(一)提防虚假客服，切勿泄漏动态码

典型案例

某小姐在购物网站上买了一条裤子，几分钟后收到了一个自称“店家”的电话，告知因交易失败需要办理退款，并提供了一个“客服”QQ 号码，某小姐加了 QQ 号 与“客服”沟通，根据其提供的“退款链接”进入一个网站，按照客服提示输入了密码等信息，最后在收到动态码后未仔细校验便急忙填入。之后某小姐并未收到退 款，而且 QQ 也再联系不上那个“客服”。某小姐立即查询了银行卡余额，发现账户遭到了盗用。

专家解读

不法分子通过非法渠道获取了客户网购信息，以“退款”或“退货”为由电话联系客户要求客户加聊天工具，并点击其提供的“钓鱼网站”的链接。而实际上，在退货及退款环节不需要校验动态码或交易密码。

小贴士

1.办理网络购物、网络退货、退款等业务时请认清官方渠道。

2.如在购物网站申请退款或退货时，建议与官方客服联系后进行操作，切勿轻信不明身份的电话、网络聊天工具或其它形式提供的非正规途径的网络链接。

3.在收到动态验证码时，请仔细核对短信中的业务类型、交易商户和金额是否正确。

4.任何客服工作人员不会向持卡人索取短信验证码，如有人索要可判定为诈骗，请立即报警;也切勿轻易泄露自己的身份证件号、银行卡信息、交易密码、动态验证码等重要信息。

(二)关注支付安全，慎设账户密码

典型案例

某先生接到银行客服的交易核实电话，称其名下的卡片发生了多笔大额消费，而某先生并未操作这些交易，便立即报了案。警方根据交易资金流向的线索破案后发 现，不法分子是通过黑客技术入侵了某网站，窃取了某先生在该网站的用户名和登陆密码，随后不法分子尝试用于网络支付，由于某先生在支付网站也设置了相同的 用户名和密码，因此被盗刷。

专家解读

由于目前某些中小网站的安全防护能力较弱，容易遭到黑客攻击，从而导致注册用户的信息泄露。同时，如客户的支付账户设置了相同的用户名和密码，则极易发生盗用。

小贴士

1.对于支付账户的登陆密码、消费密码应与一般网站登录密码区别设置，并养成定期更改密码的习惯，防止因其他网站信息泄露而造成支付账户的资金损失。

2.网络支付相对 POS 消费等传统用卡渠道，存在交易场景虚拟化，验证强度相对较弱等特点，因此主要定位于小额支付。建议客户根据自身情况设置合理的单笔与单日交易限额，防止发生大额盗刷。

3.开通短信提醒服务，可及时掌握账户动态信息，避免发生连续盗刷。

(三)网络社交陷阱多，身份验证防诈骗

典型案例

某小姐碰到过一件比较蹊跷的事情，一个正在国外进修的闺蜜晚上用 QQ 联系某小姐，聊了些近况，提到国外信用卡的便利，就问某小姐用的什么信用卡，并好奇地 让某小姐发信用卡正反面的照片给她，要比较一下国内外信用卡的差别。某小姐有点犹豫，就拨通了闺蜜的电话，结果闺蜜说 QQ 被盗了。某小姐很庆幸自己没有上 传照片，但觉得很奇怪，为什么不法分子要信用卡的正反面照片呢?

专家解读

不法分子运用社交网络的熟人关系，让持卡人放松了警惕。索要信用卡正反面照片是想获取信用卡的卡号、有效期和卡片背面末三位数字，因为这三项信息已可以进行网络支付。

小贴士

1.不要轻易在任何社交网络中发送信用卡的卡号、密码、卡片背面末三位数字、有效期、动态码等关键信息，以免不法分子通过假冒亲友或盗取聊天记录，窃取用户银行卡信息。

2.可以开通账务短信提醒服务，及时了解账户信息，一旦发现有异常，立即致电银行客服人员了解情况，并及时冻结信用卡。

(四)慎扫二维码，降低盗用风险

典型案例

某小姐经常网购。最近找到一家网店承诺购物能返 100 元的红包。某小姐挑选了一件 500 元的毛衣，并询问卖家如何获得红包。卖家给某小姐发送了一个二维码 并称只要扫描该二维码，就可以获得红包。某小姐扫描后发现，红包界面并未出现。怀疑自己遇到了骗子，于是急忙联系卖家，可卖家已下线。

不久之后，某小姐发现自己的银行卡被盗刷，并立即报了警。经警方调查，当时扫描的二维码中含有木马病毒，盗取了某小姐的银行卡信息。

专家解读

不法分子提供的二维码其实是一个木马病毒的下载地址，这种病毒被下载后，可以自行安装，并不会在桌面上显示任何图标，而是潜伏在移动终端后台中运行，持卡人的信息就能悄无声息地被盗取。

小贴士

1.应该尽量选择信誉度比较高的正规商户，不要轻信商户发送的链接、压缩包、图片和二维码等。

2.谨防“山寨”应用软件，在扫码前一定要确认该二维码是否出自正规的网站，一些发布在来路不明的网站上的二维码最好不要扫描，更不要点开链接或下载安装。

3.在移动终端安装杀毒软件等相应的防护程序，一旦出现有害信息，可以及时提醒和删除。

(五)慎用公用 WiFi，保护账户安全

典型案例

某先生为了上网方便，在手机里设置了自动连接 WiFi 的功能。某晚某先生在外吃饭，搜寻到一个不用输入密码直接登录的免费 WiFi，某先生就登录了手机网 银，并输入了自己的卡号和密码查询银行卡帐户余额。次日凌晨时分，某先生被短信声吵醒了，通知他的银行卡被消费了2000 元;随后半小时内，又接连收到银 行卡被转账或消费的信息。

专家解读

不法分子会在公共场所提供一个免费 WiFi，持卡人使用后,极易被植入木马病毒，被盗取移动终端内的银行卡信息;除此之外,不法分子会把正规网站的网址绑 架到自己的非法网站上 ,当持卡人使用其 WiFi 网络并输入正确网址时，会跳转到一个高度仿真的假网站，如进行网络支付，就会导致卡片信息泄露。

小贴士

1.在连接公用免费 WiFi 前，最好与工作人员确定下哪个才是真正的 WiFi。此外，目前国内运营商提供的免费 WiFi 热点安全性相对较高，可通过电话或短信，获取免费的 WiFi 账号、密码。

2.及时为各类移动终端安装安全防护软件，可以有效降低在使用公用网络时遭受病毒侵害的风险。

3.不要打开 WiFi 自动连接功能，减少连接上“钓鱼” WiFi 的风险。

4.切勿在连接公用 WiFi 时使用一些重要账号，包括银行卡信息、网银账号、支付宝账号、微信账号等。

(六)警惕低价陷阱，拒绝“钓鱼网站”

典型案例

某先生收到一条促销短信，告知可低价购买热门手机，某先生按短信中的网址链接登陆网站，选中心仪手机后，按提示输入了个人银行卡卡号，身份证号，姓名，手 机号码等信息，之后又输入了动态码，网站显示交易成功。但之后，某先生一直没有收到购买的手机，报案后经警方调查，才得知是误入了“钓鱼网站”。

专家解读

不法分子会通过互联网、短信、聊天工具、社交媒体等渠道传播“钓鱼网站”，持卡人一旦输入个人信息就会被不法分子窃取盗用。

小贴士

1.在信任的网站进行购物，不要轻信各渠道接触到的“低价”网站和来历不明的网站。

2.进行支付前一定要确认登陆的购物网站或网上银行的网址是否正确。因为网站页面可以伪冒，但“钓鱼网站”的网址与官方网址一定存在差异，请认真识别。若有任何怀疑，请立即致电银行或电商客服。

3.在正规网站购物，下好订单进入支付页面时，网址的前缀会变成“https”，此时页面的数据传输是加密的，可以保护个人信息。如支付页面的网址前缀仍然是“http”，就可能存在风险。

4.安装防火墙和杀毒软件，并定期更新杀毒软件，防范电脑和移动终端受到恶意攻击或病毒的侵害;下载并安装由银行或正规电商提供的用于保护客户端安全的控件，保护账号密码不被窃取。

(七)关注手机安全，谨防木马病毒

典型案例

某女士收到一条显示为“10086”发来的短信 ,称其获得手机积分奖励，可兑换奖品，并附上了一个链接。某女士点击该链接后在页面上输入了卡片信息及手机 号，并按网页提示点击下载并安装了一个“积分兑换客户端”的应用，但安装后却无法正常打开，某女士也没有在意。第二天，某女士用卡时提示卡内余额不足，查 询发现银行卡在前一晚发生了多笔大额交易。某女士赶紧报案，但已造成损失。

专家解读

某女士收到的短信是不法分子利用伪基站冒充 10086 发送的，短信中的链接其实是一个“钓鱼网站”，而下载的客户端实际上是一个木马病毒。不法分子利用木马病毒窃取卡片信息并进行网络购物，同时将发送到某女士手机上的短信验证码转移到了自己的手机上，从而完成支付。

小贴士

1.不法分子能利用“伪基站”冒充任意号码发送短信，因此即使收到中奖、软件推荐等显示为官方号码发送的短信，仍需保持警惕，建议回拨进行确认。

2.木马病毒往往会伪装成其他应用，并通过“钓鱼网站”、短信、图片、邮件、压缩包、聊天软件等方式传播，建议不随意点击来历不明的应用软件等内容。

3.安装防火墙及杀毒软件，定期杀毒并定期更新系统补丁，保护移动终端安全。

4.下载网银支付类应用要到官方网站进行下载。

5.开通短信通知服务，账户发生异常变化后，及时联系银行，封锁账户或挂失卡片。

(八)远离网络中介，严守个人信息

典型案例

某先生因近期急需一笔周转资金,听朋友介绍了一家网络商户可以套现,便在该网站“购买”了电器产品，网络支付 2 万元。第二天,便收到转至其借记卡内的钱 款。之后,他又在该套现网站如法炮制,陆续多次套现。最近，某先生发现自己的信用卡有多笔不明消费，打银行客服电话，发现已被盗刷。

专家解读

根据《最高人民法院最高人民检察院关于办理妨害信用卡管理刑事案件具体应用法律若干问题的解释》条款，信用卡套现属于违法行为,情节严重的，应当以非法经营罪或信用卡诈骗罪定罪处罚。而此类套现网站大多没有经过正规注册或备案，增加了持卡人泄露个人信息的风险。

小贴士

1.持卡人利用套现进行资金周转的行为，如被银行监测到，将会采取降额或停卡处理，对个人信用记录造成不良影响。

2.网络套现易让持卡人陷入“以卡养卡”、“以债养债”的恶性循环，容易陷入经济困境。

3.另外，一些不法分子可能会以网络中介的身份，以代办信用卡或代办提额的名义，骗取持卡人个人信息后，盗取资金。

(九)如遇问题勿急躁，合理应对降损失

1.持卡人如遇盗刷，请立即致电发卡银行或支付机构，及时冻结账户或挂失卡片。

2.一些机构需要持卡人提供报警回执作为否认交易的证明材料，由于警方对案例受理地有规定，建议在前往派出所报案前先拨打 110 咨询。

3.持卡人可了解发卡银行的相关服务或政策，签约一些被盗刷后可有一定金额赔付的保险。

4.持卡人应该了解各类第三方支付平台相关规则，注意规避风险，维护个人合法权益。

(十)提升安全意识，培养良好习惯

1.提升安全意识、养成良好的安全用卡习惯，是应付层出不穷诈骗犯罪的有效方法。

2.经常用于网络支付的银行卡不要存太多资金，或设置每日最高网络消费限额，减少损失。

3.签约一些短信通知服务和盗刷保险服务，可以为资金财产保驾护航。

4.不同网络支付账户建议设置不同密码。

5.用于网络支付的电脑、Pad、手机等工具要安装杀毒软件，并定期查杀病毒。

6.不要点击来历不明的网址，在进行网络支付或退款等操作时请登陆正规网站。

7.不要告诉他人网络支付的动态校验码等关键银行卡信息。

8.不要登录一些非法网站，避免电脑或移动终端被植入木马病毒。

[Source]