

如何处理可疑电子邮件

学习可疑电子邮件的处理方法十分必要，只有正确处理才能保障您的公司免受网络犯罪分子侵害。如果没用正确的方法，您很可能就会沦为网络钓鱼攻击的受害者。

请按照下面的安全技巧操作，正确地处理可疑电子邮件：

不要回复可疑电子邮件

如果您收到了“熟人”发来的电子邮件，但是对邮件内容有些疑惑，您很可能会回复对方，询问更多细节。但是，一旦您回复邮件，就可能引发更大的安全风险。仔细想想，如果这位“熟人”的电子邮件帐户已经被盗，回复您邮件的人又会是谁呢？您很可能正在跟网络犯罪分子打交道！

不要转发可疑电子邮件

如果收到了可疑的电子邮件，最佳实践是不要点击邮件中的任何链接或附件。但是，如果您掉入了网络钓鱼电子邮件的陷阱，点击了恶意链接，或者是打开了恶意附件，您会发现链接和附件都“货不对板”。例如，您打开了可疑电子邮件中的图片附件，却出现了软件安装窗口。或者，您点击了恶意链接，系统却重定向到了一个仿冒登录页面。

发现链接和附件可疑的时候，您或许想转发这封电子邮件给同事，寻求同事的帮助。但是，转发给同事可能会引发更大的风险。在点击链接或打开附件的时候，如果发现任何可疑的系统行为，都需要当成危险信号。千万不要转发不同寻常/可疑的电子邮件给其他同事。如果您转发的是网络钓鱼电子邮件，就会引发更大的安全漏洞风险，因为您的同事也很可能会点击邮件中的网络钓鱼链接。

不要标记可疑电子邮件为“垃圾邮件”

垃圾邮件一般是指让人生厌的广告邮件。虽然垃圾邮件不受人喜欢，但是这类邮件通常都是无害的。相比之下，网络钓鱼电子邮件伪装得真实可信，却往往伴随着钓鱼网络攻击。网络钓鱼电子邮件往往运用了行动号召 (CTA) 设计，比如要求用户点击链接、打开附件甚至是转账汇款。

如果您把网络钓鱼电子邮件标记成了“垃圾邮件”，那么系统在收到该发件人的邮件后，都会自动把这些邮件归入“垃圾邮件”文件夹中。一旦可疑邮件归入了“垃圾邮件”文件夹，就会隐藏不显示。但是，依然没有彻底解决掉后患。

保障安全的技巧

处理可疑电子邮件的最佳实践是向您的公司上报这类电子邮件。一旦上报，公司的 IT 团队就能评估和缓解威胁。

如果收到了可疑电子邮件，请按照下面的安全技巧操作来防范威胁：

- 按照公司的流程，正确地上报可疑电子邮件。按照网络安全协议的规章行事，可以让所有人的信息安全得到保障。
- 如果您不知道如何上报可疑电子邮件，请把邮件留在收件箱，不要擅自处理，然后及时请经理/主管帮忙。
- 如果您无法分辨收到的电子邮件是垃圾邮件还是网络钓鱼电子邮件，请上报给 IT 团队，留给专人处理。

