十招保护你的数据和隐私

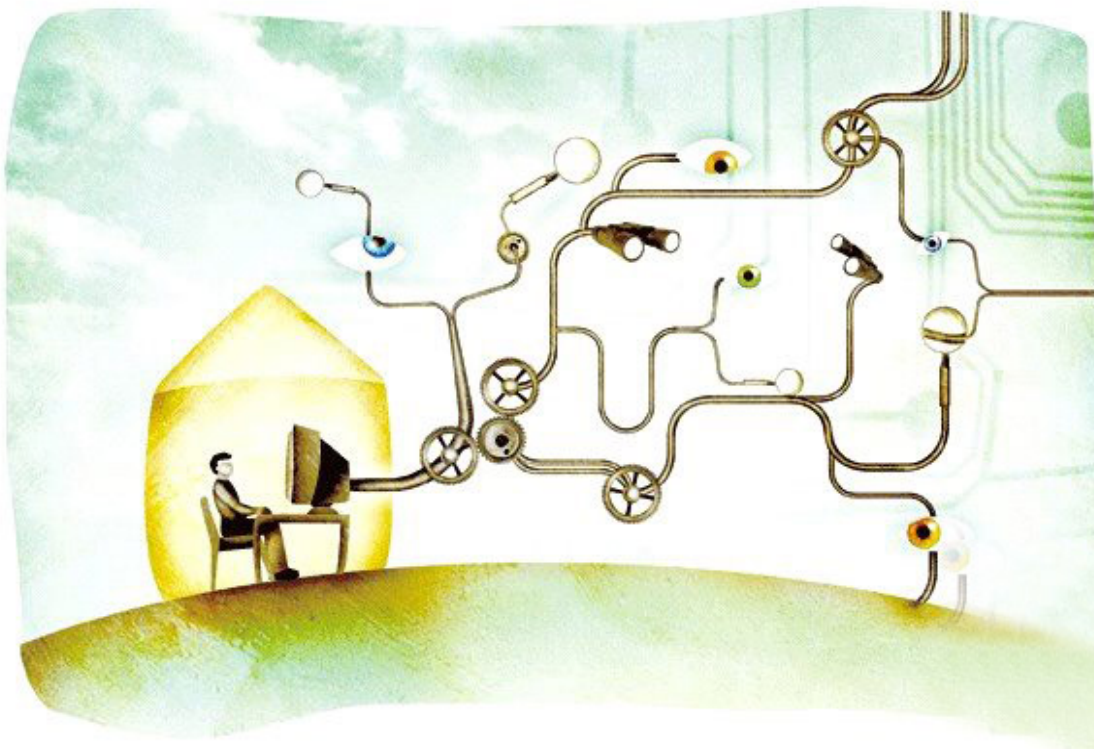
网络时代，大数据应用无孔不入，各种衣食住行的应用程序如同雨后春笋层出不穷，对个人用户的情况也了如指掌。虽然说应用程序变得越来越精准，方便了大众生活，提升了工作效率，但是也越来越容易引发安全问题，容易泄露用户隐私数据，引发信息安全危机。

在当今世界，如何保护个人信息，防止隐私泄露？科学家们提出了多项建议，希望用以下快速、简单的措施，通过各种验证手段，加强信息保护，使网络运行更加安全。

我们往往会认为，只有大公司或一线明星，才担心自己会被黑客缠上，担心吃早餐时会被人偷拍数百张照片。其实，我们的手机、电脑和平板电脑，都是储存各种信息的宝库，黑客可以利用这些信息来冒充你，或者将你的信息卖给出价最高的人。

“想想你的智能手机，可能会被人当成一种非常有效的跟踪装置，”Justin Cappos说，他是纽约大学工程学院计算机科学系网络安全专家，也是副教授。“当你下载一个应用程序时，你可能会允许它访问你的麦克风，你的相机，你的全球定位系统，你的WiFi，你的蓝牙，你的指纹，你的联系人列表，你的银行账户……这些都是非常敏感的信息。”

那么，你是否因此而将手机抛弃呢？在你把自己的手机扔进大海之前，这里有一些简单的方法，让初学者保护自己的隐私。



■ 及时更新修补漏洞

我们常常会看到电脑或者手机弹出一个窗口，要求重启系统。虽然重启系统的弹出窗口可能会让人讨厌，但它们通常是用来提醒你修补安全漏洞的。“想一想，那些要求你更新系统的提醒，每一天提醒，就等于向你发布一条警告信息。黑客现在可以随时侵入你的手机，我们要不要修好它？”Cappos教授这么说。

■ 提高防御能力

你可能会更改所有的密码，我们中的大多数人也不会点击未知电邮中发送的随机信息，但在社交媒体上，我们的防御能力下降了。这一切听起来似乎难以置信，但确实有很多人在重复同样的错误，使用那些简短而原始的密码。“简短而原始的密码，特别容易受到黑客的攻击。”Cappos说。

■ 留意社交媒体

如果你认为你在社交媒体上最冒险的举动，顶多是不让你的老板看到你在星期日深夜喝鸡尾酒，那么你不妨再想想，“身份窃贼喜欢通过各种社交媒体来收集你的有关信息，比如电子邮件或你的生日，然后用这些信息来进入你的电子邮箱。”Cappos指出。

所以，在你公布个人信息如姓名、日期和地点之前，一定要仔细掂量；同时，要确保你的密码不是人们能从你的社交媒体文章中猜到的；第三，只与你在现实生活中认识的人联系，不随便与陌生人交友。

■ 双重步骤确保手机安全

“通过采取两个步骤，验证你的身份，确保你的设备比如手机是值得信赖、可以登录的。”Cappos说。如此一来，即使黑客有你的密码，他们也需要通过你的手机才能进入你的账户。

具体而言，就是设置相应的保护密码或者安全验证机制。不要怕麻烦，因为一旦信息泄露，可能造成更大的麻烦。

■ 谨慎输入敏感信息

在公众场合，大多数WiFi都不加密，难以保护你的数据，所以千万不要在公共场合输入敏感信息———如网上银行或购物场所。当你在一个公共网吧上网时，不要透露个人资料。“还有，记住保护你的手机。另外还要记住，尽管你的计算机可能有杀毒软件，但是你的手机往往没有杀毒软件，所以要小心。”Cappos表示。

■ 云控制

随着AI人工智能技术的不断进步，并且与大数据结合，从而进一步提升机器算法的准确性。但由于大量依赖云端运算，人们常常遭遇难以预知的安全隐患。

云端运算听起来柔软可爱，但它却是黑客梦寐以求的目标———除非你有密码保护它。“云存储服务会自动备份您的信息，如照片和文件。”Cappos说，但不要认为它是安全的———这种情况可以问问在2014年被黑客盗取个人照片的那些名流。“我们必须确保只有唯一的密码可以访问您的云文件，密码随时更改，并且启用两步验证。”

此外，如果不是特别必要，最好要关掉“iCloud”，毕竟很多用户不需要这个功能。具体如何操作？网络上有很多相关的操作教程。

云控制指的是搭载了云技术实现远程控制，可以用任意一台PC通过云端控制手机终端上的任何资料，随意调取自己所需的信息，或者使用另一部手机用ID登录云服务器。

■ 提防摄像头

“如果我演示给你看，让你了解一个人闯入你的笔记本电脑、远程访问你的摄像头是多么容易，那么你会感到震惊，”Cappos说。“我强烈建议人们，当他们不用摄像头时，用贴纸或者其他东西盖住它。”

■ 清理应用程序

你运行的软件和服务越多，你面临的安全风险就越大，所以必须删除或停用你已经不使用的应用程序和服务，并定期清除浏览器上的缓存和cookies。

“最近的一项研究发现，大约有200的应用程序，可以追踪到使用者的超声波音调。”Cappos说。这些音调基本上起到了“风向标”的作用，使营销人员能够跟踪你在哪里上过网，了解你看过什么信息。Cappos警告说：“一旦这些数据被收集整理，那就是非常有用的信息。”

有时候检测某人是否进入某一地区、了解说明他们在做什么，可以通过短距离无线系统来实现，例如，人们可以使用短距离系统来确定客户是否走进一家商店。如果客户运行着某个应用程序，当他们进入商店大门时，应用程序就会告诉跟踪者。

■ 小心处理私密文件

尽量不在iCloud和共有云存储空间放置过于私密的照片或者机密文件，防患于未然是非常重要的。

在AppStore中，通讯录和文件备份应用多如牛毛，如果一家备份服务提供商有一定的可能泄露你的资料，那么用了十种备份服务的你，个人资料就有十倍的可能被泄露。所以尽量使用本地备份。

■ 维修前要保护隐私文件

如果需要维修，那么最好在维修前将自己的手机内容转移，尤其是私密照片和文件另存在其他地方，一些账户也要退出登录，以免出现问题。

人们一直认为，个性化和隐私，往往是很难兼顾的。如何在这两者之间找到一个平衡点，在保护用户隐私的同时，给人们带来足够好的个性化体验？

除了整个社会加强立法、采取有力举措外，还应推动形成全社会数据使用规范，从数据精度处理、数据人工加扰、数据周期保护、隐私数据特殊保护等入手，维护个人信息安全。

而作为个人，则应提高依法保护信息安全的意识，倡导有节制地使用个人信息，从而规避大数据技术发展带来的信息安全风险。

与此同时，也希望在不远的将来，科学家们能够交出一份令人满意的答卷。

据《南方都市报》

档案

黑客盯上明星

2014年夏天，数百张艳照被发布到网上，在全球引起了轰动，由于其中很多照片来自好莱坞当红女星和男星，所以引发了一系列讨论和关注。随后，从黑客口中得知，问题来自于苹果的iCloud漏洞，导致黑客下载了大量的照片。

之后一段时间事件持续发酵，照片源源不断地出现在网络上。到了9月份，第二次大批量集中曝光，应该是同一批黑客所为，只不过是分批泄露出来而已。

直到2016年年初，美国警方才抓到犯罪嫌疑人，这名叫做Ryan Collins的美国人在法庭上认罪，承认自己违反了计算机欺诈与滥用法以及在未经授权的情况下访问了一台受保护的计算机以盗取信息。但他没有承认使用了“撞库”的方式，而是利用钓鱼邮件骗取了受害人的iCloud和Gmail账户密码。他假借苹果公司的名义向这些受害人发送电子邮件，要求她们重设密码。最终该男子正式被判处18个月监禁。

2016年9月份，第二名涉及到艳照门事件的黑客Edward Majerczyk也被判入狱，美国芝加哥地方法院作出裁决，Edward Majerczyk非法入侵受保护的计算机并窃取私人信息罪名成立。他的作案手段与Collins类似，都是通过发送伪装苹果官方邮件来获取受害者的登录信息。他所制造的iCloud艳照门牵涉到的账号超过300个，而且也有相当一部分名人在内。

2017年，令人心痛的是，同样的事情还是再次发生了，而且今年这次出现的艳照门不仅涉及了好莱坞女星阿曼达·赛佛瑞(Amanda Seyfried)和英国女星艾玛·沃特森(Emma Watson)，甚至还有奥斯卡影帝西恩·潘(Sean Penn)的女儿黛伦·潘(Dylan Penn)。

而且这次黑客非常嚣张，甚至声称会继续分享更多女星的私密照，并且预告了奥斯卡影后詹妮弗·劳伦斯(Jennifer Lawrence)、卡戴珊的妹妹凯莉·詹娜(Kylie Jenner)等人，势头丝毫没有输给当年艳照门的劲头。