“伪基站2.0”犯罪不可怕 网上支付过于依赖“短信验证”存隐患

近年来，使用手机短信验证码验证用户身份的技术，被广泛应用于银行金融、社交媒体、电子商务等各类移动APP服务。然而短信作为一种2G网络的通信方式，其本身安全防护等级并不高。

就在近期，多地警方陆续破获一种“伪基站2.0”犯罪案件。有犯罪分子利用GSM 2G网络的设计缺陷，实现不接触目标手机就能获得手机所接收到的验证短信，进而利用各大银行、网站、移动支付APP存在的技术漏洞和缺陷，实现信息窃取、资金盗刷和网络诈骗等犯罪。

工业和信息化部日前下发通知，部署开展2018年电信和互联网行业网络安全检查工作，要求基础电信企业、互联网企业、域名注册管理和服务机构重点检查安全防护体系系列标准符合情况，可能存在的弱口令、中高危漏洞和其他网络安全风险隐患等。

相关业内专家在接受记者采访时表示，“伪基站2.0”是极小概率的犯罪方式，手机用户不需要恐慌，但这一事件也暴露了目前网上APP、支付等环节过于依赖“短信验证”这一安全短板。基于2G网络的短信安全验证犹如“沙滩上的堡垒”，便捷之外存有安全隐患，网上支付平台、APP服务提供商应尽快堵住这一安全短板，完善用户身份验证措施，以确保用户个人信息和财产的安全。

新型盗刷方式引发舆论关注

根据媒体报道，广州、南京、江宁等多地警方近期相继破获一种名为“GSM劫持+短信嗅探技术”的犯罪案件。犯罪分子通过特种设备，自动搜索附近的手机号码，然后可以拦截短信。

据广州日报报道，8月1日，网友“独钓寒江雪”的手机在半夜连续接到100条短信验证码，她醒来发现不仅自己的支付宝、银行账户被盗，还被贷了款。有人使用她的京东账户、支付宝等等，预定房间、给加油卡充值，总计盗刷了1万多元。

这一案件经媒体报道后马上引发了舆论关注，甚至有报道建议手机用户“晚上睡觉关手机”以防范。那这种“伪基站2.0”方式会否蔓延？用户的网上资金安全如何来保障，对此，记者做了深入采访和调查。

据360无线电安全研究院高级研究员黄琳介绍，基于“伪基站”的GSM短信嗅探是被动的，就是只“听”，不发射任何非法的无线信号。攻击者在利用手机信号劫持设备等工具非法截获短信验证码、手机号码的基础上，并通过社工或黑产交易等方式获取身份证号码、银行账号、支付平台账号等敏感信息，侵入各类应用实施犯罪行为。网友“独钓寒江雪”的情况很可能就属于这种。

据了解，这种被称为“伪基站2.0”的攻击手段早在2010年已出现，由于攻击技术实施难度大，当时仅掌握在少数高级攻击者手中，不法分子难以大规模利用。而且随着这几年国家对于伪基站的大力打击，不法分子要用“伪基站”劫持用户短信和手机信号，就会有很大几率暴露自身位置，因此目前此类案例非常罕见。

同时，有通信行业资深安全人士表示，要实施“伪基站2.0”犯罪需要满足四大条件：不法人员从黑产获取了用户个人身份信息“四大件”（账户名、密码、身份证、银行卡号）；不法人员在物理位置上和受害用户相近；用户手机当时驻留在2G网络上；获取用户手机号码并嗅探到用户验证码短信；实施网络转账或信用卡盗刷等行为。

上述四个环节为链条式操作，缺一不可，要满足以上所有条件，攻击者需要冒极高的风险，因此在日常操作中，短信被嗅探并导致手机银行被盗发生场景的概率是极低的，普通用户无需过于担心，更不需要在晚上睡觉时“主动关机”。

网上支付依赖“短信验证”存隐患

虽然实施“伪基站2.0”犯罪目前只是极小概率的事件，但是也给网上支付安全敲响了警钟。

随着移动支付的普及，“短信验证”是目前最便捷的验证方式，人们只需要在手机上操作，就可以便捷快速地完成开通业务、支付款项等活动。然而，科技的进步带来的不仅是便捷，还有安全隐患。因此手机短信验证码已被广泛应用于各类移动应用、网站服务。短信验证码可以帮助用户进行修改密码、修改绑定邮箱等敏感操作。

同时，短信验证码也能让用户不输账号密码直接登陆。以用户使用广泛的微博手机APP来说，在掌握手机号码的前提下，可以无密码登陆，手机只要收到系统发送的验证码，就可以快速登陆。

对手机用户来说，一旦遭遇GSM短信嗅探攻击，或者因为其他原因短信验证码内容被外泄，不法分子就可以利用获取的用户手机号码和验证码登录个人账户，用户会面临个人信息泄露甚至财产损失的风险。

记者在采访过程中，多位来自通信、安全领域的业内人士均表示，目前涉及到支付确认、修改支付密码等高度涉及用户资金安全的验证时，如果仅仅是依靠短信验证码来确认用户身份，具有一定的安全隐患，希望有关部门及网上支付平台重视这个问题，尤其是网上支付平台不能为了便捷而牺牲用户的资金安全。

从技术上来说，2G的GSM网络使用单向鉴权技术，且短信内容以明文形式传输，该缺陷由GSM设计造成，且GSM网络覆盖范围广，因此修复难度大、成本高。

更重要的是，对于网上支付平台来说，除了“短信验证”之外，在涉及大额支付及修改用户交易密码等关键环节，增加新的验证手段，比如引入人脸识别等方式，也刻不容缓。

互联网厂商应承担更大安全责任

针对“短信验证”带来的安全隐患，全国信息安全标准化技术委员会在今年2月份联合多家单位发布了《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》，明确指出了基于短信验证码实现身份验证的安全风险现状、困难点，并给出了目前专家们认为可行的方案。

《安全指南》建议，各移动应用、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。建议采用多种方式组合，加强安全性。

这份指南同时强调，个人用户应做好手机号、身份证号、银行卡号、支付平台账号等敏感信息的保护。在收到来历不明的短信验证码等异常情况时，提高警惕，及时联系相关移动应用、网站服务提供商。

对此，黄琳认为，面对层出不穷的网络攻击技术，互联网企业更应该有所行动，加强风险防范，承担最大的责任。

对于普通消费者而言，除了不泄露自己的短信验证码之外，GSM劫持+短信嗅探主要针对GSM 2G网络用户，建议此类用户尽快升级到4G网络，并开通VoLTE，或者使用支持防伪基站功能的手机，提高安全防御等级。

中国科学院院士梅宏在接受记者采访时也表示，从技术上，绝对避免这种事情的发生是有困难的。当新技术进入应用以后，确实会有一些人利用当初设计上的缺陷或者是当初未考虑到的因素来非法获利。“人类历史几千年所有的技术进步都是两面性的，没有哪项技术的发展在给人们带来便利的同时，没有带来别的负面因素的。”

梅宏认为，我们要看在发展过程中，怎么减少这种发展给我们带来的损失。在立法上，法律要有明确的界定，碰到这种问题一定要严厉打击。要靠法律的威慑力加上技术的辅助，两方面的协作。最重要的一点，是每一个用户都要有安全防范意识。在信息化社会对于消息一定要有一个自我、独立的判断，没有这些考量就很容易上当受骗。梅宏说，“要保证绝对的、全面的没有人上当受骗，这很难通过技术实现，需要多方努力。”

（据人民网）