关注黑客攻防最阴险七大黑技计算机等级考试 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/580/2021_2022__E5_85_B3_E6_B3_A8_E9_BB_91_E5_c98_580470.htm 如今，逢此“ 信息就在指尖 ”的互联网时代，不少人都拥有自己的电子邮件、QQ号码、MSN等与亲朋好友联系的通信工具，更有许多人在社交网站上注册了自己的账号，这无疑会极大地方便我们的工作与生活。但随着利欲熏心的不法之徒盯上社交网络，普通的用户在上网时便面临着巨大的“ 被黑 ”风险。 社交网络重点在于构建有着共同兴趣和活动的人们的在线社团，它也可以是对探索别人的兴趣和活动感兴趣的人员集合。许多社交网络是基于Web的，并可向用户提供交互的机会，如在文章开头所谈到的电子邮件和其它即时通信服务。 社交网络的最大危险性在于损害个人的身份信息及其它信息。它可能会导致你的相片被发到某个成人网站，抵毁你的形象。也可能会导致你的网上银行卡的机密信息被人窃取，还有可能在不知不觉之间将公司的商业机密“ 大白于天下 ”！ 不要对此掉以轻心了，不要觉得这种事情不会发生在你或你的公司身上。社交网络是网络钓鱼者、垃圾邮件制造者、僵尸网络控制者、公司间谍谋取利润的重要阵地，如果对其使用不慎，它甚至可轻易地葬送公司或个人的命运。 问题的根源在于社交网络站点本身并不安全。一般情况下，这种站点并不对用户进行鉴别，用户无法完全确认在线的所谓友人的身份，而攻击者可以轻易地利用社交网络内的“ 可信任的 ”文化，从中大块朵。但是，许多用户并未启用或部署这些站点所提供的某些安全和私密选项。 例如，社交网络应用程序开发工具，

如OpenSocial，还有一些第三方的工具可轻易地被攻击者利用传播恶意软件或泄露个人私密信息。此外，还存在着公司间谍的真实风险，攻击者可以轻易地利用网络雇员的信息实施其它攻击。而且，有些流行的Web攻击方式，如跨站脚本攻击，也可被用于对付社交网络的成员。 千万不要因为你禁止家庭住址、电话号码等私有信息而沾沾自喜，因为这样并不能使你免受安全威胁。在互联网上并没有什么真正的私密。用户只能延缓信息被泄露的风险。用户需要将整个互联网看作是一个所有资源都永存的平台。 针对社交网络的攻击才刚刚开始，因此在发布个人信息时请三思而后行，或者在接受并信任新的朋友时需要加倍谨慎。随着攻击者日益关注社交网络，其攻击将更加严重。事实显示出，社交网站已成滋生网络攻击的温床。 孙子说，知彼知已，百战不殆。要对付社交网络攻击，先要对付这种攻击，下面笔者谈谈攻击者最阴险的七大社交网络“ 黑技 ”： 一、身份假冒及针对性的个人信息攻击 二、制造垃圾邮件和僵尸网络 三、被改造的社交网络应用程序 四、个人信息与专业信息的交叉混杂 五、跨站脚本攻击或跨站请求伪造 六、身份窃取 七、公司间谍 下面逐个谈谈： 一、身份假冒及针对性的个人信息攻击 不要认为安全专家们没有受到社交网络威胁。近年来的社交网络攻击日益广泛深入，许多社交网站的个人信息被发布到了其它网站上，这说明即使是专家也有可能无法幸免于难。作恶者可以借个人身份信息威胁受害人，如将其相片发到网络上。 如果社交网站的成员快速更新了自己的所作所为，或者对多个“ 跟随者 ”作出了注释，那么这简直就是在将其它的因素引入到社交网络安全中，即物理安全。也许你并没有跟别人说自己

是谁、在什么地方，但这并不能阻止别有用心的家伙知道你的信息。 例如，将个人的太多信息（如出行信息或旅行计划等）散布到网络上，可能会导致入室行窃等的发生。由此可见，这会导致严重的物理安全问题。因此人人都不要轻易地将自己的信息发布到社交网站上。 正如哈密尔和摩尔在黑帽大会上所演示的那样，用户甚至不必拥有要攻击的社交网络的配置信息，也不必拥有账号，就可将他人的照片发送到互联网上，并获取在线的信息，构建令人深信不疑的信息。 二、制造垃圾邮件和僵尸网络 垃圾信息制造已经成为一种巨大的产业，广告、单击性欺诈、僵尸网络需要有效地传播其消息、恶意软件（或二者兼而有之）的一种机制。攻击者早已经如蛆虫一样进入了社交网络社团，劫持用户账户，并使用其地址簿传播垃圾邮件、蠕虫或其它的恶意软件。 可以看出，越来越多的恶意软件被作为附件放在了垃圾邮件中。在国外著名的社交网站中可以清楚地看到这一点。这种邮件的特点是将不明真相的人吸引到“ 特殊的 ”网页中，如引诱用户点击一个精彩的视频链接，而其实际上这是一个特洛伊木马的下载链接，它会偷偷地将恶意软件下载到用户的计算机上，并将此计算机变为僵尸网络的成员。 三、被改造的社交网络应用程序 用户们并没有过多地考虑将应用程序安装到其浏览器中的问题，不过，这些应用程序可能会获得访问用户系统的能力，而用户的一些极私密的信息可能存储在其自身的系统中，其危险性显而易见。不过，总有一些用户认为安装这些应用程序没有什么了不起。 这使得第三方的应用程序成为攻击者的一种简易工具。此外，第三方的应用程序服务还使得基于代码的攻击获得了途径。 但并不是说所有的社交网

络虚拟工具都是恶意的。如开放性社交网站opensocial向工具的开发人员提供了在其应用程序中限制恶意JavaScript的选择，但不熟练的开发者却不知道如何使用这些手段。这只是一些可选项，很少有开发者使用这种工具。最终结果是，对安全不敏感的开发人员可以构建应用程序，而其传播速度也会如枯草上的野火一样迅猛。 四、个人信息与专业信息的交叉混杂 即使用户将A社交网站的账户信息用于私用，而将另外一个社交网站的账户用于专业性网络，这也无法保证前者的图片不会出现在后者的账号中，甚至“ 跑 ”到老板的邮箱中。不妨考虑一下开放性的社交网络，不管是图片还是工作经历，都可以成为到处复制、粘贴的对象。 五、跨站脚本攻击或跨站请求伪造 跨站脚本攻击及跨站请求伪造漏洞是很显明的攻击工具，有一些社交网络蠕虫使用跨站脚本攻击漏洞帮助其传播。不过多数社交网络拥有对付跨站脚本攻击的机制。而跨站请求伪造则尚未流行起来。 跨站脚本攻击和跨站请求伪造对社交网络站点并未造成巨大的风险。在跨站脚本攻击中，恶意的代码被注入到有漏洞的Web应用程序中，查看这些网页的用户就会被“ 黑 ”。在跨站请求伪造中，攻击者会欺骗用户的浏览器发出要求登录的请求。 要知道，在任何时候，攻击者都可以强迫用户加载HTML代码，其潜在的威胁是攻击者通过XSS/CSRF利用浏览器的漏洞、感染僵尸网络、并可操纵用户账户。 跨站请求伪造攻击可以在多个社交网络站点之间跳转，而在用户不断登录之时，这种攻击能够从一个社交网络传播到另外一个网络。从总体上看，跨站请求伪造攻击是一种被人们忽视的黑客行为。 六、身份窃取 简言之，身份窃取指通过假装为另外一个人的身份而进行欺诈、

窃取等，并获取非法利益的活动。社交网络的信息可透露一些颇有价值的内容，如受害者的姓名和出生日期。身份窃贼们可以用这些信息猜测用户的口令或模仿这些用户，并最终窃取其身份。 社交网络的用户有时在不经意间将自己的信息拱手让给他人，他们可能将自己的邮件地址、出生日期、电话号码等交给并不熟悉的所谓“ 网友 ”。 我们对社交网络用户的一条忠告是，不要回答网站提交的全部问题，或者不要提供自己真实的出生日期。用户不必告诉网站自己真实的教育背景、电话号码等，还要想方设法让窃贼得到错误的其它敏感信息。 七、公司间谍 公司间谍活动在互联网平台日益发展壮大的背景下也有增无减，雇员的个人信息也有可能使公司招致公司间谍风险。 例如，为了实施钓鱼攻击，攻击者所做的是在社交网络站点上搜索公司的雇员，然后摆出一副公司老板或领导的姿态，如以人力资源部领导的身份出现，并向雇员发送电子邮件，如：“ 亲爱的某某，恭喜你加入本公司。请单击下面的链接访问本公司的内联网，并以你正常的用户名和口令登录，我们将根据你的信息更新配置文件。 ”尤其要注意的是，刚来公司上班的新人有可能会遭到这样的欺骗。 对付这种间谍行为的唯一办法是告诉雇员要限制所公开的信息，并不要将雇主或老板的名字透露出去，这可以减少通过雇员攻击公司领导及公司的机会。 总之，雇员需要知道，你在社交网络上与不法之徒也许仅有一步之遥。要明白:在社交网站上总有一些黑手在搜索你的信息。与我们互联的不仅仅是朋友，还有可能是豺狼。所以请谨慎地透露你的信息。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com