近期，多地频发冒充平台客服类电信网络诈骗案件，诈骗分子多以“192”等号段拨打电话，后又以“影响征信”“注销账户”“国家利率下调”等为由对受害人进行诈骗。

Part.1 真实案例

近日，邓女士接到了一陌生电话，对方自称是某金融平台客服，称邓女士以前开通过借款，现在国家利率下调，某金融平台上面的利率高，需要进行取消操作。然后对方告诉他一个网址，进入后显示的是借款平台网站。

在线“客服”联系了邓女士，并称其名下关联共享的第三方账户存在违规信贷，贷款违规额度未清零导致某金融平台审核失败要其配合关闭。之后，客服让邓女士下载投屏软件，并输入了投屏码。在“客服”的指导下，邓某先把贷款账户里的40000元额度提现出来进行清零，“客服”要求邓女士向一张银行卡转账一元进行查验后，又以拉流水的名义让邓女士向相同卡号进行转账，但这次并不需要邓女士输入银行卡密码。之后又以同样的理由，让邓女士在多个平台进行贷款操作。

最终，邓女士通过银行卡转账信息意识到自己被骗，遂报警。共计被骗二十余万元。

Part.2 这些知识你一定要了解！

“192”开头的电话受到诈骗分子的青睐是因为192号段是中国广播电视网络有限公司（中国广电）2022年5月17日起正式运营号段，2022年9月27日，中国广电5G全新192号段正式商用。骗子就是利用了大家对广电电话卡的不熟悉，在前期初步获取信任，为之后实施诈骗打下基础。

诈骗分子多使用“192”开头的广电电话，冒充客服人员，威胁如不配合操作会“影响个人征信”，诱导受害人进行所谓的“注销账户”“下架金条”使得其“利率调低”，最终以套取受害者网贷为目的，并屡屡得逞。

Part.3 这些心机，你躲得过吗？

1.专挑工作时间正忙时打电话

经调查研究，一些受害人反映，自己是在上午或下午工作最忙的时候接到诈骗电话，那时脑子里全是工作的事，对方的话术把气氛弄得很紧张，不跟着做征信会受到影响。脑子里塞满工作的打工人根本就来不及反应，稀里糊涂地就在他们指挥下下载了会议软件，开了屏幕共享，再下载一些借贷平台借钱后转账给了指定账户。事

后回想，自己都觉得当时脑子像被纸糊住了一样。

2.多次电话轰炸，这到底是真是假？

当第一个“客服”电话打给受害人王先生的时候，王先生毫不犹豫地挂断了电话。第二个“客服”电话打给王先生的时候，王先生还是没有给诈骗分子可乘之机，但是接下来还有第三个、第四个……原本很是坚定的王先生现在有些动摇了，难道这是真的？如果我不操作，征信是不是真的会受到影响？在这样的心理攻势下，王先生根据对方的要求进行了操作，最终踏进了骗子设下的陷阱。

即使你一开始拒绝，诈骗分子还是会一而再，再而三地打电话过来，一旦撬开了一条缝隙，诈骗分子就会顺着这条缝隙进入，让受害人的防备心理彻底瓦解。

注：大家千万别小看这一特点的变化，常规的电信网络诈骗一般不会重复拨打电话，例如冒充公检法、冒充电商客服进行商品退赔。但此类诈骗手法，打破了常规套路，多番轰炸，让人防不胜防。

3.是不是学历高的人不易中招？

经统计发现，在受骗人群中，高中及以上学历占了总数的80%。诈骗分子不是应该更喜欢对老年人和低学历人群行骗吗？为什么学历高了，反而更容易被骗了？想必大家都有这样的疑惑。如今个人征信报告已成为人们的第二张“身份证”，如果失信了，子女上学会受到影响、买房买车无法贷款了、原本很好的工作不能继续了……一旦征信出了问题，工作和生活都会受到影响。而往往学历较高的人群更重视征信，对互联网应用也更加熟悉。骗子抓住这些特征，针对性地生产相应话术，以征信进行威胁，最终成功实施诈骗。这种方法，屡试不爽。

注：此类手法也打破常规，一般认为，学历越低，文化越低，越好骗。但是针对征信问题，学历越高，工作越稳定，越在乎征信问题，所以大家务必提高警惕!

4.有虚有实，让你傻傻分不清

当代诈骗手段，以更新快为主要特点。你以为骗子只是以影响征信为借口，要求你打款到指定账户，进行资金审核吗？不，骗术早就升级了！

王先生相信“客服”后，按照他的指示，在微信上关注中国人民银行，并发送“本人申请无本无息关闭XX金条网贷账户”至该公众号，并将这张截图发送给“客服”。


发票中心
发票补开、换开、抬头管理维护受到规则限制 查看帮助
全部
换开发票
申请记录
抬头管理
抬头信息仅用于开具发票，请勿用于转账等其他用途，谨防受骗！
普通发票抬头-单位
中国人民银行清算总中心
121000004008822225T
添加发票抬头

“客服”让王先生往发票中的账户进行汇款，用于拉流水，王先生看着中国人民银行清算总中心的抬头，放心无比地将钱转至显示的银行账户，默认了该银行卡号就是中国人民银行清算总中心。

王先生怎么也没想到，发票的抬头、税号都是真的，唯独就是银行账户是假的！其实是骗子利用盗号原理，事先进入王先生的京东账号修改了相关内容。

5.为什么骗子喜欢屏幕共享

“共享屏幕”被骗子作为诈骗工具，在冒充公检法、冒充客服等诈骗套路中都会被使用。由于这些具有“共享屏幕”功能的APP大多数能直接在应用市场下载，被骗的受害人也因此放松了警惕。

“共享屏幕”一旦开启，切换到桌面或其他APP也不能中断操作，只有点击软件的“关闭共享”、关机、关闭网络才能关闭，到那时，你的手机对诈骗分子来说将毫无秘密。当你输入银行卡密码时，骗子可以通过你按键的光标轻易掌握你的银行卡密码；当银行给你发来手机验证码时，诈骗分子都不需向你开口询问，弹出的短信验证码就能直白地进入诈骗分子的视线。

因此，一定牢记，如有陌生人让你下载某个APP，开启“共享屏幕”功能，那一定是诈骗！

防骗总结

骗子的目标人群多为高学历的年轻人，以贷款利率过高或影响征信为切入点，骗取目标者在各大网贷平台中的贷款。

请注意“192”开头的来电，这并不一定都是诈骗电话，但对陌生电话请一定多加防备。

骗子会以注销虚拟资金账户为由，让受害人在键盘输入“**21*电话号码#”。其实这是为手机设置呼叫转移代码，一旦设置成功，所有的外来电话一律无法接收。

在天眼查、票税宝等平台中默认的“发票抬头”，很有可能是诈骗分子通过盗取账号帮你私自添加的，请勿用于转账等用途，谨防受骗！

不要轻易下载视频聊天或者屏幕共享软件与陌生人聊天，更不要轻易将一些银行账户操作界面共享给陌生人。

来源： 平安武汉