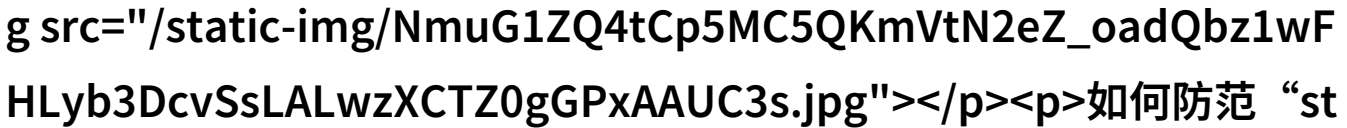
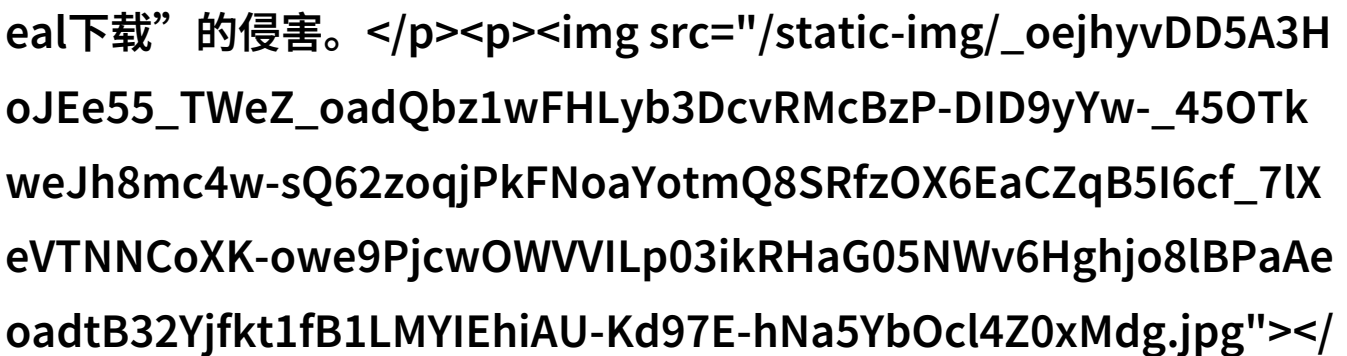


# 网络安全-如何防范steal下载软件的危害

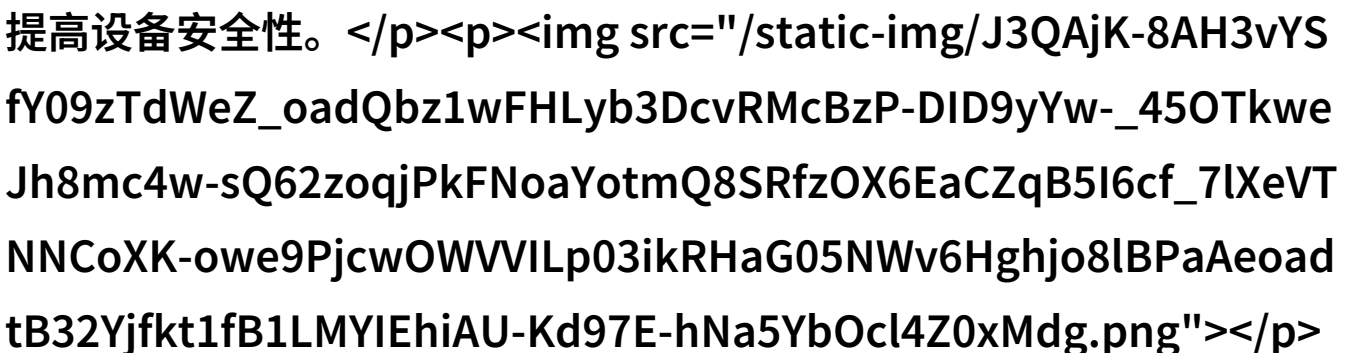
在数字化时代，互联网上的资源丰富多样，但同时也带来了诸多安全隐患。&#34;steal下载&#34;作为一种不法手段，它的存在让用户在获取所需软件或资料时面临着数据泄露、病毒感染等风险。以下是关于如何防范&#34;steal下载&#34;软件的危害的一篇文章。

如何防范“steal下载”软件的危害

随着网络技术的发展，越来越多的人开始通过非法途径获取免费软件，这种行为被称为“steal下载”。然而，这种做法往往伴随着严重的后果，如个人信息泄露、电脑系统崩溃甚至连续性犯罪。在此，我们将探讨几项关键措施，以保护自己免受“steal下载”的侵害。

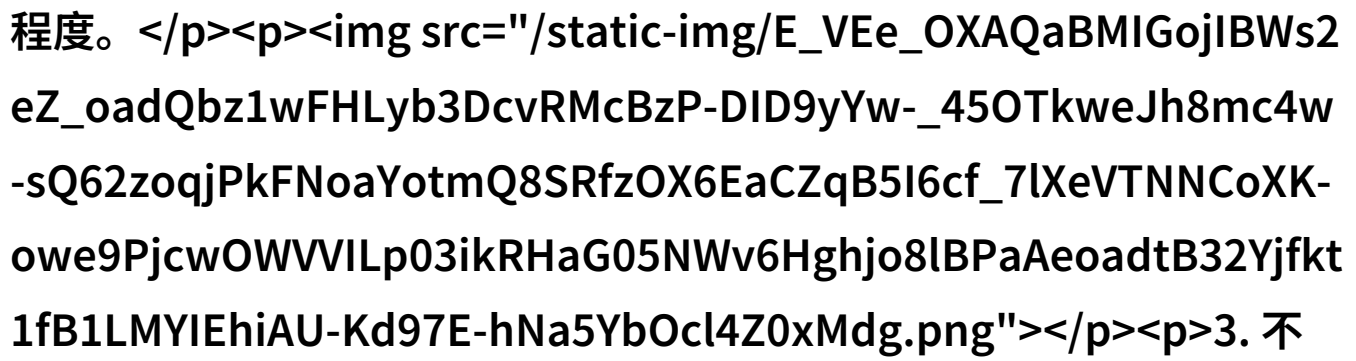
1. 确保操作系统安全

首先要确保你的操作系统具备足够高级别的防护能力。这包括安装最新版本的操作系统更新和安全补丁。此外，可以考虑使用第三方安卓应用管理器如360手机助手、Qihoo 360 Mobile Safe等，它们提供了实时扫描和清理恶意代码功能，有助于提高设备安全性。

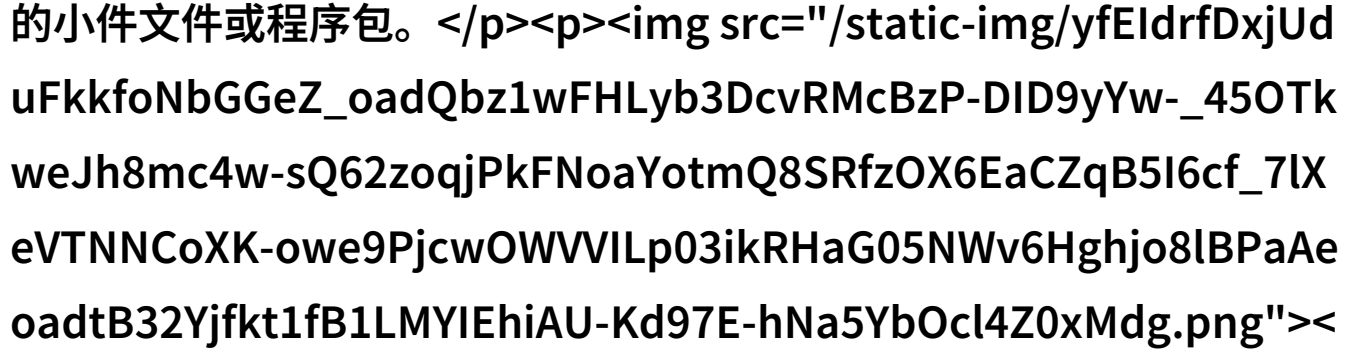
2. 使用合适工具进行文件传输

当你需要从不信任来源下载文件时，最好不要直接点击链接，而是使用专门设计用于加密文件传输和保护用户隐私的手段，比如Tor浏览器或ProtonMail服务。这些工具

可以降低被攻击者的风险，使得即使遭遇黑客攻击，也能减少数据损失程度。

3. 不要轻易相信陌生链接

网络上充斥着诱人的免费资源，但请记住，一旦点击那些看似诱惑性的链接，就可能触发潜藏在其中的小偷程序。因此，在没有确认对方可靠的情况下，不要轻易点开任何未知源头提供的小件文件或程序包。

4. 提高个人警惕性

最后，提升自己的网上意识也是非常重要的一环。一旦发现有任何异常活动，如莫名其妙的大量广告弹窗或者电脑运行缓慢，请立即断开互联网连接，并及时备份重要数据以防止丢失。如果怀疑已经感染了恶意软件，可寻求专业技术人员帮助进行清除。

总之，“steal下载”虽然吸引人，但它背后的潜在风险远远超过了短暂的心动。而我们每个人的责任，是保持对数字世界的敬畏，以及采取必要措施来保障自身信息安全。

[下载本文pdf文件](/pdf/640441-网络安全-如何防范steal下载软件的危害.pdf)