一条短信如何骗光网友财产

近日,一名北京网友发布的“为什么一条短信就能骗走我所有的财产?”的文章在网络广为传播。据该网友爆料,他在收到一条“订阅增值业务”的短信,根据提示回复了“取消+验证码”之后,半天之内支付宝、银行卡上的资金被席卷一空。到底是怎样的电信诈骗手段完成了这一卑劣的盗窃行为呢?

“在知道自己损失了几乎所有现金之后,我的内心是无比崩溃的。”日前,一名北京网友贴出一则“为什么一条短信就能骗走我所有的财产?”的文章文中以第一人称描述称,从一条短信开始自己“一夜之间,支付宝、所有的银行卡信息都被攻破、所有银行卡的资金全部被转移。”对此,有关安全专家表示,这是一起典型的综合利用“个人信息+USIM补换卡+改号软件发送诈骗短信”的电信诈骗案件。

事件

回复短信“TD”退订引发“噩梦”

“4月8日,周五,下班回家地铁上。我的手机忽然收到一条短信:显示来源为‘1065800’的号码发来了一条短信杂志,这种垃圾杂志看多了,我第一反应是回复‘TD’。该短信回复我‘发的指令不正确’。”

文中信息显示,随后该用户相继收到显示为“10086”,以及“10658139013816280086”发来的信息,提示已开通“中广财经半年包业务”,“如需退订请编辑短信‘取消+校验码’至本条短信退订”。而在另一条显示来源为“10086”的信息中,该用户收到“尊敬的客户,您的USIM卡6位验证码为*****”。此时,我只想快点退订这个破业务,压根儿不知道USIM卡验证码是什么,于是回复了“取消+*****”。

此后,该网友的支付宝、支付宝所绑定的招商银行账户,以及工商银行账户陆续发生转账。甚至,在该用户紧急将支付宝的银行卡解绑之后,“我马上检查我的网银。然后我悲伤地发现,我的中国银行、招商银行网银根本登不上,密码已经被篡改了。而我能登上的工商银行网银,一查交易明细,网银此时竟也在发生转账。”

“时间太短。”该网友写道,银行要打进客服电话,“所有卡都挂失完成,已耗去大半小时,一切为时晚矣。我知道,此时,我支付宝和银行卡里所有的钱都没了……”

该网友第二天到各个营业厅打印交易流水确认“两张卡都已空空如也。”更确认“对方”“不但攻破了我支付宝的账号,连各个银行的网银也逐个攻破”,包括163邮箱密码也被篡改。其间还包括,“对方”在该用户完全不知情的情况下,将“我的三张银行卡都绑定关联了百度钱包”,用于转账。

该网友文中称,“被问及需要哪些信息才能把我的卡关联百度钱包时,客服说‘银行卡信息、姓名、身份证号、手机号、验证码’。而我如今仍不明白,他是如何搞定我这些信息的。至今仍不明白。”该网友表示,当晚已向警方报案。

进展

移动已确认办理“短信业务”IP在海口

北京移动在核查之后就上述事件给予回复说明,并通过官微进行了公布。北京移动表示,经公司内部查证,获知相关情况如下:2016年4月8日17时54分,手机号码152****1249通过静态密码(客户自设密码)方式,登录北京移动官方网站,经网站弹屏二次确认后,办理“中广财经半年包”业务,IP地址显示登录地点为海南海口;18时13分,手机号码152****1249以同样方式登录网站办理更换4G USIM卡业务。系统向客户本机下发换卡二次确认验证码(6位USIM验证码),该验证码被输入后,换卡成功。前后过程仅用了19分钟。

北京移动指出,以上业务办理流程正常。公司将积极配合有关部门,提供相关证据,进行后续查证。同时提醒客户:为保护您的财产安全,请妥善保管并定期修改网站登录密码和客服密码;请勿将系统下发的业务办理验证码转发和泄露给他人;如收到不知情业务开通短信,请发送短信“0000”到10086查询及退订所订购的业务,有疑问可进一步致电10086咨询。

事件发生后,支付宝的相关人士表示在跟进中。根据事主写到的,支付宝目前已经赔付一笔在支付宝上非用户本人操作的充值行为以及非本人操作转账行为带来的手续费。另外,支付宝已经承诺在事主提交相关材料,并且在保险公司审核后,有可能会全款赔付。此外,百度钱包也表示在跟进中。

破解

机主实际上配合别人完成远程“补卡操作”

专业人士分析认为,上述案例信息中提及的“USIM卡验证码”是整个事件的关键之一。

“为什么犯罪分子要如此大费周章?就是首先要设置圈套,骗取用户的验证码。”分析认为,案例情况很有可能是犯罪分子通过登录机主的网上营业厅,先提交订约申请,之后利用机主着急退订的心理,紧接着发来钓鱼短信,诱使机主回复“取消+验证码”,套取了系统下发给用户的真实的验证码。之后又申请了换卡,进而确认验证码换卡成功,而后再发生更为严重的网银资产的窃取。

猎豹移动安全专家李铁军告诉记者,根据该网友披露的信息,用户的手机卡被别人补办,机主遭遇了电信诈骗中的“补卡攻击”。李铁军指出,尽管这一案例仍存在一些疑问,在目前披露的信息中还没有了解很清楚。但初步来看,银行账户被盗根本原因,在于机主不恰当地处理了一些短信信息。从客观效果来看,相当于机主配合“别人”完成了手机的补卡操作。机主的手机卡实际已经在别人的手上,在这样的情况下,就很有可能引发一系列的网银被盗问题。

李铁军介绍说,案例中涉及的远程补办业务来源于国内运营商的一项4G服务。2G或者3G、4G用户升级、换发4G卡,可以不必到营业厅办理,通过网上营业厅提交申请,运营商收到申请后,寄发空白USIM卡给用户,用户拿到后,通过换卡操作步骤说明,可以远程激活新卡生效。在这一案例来看,李铁军表示,不法分子很有可能利用非正规途径获得的空白USIM,在案件中通过改号软件,伪造了一条短信发到受害人手机上,进而骗取获得了用户的真实验证码,之后换卡“成功”。“当然案例中还有一些情况目前交代不是很清楚,需要公安机关的进一步调查。”李铁军表示。

疑点

诈骗实施前网友个人信息可能已泄露

此外,攻击者为什么能在很短的时间内完成盗窃,用户对于互联网的各种服务有足够了解和经验的前提下,他的防护速度仍然跟不上攻击者的进程,李铁军认为这说明攻击者提前已经有足够的准备,提前掌握了一定的用户信息。

“小偷要重置号码,一般需要身份证号、邮箱信息、银行账号等等。这些信息是之前已被攻击者掌握还是在事件中陆续破解,仍需公安机关的调查,但从网友描述攻击者很快完成了密码的重置以及登录等信息来看,李铁军分析,很有可能之前已有信息泄露的发生。”

据360安全专家分析,按照受害人目前的描述,判断这是一起典型的综合利用“个人信息+USIM补换卡+改号软件发送诈骗短信”的电信诈骗案件。根据百度钱包的关联来看,很有可能在诈骗实施之前,骗子已经获取了受害人的银行卡号、身份证号、姓名、手机号等个人信息。在这种情况下,骗子只需要得到受害人的短信验证码,即可进行包括网银、支付宝、百度钱包的所有转账操作。于是,骗子选择利用移动的USIM补换卡业务,直接窃取用户的手机卡,并由此可以掌握该网友的全部手机短信,包括转账必需的“验证码短信”内容。由于该案例不同于一般的网络诈骗犯罪分子的行动动机,并且根据事主现在的描述,该事件仍有一些疑点。因此,其他用户也无需过度恐慌,可以说,该案可能是一个“极端案例”。

提示

任何时候都不要把验证码给别人

李铁军指出,伴随不良分子诈骗方式与技术手段的花样翻新,电信诈骗有可能威胁到每一个人。“经常在网上海的人,其实都存在个人信息的不同程度泄露。”李铁军认为。信息泄露已经防不胜防,对于普通人,需要注意的包括,任何时候不要把自己的验证码给其他人,其中尤其是收到与银行、支付系统以及个人账户有关的短信,一定要确认自己把全部短信内容完整看完,切忌匆忙处理,更要避免贸然把验证码误发给别人。

此外李铁军建议,作为防范,每个人都应提前做好一些应急预案。比如一旦发生手机突然失效,没有信号是被攻击的典型现象,必要时第一要冻结银行卡,冻结第三方支付账号,这些只要借一部手机就可以完成。一旦发生诸如此类的意外情况,要有足够的风险意识,不能放任自己成

声音

谁该为电信诈骗事件负责?

为信息孤岛,也不能等待或者犹豫,要立即采取措施防范。

在上述案例中,网友在文中最后也发出质疑,运营商与银行等各种环节,究竟谁愿意为这一事件负责?对此,中国互联网协会信用评价中心法律顾问赵占领律师表示,类似电信诈骗由于具体方式非常多,所以需要结合具体案例的过程来看。其中厘清诈骗犯如何获得信息是关键步骤之一。进而要结合具体案例分析,界定其中是否涉及有过错责任方。

“追究责任的前提是,对方有过错。”就网友文中透露的案例,赵占领认为,如果是用户手机卡被复制后,网银密码是通过验证码重置被攻破窃取,则支付环节的责任初步看较为难以界定。而涉及运营商的环节,赵占领认为,关键要看SIM卡的补办环节是否有问题。如果犯罪分子去营业厅补办,需要用身份证,运营商在办理SIM卡中有审核身份的责任。而如果确认补卡申请与用户网上营业厅密码泄露有关,则目前也很难界定运营商的责任。

“最终需要公安机关通过刑事立案,抓获嫌疑人,才能具体厘清犯罪的过程和手段,目前来看,受害人还很难判断和证明包括运营商和银行等支付方该负什么样责任。”赵占领指出。

焦点

安卓系统比苹果系统容易受侵害?

由于电信诈骗案的频发,让用户对智能手机的安全性更加关注。虽然不能绝对地说苹果系统比安卓系统更加安全,但是从目前发生的许多案例来看,安卓系统用户受到侵害的频率相较于苹果系统用户更多。

据360安全专家介绍,这首先是基于安卓用户数量远超过苹果用户数量。因此如果开发一款木马或其他病毒程序,犯罪分子也会选择针对安卓系统来开发相应软件。

其次,安卓系统是开源系统,也就是说,任何人都可以得到软件的源代码,加以修改,进行二次开发利用。相反地,苹果是一个封闭的系统,只有开发者才可以修改系统代码。因此,从黑客入侵的难易程度来看,苹果更加安全。

另外,一些利用伪基站实施诈骗的案例,由于苹果手机用户下载程序必须去苹果商店,在互联网网站无法下载,因此骗子的木马程序仅对安卓系统用户有效,所以安卓系统受到侵害的几率更大一些。

体验

支付宝、微信、百度钱包哪个更安全?

由于该事件中出现了“一个手机验证码”便可盗取账户及进行转账操作,北青报记者昨日进行验证,发现各个支付App的验证方式和要求各不相同。

首先,记者尝试在另外一台非常用设备上登录支付宝。先利用“账号+密码”的方式登录支付宝,在输入账号密码后,常用手机会收到提示“你的账户某某于几点登录,如非本人操作,请修改密码,建议密码与你的其他网站密码不同。”随后,会用一些既往信息验证是否本人操作,比如选择“哪一个wifi是你用过的”或“哪一个商品是你购买过的”,点击正确后,才可以进入支付宝。但是如果选择用“手机号+验证码”的方式登录,则仅需输入短信验证码即可立刻成功登录。

与支付宝刚好相反,微信对于“手机号+验证码”的登录方式要求较严格,而对于“账号+密码”的方式则较信任。北青报记者同样在另一台非常用设备上登录微信,被要求进行好友验证。好友验证是给出15位微信用户头像,需要用户从中选出自己的微信好友,至少2位。但如果利用“账号+密码”的方式,则可以立刻登录成功。不论使用哪种登录方式,在常用设备上都会收到一条提示“你的微信账号于几点在什么设备上通过微信密码登录,如果不是你的操作,你的微信密码已经泄露,请尽快登录微信修改微信密码。或访问weixin110.qq.com冻结微信。”相比支付宝,微信增加了冻结微信的选项,比密码泄露后还需要通过修改密码的保护账户的选项更加实用。

最后,记者用百度钱包在非常用设备登录时,也可以利用“手机号+验证码”的方式登录,且无需其他验证。此外,用户还可以选择用绑定的手机号编辑新密码直接向一个固定号码发送短信,便可以更改账户密码。

据新华网