个人信息安全日常防护常识

【摘 要】在当下的网络化生活中，个人信息几乎遍布交易支付、娱乐、社交等生活的每一个场景，其背后的经济价值日益显著，也成为网络攻击、电信网络诈骗、敲诈勒索等网络违法犯罪的目标之一。本文主要介绍了移动互联网使用个人信息存在的安全隐患，分析了黑灰产业常见个人信息窃取手段，并据此提出了个人信息安全防范建议。

【关键词】个人信息　信息泄露

1 引言

经济的快速发展和信息网络的广泛普及，使大众对互联网的依赖性越来越强，个人信息在互联网上的留存量越来越多。与此同时，个人信息经济价值日益显著，导致侵犯公民个人信息的犯罪屡禁不绝，且成为滋生网络攻击、电信网络诈骗、敲诈勒索等下游违法犯罪的源头，社会危害日益突出。

2018 年，欧盟《通用数据保护条例》（GDPR）发布，引领全球个人信息保护监管趋势。近年来，我国也高度重视个人信息保护工作，从法规、治理、企业自律等方面多管齐下，捍卫网络安全、个人信息安全等，相继颁布了数据安全法、个人信息保护法，标志着我国在数据安全、个人信息保护等领域迎来了有法可依、有章可循的新时代。

2 移动互联网使用的各类信息存在安全隐患

2.1 手机验证码信息安全需注意

为保障用户信息安全，目前市面上的 App 在开发初期已设定好相关验证机制，涉及用户使用安全的场景均需向用户发送短信验证码进行操作验证，小到账号登录，大到账户消费。日常中的网站注册、网络购物、金额消费、转账汇款等场景，都需要利用到手机短信验证码。一旦手机遗失、号码易主或遭遇不法分子欺诈，验证码信息被窃取，个人信息、账户信息的安全将直接面临威胁。

2.2 在第三方平台的账号安全难保障

用户在第三方平台浏览资讯、购物或发表观点时，一般会被要求进行账号注册并登录，部分平台还会要求填写个人信息。虽然在平台注册页面都附有隐私保护协议，但部分平台未向用户详细说明信息收集的范围、用途、使用权限等。与此同时，大部分用户在注册及后续登录时，对于隐私保护协议内容未能做到逐条确认。基于此现状，平台服务商在对用户的信息收集、存储和利用等方面都处于有利地位。在平台服务商数据安全防护能力薄弱并成为不法分子攻击目标时，大量平台用户账号数据安全无法得到保障。

2.3 应用程序过度索取用户隐私信息

移动终端操作系统权限是系统中建立的访问与控制的机制。用户作为移动终端的所有者，根据系统设置的安全规则或安全策略，对安装应用进行授权资源的限制，包括功能级与数据级，通过权限管理，达到日常使用移动设备的最佳体验。

但随着移动互联网的普及，移动终端的激增，满足大众日常使用所需的应用类别不断扩增，一些 App 会通过借助操作系统向用户申请开启权限来收集相应的个人信息。App 在挖掘用户需求的同时，可利用大数据的独特优势，对用户提供更加精准的服务，获取更多的商业利益，也使过度索取权限成为行业的“潜规则”。反观用户角度，大多数人在面对 App 的权限授权提示时，并未深究其授权目的，也较难判断必要权限与过度索取权限，导致个人信息被过度收集，对个人信息安全与数据安全造成潜在威胁。

2020 年，央视 3·15 晚会曝光了一批向用户手机内植入软件开发工具包（SDK）插件并实施窃取信息的违规应用。具体行为是在用户不知情状态下，涉嫌窃取用户隐私，涉及的 App 达 50 多款。

3 黑灰产业窃取个人信息技术手段多样

当前处于大数据红利期，用户信息在某种意义上等于金钱，身处移动互联网时代，个人隐私似乎不再是“隐私”。在“无感知”状态下，用户的敏感信息有可能就已经遭到泄露，当各类骚扰、诈骗接踵而至时，用户才有可能意识到，自己的敏感信息已然遭到泄露，但对于何时、何地、何种情景下事件发生，用户却不得而知。随着社会各界对个人隐私保护关注度的提高，信息泄露背后的黑灰产业链条慢慢浮出水面，人们发现其背后的运作模式与技术手段已经十分成熟。以下针对黑灰产业中典型隐私窃取手段进行解析。

3.1 GSM 劫持+短信嗅探技术，无声无息中实现账户盗刷

短信验证码的广泛应用使其安全性已经直接影响用户个人信息安全及账户财产安全，“GSM 劫持+短信嗅探技术”正是通过盗取验证码短信以实现账户盗刷。

这项技术的实现原理实际与伪基站极为相似。“GSM 劫持”可以理解为“伪基站 2.0 版本”，属于伪基站的技术再升级，不法分子通过伪基站劫持的方式将用户的手机信号降为 2G，然后利用技术手段获取到一定范围内的手机号码后，再利用“GSM 嗅探”技术窥探用户短信中的验证码信息，以便完成密码重置、身份验证等步骤。借此可以实现实时获取用户手机短信内容，从而利用银行、网站、移动支付 App 的技术漏洞和缺陷，最终实现信息盗取、钱财盗刷、私自借贷等诈骗犯罪目的。整个过程中，不法分子无需直接与用户接触，只需利用“GSM 劫持+短信嗅探技术”就可以完成窃取信息与钱财，而用户毫无察觉。它就像一条经过专业训练的猎犬，无声无息地辨别事物，所以被专业人士叫做“短信嗅探”技术。

3.2 高仿 App 传播量广，恶意获取权限，非法窃取大量个人信息

使用手机 App 处理各项生活事务已渐渐成为现代人的日常所需，各企业顺势推出官方业务 App，将更多需要线下处理的业务搬至移动互联网，向用户提供更加便利的服务。但在各大应用市场中，出现不少“高仿”App，图标及页面与官方 App 极为相

似，下载量甚至高达几十万次。这些高仿 App 多为生活类应用，具备收录用户各项个人信息的功能。在用户安装后，App 会获取用户各项敏感信息权限，但并不具备实际业务功能，甚至还包含不少广告。当用户无法在 App 正常办理生活业务时，才发觉下载的不是官方 App，但个人信息已遭到泄露。

3.3 通过移动端漏洞攻击窃取用户个人信息并贩卖获利

漏洞的存在，很容易吸引不法分子的侵入及病毒的驻留，导致数据丢失、被篡改，隐私泄露，乃至金钱上的损失。移动智能设备的爆发式增长使漏洞从过去以电脑为载体延伸至移动端，而安卓系统由于具备开放性特点，其信息安全问题尤为突出。一些不法分子受利益驱使，利用系统或应用程序漏洞，使恶意软件可以伪装成任何安卓应用程序，从而使攻击者在用户不知情的情况下运行恶意进程，获得相机、短信等权限，窃取用户的相册、位置等隐私信息，甚至是劫持手机中其他应用，向用户显示一个虚假应用界面，盗取用户输入的账号、密码等敏感信息。

4 个人信息安全防范建议

近年来我国从立法、执法、普法等多个方面加强对个人信息的保护力度，但部分黑灰产业人员仍顶风作案，违法获取、非法买卖个人信息，给人们正常工作生活造成恶劣影响。个人信息的黑灰产业链路主要经历非法获取、加工处理贩卖、变现 3 个阶段，本文针对上述 3 个阶段提出个人信息保护建议。

4.1 防止个人终端设备隐私被窃取

黑灰产窃取个人信息的手段多种多样，主要是利用病毒、漏洞攻击个人终端设备，或是通过钓鱼网址、恶意 App 窃取私密信息。针对这一问题，用户需及时更新升级终端操作系统，安装完善系统补丁，防止因系统漏洞问题，产生信息泄露、终端入侵风险。

对于 Windows 系统，可在“更新和安全”功能处进行系统、补丁升级，也可使用相关杀毒软件进行系统补丁升级。

对于安卓系统，由于其开源特征，存在各种发行版本，早期旧版本的安卓系统应用管理权限机制不完善，加上部分手机系统更新生命周期较短，安卓系统的补丁安装不及时，在日常使用手机时需特别注意要安装杀毒软件，及时通过“关于手机”板块或“安全中心”功能更新系统和病毒库，保障终端的安全。

4.2 警惕应用程序的过度索权

（1）加强对正规应用的权限和隐私管理

应用程序 App 为保障功能的正常运行需收集个人信息，部分程序在运行时会调用大量系统的权限维持运行，调用的部分权限比较敏感，会涉及用户的个人信息数据，如通讯录权限、短信权限、定位权限。因此，用户在注册、使用 App 时，必须仔细查看相关用户协议、隐私声明，也可结合 App 中的个人信息收集清单、第三方信息共享清单功能，了解该 App 收集的信息内容、对应的业务场景，防止超权收集行为。定期对这些应用权限的调用情况做好管理，一定程度上可以避免个人信息被滥用。

（2）规范个人网络行为，避免被恶意应用“感染”

在一些诈骗场景中，不法人员会使用话术诱导受害人，通过非应用商店的方式安装应用，如访问指定二维码（下载链接）安装应用，此类非正规渠道的应用多存在隐私窃取功能，非法窃取个人信息。如，敲诈类应用会窃取通讯录、短信，并上传至诈骗人员服务器进行后续敲诈勒索。除此之外，在日常生活中，一些盗版电影类应用也可能含有隐私窃取行为。对此，用户必须切实提升个人网络行为的安全意识，对于来源渠道不明的应用安装包、网站、二维码等，要谨慎点击或扫描，建议通过正规渠道下载安装应用。

4.3 不要轻易泄露支付验证信息

早期黑灰产业冒充电子停车收费系统（ETC）、银行机构向受害人发送含钓鱼网址的短信，通过高仿的页面，诱导受害人填写银行账号信息、支付短信验证码等，进而盗刷受害人的资金。随着攻防对抗的升级，黑灰产业现在使用电话联系上受害人后，以话术诱导受害人安装含屏幕共享功能的会议 App，再通过屏幕共享功能远程查看受害人收到的支付短信验证码完成资金盗刷操作。

面对此类针对短信验证码的“精准诈骗”和“组合攻击”，首先要对“运营商”“银行”等与资金往来相关的短信和来电进行认真甄别，及时与官方人员取得联系进行二次确认，不轻易向对方提供验证码。其次，由于短信验证码与手机卡直接关联，当

手机丢失或手机卡丢失时，极易被不法分子利用，因此建议用户给手机SIM卡设置密码，防止手机丢失后被盗用。最后，要给手机设置复杂的解锁密码（超过6位的数字+字母），防止手机锁屏密码短期内被破解，同时给手机应用设置安全锁，防止他人获得手机应用内的信息。

5 结语

在万物互联的大数据时代，碎片化的个人信息不断涌入互联网浪潮中，面对错综复杂的网络环境，如何保障个人信息安全，是政府、企业、个人都要面临及解决的问题。一方面执法机关要从互联网信息传播源头，加大对违法违规获取个人信息行为的打击治理；另一个方面，企业需提高社会责任感，提高对个人信息保护的重视程度，建立必要的个人信息存储、使用以及发生信息泄露事件后的个人信息安全保护机制。同时，个人也需提升自身的信息防护意识，增强警惕心，积极学习并实践各类信息保护手段。

（原载于《保密科学技术》杂志2023年4月刊）

（来源：国家保密局 http://www.gjbmj.gov.cn/n1/2024/0919/c411145-40323491.html）