日前，国内信用卡网络支付中爆出严重安全隐患问题，包括持卡人身份证号、银行卡号、卡后三码等都有泄露可能。为此，记者采访了相关专家。

后三码重要性近乎密码

信用卡后三码是在非面对面支付环境如机票、酒店等订购中用来确认本人使用的关键要素之一。中国银联资深风险专家王宇介绍说，不同国际卡组织对其称呼略有不同，如银联称为CVN2，威士卡组织称为CVV2，万事达卡组织称为CVC2，但功能基本一致。

“后三码的重要性接近于银行卡密码，持卡人应妥善保管，不要向任何人透露后三码，更不要对银行卡进行复印。”王宇说，很多消费者对后三码的重要性缺乏认识，因而后三码泄露导致的安全问题越来越多。

因此，用卡人如遇到疑似钓鱼网站、诈骗电话和短信等索取卡片后三码，应果断拒绝。如发觉后三码泄露，应立即致电发卡银行，根据提示进行处理。

快捷支付小心用

网络快捷支付作为一种新兴的互联网支付方式，深受消费者喜爱。目前，快捷支付主要分为静态要素、静态与动态要素相结合的认证方式保障安全。静态要素一般包括账户密码、信用卡有效期、CVN2、持卡人姓名等信息，动态要素一般包括通过手机短信或动态令牌等方式，发送给客户的一次性验证码。

王宇建议，持卡人在使用快捷支付过程中，首先要认真查看支付流程说明，尽量选择静态与动态相结合的支付产品。而在网上支付时，尽量采用独立银行卡支付，与储蓄账户分离，同时设置网上支付额度，将快捷支付限制在小额支付时使用。

手机安全需留心

目前，银行在信用卡办理过程中，一般都要求用户填写本人手机号，并将手机号绑定信用卡，作为使用过程中的重要验证渠道使用，这给手机安全提出了更高的要求。

王宇提醒消费者，要格外留心手机安全，开户时不要绑定他人手机号码，使用过程中要防止手机中毒等造成的安全漏洞。二维码是现在流行的一种获取信息的新途径，但对病毒程序来说，二维码对应的连接文件包含着恶意程序或木马病毒，因此消费者不要扫描来历不明的二维码，防止中毒而导致账户资金受损。

此外，对于不明原因的手机停机，消费者也应特别注意，因为银行卡与手机绑定，如果发生了不明原因导致的手机停机，有可能是不法分子通过补号码的方式关联卡片并窃取卡内资金，要在第一时间联系发卡行确认账户信息和资金状态。

网上支付防钓鱼

对于钓鱼网站的防范，王宇说，钓鱼网站与正规网站最大的区别是：正规网站存储过持卡人注册登记的预留信息，而钓鱼网站没有持卡人的信息，也就无法进行验证输入信息是否正确。因此，持卡人可采用首次输入错误的用户名及密码的方式，对网站进行反向验证真伪。如错误的用户名可以登录网站，则证明该网站是钓鱼网站。

一般来说，银行等金融机构和主要电子商务网站，基于信息传输保密的考虑，域名大多以“https”开头，如果域名是“http”开头，在支付时需要特别注意。而通过短信、邮件和QQ等各类社交软件发来的陌生来源的链接，在无法确认真实性的情况下，需要特别警惕。

此外，钓鱼网站经常伴随着“办理退款”“升级系统”等短信方式推送给持卡人，遇到类似的情况，消费者要首先联系官方客服确认是否属实。