# 如何保护家庭摄像头

**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** | Top Tips for Securing Home Cameras | | |
| **原文作者** | Matthew Rosenquist | **原文发布日期** | 2017 年 1 月 4 日 |
| **作者简介** | Matthew Rosenquist 于 1996 年加入英特尔公司，在安全领域工作了 20 多年。他专注于安全战略，衡量价值，开发具有成本效益的能力和组织。https://securingtomorrow.mcafee.com/author/matthew-rosenquist/ | | |
| **原文发布单位** | 迈克菲实验室 | | |
| **原文出处** | https://securingtomorrow.mcafee.com/mcafee-labs/top-tips-for-securing-home-cameras/ | | |
| **译者** | 安天技术公益翻译组 | **校对者** | 安天技术公益翻译组 |
| **免责声明** | • 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共方式，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。<br>• 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。<br>• 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。<br>• 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。 | | |

# 如何保护家庭摄像头

Matthew Rosenquist

2017 年 1 月 4 日

安装家庭监控摄像头有很大的好处，但也可能会导致新的隐私和网络安全风险。用户希望在提高安全性的同时避免网络安全威胁。我们给出了三个建议，您可以在购买、安装和配置家庭摄像头时予以参考。

## 风险

家庭连网摄像头是网络犯罪分子的重要目标。最近发生了很多大型的物联网（IoT）攻击事件，黑客感染了数十万的物联网设备，并将它们纳入大规模僵尸网络。这些僵尸机器(包括 IP 摄像头，数字录像机和家庭路由器等）根据控制者的指令，将网络流量发送到指定的站点。大量的数据流导致目标站点崩溃，使其无法提供正常的服务。最近针对 DNS 服务提供商 Dyn 的攻击使得美国东海岸大部分网站(包括 Twitter，Spotify，Netflix，Amazon，Tumblr，Reddit，PayPal 等）下线。攻击家庭设备已经成为网络犯罪分子的一个有效手段。您正在考虑的家庭摄像头可能会成为黑客窥探您的工具！

大多数攻击没有想象中的复杂。我们能够将它们追溯到设计不够安全的产品，未打补丁的漏洞和较差的安装配置。保护设备的安全不一定多么困难或耗时，但确实需要预先考虑和

持续关注。

## 保护家庭摄像头的三大建议

### 选择可靠的厂商

良好的开端等于成功的一半。如果隐私和安全对您来说很重要，那么您在购买摄像头时应加以充分的考虑。并非所有的家庭摄像头厂商都是一样的。请选择那些努力保护用户隐私和安全的厂商。该如何分辨呢？不要看他们的营销广告（因为所有厂商都会鼓吹“安全”一词），而是去他们的网页看看。您要考虑的问题是，厂商是否认真地考虑安全性并采取相应的措施。请查看他们是否发布了安全更新，是否设立了安全小组，是否详细说明了他们如何保护产品和服务。

没有什么产品能够永远安全，特别是物联网设备。重要的是厂商为保持客户的产品安全做出了什么程度的努力。如果厂商开发安全补丁并向客户解释发现了什么漏洞，那么他们就是负责任的。透明是信任的标志。而您要做的，就是为产品打补丁。

许多厂商不愿费劲去成立一个安全团队。如果厂商没有专业的安全团队，您就要小心了。这意味着他们不太可能设计出强健的安全功能，意味着他们没有漏洞查找人员，没有补丁开发人员，没有验证补丁安全性的人员。

拥有安全团队的厂商应该公开讨论产品设计中的控制措施、测试标准、认证以及发现的漏洞。我很欣赏那些设立了漏洞赏金计划的公司，他们会奖励并关注那些发现漏洞的白帽黑客。让黑客们帮忙查找产品漏洞的确是个好主意。

这是最重要的一步。您必须选择可信的摄像头、软件和服务厂商。您可以查看客户的评论和测试这些摄像头的安全专家的评论。选择靠谱的厂商，您一定会获得回报。

### 设置在非敏感区域

监控摄像头是了解家庭情况的好工具。但是在某些时候，即使最好的产品也会被感染。因此，放置摄像头的位置至关重要。家门口、公共区域和婴儿房就是不错的地方。最好不要放置在卧室、更衣室、浴室和其他私人区域。许多现代摄像头配备了麦克风和其他传感器。所以即使在公共区域，您也要注意自己的言论。家庭摄像头便于设置，处理数据时也不麻烦。大多数家庭摄像头利用云服务存储数据，您可以随时随地地查看。这是一个很棒的功能，但

这也意味着监控视频不由您直接控制 ,因此也是一个攻击点。请考虑要在云中存储哪些数据，您肯定不想让尴尬或私人视频出现在网上。摄像头的安装位置将决定这一点。

## 更改默认密码

家庭摄像头有很多默认设置，便于用户轻松设置。大多数设置不需要修改，但是您必须更改默认密码！请创建唯一的强效密码，将它存储在安全的地方。最糟糕的情况是，如果您忘记了密码，可以在摄像头上进行重置。很多物联网僵尸网络变种正是以大量采用默认密码的设备为目标，攻击者可以从网上找到这些密码，进而访问这些摄像头。一些厂商强制要求用户在安装时更改默认密码，其他厂商则不这样要求。请您务必要更改默认密码，这会带来很大的不同。

家庭摄像头的确很棒。它们为我们的现代生活提供了新的安全感和灵活性。但是您必须在这些好处和伴随的风险之间取得平衡。遵循这三个建议，您可以更好地控制摄像头，使自己更加安全。