

新年伊始，反诈走起

提高防诈意识 守好财产安全

□ 乔宁

岁末年初一直是电信网络诈骗的高发期，一些不法分子抓住群众新年消费、转账频繁的时机，开展诈骗活动，妄图大骗一笔，过个“丰收年”。泰安警方提醒广大市民，新年伊始一定要提高防诈意识，守好自己的“钱袋子”。

网络游戏虚假交易诈骗

宅在家里玩游戏是不少市民的假期首选，这部分市民要警惕网络游戏虚假交易诈骗。这类诈骗中，骗子多以低价出售游戏装备、游戏账号、游戏点卡、游戏元宝、游戏材料等名义，诱导游

戏玩家进行线上交易，收到钱后立马消失，骗取游戏玩家钱财。

警方提醒：玩游戏要到正规游戏平台进行交易，不要购买明显低于市场价的游戏商品，以免上当受骗。

虚假红包诈骗

新年期间，“红包大战”一触即发，虚假红包诈骗也随之来袭。骗子会借助社交平台散布包含“钓鱼”链接的“红包”，诱导市民点击、分享、关注公众号、填写个人信息等，最终窃取用户信息，盗刷用户银行卡。

警方提醒：警惕陌生人发来的“红包”、链接、二维码，自觉做到不点击、不扫描，以免遭遇“钓鱼”网站和木马病毒。一旦点击，页面提示“输入个人信息，领取红包福利”时，应立即关闭链接。

积分清零诈骗

新年伊始，各大平台积分兑换迎来高峰期，骗子会冒充银行、手机运营商客服等，发送“钓鱼”短信，诱导市民点击，骗取市民金融平台账户、密码、验证码等，窃取账户内钱款。

警方提醒：正规平台的客服人员绝不会向客户索要密码、验证码等敏感信息。进行积分兑换时，建议市民登录银行、手机运营商的官方网站进行操作，切勿点击可疑短信链接。

中奖信息诈骗

新年期间，不少市民会收到提示中奖的信息，信息中往往包含网站链接或咨询号码，诱导市民点击或拨打电话进行咨询，从而进行诈骗。

警方提醒：天上不会掉馅饼，收到此类中奖信息应立即删除，千万不要心存侥幸点击链接或回拨电话，以免掉入诈骗分子的陷阱。

虚假购物网站诈骗

岁末年初是市民置办年货的高峰期，随着网购的兴起，不少市民习惯在网上采购年货。一些不法分子利用网络技术，伪造与真实网购平台高度相似的虚假购物网站，然后通过各类低价促销手段吸引市民下单，骗取市民的网购账户、支付密码、网银信息

等，从而盗取市民网购平台或网银账户中的钱款。

警方提醒：市民网购时，一定要选择安全度高的第三方交易平台，同时核实网购平台的网址域名是否为官方平台网址，谨防登录虚假购物网站，泄露重要个人信息。

冒充电商平台退款诈骗

新年期间，各大电商平台会开展各种打折促销活动，吸引市民消费。与此同时，骗子会通过各种不法手段收集市民网购信息，然后假冒电商平台、网店客服、快递网点联系市民，假借商品缺货退款、快递丢失赔付、商品打折退差价等理由，骗取市民的网银账号、银行卡号、支付密码、验证码等信息，从而窃取市民网银账户中的钱款。

警方提醒：在这类诈骗中，由于骗子掌握了市民真实的网购信息，因此很容易获取市民的信任。市民网购后，如接到自称电商平台、网店客服、快递网点的退款电话，一定要通过当初的购买渠道，二次核实对方身份。此外，真正的电商平台、网店客服、快递网点，绝不会索要客户的支付密码和验证码，凡是索要支付密码和验证码者，都是骗子。

信用卡类诈骗

岁末年初，不少市民急需用钱，信用卡类诈骗应运而生。在这类诈骗中，骗子会发送“代办高额度信用卡”的短信，诱导有办卡需求的市民与其联系，并以“代办信用卡需要提供资金证明”为由，让市民向自己名下的借记卡存入资金。由于资金存入的是自己的借记卡，市民往往不会怀疑，但接下来，骗子就会以“方便代办”为由，要求市民将借记卡绑定的电话更改为骗子

的电话号码，从而盗取卡内资金。

警方提醒：市民应通过银行正规渠道办理信用卡，同时做好信用卡相关信息的保密工作。市民登录信用卡开户银行时，应注意甄别网址的真假（信用卡背面有开户行官方网址，可供用户核对），切忌登录不法分子提供的网址，更不要随意下载、运行来历不明的“加密软件”，以防不法分子通过木马对市民的手机、电脑进行远程控制。

● 反诈小贴士

1. 不参与任何形式的网络刷单，一切刷单、返利都是诈骗。
2. 不在银行及正规网络金融机构以外的任何机构贷款。
3. 不相信任何网络投资项目，不在非正规金融网站及各类小程序上进行投资。
4. 在核实清楚对方身份前，不进行任何汇款、转账操作。
5. 不相信任何自称社保、医保、通信局或公检法工作人员的电话核查，不向任何“安全账户”汇款自证清白（公检法工作

- 人员从不通过电话、网络办案）。
6. 不轻信任何中奖信息，坚信“天上不会掉馅饼”。
7. 不点击来历不明的网络链接，不在非正规网站购物。
8. 不理睬任何自称网购平台、网店客服、快递网店的理赔、退款。
9. 不理睬任何代办开卡信息，绝不将个人手机卡、银行卡信息出借、出租、出售给他人（此举不仅有被骗风险，还涉嫌帮助他人诈骗）。

