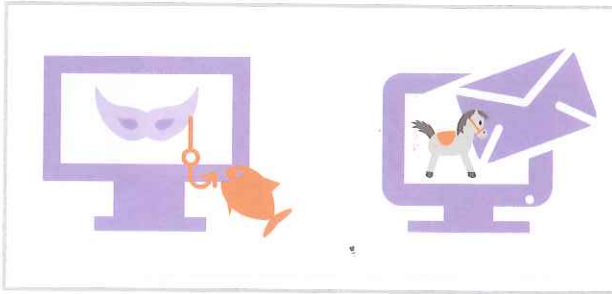
网络支付陷阱多，安全防范很重要！

网络支付的出现，让我们的支付变得更加快捷，省时省力，随时随地，足不出户，就可以办理多项业务。网络支付是在网络的开放环境中开展的。由于它涉及到资金转移，非常容易成为犯罪份子觊觎的对象。

我们面临的网络支付风险主要有哪些?



1

被钓鱼或者被植入木马

不法分子通过假网站、假电子商务支付页面等“网络钓鱼”形式，通过假的支付页面窃取客户网上银行信息。比市场同类商品便宜很多的东西，你需要小心谨慎了！

通过木马窃取也是一种常见的风险。不法分子通过木马程序等网络技术手段窃取客户的文件证书或盗取网上银行账号和密码。

2

个人信息的泄漏

个人信息的泄露有两种，一种是由于个别网站系统被攻破，导致系统存放的个人敏感信息泄露，给相关的消费者造成资金损失。另一种是由于用户的疏忽或者被欺骗，导致你的账户、密码或者手机验证码等信息被他人非法获得。

3

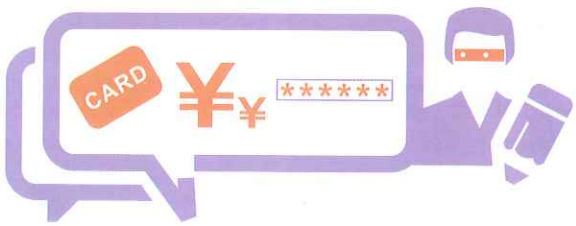
由于密码过于简单或者具有明显特征，导致密码泄露

客户设置的卡密码过于简单，没有真正起到保护的作用，容易被不法分子窃取或猜中。

4

支付数据被篡改

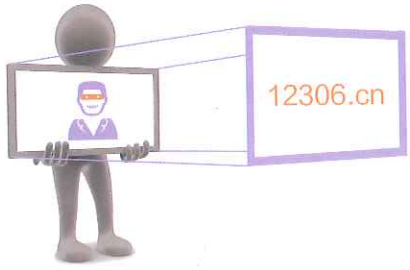
在缺乏安全防范措施情况下，攻击者可以通过修改互联网传输中的支付数据。比如，可以修改付款银行卡号、修改支付金额、修改收款人账号等，达到谋利目的并制造互联网支付事件。



常见的诈骗

故事一：

某网友最近在一家社交网站的用户名和密码被盗，她也没在意，就重新注册了一个，谁知道没过两天，其支付账户上却被人盗用在网上购买了几百元的游戏点卡——原来，其为了省事，微博、邮箱和网络支付账号都使用相同的账户与密码，结果被人盗用了支付账户。



故事二：

某网友在一家宾馆电脑访问12306.cn网站购票付款时，网页自动跳转到游戏点卡交易页面，网银付款对象也从“铁道部资金结算中心”变为第三方支付平台，收款商户是某网络科技有限公司。网友并没有注意看收款方，导致资金被转移。事后得知，电脑事先已被植入木马，劫持火车票款为黑客购买游戏币。

看到这里，你是不是觉得网络骗子太可怕了，简直防不胜防。不用担心，小编告诉你如何保障网络支付的安全！

1、电脑环境安全：包括使用正版操作系统、正版杀毒软件、稳定版浏览器。及时安装补丁与升级包；

2、支付安全：在资金账户使用数字+英文+符号的高强度密码、尽量不要用身份证、手机号设置登录与支付密码、同时注意网银的密码安全。

3、网络支付安全工具：数字证书、短信验证码、动态口令、Usb Key。这四样工具其中，短信验证码及动态口令，银行、支付宝、微信都不会问你要的，所以问你要这两个的一定都是骗子。

4、网络信息安全意识：不接受陌生文件、不同网站用户名与密码做区分、网络密码不放在电脑内。

5、把正确的网络商店地址放到你的浏览器收藏夹内。如淘宝网、支付宝、京东等，确保进入正确的网站购物，这是防止钓鱼的最有效方式。

6、您不确定登录的网站是否真假时，你可以采用“尝试输入法”。也就是随意输入一个用户名及密码，如果这个网站提示您登陆成功的话，那么基本可以断定为钓鱼网站。

7、QQ、微信上亲朋好友问你借钱需谨慎，先打电话确认。利用网络进行诈骗的不法分子越来越多，我们需要时刻保持警惕，确保资金安全。