避免在公共WiFi下网购

免费WiFi会“偷”钱，诈骗电话背后的运营商是推手、微信AA收款有陷阱、手机实名制形同虚设……随着互联网对人们生活的渗透不断深入，全新的安全威胁也如影随形。在今年的央视3·15晚会上，互联网、移动通信领域的各类骗局被大量曝光，让不少消费者心头一惊。那么，对于这些被曝光的安全问题，我们应该怎么防范呢？

黑客可利用虚假WiFi盗取用户的手机系统、品牌型号、自拍照片、邮箱账号密码等各类隐私数据，这可不是虚构的事情。根据央视曝光的情况，目前公共场所的免费WiFi网络中就存在不少“钓鱼”WiFi，一不小心，用户的个人信息就会落入这些居心叵测的人手中。

那么，这是否意味着我们对所有的公共WiFi都要拒而远之呢？

网络安全专家表示，当用户的邮箱账号密码被黑客获取后，的确可能会导致私人邮件和商业邮件的泄露，还会导致通过邮箱注册的微博、网站以及网络支付账号密码泄露，最终导致财产损失。而当前各大商场、饭店、酒店、娱乐场所均提供免费WiFi上网服务，很多手机用户也已经习惯“蹭网”，因此保障WiFi上网安全变得至关重要。据360手机安全中心发布的《2015中国WiFi安全绿皮书》显示，全国超过1亿个家用WiFi中，有超过400万的家用WiFi使用了简单的数字组合弱密码，而这种弱密码在15分钟内即可破解成功。而相比家庭WiFi，连接公共WiFi更容易掉入黑客陷阱，遭受财产损失、账号安全、隐私泄露等威胁，广大手机用户在蹭网、连接打着官方名称的WiFi时，都应提高警惕。

对于日益严重的虚假WiFi现象，腾讯手机安全专家表示，首先行业内应该建立免费WiFi安全接入标准，其次手机用户在连接免费WiFi时，可先通过手机安全软件进行网络安全检测。用户在公共场合使用免费WiFi时，不要登录没有密码的WiFi，尽量不要在公共WiFi下网购或登录网银、第三方支付平台，防止用户个人信息、重要账号、密码泄露等。此外，也不要使用破解WiFi密码的手机工具，谨防被此类工具盗取隐私。

多种手段验证诈骗电话

在央视的3·15晚会上，“透传”一词一夜走红，这本来是电信领域的专业术语，但和一些不法呼叫中心的“改号”（学名：虚假主叫）行为相结合，却成为骚扰电话、诈骗电话日益猖獗的温床。对此，日前工信部已经责成三大运营商和所在省市的通信管理局展开调查，而被曝光的移动、电信、铁通等运营商也相继公告称，一旦查实将严惩。不过，由于目前调查结果还没有公布，整治效果如何，我们还不好判断。在这种情况下，我们有没有什么办法来提高辨别真假的能力、保护自身的权益呢？

办法当然是有的。据安全专家介绍，对于此类被“透传”的骚扰电话或者诈骗电话，回拨验真是一个比较简单直接的方法。因为不少骚扰电话、诈骗电话都是通过电脑拨打出来的IP电话，直接回拨的话是无法接通的。此外，智能手机用户可以通过安装一些第三方应用厂商提供的防骚扰电话软件进行智能化识别。例如搜狗号码通、360安全卫士、小米黄页等软件都提供了这种功能，这类软件提供的电话标记功能大多建立了云端数据库，可以将用户标识的骚扰电话号码的信息存储在云端，在有电话呼入的情况下进行比对，从而起到一定的警示作用。不仅如此，目前这些互联网安全厂商还正在开发号码呼入的同时，进行联网询问号码主人是否在进行呼叫的验真功能，这主要针对的是银行、信用卡中心等社会机构，虽然成本比较高，但安全防护的效果也更好。

另外，有关政府部门也反复强调，110、119等公共号码是不会主动呼出给用户的，而那些有着明确区号前缀的“110”等号码，百分百都是骗局，对此，普通消费者也要时刻谨记，以免上当受骗。

安全软件搞定手机病毒

其实，除了央视3·15晚会上曝光的种种信息安全问题之外，随着智能手机的日益普及，手机病毒、木马也正在成为个人用户信息安全的一个重大威胁。近日，就有不少手机用户反映，一种名为“10086积分兑奖”的新骗局正在流行。对此，猎豹移动安全实验室的专家表示，这其实是诈骗分子利用钓鱼网站引诱用户提交个人信息并下载手机病毒的典型案例，一旦用户的手机中毒，其银行卡的钱就很可能被犯罪嫌疑人通过捆绑第三方支付转移。

不仅如此，今年3·15前，广州警方成功抓获的“相册”新型手机木马病毒也相当可怕。据披露，该病毒的制作者何某利用笔记本电脑和短信群发器工具，已经控制了1.2万台手机，盗取了400多万条手机短信。除了短信钓鱼之外，年轻人热衷的社交网站和大型网游中，也同样有不少盗号的木马病毒触摸，这些骗局的手法也惊人的相似，都是通过隐藏聊天界面向用户弹出网络异常或者钓鱼登录框，诱导用户输入账号和密码，从而盗取其账号及游戏装备。

对于这些横行的木马和病毒，腾讯网络安全专家表示，当用户收到可疑的短信时，最好不要轻易打开其中的网址链接，不要填写银行账号密码等重要信息；不轻易点击短信中的链接安装软件；注意保护好身份证号码、常用手机号等个人信息，不要泄露给陌生人；其次，手机用户应养成使用安全软件来保护手机安全的良好习惯。用户在接到“网购退款”、“航班改签”等电话诈骗和短信时需提高警惕，谨防上当受骗。

网络安全要开放也要自律

马化腾在全国两会中指出：“研究制定我国公共数据开放战略，将政府公共信息与数据向全社会开放，打破行业信息孤岛，确保社会公众能及时获取与使用公共信息；同时，逐步建立数据安全保护体系和数据开发利用的标准，确保数据的有效使用和相关方权益。”事实上，应对网络安全问题，“开放做安全”的理念与把数据共享与开放付诸实践，比互联网其他领域所声称的开放更加重要和实际。毕竟，当安全都要分平台分派系的话，那本身就是不安全的一种体现。

中国互联网协会网络与信息安全工作委员会秘书长严寒冰曾强调，“随着智能终端的广泛普及，网民在享受智能终端带来便利的同时，也在遭受恶意扣费、隐私骗取、变相欺诈等恶意APP侵蚀用户利益的不法行为，我们必须及时遏制恶意APP的传播，避免其造成大范围的严重危害，影响人民生命财产安全。”目前在移动互联网的大潮中，用户对于应用本身的了解更加趋向于应用层面，而应用本身能够自律则成为了安全的关键，依靠安全企业的查杀固然是一种净化的渠道，但毕竟不是长远之道。（新华）