如何在打开二维码前判断是否安全（网络钓鱼防范指南）

二维码网络钓鱼（Quishing）正在迅速蔓延。了解扫描前的危险信号以及扫描后点击『打开』前应检查的内容。

作者：Lubor Šimůnek • 发布日期：August 23, 2026 • 安全

在线版本：https://appstoryo.com/zh-hans/blog/qr-code-safe-quishing-guide



什么是Quishing?

Quishing是通过二维码实施的网络钓鱼攻击。攻击者制作一个二维码，扫描后会将用户引导至恶意网站，目的是窃取账号密码、安装恶意软件或呈现虚假支付页面。这个词由『QR』和『phishing（钓鱼）』合成，由于人们几乎不加思考地信任二维码，此类攻击正在快速增长。

二维码为何具有特殊风险

对于普通链接，可以将鼠标悬停在上面查看URL再决定是否点击。但对于二维码，在扫描器解码之前无法看到目标地址——而且许多相机应用会直接打开浏览器而不显示地址。就在这短暂的瞬间，恶意网站已可能开始追踪您的设备。

二维码还能完全绕过垃圾邮件过滤器。过滤器会扫描可疑文本或已知恶意URL，但二维码图片看起来完全无害。正因如此，网络钓鱼邮件越来越多地用二维码替代超链接，尤其是在针对企业员工的攻击中。

现实生活中，Quishing常见于：贴在停车收费机合法二维码上的贴纸、伪造的餐厅菜单、投入信箱的快递诈骗通知，以及要求『扫码付款』的虚假公共充电站。

扫描前需注意的危险信号

- 贴在原始二维码上的贴纸。贴在另一个二维码上的二维码贴纸是典型的替换手法。轻轻掀起一角——

如果能揭开，请勿扫描。

- 陌生传单上的紧迫性语言。'立即扫描领取奖品'或'您的包裹被扣押——扫码重新安排派送'是施压手段。
- 未经请求的邮件或信函。来自银行、快递公司或政府机构的意外通信，以二维码作为主要行动号召，是强烈的警告信号。

扫描后、打开前需检查的内容

- 域名是否符合预期？如果您在银行扫描了二维码，URL应该位于官方域名上。
- 是否使用了短链接服务？bit.ly或tinyurl.com等服务隐藏了真实目标地址。访问前请使用URL展开服务查看真实地址。
- 拼写错误或仿冒域名。注意paypa1.com（用数字1代替字母L）或g00gle.com（用数字0代替字母O）。仔细阅读每个字符。
- 可疑子域名。login.secure.amazon-delivery-cn.com看似合法，但真实域名是amazon-delivery-cn.com，而非amazon.com。

QR Code Reader Without Ads如何提供帮助

QR Code Reader Without Ads在打开任何内容之前会显示完整的URL预览，让您有时间检查链接后再决定。如果地址看起来可疑，只需不点击『打开』即可。该应用在您的设备上本地保存扫描历史记录，不收集数据，也不显示广告。请在App Store或Google Play搜索『QR Code Reader Without Ads』。

立即在 iOS 或 Android 上免费下载 **QR Code Reader Without Ads**——无广告、无跟踪，完全离线运行。

引用格式: Lubor Šimůnek (2026). 如何在打开二维码前判断是否安全（网络钓鱼防范指南）. AppStoryo, lapnito.cz s.r.o.. https://appstoryo.com/zh-hans/blog/qr-code-safe-quishing-guide
© 2026 lapnito.cz s.r.o.