支付宝在发送验证码的短信里有一个卖萌的提醒：打死都不能告诉别人的验证码是……其实这是相当严肃的一个提醒，因为要发送验证码的场景都是在进行修改密码、快捷支付、绑定手机等敏感操作的时候，验证码作为一种“一次性密码”就显得格外重要。

融小妹曾为大家提供了信用卡诈骗的典型案例，对于各类验证码，我们也必须提高警惕，防患未然。

能够设置任意发送短信号码的伪基站

蔡先生收到了10086发送的积分兑换现金的短信，因为是熟悉的运营商短信，蔡先生便也没有太多戒心，点开网站，输入了自己的身份证号、手机号和银行卡号，又填上了收到了手机验证码。结果却发现随后那张银行卡就被盗刷几千块。

事实上，那条短信是诈骗分子通过伪基站发送出来的，并且在短信里添加了钓鱼网站，在获取蔡先生的个人信息和验证码后，便通过电商和支付平台完成了银行卡盗刷。

如今的诈骗也确实越来越有技术含量，伪基站就是诈骗分子生产组装的一种仪器，能够强行向一定范围内的手机发送短信，而且能随意更改发送短信的号码，比如10086等运营商号码或是95555等银行号码，有些也可能是掩人耳目的区号加10086、010086等。

所以对我们来说擦亮双眼不被山寨号码欺骗是重要的一点，但面对跟官方号码一模一样的号码，我们只能向官方询问，比如牢记中国移动到目前为止是没有积分换现金的活动的，不要为了一时小利而损失更多。

长得和官方网站极其像的钓鱼网站

刚才的那个案例中，我们也说到了钓鱼网站。因为这些钓鱼网站长得和官方网站很像，我们一不注意就很容易落入不法分子的圈套，按照网站上的要求输入了自己的银行卡号、密码、手机验证码等重要信息，导致银行卡的盗刷。

而且，冒充银行或者运营商客服群发诈骗短信的花样是不断的翻新，什么网银密码器失效、积分有效期到期等等，只为让你点击那个网址链接，一看到网站就信以为真，输入了各种重要信息，不法分子们就坐等转账了。

所以，我们不一定知道每个银行或者运营商的网址是什么，但我们必须知道正规的网址必定是简洁清楚的，要是出现一些不知所云的网址，还是谨慎为妙。

引诱你去点击的短信木马

张小姐有一天收到一条短信，内容大概是“这是我们聚会的照片，我做成了电子相册，打开看看吧……”之后就是一个网站链接。张小姐半信半疑，但觉得无非就是一个链接，于是想就点进去看看。结果却发现银行卡里的存款有了异动。

原来这条蹊跷的短信里有一个木马程序安装包，只要点击就会激活，从而拦截你的手机短信，在此之后收到的所有验证码就转而发到了不法分子手中，利用第三方支付平台把钱盗走。

好奇害死猫，来路不明的短信，还是不点为好。