捂好钱袋 别给他们发"年终奖"

春节临近,人们购物、送礼、聚会,踏上 归途,满心欢喜地期待与家人团圆。而随着智 能手机的普及, 过年抢微信"红包"也成了增 添节日乐趣的一项活动。不过, 在大家喜气洋 洋过年的时候, 有些别有用心之人却还没有休 息,他们准备趁着众人放松警惕的时刻再"捞 一把", 赚一笔"年终奖"。

外出会亲友 留意"三只手"

徐某在川沙地区经营着一家服装店, 凭着多年辛勤 的工作, 小日子过得红红火火。每年春节, 店铺客源稀 少,他会适时地休息几天与家人一起欢度假期。休息之 余,他会抽空到店里检查一下门窗、电源,生怕有什么 意外发生。

去年大年初三,徐某一早骑车来到店门口,规整地 上锁,一切显得那么井然有序。在沪打拼多年, 他做事处处小心谨慎,非常珍惜这来之不易的生活。锁 好车后,他就匆忙转身进了店,也许是平常养成了停车 上锁的习惯,让他潜意识内认为只要上锁,自行车就是 安全的,竟完全疏忽了放在车兜里的手提包。也就几分 钟时间,手提包连同 4 万元现金不翼而飞。徐某站在街 头四处徘徊,焦虑、悔恨,最终还是拨通了 110,寄希 望于警方能帮他找回这只"未上锁"的手提包。

浦东公安分局川沙派出所民警接报后,根据徐某描 述,调阅案发地周边监控,很快便锁定了嫌疑人。民警 循线追踪,实地走访,离案发时间仅2个小时,犯罪嫌 疑人肖某就落网了。

经审讯, 肖某交代当天路过案发地时, 无意间看到 了徐某遗忘在车兜里的黑色手提包, 便起了贪念, 旁若 无人地将手提包顺走了。

徐某的经历许多人或许都有过,特别是过年期间, 大家多会选择出外游玩或者购物,且往往都会携带有大 量现金。朋友相聚, 兴致一高很容易就会放松警惕, 而 在购物街、商场饭店、旅游景点等地方人员相对密集, 犯罪分子往往容易利用这一机会,进行扒窃、拎包作

同时,春节中,在外用餐、游玩频率增加,致使许 多居民家中白天或者夜间无人居住成为安全防范盲点, 犯罪分子极有可能乘此机会作案。大家外出时要记得关 闭、锁好门窗, 低楼层住户可考虑加装限位器、报警 器、防盗窗等必要的技防物防设备,切莫因大意失窃。 一旦发现有可疑人员要拨打报警电话。

开车出行时,为了避免不必要的损失,尽量避免在 车内放置现金及贵重物品。夜间停车时,要注意检查车 门、车窗是否关好。锁上车门后,要有再拉一下车门的 习惯,确保车门真正锁死,避免给偷盗者留下可趁之

而对厂区、公司等单位而言, 也要注意采取安保措 施,避免因人防、物防、技防力量减弱留给犯罪分子可 乘之机。



资料图片



资料照片

商场忙促销 票券被克降

年终岁末, 商家常印制并出售大量 代金卡、代金券,由于这些代金卡、代 金券不属于法律意义上的有价证券, 在 印制和使用上缺少相关规定和防伪标志, 让一些不法分子有空可钻,以伪造的代 金卡、代金券诈骗商家货物

去年春节期间,大连警方就接到一 家超市的报警,超市表示自己之前搞了 个活动,购物满499元就赠一张提货单, 这张提货单是50元的额度,可以当50 块钱用,但是在这个活动结束之后,这 家超市在清点提货单的过程中,发现提 货单多了55张。

这家大型超市当时一共就发了500

张提货单,可活动结束后一清点,竟然 点出了555张,这多出来的55张提货单 是哪来的呢?据了解,每张提货单下面 都有自己的编号,警方通过比对找出了 55 张假的提货单,从印章还有各种方面 都与真的提货单有明显的不同,肯定是 有人伪造了提货单,并使用这伪造的提 货单在超市购物。

民警调取了这家超市活动期间的监 控视频,在收银台口的视频里,一名女子 引起了民警的怀疑。她在同一天,多次在 这个超市内购物, 最多可以达到七八次。 民警在超市排查时,从收银员那里得知, 这名女子每次都在不同的收银台结账,购 买的大多是烟酒、零食等年货,一次会用 掉六七张提货单,而购物金额也都控制得 很好,提货单从不浪费,甚至差个一两块 钱,还会买一沓塑料袋带走,这让收银员 对她印象很深刻,并认出这女子就在超市 楼上的商场里上班。

随即民警对嫌疑人杨某进行了传唤, 她承认了自己伪造提货单进行购物的事 实。原来当时杨某偶然得到了一张超市 的提货单,就想出了复制伪造的点子, 她在网上找了一个人印制了55张单子, 在春节前全都用了出去。杨某此后被警 方行政拘留,并将使用的55张提货单, 折合 2750 元交还给了超市。

欢乐抢红包 小心有陷阱

家住南京的周女十经常参与微信"抢 红包"活动。一天,她的一名"好友"给她发 来一个红包,红包还包含"开抢500元代金 券"的链接。周女士点击链接,发现自己竟 抢到了"500元代金券"的头等奖,立即喜 滋滋地点击指定网址领奖,并输入了身份 证、手机号、微信账户等一大堆个人信息。 输完信息后,对方还要求她扫描一个二维 码。周女士虽有些犹豫,但想到是朋友发 来,还是决定扫码。扫完码刚几分钟,周女 士收到一条银行短信,银行卡里被转走了

周女士立即打电话向朋友核实情况, 朋友告诉她微信号被盗了。周女士这才 发现自己上当受骗,立即拨打电话报警。

经公安机关检测,周女士扫描的二 维码里藏有木马程序。嫌疑人利用木马 程序窃取了周女士的个人信息,又通过 木马转发周女士的支付验证短信,并盗

随着网络技术和移动互联网的普及, 不法分子很容易在微信等 APP 互动界面 中嵌入钓鱼网址,一旦用户打开链接, 其个人信息便被盗取。微信红包更被众 多不法分子利用,这些人会潜藏在人数 较多的微信群或朋友圈中, 通过分发嵌 人钓鱼网站、木马程序下载地址的红包, 盗取用户信息,甚至控制用户手机。特别注意以下几类"红包"不能抢:

1、需要个人信息的红包不要碰。领 取红包时,要求输入收款人的信息,比

如姓名、手机号、银行卡号,这种很可 能是诈骗。而事实上,正规的微信红包, 一般点击就能领取,自动存入微信钱包

- 中,不需要繁琐地填写个人信息 2、分享链接抢红包系欺诈。看到朋友 圈分享的红包,比如送话费、送礼品、送优 惠券等,点开链接要求先关注,还得分享 给朋友的情况。这种红包涉嫌诱导分享和 欺诈用户,点击右上角举报即可。
- 3、与好友共抢的红包需谨慎。朋友 圈有不少跟好友合体抢红包的活动,要 求达到一定金额,比如100元才能提现。 玩这种游戏要格外注意,红包页面的开 发者是否正规,很可能只是一种吸引粉 丝的骗局。
- 4、高额红包不可信。单个微信红包 的限额是200元,因此如果收到比如 "888"之类面额的大红包,基本 上可以确定就是骗子。
- 5、警惕"AA 红包"骗局。还有一种"AA 红包"也要警惕,此类红包往往 对微信 AA 收款界面进行略微改动,加 "现金礼包"等字样,让用 户误以为是在领红包。微信红包有自己 的专属橙红色界面,不需要进入 AA 收 款界面;另外,用户收红包根本不需要输 入密码,点击领取就能存入微信零钱包。
- 6、拆红包输密码恐有诈。如果有商 家或者朋友发来一个微信红包, 拆时却 要输密码,那就要警惕了,因为这可能 是假红包。真正的微信红包在收的时候

是绝对不需要输入密码的。因此,切勿 轻易点击微信群中来历不明的红包、优 惠券等,以免个人隐私信息的泄露。

此外,每逢春节,测试来年运势的 各种链接便会在朋友圈内刷屏, "发大 "桃花运"等测试结果让朋友们纷 纷参与转发。很多人觉得这种毫无依据 的测试就是娱乐一下,但是骗子就是利 用这种心理,制作假的微信链接,称测 新年运势, 让参与测试者填写自己及家 人的姓名、生日等比较私人的信息,从 而搜集个人信息。要牢记,就算是为了 娱乐也不要将自己或家人的信息随便透 露给陌生人,以免对方通过获得的信息 一步实施精准诈骗。

过年期间,走亲访友以及与朋友的 各种聚会必不可少。在此期间,有不少 人会收到诸如同学聚会的照片短信,并 配以"这是我整理的照片,有空记得看" 的文字和链接,一旦点击了短信中的链 接, 手机就会被植入木马病毒, 手机内 存的银行卡、支付宝信息就会到骗子手 里。如若收到这类短信,请立即删除。 如果不小心点开链接, 应第一时间关机, 取出手机卡,重装系统、恢复出厂设置 或用杀毒软件查杀病毒。同时,第一时 间通知通讯录里的亲朋好友,立刻修改 自己的银行卡、支付宝等账号密码,将 损失降到最低。

(综合整理自新华社、警民直通车、 看看新闻、重庆晚报等)