国家网络安全宣传周
China Cybersecurity Week

网络安全为人民
网络安全靠人民

2016年国家网络安全宣传周

如何应对常见网络安全风险

电信诈骗

电信诈骗是指犯罪分子通过电话、短信或网络方式，编造虚假信息，设置骗局，对受害人实施远程、非接触式诈骗，诱使受害人给犯罪分子打款或转账的犯罪行为。

威胁

我是公安部反洗钱中心。你的身份信息被盗用，涉嫌洗钱犯罪，请按要求把资金转入“安全账户”配合调查。

别怕别怕，这是诈骗分子狐假虎威，国家从来就没有什么“安全账户”。平生未做亏心事，干嘛要怕鬼敲门？！

恭喜您获得《奔跑吧兄弟》节目幸运观众一等奖，奖金10000元！请按有关规定缴纳个人所得税后，前往领取。

别喜别喜，当心骗子盯上了你。我国《反不正当竞争法》规定，抽奖活动的奖金不得超过5000元，否则就是违法！

我是XXX教育局，有一笔助学金，今天就要截止啦。请你赶紧带上银行卡去取款机上领钱。

别急别急，凡事要政策清楚，流程清晰。每年9月30日前，学生可向就读的高校提出助学金申请，评审后高校将按月发放。入学前收到的助学金电话很可能是诈骗。

防范

一、网上晒图要注意，尽量不标注位置信息。限制信息谁能访问，以防“李鬼”冒充上门。

二、170、171号段属于虚拟运营商，实名验证监管不严，被诈骗分子大量利用。留心来电口音和号码归属地，网上搜索电话号码可以查看他人对该号码的标注情况。

三、学学古代招财进宝的神兽貔貅，钱财只进不出。接听陌生电话时只听数字忽略动作，坚决不汇款。

四、发生诈骗后第一时间拨打110及时报警，对嫌疑人的银行卡紧急止付，尽最大努力保护资金安全。

天上不会掉馅饼，陌生电话藏陷阱

口令安全

你说你是你，凭啥相信你？报上口令来，偶来比一比！口令俗称密码，是人们向电脑表明自己身份的一串字符，比如123456、1q2w3e、Pa$$w0rd等。

风险

1、暴力破解。我猜我猜我猜猜！6位数字的口令有100万种可能，但黑客利用口令破解软件可以瞬间破解。

2、字典攻击。标准单词拿来用，个人信息做变换？自己记得很简单，黑客破解更不难。破解软件可以搜索标准词典，或根据用户个人信息构造可能口令列表，比如password -> password123 -> pa$$w0rd

3、网络嗅探。口令不光本地用，还会经常发上网。如果传输没加密，黑客截获没商量。为了对抗嗅探器，可找小“s”来帮忙！http不加密，https做改良！

4、木马有硬也有软，偷记口令发网上。背后有人喝咖啡，把你口令记心上。写下口令怕遗忘，垃圾桶被翻得底朝上！

对策

强口令

- 至少8个字符
- 包含至少大写和小写字母
- 包含至少一个数字
- 包含至少一个特殊字符，如 ~!@#$%^&*()_-+=

弱口令

- 登录名的任何一部分
- 字典中的任何单词
- 曾经用过的口令的任何一部分
- 字母或数字的重复序列
- 键盘上相邻的键，如qwerty
- 个人信息，如驾照、电话、地址等

1、开头和结尾替换：顿顿七八两->dun dun qi ba liang->ddqbl->365@00qbl!!!

2、空格和字母替换：天王盖地虎 要上985-> twgdh ys985->twgdh@9-8-5

口令像牙刷，质量好、常换、不借人

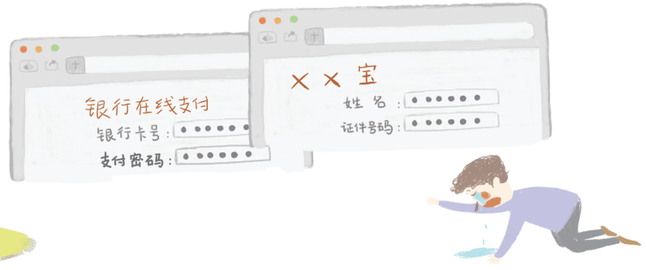
钓鱼网站

网上诈骗套路多，征婚、算命、中奖、低价打折……。点进网站输信息，赔的远比赚得多！这种诱骗用户点击，窃取用户QQ密码、银行帐号等敏感信息的假网站，就是钓鱼网站。

表现形式

No.1. 以“公司周年庆”、“幸运观众”、低价机票、电话充值、征婚交友为名，诱骗用户填写身份证号码、银行帐户等信息。

No.2. 模仿支付宝、网上银行等网站，窃取用户的支付帐号及密码、银行卡账号及密码等信息。



辨别

一、从http://开始的第一个斜线，以及这个斜线向左的第二个“.”之间的是网站的真正域名。http://www.sina.com.cn.sinainfo.cc/login/sina.com/index.html的域名是sinainfo.cc，而不是www.sina.com.cn。

二、细心留意看做工。留心网站的配色、内容、链接等细微处。

三、已被举报加入黑名单的网站，安全浏览器会提示“危险网站”。

四、以https开头的一些网站，在网络地址栏会有彩色的图标和锁头，可以点击查看网站被权威机构认证的信息。

五、不盲目相信搜索引擎的推荐，不乱点微信、微博、短信中的网址。

网络钓鱼钩本直，火眼金睛来辨识

恶意二维码

二维码是由一组黑白相间的小方块组成的图形，图形中蕴含着信息。手机扫一扫就可以恢复出其中蕴含的信息。二维码大量用于信息获取、广告推送、优惠促销、防伪、支付等各行各业。

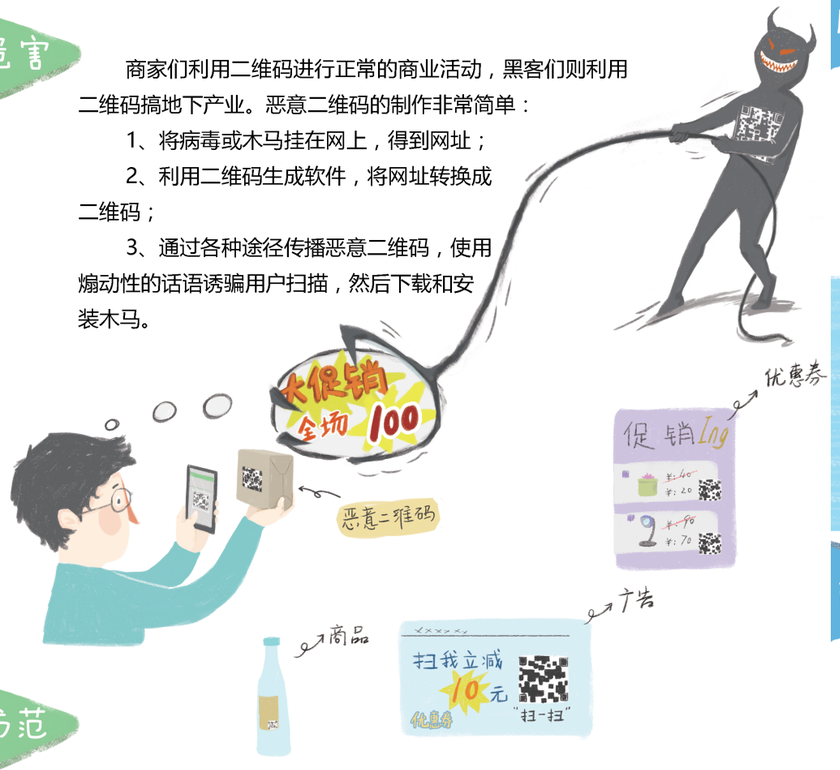
危害

商家们利用二维码进行正常的商业活动，黑客们则利用二维码搞地下产业。恶意二维码的制作非常简单：

1、将病毒或木马挂在网上，得到网址；

2、利用二维码生成软件，将网址转换成二维码；

3、通过各种途径传播恶意二维码，使用煽动性的话语诱骗用户扫描，然后下载和安装木马。



防范

一、提高安全意识，对街边各种二维码提高警惕，不扫描不明来源的二维码。

二、利用二维码安全检测软件协助判别是否为恶意网址，背后是否有恶意软件。

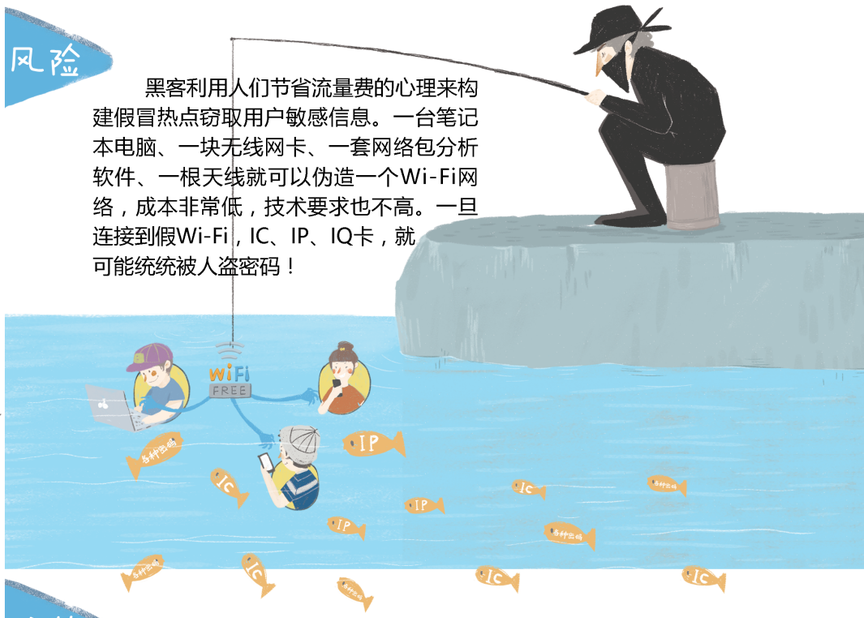
街边乱扫二维码，引狼入室招木马

假冒热点

手机上网有点贵，蹭网节省流量费。免费热点见就连，不知背后有风险。

风险

黑客利用人们节省流量费的心理来构建假冒热点窃取用户敏感信息。一台笔记本电脑、一块无线网卡、一套网络包分析软件、一根天线就可以伪造一个Wi-Fi网络，成本非常低，技术要求也不高。一旦连接到假Wi-Fi，IC、IP、IQ卡，就可能统统被人盗密码！



防范

一、公共场合的Wi-Fi，使用前一定要先仔细辨认。要向Wi-Fi提供方确认热点名称和密码；无需密码就可以访问的Wi-Fi风险较高，尽量不要使用。

二、使用公开的Wi-Fi时，不要登录支付宝进行购物，不要登录网上银行进行转账，避免输入个人敏感信息。

三、关闭Wi-Fi的自动连接功能。黑客会建立同名的假冒热点，利用距离近信号强的优势成为真热点的“邪恶双胞胎”。一旦手机自动连接上去，就会造成信息的泄露。

蹭网流量值不值，当心热点被劫持