点击短信链接 11万元不翼而飞

北京警方破获新型电信诈骗案

有团伙负责往手机中发送被植入病毒的链接，有团伙负责盗刷银行卡，有团伙负责收红包并通过第三方转账的方式提现，已经形成黑链条。昨天上午，记者获悉，北京警方辗转千余公里、历时40多天，近日一举打掉一新型电信诈骗犯罪团伙，抓获涉案嫌疑人9名。

银行卡11万元不翼而飞

“我是房某某，照片里这几个人你认识吗？http：//guo.kr/bd……”今年2月底，事主许先生接到171开头的手机号发送的短信，以为是朋友发的，未加思索打开短信点击了一下链接。事主不但没有看到照片，反而不停接到空白短信，刚开始并未在意。

直到当日中午12时许，银行打来电话告知其银行卡被盗刷11万余元，其才知道是诈骗短信，立即向警方报案。

无独有偶，警方在前两日也接到同样的报警，几天之内便发生两起类似案件，引起警方重视。为防止更多人被骗，北京警方成立了专案组迅速开展侦查。

支付平台转账套现

经初步调查，民警发现，嫌疑人作案手法系通过事主点击短信网址链接，将病毒程序植入手机，以盗取事主绑定的银行卡账户、密码等信息，进而通过网站购物消费、第三方支付平台转账等方式套现获利，与之前常见的通过银行转账套现方式有所不同，作案手段较为新颖，是一种新型的电信诈骗。

于是专案组循线追踪，经过3个昼夜，最终锁定利用第三方平台转账的实际操作人胡某（女，36岁，湖北省武汉市人）。3月8日，在武汉警方的配合下，专案组将胡某成功抓获归案。

据胡某供述，她通过QQ聊天，认识了一名网友，只是网上偶尔闲聊几句。前几天，该网友提供给胡某一个第三方支付平台的账户和密码，由胡某登录该平台接收红包，然后马上提现，现金转入与接收红包账号所绑定的一张银行卡内，银行卡在该网友手中，胡某从中赚取转账总金额的一定比例的好处费。

根据胡某的供述，3月11日专案组火速南下远赴海口，3月15日，在海口警方的配合下，专案组将涉案的“网友”王某某等5人全部抓获归案。

据王某某供述，他以帮人盗刷银行卡提现牟取不法利益，每次获取提现金额的3成回扣。但诈骗短信不是他们发出的，他们只是通过网上与上家联系。

病毒会发给通讯录朋友

根据线索，广西宾阳县人赵某某进入警方视线。专案组转战广西，决定彻底铲除犯罪根源。

4月2日，专案组侦查员查清了赵某某等3人犯罪团伙的基本情况以及藏匿地。4月3日凌晨，专案组兵分两路，实施抓捕。

“不许动，警察！”广西宾阳县一饭店，一路抓捕组将正在吃饭的犯罪嫌疑人赵某某等2人抓获。2人对自己实施诈骗的犯罪事实供认不讳。与此同时，另一路抓捕组也传回捷报，该团伙另一名成员在广西上林县成功落网。

据赵某某交代，他从网上购买用户手机号等个人信息，向事主手机发送带有木马程序的短信，事主一旦点击短信中的网址，木马程序便植入手机，获取事主通讯录信息，同时获取关联的银行卡等信息，通过拦截获取支付验证码，在网上购物消费变现或通过第三方支付平台红包转账提现。

赵某某进一步交代，若事主点击链接，该木马病毒会再次向事主通讯录联系人发送木马程序短信，若再有事主点击，便依次发送下去，从海量人群中碰撞成功几率。

目前，案件仍在进一步审理中。

重点防范170、171号段

侦查员表示，收到网址链接不要轻易点击，这是事主避免被骗的最直接最有效的方式。即使是银行等机构发来的安全链接，也不要轻易点击，要跟银行官方电话核实后，再决定是否操作，从而避免被骗。

当下，因为170、171号段的手机号是虚拟运营商经营，使用成本较低，被不法犯罪分子利用的几率较大。事主在收到这些号段发送的短信链接千万不要点击，否则追悔莫及。

据《法制晚报》

一名寺庙火灾伤者的亲属在哭泣。

印度一寺庙起火 已致110人死亡

4月10日凌晨3时30分左右，印度西南部喀拉拉邦一座印度教寺庙发生火灾，目前已造成110人死亡、390人受伤。

警方已开始对事故原因展开调查，并初步认定有活动组织者把非法爆炸物带入寺庙。目前已有5名嫌疑人被警方控制，其中两人也被严重烧伤，正在医院接受抢救。

据报道，火灾发生时，寺庙内有1万至1.5万人，正在举行一年一度的烟花鞭炮竞赛庆祝活动。

据新华社