网络安全为人民
网络安全靠人民

国家网络安全宣传周
China Cybersecurity Week

2019 国家网络安全宣传周
CHINA CYBERSECURITY WEEK

如何应对常见网络安全风险

主办单位

中央宣传部、中央网信办、教育部、
工业和信息化部、公安部、中国人民银行、
国家广播电视总局、全国总工会、共青团中央、全国妇联

1 暑期升学季冒充“助学金”信任诈骗多，九月入学季“装可怜求助”的同情诈骗多，“双十一”购物季“低价购物”的贪婪诈骗多，……。骗子是全天候“工作”的，遇事要多想多问多商量！

2 留心来电口音和号码归属地，网上搜索电话号码查看该号码是否已被标注为骗子。只要一谈到“银行卡、中奖、转接公检法、安全账户”，一律挂掉。

3 不要通过ATM机向陌生人转账，老年人要守住儿女的辛苦钱，青年人要守住老人的保命钱。

4 发生诈骗后第一时间拨打110报警，说明嫌疑人和受害人的银行卡号，通过紧急止付最大程度上保护被骗的资金。

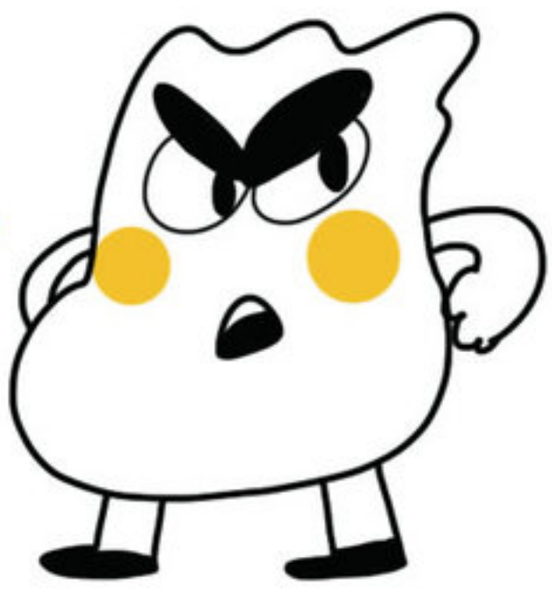
电信诈骗

定义

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。

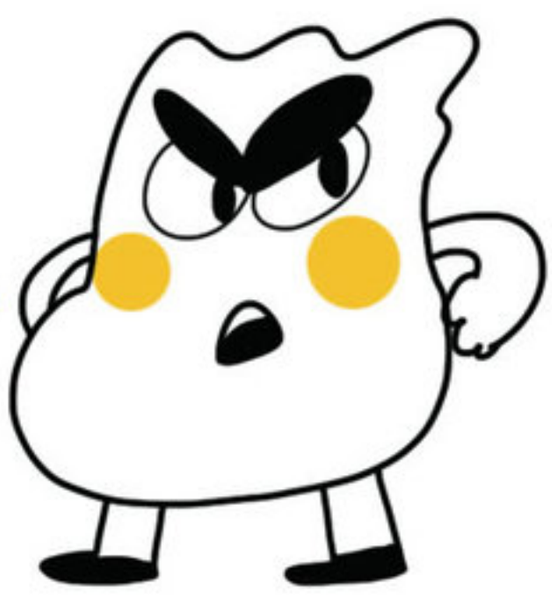
我是“公安部反洗钱中心”，你涉嫌洗钱犯罪，请按要求把资金转入“安全账户”配合调查。

别怕别怕，诈骗分子狐假虎威，国家没有“安全账户”。平生未做亏心事，干嘛要怕鬼敲门？！



恭喜你获得“☆★☆节目”幸运观众一等奖，奖金10万元！赶紧点击链接领取奖金，过期作废！

别喜别喜，骗子已经盯上你。我国《反不正当竞争法》规定，经营者进行有奖销售不得存在下列情况：抽奖式的有奖销售，最高奖的金额超过五万元。



假

假

假

关注来源

对街边各种二维码提高警惕，不扫描不明来源的二维码，向商家询问确认二维码的真实性。

安全扫描

利用二维码安全检测软件协助判别是否是恶意网址，背后是否有恶意软件。

分辨真假

当心“码上码”。有骗子在共享单车上的解锁二维码上覆盖粘贴一层新的、底色透明的二维码，或打印纸张贴在车上。要求转账或下载软件时要注意辨别资金去向和软件来源！

保护付款二维码

付款二维码是自己向对方付款，对方只需快速扫描二维码，输入支付金额即可完成交易，不可随便轻易发送给别人。

恶意二维码

定义

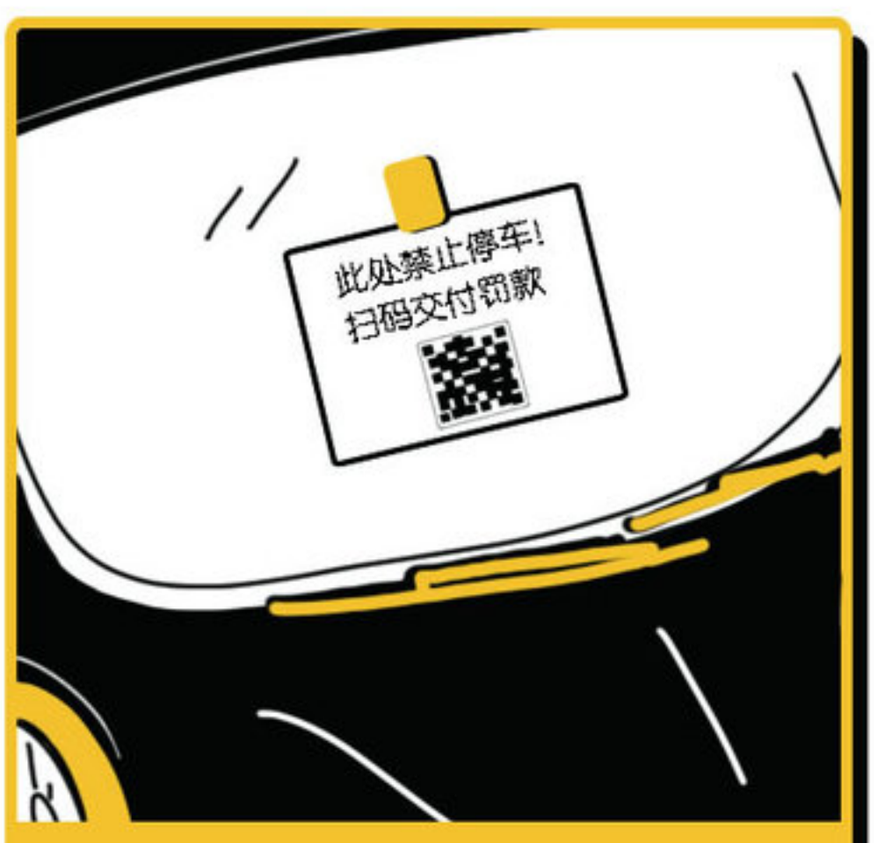
二维码是在平面上使用若干个与二进制数字0或1相对应图形来表示数据信息的几何形体。角落上的三个方块用于二维码扫描设备进行定位。大量用于信息获取、广告推送、优惠促销、防伪、支付等活动。

扫码中百万大奖？当心！

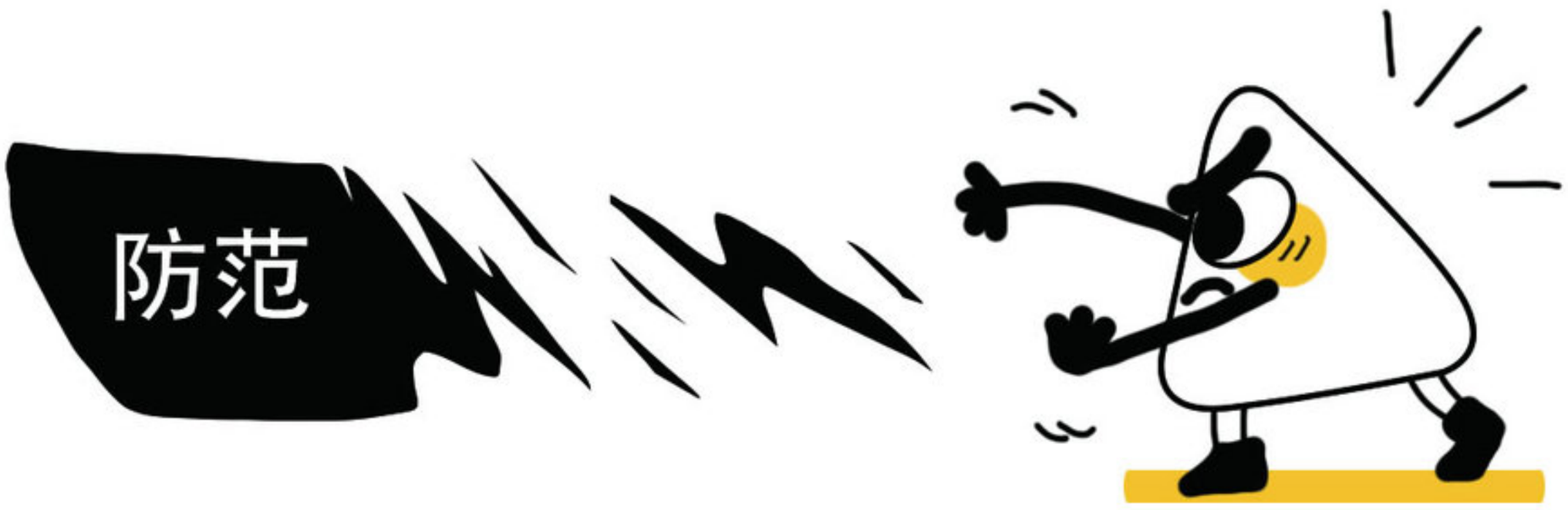
促销扫码送礼品？当心！

扫码帮忙刷个单？当心！

扫码支持他创业？当心！



罚单扫码交罚款？当心！



1) 仔细辨认真伪：向公共场合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。

2) 避免敏感业务：不要使用公共Wi-Fi进行购物、网上银行转账等操作，避免登录帐户和输入个人敏感信息。如果安全性要求高，有条件的话可以使用 VPN服务。

3) 关闭Wi-Fi自动链接：防止手机自动连接到合法Wi-Fi热点的“邪恶双胞胎”，造成信息泄露。

4) 注意安全加固：为Wi-Fi路由器设置强口令以及开启WPA2，关闭WPS，是最有效的Wi-Fi安全设置。

5) 运行安全扫描：安装安全软件，进行Wi-Fi环境等安全扫描，降低安全威胁。

假冒热点

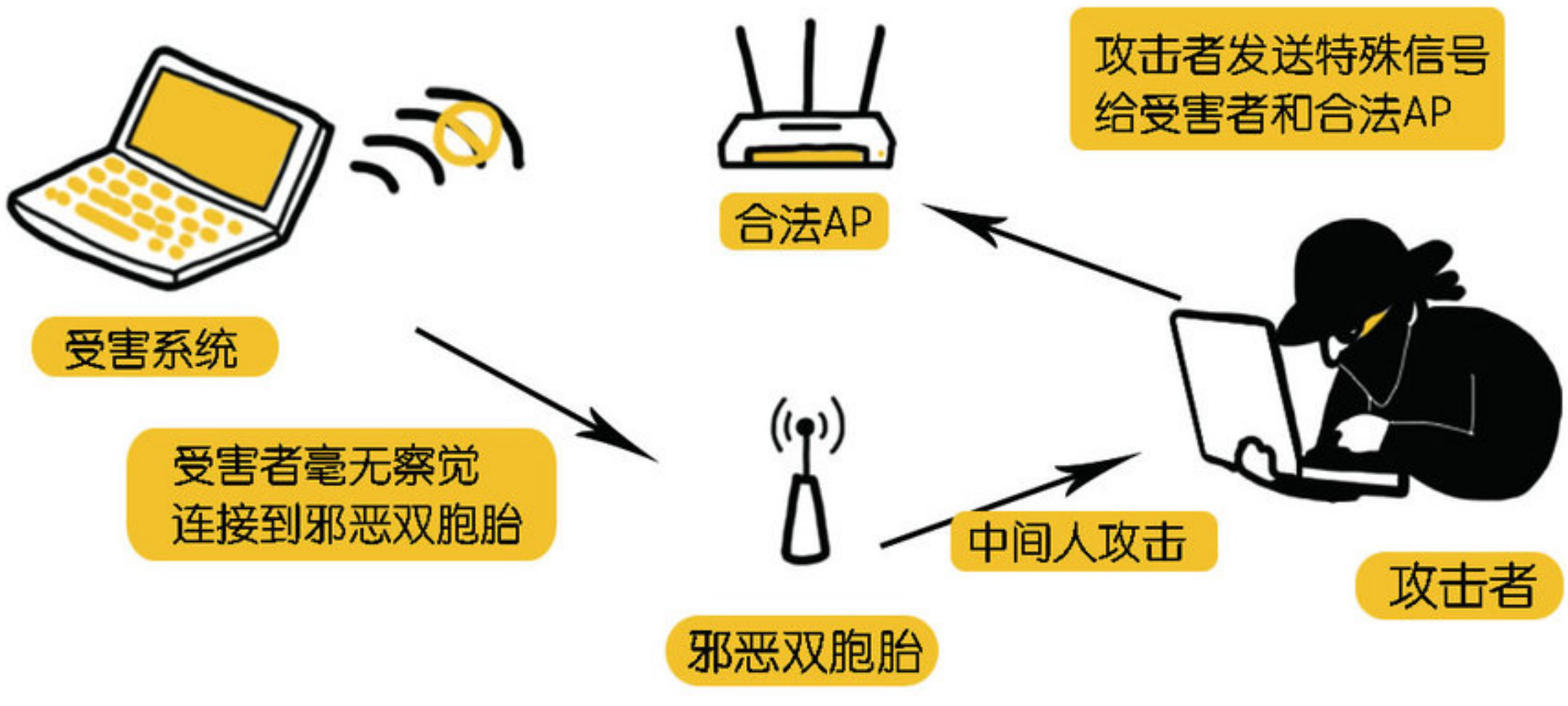
定义

无线接入点（Access Point，AP）俗称“热点”，扮演无线工作站和有线局域网的桥梁。有的一体设备同时执行接入和路由工作；而纯接入设备只负责无线客户端的接入，与其他AP或者主AP连接以扩大无线覆盖范围。

风险

手机上网有点贵，蹭网可省流量费。
免费热点见就连，当心背后有风险！

1. 攻击者架设假冒/高仿/山寨Wi-Fi热点，用相近的名字吸引用户连接（如：李逵机场免费Wi-Fi VS 李鬼机场免费Wi-Fi），你的所有上传下载内容都被黑客掌握！可谓，IC、IP、IQ卡，统统可能丢密码。



2.攻击者架设的Wi-Fi热点和真的同名，通过发送特殊数据包强制断开受害人电脑与合法AP之间的连接，转而连到“邪恶双胞胎”热点上。

个人信息保护

定义

个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。个人敏感信息，是指“一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息”。除了财产信息、健康生理信息、生物识别信息、身份信息和网络身份标识信息以外，还包括电话号码、网页浏览记录、行踪轨迹等。

风险 数据是二十一世纪的石油！！

1.信息泄露事件频频发生

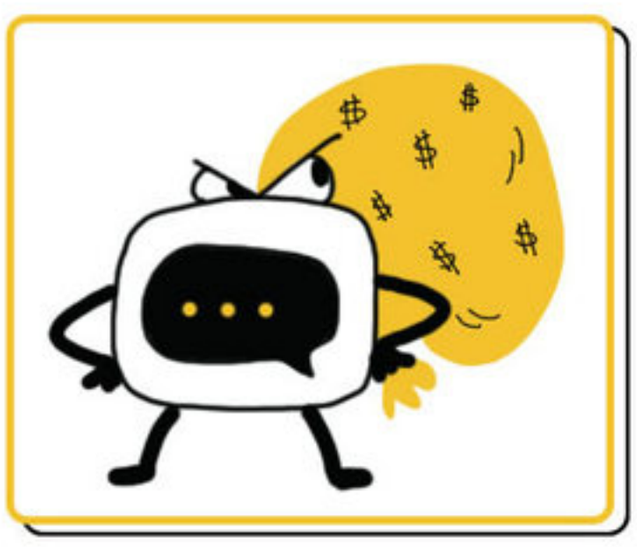
- 7大酒店的数千万条开房信息被泄露
- 30多个省市的社保系统、户籍查询系统等存在高危漏洞

2.个人信息过度收集屡禁不止

- App要求用户提供与服务不相关的隐私信息
- App在用户不知情情况下后台读取用户通讯录、通话记录、GPS位置信息

3.个人信息非法买卖日益猖獗

- 几百万条考研报名数据、快递个人信息在网上打包销售
- 20万儿童信息被打包出售，信息精确到家庭门牌号



4.个人信息滥用助长恶意违法行为

- 助长短信诈骗、电话诈骗
- 年度经济损失近千亿元，网民人均损失上千元

治理举措概观

1、2017年6月1日起施行《网络安全法》，筑牢个人信息保护的法律防线

第四十条　第四十一条　第四十二条

第四十三条　第四十四条　第四十五条

2、2017年9月24日，个人信息保护倡议书签署仪式在京举行，公布了个人信息保护提升行动之隐私条款专项工作十款产品和服务隐私条款的评审结果。

3、2019年1月25日，“App违法违规收集使用个人信息专项治理”新闻发布会，正式对外发布《关于开展App违法违规收集使用个人信息专项治理的公告》。

4、2019年5月27日，国家网信办发布了《百款常用App申请收集使用个人信息权限情况》。

5、2019年5月31日起，国家网信办就《儿童个人信息网络保护规定（征求意见稿）》征求社会意见。

危险和防范

典型信息泄露行为	信息泄露内容	防范要点
随手乱丢快递单	姓名、电话号码、工作地点或住址	完全撕碎快递单
星座、性格测试	姓名、出生年月	拒绝参加
分享送流量	不法分子确认手机号是有效的	确认是官方产品或业务活动，否则涉嫌诱导分享
抢红包输入个人信息	姓名、手机号	凡是要求输入个人信息领取的都是假红包
微博发帖、朋友圈分享旅行信息	家中没人可能引来窃贼	旅行途中尽量不晒图
机构数据泄露	账户信息、医疗信息等	关注信息泄露事件，及时调整设置口令、更换信用卡等

网络分享乐趣多　敏感信息需“减排”

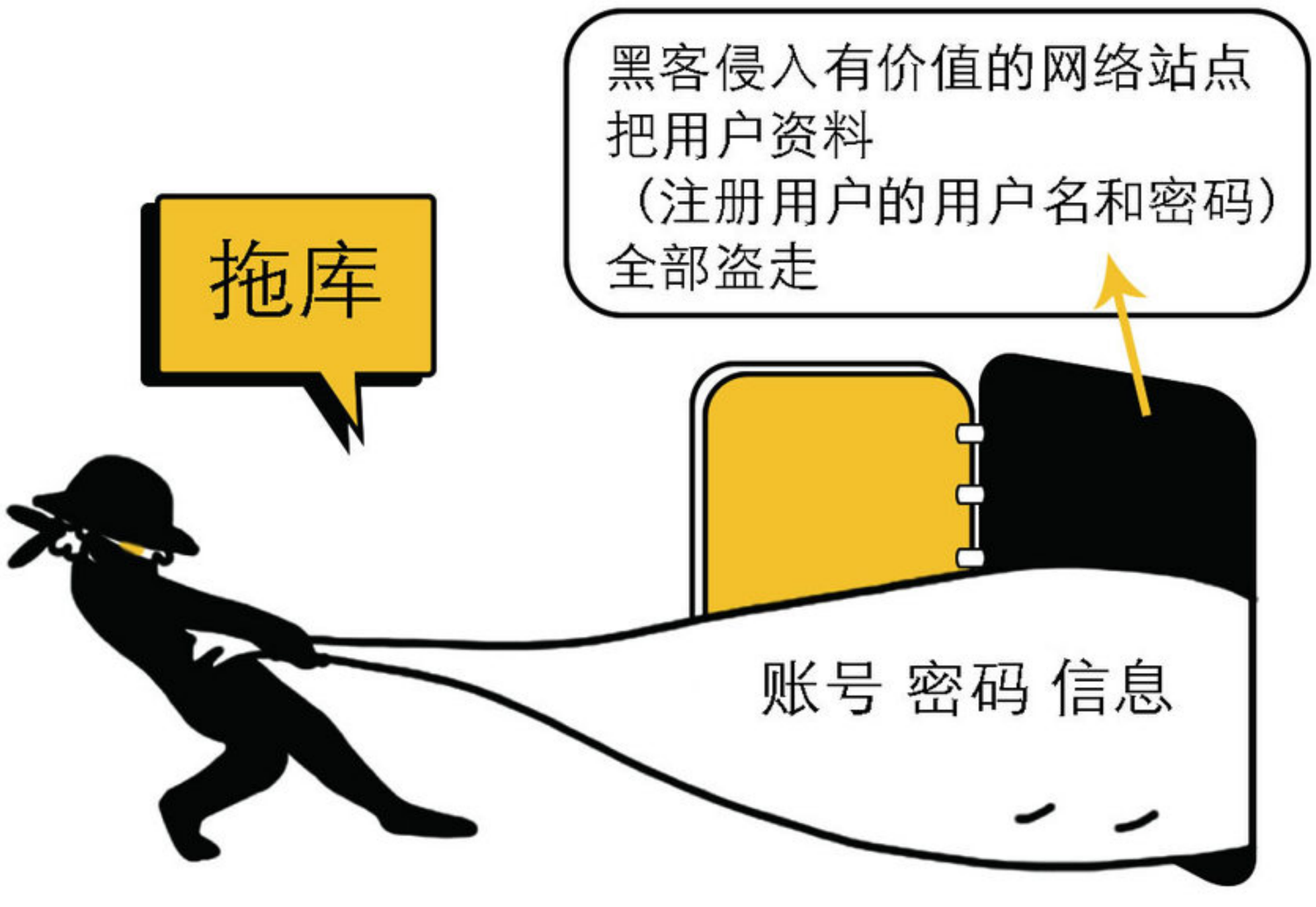
口令安全

定义

拖库： 指网站遭到入侵后，黑客窃取其数据库。

撞库： 指黑客获得一批A网站的账号口令（俗称密码）后，批量尝试登录其他网站，得到一系列可以登录的用户。

据监测统计，恶意登录尝试每小时可达上千次，平均每月可高达37.5亿次。



账号一大堆，密码都要强。记忆很疲劳，干脆设一样。以为能省事，黑客喜欲狂！

避免弱口令

- 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
- 个人信息相关，如驾照、电话、地址等

设置强口令

- 至少8个字符
- 包含至少大写和小写字母 (e.g. A-Z, a-z)
- 包含至少一个数字 (e.g. 0-9)
- 包含至少一个特殊字符(e.g. ~!@#$%^&*()_-+=)
- 不同网站设置不同的用户名、口令
- 使用KeePass等软件来帮助管理口令

小窍门[从一句话开始，做替换和变换]

1. 天王盖地虎，要上985： Twgdh@ys9-8-5
2. 七八颗星天外，两三点雨山前： 78k*tw,23.Yu3qian

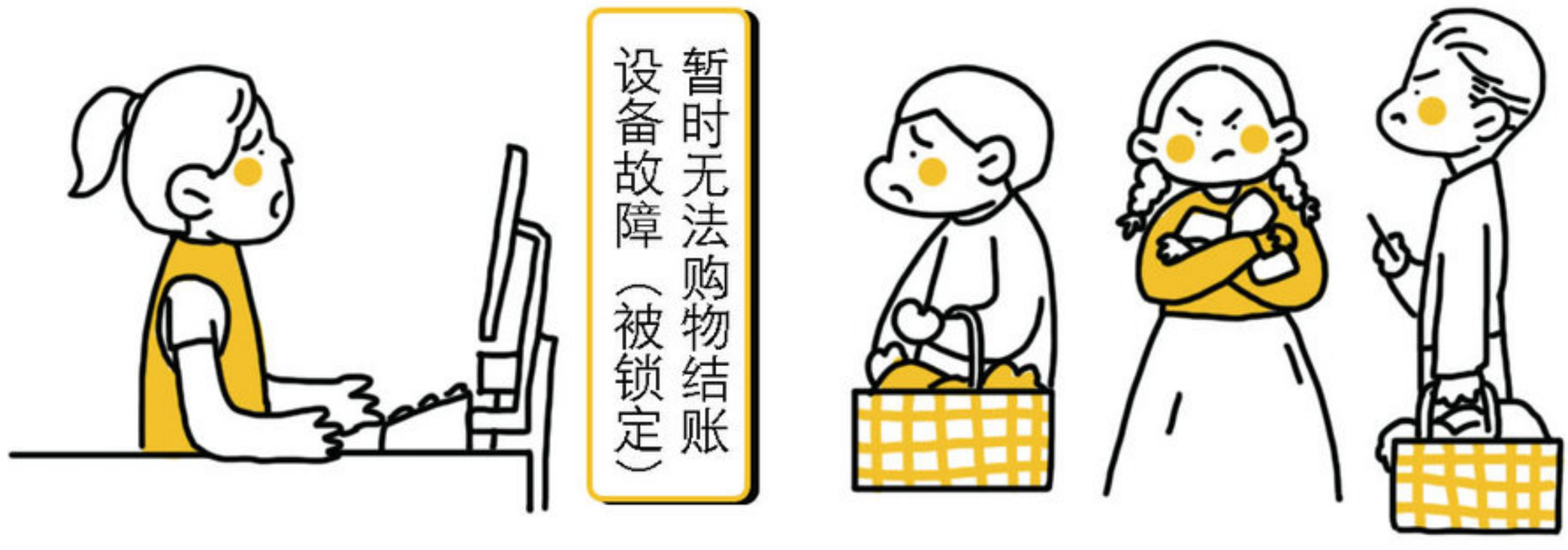
勒索软件

定义

勒索软件是通过锁定系统屏幕或锁定用户文件来阻止或限制用户正常使用计算机，并以此要挟用户支付赎金的一类恶意软件。

勒索软件的吓人策略包括：锁定屏幕、删除备份文件、加速删除文件、提高赎金金额等。赎金形式包括：真实货币、比特币以及其它虚拟货币。

医疗设备被锁定，无法挂号做手术

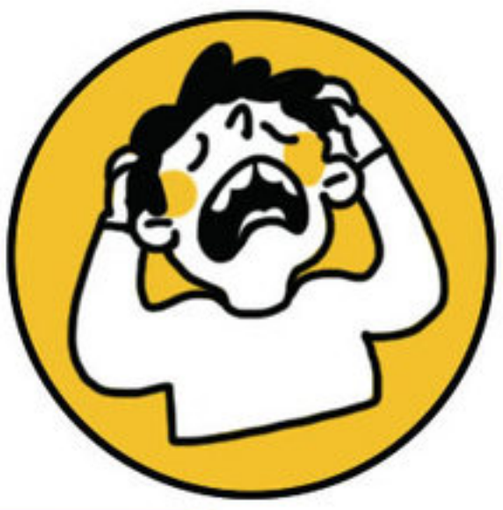


超市收银机被锁定，无法购物

个人电脑数据被加密，必须支付赎金

传播背后的心理学

乐观主义者： 网海一粒米，哪会盯上你，不用去搭理



悲观主义者： 黑客黑科技，想防没实力

现实主义者： 人在网上漂，难免会挨刀；不等黑客下手，先备份数据、打补丁、堵端口

防范建议

拒付赎金： 支付赎金会助长攻击者的气焰。攻击者还会通过用户支付赎金速度对用户财务、数据价值等情况进行分析，可能从此被盯上。

防毒杀毒： 尽量到官方网站下载软件，安装正规杀毒软件，运行下载软件之前先进行病毒扫描。

及时更新： 关注操作系统安全公告，及时安装安全补丁，尽早堵住漏洞。

封堵端口： 关闭无用的计算机服务/端口，开启Windows防火墙，减少被攻击的“通道”。

做好备份： 使用光盘/移动硬盘等介质，对文档、邮件、数据库、源代码、图片、压缩文件等各种类型的数据资产定期进行备份，并脱机保存。

数据备份至最新　不怕勒索要赎金

钓鱼网站

定义

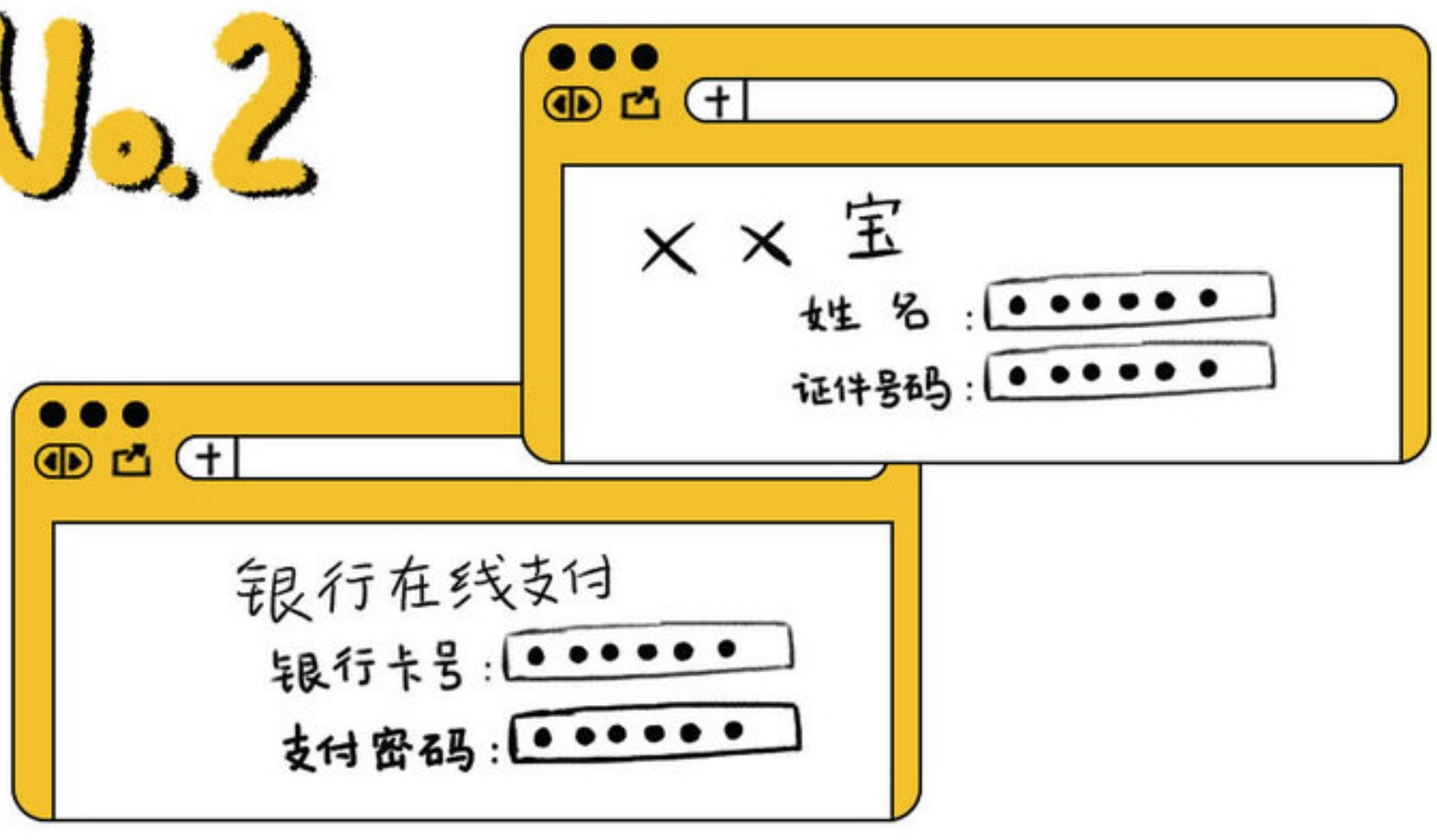
网络套路深，遍地都是坑。网页仿冒是通过构造与某一目标网站高度相似的页面诱骗用户的攻击方式。钓鱼网站是网页仿冒的一种常见形式，常以垃圾邮件、即时聊天、手机短信或网页虚假广告等方式传播，用户访问钓鱼网站后可能泄露账号、密码等个人隐私。

表现形式

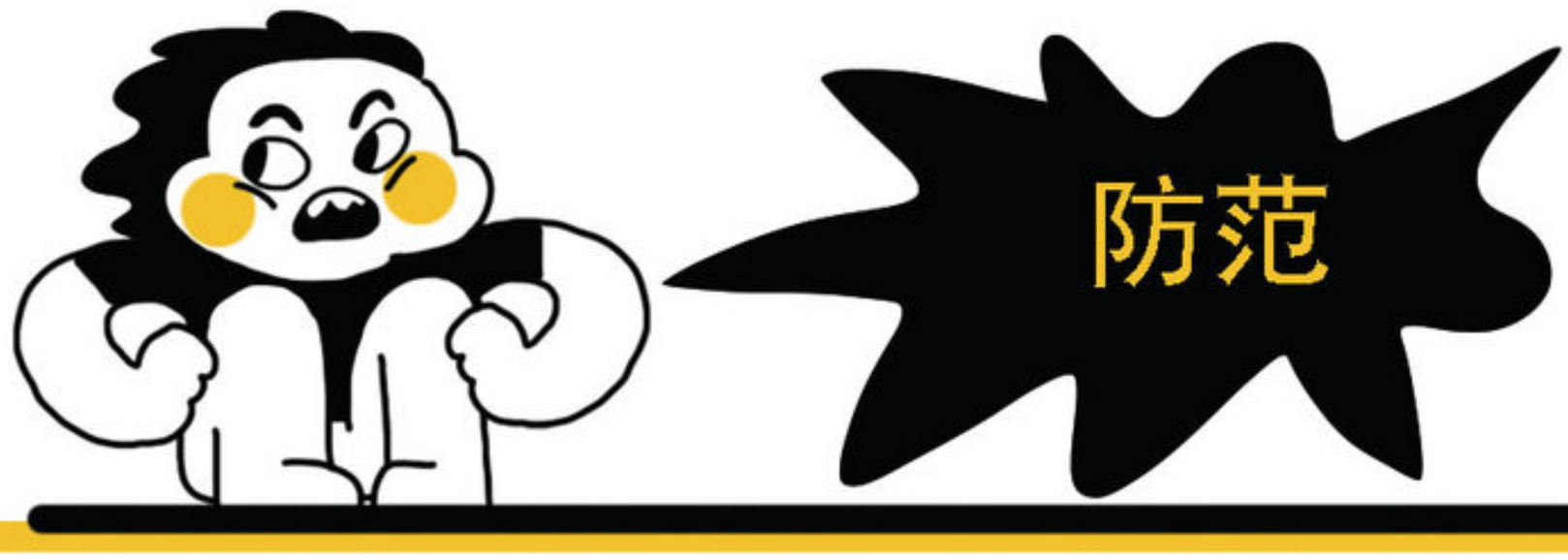
No.1

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、银行账户等信息。

No.2



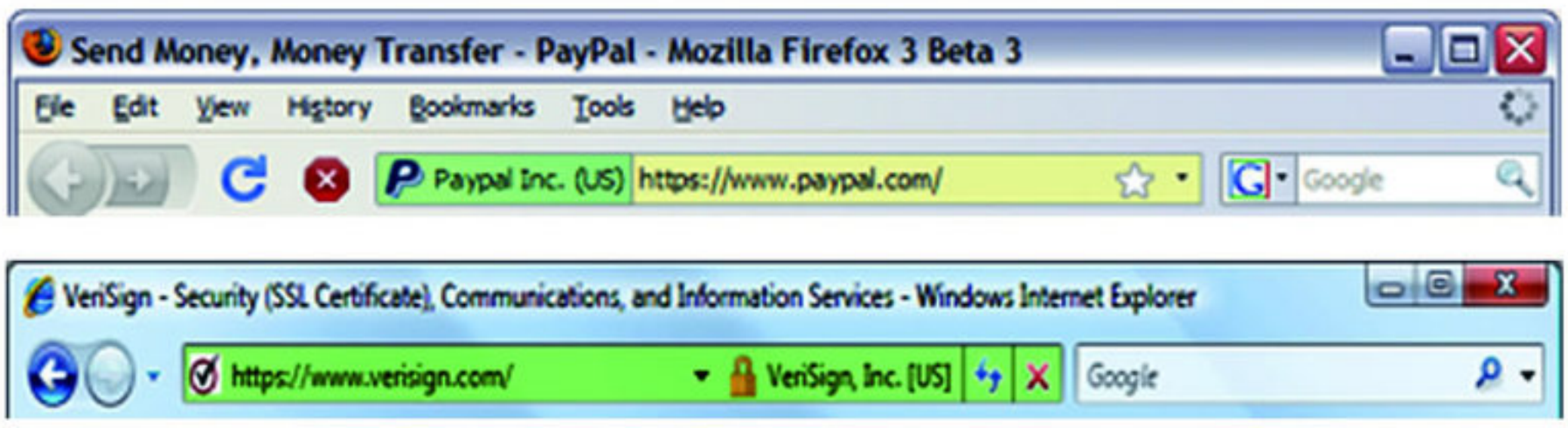
模仿支付宝、网上银行等网站，窃取用户的账号及密码等信息。



1 察颜观色：留意网站配色、内容、链接等细微之处。但对攻击者完整克隆网站的钓鱼方式无法适用。

2 注意提示：已被举报加入黑名单的网站，安全浏览器会提示“危险网站”。

3 安全标志：支付相关的网站一般网址以https开头，在网络地址栏会有彩色图标或锁头，可点击查看网站被权威机构认证的信息。



4 悬停鼠标：不盲目相信搜索引擎的推荐，不乱点击邮件、微信、微博、短信中的网址，尤其是短网址。

5 细辨网址：如工商银行网址icbc.com.cn被混淆为lcbc.com.cn；www.microsoft.com被混淆为ww-w.rncrosoft.com。

6 高级技巧：从http://开始向右遇到第一个斜线，从该斜线向左至第二个“.”之间的网址是网站的真正域名。例如：http://www.sina.com.cn.sinainfo.cc/log-in/sina.com/index.html的域名是sinainfo.cc，而不是新浪。