

二维码的安全问题

简译版

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	QR Code Security: What You Need to Know Today		
原文作者	迈克·埃尔根 (Mike Elgan)	原文发布日期	2021 年 1 月 19 日
作者简介	迈克·埃尔根是 Computerworld 的专栏作家。		
原文发布单位	Security Intelligence		
原文出处	https://securityintelligence.com/articles/scan-qo-what-to-know-about-qr-code-security-today/		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antivy.cn 安天公益翻译板块		
免责声明	<ul style="list-style-type: none"> 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公有方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。 		

二维码的安全问题

迈克·埃尔根

2021 年 1 月 19 日

如今，二维码（QR）的使用非常普遍，这促使攻击者开始利用它们进行牟利。那么，攻击者如何利用二维码牟利呢？企业又该如何增强二维码的安全性，以防止此类诈骗呢？

二维码的使用范围

二维码（“快速响应代码”的简称）诞生于 1994 年，是日本汽车零部件制造商 Denso Wave 用于跟踪汽车工厂中零部件的一种方法。通过扫描这些二维条形码，智能手机的相机可以即时读取多达 4000 个字符的信息。

在数十年的使用和推广之后，二维码达到其巅峰时期。在 2020 年，大量消费者和企业开始采用非接触式解决方案。以应用程序为中心的支付公司、慈善机构、非营利组织和销售点系统，开始使用在线二维码生成器创建消费者门户，从而避免按键和信用卡交易。

大型科技公司正在大力推广二维码的使用。硅谷公司（以及其他公司）发现，二维码可用于推广零售商店、交易等用途中的自助服务信息。最有趣的是，二维码对增强现实也是有帮助的。物体、墙壁或桌子上的二维码贴纸既可以充当 3D 空间中虚拟现实对象的锚点，又可以充当数据源。

如今，智能显示器也支持二维码，消费者可以扫描二维码将物品添加到购物清单中。此外，社交网络也开始使用二维码，用户可以扫描二维码查看对方的个人资料。毫无疑问，二维码已经成为一种主流趋势。

MobileIron 的一项调查发现，84% 的受访者曾扫描过二维码，三分之一的受访者在之前一周扫描过二维码。这就引发了一个问题：二维码安全吗？

二维码的安全问题

对用户来说，二维码的确很方便。但是对于犯罪分子来说，二维码的功能同样很强大。

首先，二维码可以用作 URL，给用户带来与“在手机上打开恶意网站”一样的风险。但是相比于 URL，用户识别出恶意二维码的可能性更小。除了用作 URL 之外，二维码还可

用于编写电子邮件或短信，以及打电话，这也会为犯罪分子提供便利。然而，超过三分之一的 MobileIron 受访者表示，他们并不担心使用二维码会带来安全风险。

攻击者可以通过即时消息、社交媒体、电子邮件、短信等途径发送恶意二维码。二维码可以在智能手机上启动操作，例如启动支付应用进行付款、添加联系人或关注社交媒体上的恶意账户等。此外，它们还会泄露受害者的位置或添加恶意 Wi-Fi 网络。

动态二维码是一种特殊的风险。它们可以更改存储在其中的数据，也可以将不同的数据呈现给不同类型的设备。

二维码的兴起也伴随着加密货币的兴起，这会带来严重的后果。比特币地址通常通过二维码传输，这比输入冗长的比特币地址要方便得多。二维码中会注入数据，而比特币就是数据，因此攻击者会利用二维码窃取比特币，这是不可避免的。

防御二维码诈骗的建议

用户可以通过下述几种方法，最大程度地减少二维码诈骗和安全风险。

- 如果有人向你发送了二维码，请与其所声称的“发送者”联系，向其询问是否发送了二维码。
- 如果扫描二维码后出现 URL 链接，则这些链接可能是恶意链接。
- 面向企业的建议：部署移动防御解决方案，以防止网络钓鱼、漏洞利用、手机劫持和未经授权的下载等攻击。
- 采用多因子身份鉴别，来代替对应用程序和云资源的口令访问。

如今，企业应注意，在保护移动数据时，要涵盖所有的数据库，将防范不断增长的恶意二维码放在首要位置。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队,始终坚持自主先进的能力导向,依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累,研发智甲、探海、镇关、捕风、追影、拓痕等系列产品,为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系,依托全面持续监测能力,建立系统与人员协同作业机制,指挥网内各种防御机制联合响应威胁,实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合,协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设,支撑起协同联动的实战化运行,赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方,全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴,目前,安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点,在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面,实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体(如 APT 组织)及其攻击行动,进行持续监测和深度解析,协助客户在“敌情想定”下形成有效防护,通过深度分析高级网空威胁行为体的作业能力,安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可,已连续六届蝉联国家级安全应急支撑单位,是中国国家信息安全漏洞库六家首批一级支撑单位之一,亦是国家网络与信息安全信息通报机制技术支撑单位,国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日,在习近平总书记主持召开的网络安全和信息化工作座谈会上,安天创始人、首席架构师作为网络安全领域发言代表,向总书记进行了汇报。2016 年 5 月 25 日,习近平总书记在黑龙江调研期间,视察了安天总部,并对安天人说,“你们也是国家队,虽然你们是民营企业”。

安天实验室更多信息请访问: <http://www.antiy.com> (中文)

<http://www.antiy.net> (英文)

安天企业安全公司更多信息请访问: <http://www.antiy.cn>

安天移动安全公司 (AVL TEAM) 更多信息请访问: <http://www.avlsec.com>