信 / 息 / 安 / 全　　意 / 识 / 为 / 先

安全意识 SECURITY

微信安全

- 网络诈骗手段频发 微信诈骗占多数
- 网络诈骗花样翻新 微信红包里可能藏着陷阱

GooAnn
gooann.com 谷安天下

概　览

作为网络大时代的社交工具，自问世以来，微信就收到用户的广泛欢迎，已不单单只是一个充满创新功能的手机应用。它已成为中国电子革命的代表，覆盖 90% 以上的智能手机，并成为人们生活中不可或缺的日常使用工具，但随之而来的信息安全事件也层出不穷。

微信安全，我们必须关注。

发 现

刷存在感：

更新朋友圈动态、微信群内分享知识资讯

移动互联时代，如果你不刷朋友圈，好像你就和朋友脱节了。

每天做了什么、吃了什么、玩了什么、去了哪里、和谁在一起等，拍成照片，附上文字，往微信朋友圈一发，晒晒自己的生活，成了许多人生活中不可缺少的一部分。

经常晒的有个人出生年月、长跑路程、外出旅游、个人电话号码更改等。

除以上几种个人信息外，还有个人家庭住址、感情生活、度假计划、工作情况等信息，这些也是容易让别有用心的人直接了解或推论出不少个人信息的内容。

除了朋友圈，许多人都会有自己的微信群，或许是同窗老友，或许是爱好相同的网友，时不时把自己看到的信息分享到微信群也成为不少人乐于刷存在感的地方。

微信红包大家抢

收发微信红包已是春节的一大“盛景”。除夕当天，4.2 亿人参与了微信红包，收发总量达到 80.8 亿个，创下历史新高。与此同时，腾讯旗下的 QQ 红包收发总量达到 42 亿个，环比增长高达 560%，创造了 QQ 红包收发总量的新纪录。腾讯两大红包收发总量超过 122 亿个，达到去年同期的 7.5 倍。

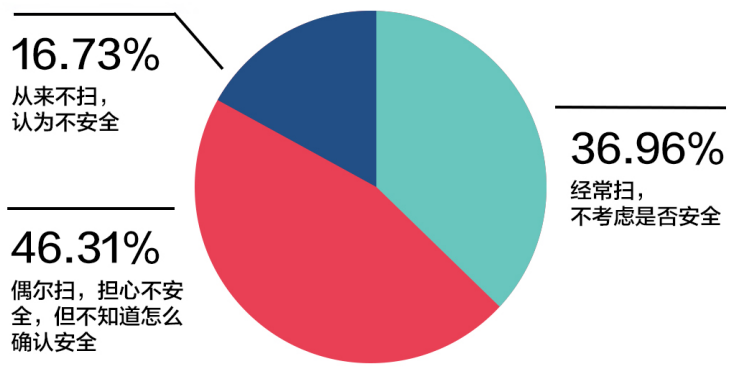
2 月 13 日，微信公布了除夕到初五的红包整体数据，共有 5.16 亿人参与微信红包，春节总收发次数达 321 亿个，比上年的收发 32.7 亿个，增长了近 10 倍。

不但参与人数和互动次数创下新高，指间新年俗——红包的渗透率也在地域上和年龄上开始扩展。从地域来看，微信红包的影响力正从一二线城市向三四线城市用户渗透，从用户年龄层次和新增用户来看，也开始向各个年龄阶层拓展。

微信红包数据显示，最喜欢发红包的省份是广东，江苏和浙江紧随其后，最喜欢发红包的前三个城市是北京、深圳和广州。在发红包排名前 20 的城市中，三四线城市数接近一半。

扫描二维码太随意

二维码在最大程度上诠释了“方便”这个词。一键扫描可登陆浏览，一键扫描可添加好友，一键扫描可快捷支付。但是借助二维码进行传播的手机病毒、恶意程序也日益增加，由于二维码技术已经相对成熟，普通用户即可通过网上的二维码转换软件，任意合成二维码，并且从外观上并不能判断其安全性，这就更加方便了黑客针对二维码进行各种非法操作，用户一旦扫描了嵌入病毒链接的二维码，其个人信息、银行账号、密码等就可能完全暴露在黑客面前，酿成的后果可想而知。



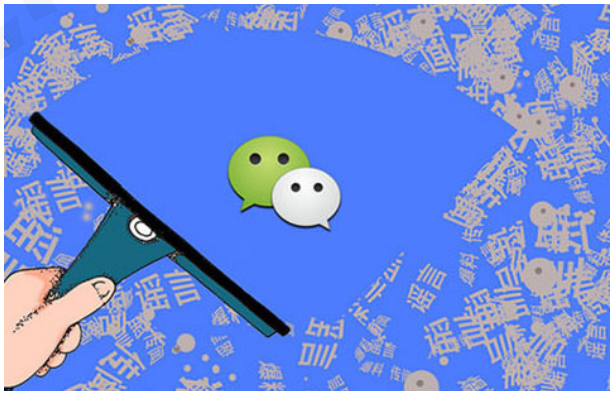
二维码扫描情况

网络诈骗手段频发　**微信诈骗占多数**

随着网络信息时代的高速发展，不少人利用互联网进行诈骗。近段时间，网络诈骗案件日益增多，通过网络进行木马盗号、利用网络支付进行诈骗的现象在网上已屡见不鲜。

而在多类诈骗手段中，微信诈骗在网络诈骗中占多数，有伪装身份、代购、爱心传递、点赞、利用公众账号等进行诈骗。其中，如最近较热的微商代购，犯罪分子便会在微信圈假冒正规微商，以优惠、打折、海外代购为诱饵，待买家付款后，又以“商品被海关扣下，要加缴关税”等为由要求加付，一旦获取购货款则无法联系。

微信谣言继续传播，**健康养生类话题**成重灾区



日前，中山大学大数据传播实验室、宏博知微共同推出了新一期《微信“谣言”分析报告》。报告分析了自 2015 年 4 月 10 日至 6 月 5 日的周举报数排名前 100 位“谣言”，共 600 篇公众号文章，排名靠前的“谣言”主题是：健康养生、疾病、金钱、人身安全、政治、政策相关、社会秩序、呼吁求救，其中以“养生食品安全”等死亡焦虑为主题的谣言占 55%。

报告指出，健康养生、疾病主题的“谣言”在引起读者恐慌情绪和死亡焦虑上有着不容小觑的能力。巧用病从口入的传统观念，将近三分之一 (32.2%) 的疾病、健康类谣言都涉及食品安全。在这些谣言里，生病是因为吃了不健康的食物，例如含有激素、致癌的牛奶；含有重金属和寄生虫的小龙虾；长了三四只翅膀的变异鸡……而这些“病从口入”的谣言，看准了“吃货”们的心理，在这“民以食为天”的国度，偏偏要让人吃得不安心。

同时调查发现，30.8% 的谣言都提到了癌症。癌症因其致死率高、治疗过程痛苦、病因复杂等原因，成了造谣者信手拈来的一种简单好用的必杀器。另一方面，谣言也用防癌当诱饵，趁机卖起了净水器和保险。谣言常常用身边常见的食品用品当陷阱，例如鸡蛋、牛奶、西瓜、蒸锅、肥皂等等，这些你平时食用使用时未加思考的东西，突然变成了致命毒药。

警 钟

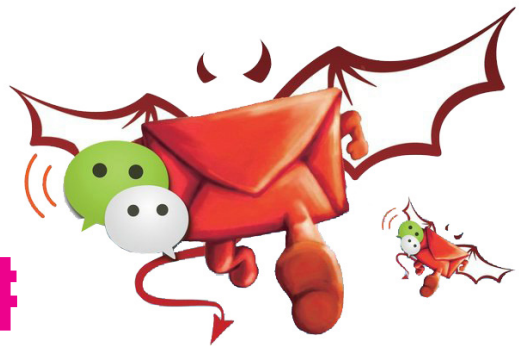
祸起微信群内泄密
证券高管停职受调查

中信证券首席分析师张明芳在其所处微信群和朋友圈发布消息称，丽珠集团将于下周二公布管理层限制性股票加期权方案……随着股权激励的完善，未来三年业绩增速逐年加快确定，维持“增持”评级。消息一出，市场一片哗然。由于涉及到内幕消息泄密，张明芳所在群的许多人忙着退群以撇清关系。随着丽珠集团公告的披露，张明芳泄密已是板上钉钉的事，并引发外界关于内幕交易的质疑。

“泄密”事件使得丽珠集团最终推迟了股权激励计划，公司董事会秘书李如才因此辞职；据记者从中信证券了解，事发后张明芳也被停职配合调查。

时隔 1 年多后，证监会公布了调查结果以及对张明芳和李如才的行政处罚决定，认定张明芳和李如才构成泄露内幕信息行为，张明芳被罚 20 万，李如才被罚 10 万。

网络诈骗花样翻新
微信红包里可能藏着**陷阱**



在微信里发红包、抢红包，成了眼下不少人热衷的一种社交和娱乐方式。看到微信群里不时冒出的红包，你会不会随手就直接点开，开心地去抢红包?

以后，在抢红包的时候可要多个心眼了，因为微信红包正在成为一些不法之徒新的诈骗手段。尤其是现在春节临近，一些不法商家和不良公众号也开始打起了微信红包的主意，各类新型红包诈骗手段花样百出。不法分子盯上了人们喜欢抢红包赚快钱的心理实施诈骗，导致不少网民个人信息泄露，造成财产损失。因此需要提醒大家的是，不要随便被陌生人拉进陌生群，更不要随便透露个人信息。

微信红包骗局 1：“靠谱互助配对微信群”

据媒体报道，近日微信朋友圈出现了一种新型红包诈骗。“靠谱互助配对微信群，投资 500 元即回 1000 元，交 50 元注册费即可等待匹配收米。”市民王女士被号称“利息高，回本快”的微信群游戏吸引，加入了此类微信群。按照规则，在交了几十元注册费后，即可按进群的先后顺序拿到数百元的回款。眼看着要轮到自己赚钱，群主却突然把微信群解散了。

微信红包骗局 2：“花钱进微信群可以得红包”

做化妆品生意的微商小雨有一次在微信群里看到了一个顾客转发的消息，说是只要付 100 元，就可以收获大量好友、参与活动以及产品推广等诸多福利。平台会给一个专属的二维码，如果你分享给别人，别人加入了就会成为你的亲友团，同时还可以得到10元、15 元、20 元、25 元不等的红包。小雨觉得 100 元也不是什么大钱，就给了。结果，进去之后发现里面几乎全部是微商，你可以一个个点击加他们好友。当晚小雨加了十来个人，等第二天进去的时候发现页面打不开了，过了一会页面打开却显示“该网页可能包含恶意欺诈内容，现已终止访问该网址。”

微信红包骗局 3：“点击链接可以拿红包”

市民邱先生见群里有人发了红包链接，链接写着某某公司，邱先生没多想这个公司是不是真有，就立即点击了“抢红包”，显示抢到了 200 元的现金礼包。邱先生随即点击兑换取现，但系统要求输入姓名、身份证号和银行卡号等信息。邱先生没有警觉，按要求输入了个人信息。没过几分钟，他收到网站发来的验证码短信，他立即输入了短信中的验证码。然而，邱先生收到的不是红包的确认消息，而是信用卡被刷走 1000 多元的短信通知。

原来，这是不法分子在微信互动界面中嵌入了钓鱼网址，用户点开链接的同时，其相关个人信息便被盗取。

专家提醒，一旦看到需要输入身份证号、手机号、银行账户等较为隐私的个人信息的红包时，一定要提高警惕，很可能是假红包。此外，碰到需要下载不明软件时也要多留一份心，小心下载的是木马软件。

盗QQ获微信出游信息 诈骗玩起了“量身定制”

这个春节，市民何先生带上全家去新加坡过年。让他万万没想到的是，在微信上晒了这次出游后他竟被不法之徒瞄上，被“量身定制”了一出骗局。

“没问题吧，护照的状况能搞定吗？”刚准备好好享受这次假期之旅，手机上跳出这样一条好友微信让何先生有些摸不着头脑。一看和“护照”有关，他紧张了起来：“什么意思，护照怎么了？”此时，好友发来的一段 QQ 聊天记录截屏把他吓了一跳。何先生告诉记者，最近一段时间，他很少上 QQ，一看聊天内容，根本不是他本人所发。“那人冒充我给我朋友发消息，也可能是群发的，说我的护照出了点问题，今天必须回去办理，让朋友帮我联系国内航空公司一个姓周的经理，说是之前让他预留了机票，问问定好没有。但事实上，我的护照没有出任何问题。”

随后，记者拨通了这位“周经理”的联系电话。“您好，南航票务查询！”电话那头的男子用标准普通话接起电话，听说记者要询问何先生的订票情况后，“周经理”表示马上帮忙查询，等待的半分钟内，不时能听到敲击电脑键盘的声音，“已经帮您查到，您有五张今天 13 点 15 分从新加坡飞南京的特价票，不过目前还没有缴费记录，您赶紧问一下何先生还要吗？”说完，周经理还不忘补充一句“他是怎么联系您让您查票的，您就怎么联系他。”当记者表示可以通过微信语音确认，和何先生本人沟通时，“周经理”立马挂断了电话。

“再通过被盗的 QQ 与‘我’联系，骗子自然会称自己暂时不方便购票，让朋友‘帮忙先垫上’。”目前，何先生已通过微信朋友圈和 QQ 签名发布提醒信息，希望看到的朋友别再上当。

何先生表示，正是因为自己的 QQ、微信等通讯软件相互绑定，骗子通过 QQ 帐号密码登录了他其他的通讯软件，从而获取了自己近期的出行信息，才“量身定制”出如此具有迷惑性的骗局。在此，也要提醒市民，如今不少人手机里各种软件互相绑定、关联，这在提供方便的同时，也为信息泄漏带来了风险，时常关注是否存在异常很有必要；眼下诈骗花头经层出不穷，假如收到朋友发来的涉及到钱财的求助信息，务必要多留个心眼，先以最直接的方式与对方本人联系核实后再处理。

诈骗"黑手"伸向微信：求发验证码盗号骗钱

“我的手机刷机了，你把你的手机号以及系统生成的短信验证码发过来。”如果你的微信好友突然这样说，一定要警惕，不然很可能被盗号骗钱。

以前广大网友对ＱＱ上冒充好友等行骗手段已很熟悉，不过随着近年来微信的火爆，骗子又开始玩起了新花样。据腾讯公司发布数据显示，目前我国使用微信人数已超 5.49 亿，逐渐成为人们不可或缺的日常交流工具。随着微信的功能不断增加，其绑定的内容也越来越多，“比如绑定银行卡、财付通账号、手机号码、QQ 号码、电子邮箱等。微信账号一旦被盗，意味着其绑定的所有内容都面临着连环被盗的风险，会造成更大的损失。此外，微信中的大量私密照片、个人隐私等也面临被泄露的风险。”一名从事互联网安全工作的人士表示。

专家建议，市民一方面可加强微信支付的密码保障，如手势密码，另外要格外警惕任何索取验证码的行为，有好友在微信里提到验证码或者金钱的时候，最好亲自打电话给好友本人进行确认，以免被骗子蒙骗，遭受损失。一旦社交软件被盗，应立即向软件提供商申请冻结账号，防止进一步的损失。

警方发布提醒，除了这类盗号方式外，扫描含病毒二维码、谎称海外代购补加关税、散布虚假中奖消息、伪装搭讪色情交友、点赞套取个人信息、仿造正规公众账号也是常见的诈骗手段，需要格外留意。

防 范

安装

1. 安装手机安全软件
2. 要从官网下载的正版微信，如果有安全软件则更佳
3. 最好设置微信独立账号和密码，不共用其他帐号和密码

使用

1. 手机设置锁屏密码
2. 切勿轻易向他人透露自己的帐号、密码等重要信息
3. 有选择地刷二维码，切忌见码即刷
4. 关闭“回复陌生人自动添加为朋友”
5. 如不希望他人查看你的手机号，则取消“通过手机号搜索到我”
6. 取消“允许陌生人查看十张照片”功能
7. 不用时关闭“附近的人”和“摇一摇”
8. 使用完“附近的人”，选择“清除位置信息并退出”

社交

1. 通过微信交友要谨慎，尽量通过手机通讯录添加好友，保证微信好友都是生活中熟悉的人
2. 给微信名添加备注，降低冒充身份的风险
3. 提及转账等敏感信息，首先确认对方身份的真实性
4. 晒工作，晒生活一定要有限度
4. 收到网站链接时，在确认来源可靠前，不要轻易打开网站地址

支付

1. 尽量避免把手机、银行卡、身份证放在一起
2. 微信钱包设置手势密码
3. 一旦发现手机和钱包丢失，立马联系银行冻结帐号，并及时修改微信帐号密码

账号保护

1. 进入微信后，点击右下角的栏目“我”—设置—帐号与安全—手机号，根据提示完成绑定
2. 绑定手机后，帐号保护一栏如显示“已启用”，此时微信即处于设备锁的保护状态下
3. 如果已绑定手机，但帐号保护一栏显示“未启用”，则点击此栏进入后将帐号保护开启即可