件程序对手机进行扫描
- 使用另一台设备检查您的银行/Singpass/公积金计划(CPF)账户等是否有任何未经授权的交易
- 向本行和有关当局报告任何未经授权的交易，并向警方报案
- 完成上述步骤后，如果您认为您的设备未因感染病毒而被植入恶意软件，您可以继续使用该设备
- 作为进一步的预防措施，如果您的设备仍有被感染的迹象，请考虑将其重新格式化为出厂默认设置并对重要密码进行更改