随着生活水平的提高,以及个人消费习惯的改变,不少人的钱包中摆满了各式的信用卡。信用卡使用方便,但使用不当就会带来风险,造成经济损失。然而,若养成好的用卡习惯,一些不必要的风险是可以避免的。《第1金融街》梳理了一些典型案例,为读者安全用卡提供借鉴。

现代快报记者 张瑾

伪基站、手机病毒、克隆卡……

揭秘信用卡盗刷四种常见伎俩

伪基站推送“官方短信”

去年4月份，市民王女士收到某银行“95×××”的官方号码发来的“积分换现金”信息,声称“登录×××××网站可激活领取礼品”,落款为“某某银行”。王女士表示看到是银行的官方号码，没有多想就点开了链接，并按照网站的要求提供了自己的身份证号、信用卡卡号和密码等,结果不多久就接到了该行发来的消费1万元的短信,王女士意识到自己的信用卡被盗刷了。

专家指出,通过手机和移动互联网实施的诈骗中,利用伪基站群发“假冒银行官方号码+钓鱼网址”的短信占据很大的比重，而且官方号的迷惑性较强,持卡人稍不留神就可能上当。如遇到类似情况难辨真伪，可致电相关银行信用卡官方热线进行核实,不要随意点击,更不要在对方提供的链接上填写个人信息和银行的账号和密码等。

木马软件复制手机信息

今年3月26日，家住江苏的周先生收到一外地陌生号码发来的短信。尽管觉得有点“蹊跷”，但周先生一看对方知道自己的名字,而且提到自己认识的人，没太多想就点击了网址,并下载安装了相关程序。之后,他发现手机绑定的银行卡内1.5万元现金不翼而飞。

专家介绍，用户安装程序后,会在手机上自动下载木马病毒,该病毒会复制下载手机上保存的各类信息，包括通话记录、通讯录、使用的APP软件。如果用户点击后又登录了一些带用户名、密码的APP,那么手机内的相关信息也会被不法分子窃取，他们会随时登录用户账号,盗取用户钱财。

消费时卡片信息被“克隆”

去年,贵阳的崔先生来到酒店收银台,拿出信用卡准备支付预付款,收银员刘某拿走崔先生的信用卡，为其办理入住手续。趁崔先生低头填写资料,刘某弯下腰,借着柜台的遮挡,迅速地将信用卡在读卡器上刷了一下。

刘某的异常举动,引起了崔先生的注意,崔先生报了警。经警方调查,刘某应聘收银员目的是接触客人的银行卡,利用为顾客提供刷卡服务之际,私下记录信用卡信息并窃取密码,之后快速将这张卡的信息传递给其他团伙成员,做出复制卡。

对此,专家提醒,刷卡消费时应尽量让银行卡保持在自己的视线范围之内,防止在交易过程中被不法分子使用盗码器盗取信息、套取持卡人的签名等;每次交易完成后,应妥善保存交易或查询凭条，不要随意丢弃,以防止不法分子根据交易凭条上的信息克隆银行卡。最好开通短信提醒服务,及时掌握银行卡的使用情况。

泄露CVV2码导致被盗刷

市民徐女士接到一个来电显示为“区号+银行服务短号”的电话,对方,准确地报出了她的全名，还说因为她信用良好,根据银行规定可提升额度。提升额度需提供银行卡卡号、有效期和卡背后的三位数CVV2码。徐女士没有多想,便一一告知。随后的10分钟内,她接连收到了4条消费短信,损失近万元。

银行业内人士表示,信用卡背面的CVV2码是网络交易的要件,重要性等同于密码,只要得到卡号、有效期、CVV2码即可上网刷卡，视同本人操作,目前尚无特殊的强制手段来对无需密码的交易形式进行限制。业内人士建议,持卡人可以剪一块小胶布把CVV2码贴住,以防泄露。在拿到信用卡后,务必先在卡背面签名;在刷卡消费时建议选择“密码+签名”的方式,不轻易将信用卡及密码交给他人使用。

小招支招

“三步”拆解最新诈骗手法

招行给您说清拆解诈骗手法,支招防骗技巧。

现象一:手机突然无法接听或拨出电话,发现资金丢失

第一步:不法分子通过非法渠道获取了您的身份证号、银行卡卡号、密码和手机号等。

第二步:伪造一张您的身份证件,试图在通信运营商营业厅挂失补办您的手机SIM卡。目的是为了截获银行向您手机发送的信息。

第三步:通过网上银行或手机银行将您的资金转出。

现象二:客户点击“银行”发送的短信链接,随后资金被盗

第一步:不法分子通过“伪基站”技术,模仿银行客服电话号码向您发来短信,“提示”您积分兑换现金,然后附上“积分兑换”、“升级”的链接。

第二步:您信以为真,点击链接,结果进入了不法分子伪装的钓鱼网站,该网站页面可能会与银行官网极为相似,页面也会引导您一步步输入信息,比如身份证号、卡号、密码、手机号、验证码等信息。或者在短信链接嵌入木马病毒,您一点击手机就中了病毒,该病毒可拦截银行向您发送的各种短信(包括转账时的短信验证码和账务变动通知)。

第三步:通过网上银行或手机银行,将您的资金转出。

如何才能躲避这些骗子,安心舒畅地在互联网上玩耍呢,下面为您支支招:

1.收到95555相关短信存在疑问,不要做任何操作,请及时拨打95555客服电话进行确认(请注意:显示为95555发出的短信也可能是伪基站所发)。

2.任何以“积分兑换、手机银行过期升级等”理由要求您录入“银行卡信息”的短信都是诈骗行为,千万不要随意点击短信链接录入银行卡信息。

3.资金转出时,银行都会校验银行卡的取款密码，因此特别提醒您，取款密码不能和登录密码一样,也不能和其他银行卡、互联网用户的密码一样。

4. 请默记招行官网和手机银行网址,谨防钓鱼网站以假乱真：官网:www.cmbchina.com手机银行:mobile.cmbchina.com

工银e投资 外汇投资理财神器

为了给外汇、贵金属、原油期货交易客户打造更加完善直观、便捷有效的交易体验,中国工商银行的“工银e投资”交易软件横空出世。工银e投资是汇集外汇、贵金属、原油期货等行情、资讯、交易和服务于一体的综合平台，平台包含行情端和交易端,行情端主要为客户提供行情查看及技术分析功能,交易端可提供交易下单、账户管理等功能,不论你是不是工行的客户,都可以使用它进行信息查询。

据了解,工银e投资客户交易终端提供丰富的资讯服务，并集合了贵金属、外汇、期货、债券等八大资讯板块，以及“工行看市场”专业观点板块的丰富资讯服务,拥有强大的分析功能。同时交易终端保证高频行情刷新，最快可以实现4秒刷新一次,有利于用户整体了解价格变化趋势，及时调整投资策略。

在专业性方面,工银e投资交易终端提供了强大的技术分析功能，除了各类行情一目了然之外，还包含了15个重要技术指标分析工具、画线工具等,适用于擅长技术分析的用户,为投资决策提供专业参考。在安全性方面,工银e投资客户交易终端提供“自动锁屏”、“预留验证信息”等功能,为客户的资金提供全面安全的银行级保障。此外,该平台还支持客户长时间无操作监控行情，具有用户自定义闪电预警功能，可以更好地辅助用户进行交易。

南京工行为庆祝工银e投资软件正式上线一周年,现举办“账户投资到工行”为主题的工银e投资杯账户交易大赛活动,2016年3月1日至2016年6月30日,参与账户贵金属、账户外汇、账户原油三项产品交易的个人客户交易量每月从高到低排名,排名靠前的50名客户作为竞赛胜出者,均可获得价值300元的精美礼品一份。