随着“双11”购物节网购节日的临近，不少消费者已经跃跃欲试准备好自己的信用卡，想通过网络支付来享受购物的狂欢。不过，网络支付在为生活带来巨大便利的同时，也对个人银行账户的安全造成了威胁。那么，在即将到来的网购“狂欢季”里，持卡人应如何保证自己口袋里信用卡的安全，安心刷卡消费呢？

“后三码”泄露个人信息

一张信用卡，在不少网站无需密码就能划账，而这一秘密就在于信用卡背面的3位验证码。

据一秒通专业融资顾问介绍，信用卡“后三码”其实就是安全码，是一个用于身份验证的校验码，通常是印在信用卡背面签名处的最后三位数字，用于证实付款人在交易时是拥有该信用卡的，从而防止信用卡欺诈。校验码相当于信用卡的身份证，持卡用户可凭此码进行消费交易。其重要性几乎等同于密码。

记者在登录多家网站后发现，有的网站在用信用卡支付时只需提供信用卡号、有效期、持卡人姓名以及卡背后签名处“后三码”即可完成支付，在整个支付过程中，并不需要持卡人信用卡交易密码。也就是说，只要有这些卡面的信息，不需要任何实物卡和密码即可进行消费，卡号、有效期和安全码在信用卡上都有体现，而持卡者若稍不注意保密，就有可能被不法分子窃取信息并盗刷。

据记者了解，一般人的用卡习惯仅仅是给信用卡设置消费密码，对卡背面的签名处则相对不够重视。而现在网络支付一般需要持卡人提供卡号、有效期、卡背面“后三码”及密码，但在不少境外网站上购物时不需要密码即可完成交易。另外，国内也有商家与银行签约，在网络或电话交易时同样无需密码，仅凭安全码就可完成划账。

对此，有的网站客服称网站内部都有严格的安全控制措施，网站内部不会随意泄露消费者信息，这些信息的传输和保存始终处于加密状态，任何未经授权的人员都无法取得这些资料。不过，有时候持卡人预订酒店、机票，或者网上支付时，持卡人通过商家的POS系统，提供信用卡账号和后三码等信息后即可完成交易，此时，持卡人若无法妥善保护信用卡及信息，很可能面临资金和信用损失的双重风险。因此，信用卡以及卡片信息很重要，轻易泄露可能会导致卡被盗刷的风险。

轻易扫描二维码可能遭盗刷

很多时候，持卡人信用卡手机银行无故“被消费”，一个比较普遍的原因往往是持卡人在消费时无意中所扫描过一些二维码，记者了解到，其中有一些二维码很可能是一种诈骗手段。

据一秒通专业融资顾问介绍，一些消费者在网购时，接触到类似二维码的图样，店主会告诉消费者扫描某某二维码可享受一些回馈。而诈骗分子正是利用这些二维码将手机木马植入被害人手机并自动提取相关信息，就是这短短几秒钟的行为，持卡人的手机号、卡号、密码等个人信息很可能已经被传到别人手中。

融资顾问提醒，如今手机上网已成趋势，若干的手机APP携带着诱人的赠礼品等模式出现在消费者的手机上，甚至有些短信的发送号码，还伪装为某客服、某官方网站的短信号码，当点击这些链接，下载了相关的软件后，噩梦就开始了。因此，上述人士建议在手机上下载APP软件时，最好到官方网站进行下载。

一家国有银行信用卡中心人士则表示，针对目前日趋严峻的信用卡网络盗刷风险，各大发卡机构都在加大监测力度和风控力度，并对相关服务和产品进行升级，不过，每年的黄金购物季都是刷卡消费高峰期，建议持卡人在尽享购物优惠之余，最好时刻关注自身信用卡安全，警惕用卡风险。

免费WiFi使用或遇“李鬼”网站

随着网络越来越发达，免费的WiFi供应已经成为时下公众场所的“热宠”。越来越多的商场、饭店、咖啡厅等公共场所，为投顾客所好都有提供免费公共WiFi，“蹭网族”也越来越壮大。不过，就在人们使用方便快捷网络的同时，也让一些不法分子有机可乘。有时候，持卡人仅仅因为连接来路不明的WiFi，就会遭遇信用卡账号资金被盗刷。

记者了解到，由于现在大部分的智能手机和平板电脑等设备都具备自动搜索附近无线网络的功能，不法分子用钓鱼WiFi吸引他人搜索，一旦有蹭网者通过钓鱼WiFi信号上网，手机和平板电脑等移动终端可能被植入木马病毒，从而盗取移动终端内的银行卡信息，持卡人在登录网上银行时，输入的银行卡卡号和密码都会被记录下来并被解码，持卡人的个人信息就这样被非法掌握了。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，便导致卡片信息泄露。

另外，由于目前一些中小网站的安全防护能力较弱，容易遭到黑客攻击，不少注册用户的用户名和密码也会因为连接钓鱼WiFi信号而遭遇泄露。而如果用户的支付账户设置了相同的用户名和密码，则极易发生被盗用。

因此，一秒通融资顾问提醒持卡人，在公共场所搜索到的WiFi热点，最好不要轻易使用，如果一定要用，简单地浏览页面就可以了，任何涉及到登录账号、使用密码的操作，都不要使用，尤其是网上支付的这种超级敏感的账户，坚决不要用免费WiFi。

设置刷卡限额防止信用卡盗刷

那么，到底如何保护我们的个人账户信息？万一发生信息泄露或信用卡被盗刷的情况，持卡人又该怎么办？

一秒通融资顾问提醒，如果绑定网银的信用卡不涉及大额交易，建议给这张卡设置刷卡限额，万一被盗刷，可以防止出现大的损失，同时，也建议开通现金交易的短信提醒功能，信用卡的交易情况可以随时了解。持卡人要仔细核对每月的信用卡账单，如果发现账单上出现疑问交易的情况，可立即与银行联系。此外，持卡人还需要保管好身份证、驾驶证、房产证等身份财力证明信息。如果收到以银行名义发来的短信或者打来的电话，请注意信息的真实性，需要及时拨打银行服务电话进行确认。

而持卡人一旦遇到信用卡被盗刷的情况，首先要立即致电信用卡客服电话，要求银行对被盗刷信用卡予以冻结，防止二次刷卡，多数银行赔偿客户失卡后前48个小时的损失。随后，持卡人需要去所在地就近网点或ATM上打印盗刷卡片查询单，证明盗刷时自己所在地点和盗刷卡仍在自己身上。其后，要尽早去当地公安机关报案，开具公安报案受理证明，并去开卡行办理盗刷申报申请，按开卡行相关要求提供证明文件。