免费WiFi勿随便连 二维码切忌随便扫

快过年了,各种积分都在催人兑换礼品;亲朋好友聚餐,第一个动作是连接免费公共WiFi……这些貌似平常的举动,分分钟都可能把你银行卡里的钱送到坏人的口袋里。近日,全国首个反信息诈骗联盟“天下无贼反信息诈骗联盟”首次对诈骗及被骗人群进行精准画像,结果令人惊讶:40岁以上的高知人群最容易受骗。

每天有60万人次连接风险WiFi

不少人一到公共场所就立即搜索周围的免费WiFi,一看到二维码就想扫一扫。但据《移动支付网络黑色产业链研究报告》显示,每天大约有60万人次连接了存在安全风险的WiFi。不法分子通过搭建免费WiFi诱导你连接,从而盗取你手机上的重要信息,包括各类移动支付的用户名和密码。

不法分子还经常用恶意二维码伪装成活动福利,在公共场所引导用户扫描,一扫描手机就可能被植入木马病毒。各种网银账户密码、短信验证码将会被木马病毒盗取,后果不堪设想。

带有链接的短信不要随意点击

另外,春节临近,如果你收到聚会相册、结婚请帖或者是红包福利等“带链接的短信”,请务必要警惕!殊不知,这很有可能是一条手机木马病毒链接。

据业内人士透露,去年以来,移动互联网欺诈行为更加往“高技术化”“综合化”及“多平台”发展。从前,大部分的网络诈骗属于社工诈骗,比如盗号冒充好友让你转账。如今,犯罪分子是通过伪基站发送各种钓鱼短信,比如假冒10086、银行、学校用户发送短信,随短信附上一条木马病毒链接。在用户点击后,木马病毒随即植入用户手机,并盗取用户个人信息。不法分子用这些信息登录电商平台购物,并用手机木马病毒拦截银行短信验证码实现盗刷,最后卖掉物品来套现。

警、企、民协作利用大数据打击犯罪

目前手机用户往往都拥有多个网络账号,但有七成以上用户所有账号都使用同样的用户名与密码。一旦不法分子盗取一组账号信息,就很有可能成功盗用该用户的其他账号,包括移动支付账号。

数据统计,2015年移动支付安全领域,七成以上被侵害的用户为男性,年龄则集中在19~35岁的青年群体。资金受损最严重的省份是广东,而资金受损城市前五位中广东省占了两个(广州、深圳)。

近日,深圳市公安局公共信息网络安全检查分局副局长薛克勋表示,诈骗分子通过获取网民的网络行为和消费数据,可锁定被骗人群并有针对性地设计诈骗场景;诈骗渠道也拓宽到线上为主,网民的“移动钱包”成为诈骗实施的最新目标。

腾讯公司副总裁马斌介绍,“天下无贼反信息诈骗联盟”的警、企、民协作反诈骗防御体系已初见成效。截至2015年12月31日,联盟共接到群众来电132万余次,咨询员直接劝阻2.2万余人避免被骗汇款,涉及金额达1.8亿余元,帮助2.14万名事主快速拦阻被骗资金3.54亿余元,避免、挽回群众损失合计近5.34亿元。

40岁以上人群最容易受骗

《2015反信息诈骗大数据报告》显示:

1.40岁以上人群最易受骗,占受骗总人数的62%,职业多为事业单位职工、无业和离退休人员,文化水平往往较高;

2.作案者八成是90后。与受害人年龄层偏高不同,作案者则呈现年轻化态势,90后占犯罪人数的八成以上;

3.作案者多选择11时和16时作案;

4.虚拟号段要警惕。网络诈骗比重在迅速增加,且危害性最大。值得注意的是,用户对400、17×开头的虚拟运营商号段要仔细甄别。 **(据《广州日报》)**

QQ、微信、支付宝……用同一密码

一个账号被盗,其他全遭殃

近日,宁波市北仑区检察院以李某涉嫌盗窃罪、敲诈勒索罪向北仑区法院提起公诉。

手机突然被人锁屏

都说苹果手机现在是“街机”了,但很多人对它的功能还真不一定了解。比如说,只要用注册的账号和密码就能远程对手机进行锁屏,这个功能陈女士就不知道。

2015年5月14日晚上9时半,家住北仑的陈女士在家中用iPhone 6手机上网,突然手机被锁住了,屏幕上还显示一行字:“支付宝打6000元,我全部解除,支付宝账号:××××××@sohu.com”。

陈女士大吃一惊,她拿出另外一部iPhone 6 plus手机一看,也被锁屏了。这到底怎么回事?手机明明在身边,没有被盗,怎么会被锁屏?

陈女士的两部苹果手机用的是同一个ID账号,她觉得唯一的可能是自己的手机ID被人盗了。于是第二天一早,她把手机送到店里去解锁,并更换了两个密码。做完这些,陈女士悬着的心也放了下来。但是她没有想到,这才是刚开始。

当天晚上,她的iPhone 6 plus手机上的微信突然被人异地登录,当陈女士再次登录时,她支付宝捆绑的银行卡被人分32次转走4400元,这些钱被转到她的微信钱包里了。

银行卡里的钱进进出出

5月16日一早,陈女士打电话给微信客服,申诉微信账号被盗,并要求微信客服冻结微信钱包里的钱。

第二天,陈女士拿到新密码重新登录微信后,发现微信钱包里的4400元已经被人用掉170元,陈女士赶紧把剩余的钱提现了。

一周后,陈女士崩溃地发现自己的支付宝捆绑的银行卡又被人分7次转走1000元,她通过银行账单查询,得知钱被转到了深圳财付通科技的账号里。

陈女士又一次致电微信客服,客服告知,这7笔钱通过财付通科技又转到了一个微信钱包里,而这个微信账号居然是用陈女士自己的资料注册的。

不可思议的是,陈女士根本没有注册过这个微信账号,也不知道账号和密码,这1000元因此无法冻结。就在这时,她的银行卡里突然打进来910元,3分钟后又划走了900元!

钱被划进划出的节奏,陈女士是真看不懂啊,她赶紧又去查银行账单,发现原来是有人冒用她的身份资料到APP公司申请了贷款!陈女士对于这个贷款公司一无所知,贷了多少金额也不清楚,因为资金不是很多,陈女士也没有报警。

所有账号用一个密码:一个账号被盗,其他全遭殃

6月10日陈女士的银行卡再次被盗刷,盗刷的3000元转入了另一个微信小号钱包里,这个小号依然是用她自己的身份资料注册的,3000元也不能被冻结。

陈女士最终选择了报警。

6月13日,犯罪嫌疑人小李在安徽老家被北仑公安抓获。由此,陈女士才搞明白了是怎么回事。

原来,陈女士在一个QQ群内认识了小李,拜托他办理小额贷款,把自己的身份证照片、结婚证照片、银行卡卡号通过QQ发给了小李。

为方便办理贷款,陈女士还将自己在网上注册的平安易险小额贷款账号和密码告诉了小李。

但后来,小额贷款没有办成功,两人也就不再继续联系了,但是陈女士并没有将平安易险小额贷款账号密码更改,小李也没有将陈女士的身份信息资料删除。

5月15日晚上,小李在电脑上登录了一个叫“查找苹果”网站,抱着随便试试看的想法,输入了陈女士的QQ邮箱,之后又输入了陈女士告知的小额贷款账号的密码,居然成功登录了。

惊喜的他立刻在网站上点击丢失模式,并在备注栏内写下了一行字:“支付宝打6000元,我全部解除,支付宝账号:××××××@sohu.com”。

第二天,小李又尝试用小额贷款密码登录陈女士的QQ、微信、支付宝。他发现,陈女士所有的账号用的都是同一个密码!

他马上登录陈女士的微信,通过小额提现方式,每次提现200元,分多次将4400元转至陈女士的微信钱包中,然后用这笔钱充值了30元的QQ币,并给自己的手机号码充了100元话费。

得知陈女士已经将这笔钱申诉回去,自己也无法登录这个微信号后,小李又想到了另一种不会被冻结的盗刷手段。

小李用陈女士之前办理小额贷款时交给自己的身份证照片、结婚证照片等资料注册了一个微信小号,同时又绑定了陈女士的银行卡,之后分多次将银行卡里的1000元钱充值到微信小号钱包里。

光注册微信小号盗刷银行卡还不够,小李又想到了更高明的盗窃之法。

他成功登录了陈女士平安易险的手机贷软件,并以陈女士的名义成功贷款1000元,扣除手续费后还剩余910元,通过之前一样的方法将钱转到了自己的微信小号钱包里。

如今,李某已因涉嫌盗窃罪、敲诈勒索罪被提起公诉。 **(据《钱江晚报》)**

■ 记者部:3215881 出版部:3352588 发行部:3319180 3319015 3221991 3313857 ■ 广告经营许可证:41060030012 ■ 社址:鹤壁市淇滨区华夏南路 邮编:458030 ■ 定价:0.80元