责编：赵鹏姣
制版：包聪颖
内蒙古法制报

短信『半夜盗刷』频发 用户需提高警惕

犯罪分子用特殊设备嗅探用户短信 『睡觉前关机』是最简单应对方法

“一觉醒来，手机里多了上百条验证码，不仅账户被刷光还背上了贷款”——近期犯罪分子利用“GSM 劫持+短信嗅探”的方式盗刷网友账户的事件成为网络热点。那么，该如何防范这种短信嗅探犯罪呢？安全专家指出，最简单的一招就是睡觉前关机，手机关机后就没有了信号，短信嗅探设备就无法获取到你的手机号。

在主流 App 中，许多账户登录及资金操作都可以通过手机号码加短信验证码的方式实现，对于用户来说，这种操作为自己带来方便，无需记忆复杂的密码；但对于别有用心的犯罪分子来说，他们可以利用简单的设备获取用户的验证码，从而操控用户账户，提现、消费，甚至贷款。专家表示，这是犯罪分子利用“GSM 劫持+短信嗅探”的方式，把银行卡或其他账户里的钱盗刷或者转移了。

事件

一觉醒来收百条验证码 存款全无

本月初，家住深圳的网友“独钓寒江雪”发文称，自己当天起床发现手机接收了 **100** 多条验证码，包括支付宝、京东、银行卡等，查询发现，“支付宝、余额宝、余额和关联银行卡的钱都被转走了。京东还开通了金条、白条功能，借走一万多元。”

手机截图显示，她从凌晨 **1** 点多起，陆续收到来自中国银行、京东、京东支付、环迅支付、房天下等多个号码发来的“验证码”短信，仅在 **3** 点 **11** 分就收到了 **4** 条短信，一共 **100** 余条。

如京东金融自 **2** 点 **34** 分起，陆续发送了“(借款成功)您成功申请金条借款 **10000.00** 元，将于 **30** 分钟内到尾号 **0152** 的银行卡”“恭喜您开通白条，额度为 **5000** 元”等多条短信，京东支付的短信显示：“验证码：**362661**，您现在正在进行支付，短信验证码请注意保密……”环迅支付显示：“验证码 **219860**，你正在使用快捷支付，校验码很重要，不要告诉任何人哦！”**10086123** 的短信显示：“您的短信验证码为 **351525**，请本人及时输入，切勿向他人透露。”

另外，她还查询到自己的多个账户中的钱已被交易，对方用自己的支付宝绑定的工商银行卡购买了 **1000** 元的 **Q** 币，还预定了南京一家高档酒店的套房，用京东卡充值了 **2000** 元的中国石化加油卡等。

分析

利用短信嗅探 专挑熟睡时段作案

那么为何会出现“睡一觉把存款睡没”的情况？腾讯安全的技术人员表示，“这些人都是被犯罪分子用‘**GSM** 劫持+短信嗅探’的方式，把银行卡或其他账户里的钱盗刷或者转移了。”

据技术人员介绍，短信嗅探通常由号码收集设备(伪基站)和短信嗅探设备组成。其犯罪具体分为以下四步：第一步，犯罪团伙基于 **2G** 移动网络下的 **GSM** 通信协议，在开源项目 **Osmocom-BB** 的基础上进行修改优化，搭配专用手机，组装成便于携带易使用的短信嗅探设备。

第二步，通过号码收集设备（伪基站)获取一定范围下的潜在的手机号码，然后在一些支付网站或移动应用的登录界面，通过“短信验证码登录”途径登录，再利用短信嗅探设备来嗅探短信。

第三步，通过第三方支付查询目标手机号码，匹配相应的用户名和实名信息，以此信息到相关政务及医疗网站社工获取目标的身份证号码，到相关网上银行社工，或通过黑产社工库等违法手段获取目标的银行卡号。由此掌握目标的四大件：手机号码、身份证号码、银行卡号、短信验证码。

第四步，通过获取的四大件，实施各类与支付或借贷等资金流转相关的注册/绑定/解绑、消费、小额贷款、信用抵扣等恶意操作，实现对目标的盗刷或信用卡诈骗犯罪。因为，一般短信嗅探技术只是同时获取短信，并不能拦截短信，所以不法分子通常会选择在深夜作案，因为这时，受害者熟睡，不会注意到异常短信。

据腾讯安全的技术人员介绍，嫌疑人的设备包括两种，一种是收集设备，一种是嗅探设备。收集设备由一个伪基站、三个运营商拨号设备以及一个手机组成。这台设备启动后，附近 **2G** 网络下的手机就会被轮流“吸附”到这台设备上。此时，与设备相连的那台手机(中间人手机)就可以临时顶替被“吸附”的手机。也就是说，在运营商基站看来，此时攻击手机就是受害者的手机。嫌疑人的短信嗅探设备则由一部电脑、一部最老款的诺基亚手机和一台嗅探信道机组成。利用该劫持设备，犯罪分子可以看到这个基站区域内所有用户收到的短信，并且用户毫无知觉。

关注

短信嗅探盗刷到底该如何防范

由上可见，嫌疑人要实现盗刷需要很多条件：第一，受害者手机要开机并且处于 **2G** 制式下；第二，手机号必须是中国移动和中国联通，因为这两家的 **2G** 是 **GSM** 制式，传送短信是明文方式，可以被嗅探；第三，手机要保持静止状态，这也是嫌疑人选择后半夜作案的原因。第四，受害者的各类信息刚好能被社工手段确定；第五，各大网站、**APP** 的漏洞依然存在。

那么，作为普通网民来说，如何防范这种短信嗅探犯罪呢？腾讯安全的技术人员表示，最简单的一招就是睡觉前关机，手机关机后就没有了信号，短信嗅探设备就无法获取到你的手机号。如果发现手机收到来历不明的验证码，表明此刻嫌疑人可能正在社工你的信息，可以立即关机或者启动飞行模式，并移动位置，逃出设备覆盖的范围。另外还要注意自己手机信号模式改变。在稳定的 **4G** 网络环境下，手机信号突然降频“**GSM**”、“**G**”或者无信号时，警惕遇到黑产实施的强制“降频”及 **GSM Hack** 攻击，要及时更换网络环境，重新连接真实基站，检查移动 **App** 异常恶意操作情况。

在手机设置上，用户可以使用“**VoLTE**”保护信息安全：在手机设置中开启“**VoLTE**”选项，目前主流安卓或 **iphone** 手机均已支持。(**VoLTE**：**Voice over LTE**，是一种数据传输技术，无需 **2G** 或 **3G**，可实现数据与语音业务在 **4G** 网络同时传输)

同时，用户最好关闭一些网站、**APP** 的免密支付功能，主动降低每日最高消费额度；如果看到有银行或者其他金融机构发来的验证码，除了立即关机或启动飞行模式外，还要迅速采取输错密码、挂失的手段冻结银行卡或支付账号，避免损失扩大。

提示

平时需做好敏感私人信息保护

此外，据犯罪嫌疑人交待，他们利用设备登录一些防范能力较低的网站（一般只需要手机号+验证码)绰绰有余。但是他们的目的并不仅限于成功登录，而是要盗刷你名下的钱。所以还需要通过其他手段获取姓名、身份证号、银行卡号等信息，他需要社工手段来确定这些信息。因此，用户平时要做好手机号、身份证号、银行卡号、支付平台账号等敏感的私人信息保护。

那么，骗子如何获取用户的这些信息呢？例如如何获知附近用户的手机号？据腾讯安全技术专家介绍，手段千奇百怪，比如骗子劫持到中国移动 **139** 邮箱发送来的短信“中国移动 **139** 邮箱狂欢来一波**!100%**有奖!点击查看邮件详情 **xx**”后，复制其中的链接到浏览器，点击“进入掌上营业厅”，就可以直接看到手机号了。知道了手机号以后，再通过登录其他一些网站，利用社工手段就可以很轻松地知道这个人的银行卡账号、身份证号。

在获取了用户信息后，骗子就可以利用这些信息实施犯罪。其一，登录各种网站修改密码，如许多电商、旅游网站允许使用“手机号+验证码”的登录方式，而骗子又可以实时监控到验证码，所以很容易就可以登录。其二，可以盗刷资金，许多 **App** 的安全策略较低，不少 **APP** 只要输入“姓名+银行卡账号+身份证号码+手机号码+动态验证码”，就默认是本人操作，骗子进入以后马上就会盗刷或者购买点卡类虚拟物品。其三，利用网站身份申请贷款等，有些嫌疑人刷完了银行卡中的钱，还会通过这些信息在一些小的贷款网站、平台申请小额贷款，让受害人不但积蓄全无，还会背负债务。通过非法获取和贩卖用户的隐私信息，黑产还可实施精准的电信网络诈骗、敲诈勒索、恶意推广营销等不法活动。

建议

网站需提高短信验证码安全系数

而针对网络平台，全国信息安全标准化技术委员会也下发了一份《网络安全实践指南——应对截获短信验证码实施网络身份假冒攻击的技术指引》，建议个各 **App**、网站服务提供商对业务系统中短信验证码的使用方式进行摸底。例如在用户注册、密码找回、资金支付等环节的短信验证码使用情况，并评估相关安全风险，优化用户身份验证措施。全国信息安全标准化技术委员会建议的方式包括：短信上行验证、语音通话传输验证码、常用设备绑定、生物特征识别、动态选择验证方式等。

如短信上行验证具体是：提供由用户主动发送短信用以验证身份的功能，如要求用户在规定时间内（如 **60** 秒)，使用已绑定的手机号码向移动应用、网站服务提供商指定的短信服务号码发送指定内容短信，移动应用、网站服务根据短信内容对用户身份进行验证。常用设备绑定为：提供将用户账号与常用设备绑定的功能，原则上支付、转账等敏感操作只能通过该绑定设备执行。设备绑定、更换等操作应采用短信上行验证、语音通话传输验证码等方式，并采用诸如要求用户回答预设问题、提供注册时填写的相关用户信息或核对该用户账号近期操作记录等方法进一步确认用户身份。 （温婧）

广告发行部电话：(0471) 4687563 广告经营许可证：呼工商广字 1501004000013 邮编：010010 本报激光照排印刷：呼和浩特日报社印刷厂 本报零售：每份 1.6 元