

# 短信验证码，说啥也不能给

## 年末银行卡网络诈骗增多，花样虽多但万变不离其“码”

不到一周的时间，青岛有多位市民反映，他们遭遇了骗子通过手机、网络进行的诈骗。有的骗子尽管无法一次性将用户银行卡内的钱拿进腰包，却能让它暂时“隐身”，再自编自导自演好戏，向市民骗取关键的短信验证码。

本报记者 姜宁

### 卡里的钱被人买了基金，骗子来电“求码”

11月3日晚，青岛姑娘小芳收到了一条短信：“您的银行卡购买X X基金X X元，余额X X元。”这时，“银行客服电话”打了过来询问购买基金的情况。

小芳明确答复对方自己并没有购买基金，对方又说：“现在很多人银行卡被盗刷了，所以我们要核实每一笔交易是否本人所为，如果不是本人消费，可以把钱退给您，我们已经向您手机发送短信验证码，请您把验证码告诉我们就可以了。”谨慎的小芳听完之后感觉不对劲，于是挂断了电话。

同样的事情发生在11月5日，张先生在网购付款时，发现卡里的1万多元不翼而飞了。张先生登录网银查询明细，发现账户里的余额被转入了名为财通可持续发展的股票基金。张先生先在网上银行办理了挂失，然后来到银行网点咨询，这才得知差点上了不法分子的圈套。

这种将储户的钱先变成基金或者黄金，骗取短信验证码后再盗刷的方式是最近以来的一种新骗术。“首先骗子取得手机银行的登录密码等信息。通过网上支付渠道，在用户的银行卡上

购买基金、外汇、黄金，造成发生‘扣款’或者‘退款’的假象迷惑客户。但值得注意的是，骗子由于没有手机银行的支付密码，因此无法将钱彻底取走。为此骗子利用已经掌握的储户信息为客户开通快捷支付，这时验证短信会发送到客户手机上。随后骗子冒充客服或者公安人员打电话给储户，告知银行卡被盗刷，诱骗得到储户的短信验证码，而一旦得到了验证码，储户账户上的资金也就不翼而飞了。”交通银行青岛分行一位工作人员告诉记者。



#### 行骗步骤解析

- 1、获得手机银行、网银的登录密码
- 2、通过手机银行、网银进行交易，购买基金、理财、黄金等产品（此时，骗子由于没有银行交易密码，无法将钱转移走。这时虽然会显示扣款，但钱的所有权仍是用户）
- 3、开通快捷支付功能，此时用户会收到短信验证码
- 4、冒充公安、银行人员，诱骗得到用户验证码
- 5、转移资金，骗术得手

#### 相关链接

### 骗钱成本几千 防骗成本千万

本报记者 姜宁

几个月前，市民小金曾经被盗刷了3800元钱，当他匆匆赶到银行时，只剩下手中的“您的银行卡已成功完成交易”的短信。

而在近期，青岛农商银行在胶州、胶南地区也及时制止了几起电信诈骗的案件，而相比于城市居民来讲，乡镇中的住户更容易被“卷入案件”、“涉嫌贩毒”等词吓住，从而轻而易举地说出自己的短信验证码或者取款密码。

不少储户绞尽脑汁也想不出自己出了什么差错，据小金回忆，在报案后，警方初步推测是由于小金点击了骗子用伪基站发送的钓鱼网站导致银行卡被盗刷，而从银行方面的反馈信息显示，今年在青岛市周边的县级市中都曾发现伪基站的身影。

一台电脑，几部电话，如果要盗刷，还要加上读卡器，用来摄像的MP4和写卡器，整套设备不过万元左右。“最近做的人多了，在网上就可以买到，价格只需要几千元。”银行业内人士说，此类手法从港台传来后，最早出现于华南地区。

但是对于银行来说，如果要防骗，那这种成本可就相当高昂了。“简直是防不胜防，以电信诈骗来讲，对客户的教育，根本跑不过骗子花样的翻新；而如果是银行卡防盗刷，现在比较好的方式是统一更换芯片卡，但是现在我们这类大银行光在青岛有几百万发卡量，每张卡的成本在10元钱左右，这一笔就要有上千万元的支出，代价太大。”一家国有商业银行的工作人员表示，要做好防盗刷、防电信诈骗，各项成本都很高。

### 点了不明链接，22万差点被騙走

半个月前，青岛市民李女士在网上购物时，曾点击了卖家发来的另一个链接，并输入了自己的身份证号码、银行卡号和密码等信息。

10月30日下午，李女士卡内资金突然被转出22.3万元。这下子李女士可慌了神，这些钱可是她和丈夫的毕生积蓄，本来要用来做点小生意，谁知一时大意，

20多万元顷刻间“蒸发”了。

焦急的李女士赶紧来到交通银行，银行主管迅速打印出李女士的账户流出，发现骗子通过“钓鱼网站”窃取账户信息后，进行了网上转账操作。但由于没有短信验证码，这笔钱尚在央行转账支付系统中，并没有支付到骗子的个人账户里。

就在李女士和银行工作人

员商量对策时，骗子开始操作转账系统，李女士收到由银行发来的短信验证码。而这时，骗子也打来电话，谎称是银行后台工作人员索要短信验证码。

在银行工作人员的指导下，李女士和骗子周旋，银行迅速将账户进行了冻结处理，并及时报案，最终找回了失踪的22.3万元。

### 克隆银行号码行骗，多瞄准国有大银行客户

5日上午，王女士收到了“95588”的短信，提醒自己电子密码器将要过期，要登录“www-icbc-m.cn”进行升级。

因为经常登录工行的网银系统，王女士一眼就看出了这不是工行的官网域名，但是骗子为何能够伪装成95588发送短信呢？“这种改号器在一些购物网站上就有销售，而且价格也不贵。骗子以极低的成本购买一套设备后，通过这种伪基站来发送

短信，诱骗市民点击这些虚假的钓鱼网站，以此来窃取储户的信息。”青岛银行一位负责人说，一般来讲骗子比较喜欢伪装成五大国有银行的客户号码，因为大银行的客户保有量比较多，一般人也都有五大行的银行卡，接到短信后比较容易上当。

记者调查发现，在烟台市南大街的金融聚集区内，工行、建行等不少大银行在门口LED屏上不停地播放着“近期有不法分

子假借本行密码器升级来行骗，请市民提高警惕”的信息。据了解，这种骗术在全省范围内较为常见，济南、烟台、青岛等地都曾出现过骗子的身影。

此外，除了假借密码器升级之外，骗子还经常借助“年底积分换购”、“买车退税”等方式诱骗储户点击钓鱼网站，窃取市民的信息，通过克隆银行卡或者网上转账的方式盗刷银行卡。

# 消防水枪打准，最快也得18秒

## 志愿者体验消防训练，感慨“练过跟没练过差别太大了”

### 互动消防 全民参与



本报济南11月8日讯（记者 尉伟 时培磊 通讯员 张超 杨林）8日，五名志愿者来到济南公安消防支队特勤二中队，进行了接水带打水靶、甩水带、穿消防战斗服等技能比拼。

首先进行的是接水带打水靶。志愿者们要迅速把水带铺接完毕，拿着水枪把25米开外的靶子击中，计时越快名次越高。一声令下，志愿者张硕把一个水带接口卡到分流阀上，另一只手拿起水枪就往另一个接口对接，站起身子拉动水带向前跑过去，在到达喷射点后，同时水带里的水流像蛇一样游到枪口处。这股水流的力量让张硕的身子略微一晃。一瞬间，他推平水枪开关，水柱直喷出十多米远，他调整力度和方向，几秒钟内，水柱便压过靶子。“20秒。”这是一个不错的成绩。而整个比赛下来，志愿者付



志愿者们来到场外，进行灭火训练的实战演习。本报记者 陈文进 摄

保洁以一枪击中靶心，18秒的成绩稳居首位。

接下来，志愿者又进行了甩水带比赛。六米开外有一处靶子，甩水带击中目标就算获胜。比赛开始后，几名志愿者连续失手，看着水带被快速甩出去，走到半路就拐了弯，六米外的靶子纹丝没有动过。最后，也只有一位志愿者击中了靶子。

最后一轮是比赛穿消防服。经过前几日的练习，志愿者的动

作娴熟了很多。他们穿上鞋提起裤子，小蹦几次调整裤子背带松紧，双手交叉伸进上衣袖子一个转身胳膊就套了进去，腰带系好，头盔戴上。“完成！”一分半的时间，3名志愿者就已经穿好了全身装备。

比赛落幕，两天的体验让志愿者们有些不舍。“希望以后还有机会参加这样的活动，平时真的很实用，练过跟没练过差别实在是太大了。”志愿者们感慨。

### 回报他们，就要提高安全意识

本报记者 时培磊 整理

经过几天的近距离接触，前来体验消防生活的志愿者们受益匪浅。不仅掌握了一定的消防技巧和知识，对于责任与纪律，他们也感受颇深。

济南3路公交驾驶员 郝传林：

我也曾是一名军人，今天来到消防官兵的军营进行体验，有相同的感受，也有不一样的体会。

包括消防车在内的装备管理规范、严格，这一点和我们炮兵是一致的，就连消防服，他们也都称为“战斗服”，这让我有一种亲近感和使命感，有上战场的欲望和必胜的信心。令我没想到的是，他们这一身的装备如此沉重，战斗服、氧气瓶、水枪等加起来有一百多斤。当过炮兵的我穿

上后，只是走走路就感到气喘吁吁，体力不支，可以想象在救火现场他们是怎样的辛苦，向他们敬礼！

我想，对他们最好的回报和尊敬就是我们大家都提高消防安全和道路行车安全意识，不留一丝安全隐患，不出大的交通事故，让这些和我同龄的消防官兵们少出警、多休息！

济南3路公交驾驶员 张硕：

经过参观学习，我们对消防有了新的认识，消防员的工作远比想象中更加危险和困难，消防员那为人民服务的矫健身手也着实让人佩服。感谢他们，因为他们用自己的生命书写着：“责任”二字！同样，作为一名公交驾驶员，责任也是重于一切，当有危险来临时，驾驶员对乘客的安全负有不可推卸的责任。