移动场景下通讯信息诈骗的特点分析及应对策略

● 于成丽 / 中国信息通信研究院

近年来，通讯信息诈骗日益猖獗，严重威胁人民群众的财产安全，影响社会和谐稳定。根据相关数据显示，2016年全国公安机关破获电信网络诈骗案件8.3万起；2017年第一季度全国专线诈骗报案总案件数为25.3万件，涉案金额33.4亿。可见，通讯信息诈骗高发、频发的态势依然严峻。随着现代通信技术和银行支付行业的快速发展，诈骗手法日趋多样化、复杂化。特别是在移动智能终端设备的泛在普及潮流中，出现了利用移动终端恶意代码结合网络钓鱼的手段来实施电信诈骗这一新技术手段。

在2016年，首款专用于通讯信息诈骗的Android木马被监测发现，该木马伪装成“相关案件查询系统”，集隐私窃取、网络钓鱼、短信拦截、远程控制等多种恶意行为属性于一体，可在受害人不知情或未授权的情况下转走银行账户资金。此类木马的涌现，进一步凸显出通讯信息诈骗技术、手段不断升级演化，专用的诈骗木马已向移动端渗透扩散，诈骗平台从PC端向移动端过渡转移。而移动终端承载了支付宝、微信等生活所必需的各类应用软件及海量用户个人数据，诈骗者通过非法窃取或购买用户信息，利用大数据分析实施精准诈骗，并借力于在移动端植入的木马病毒完成转账等非法操作，使得通讯信息诈骗的范围不断拓宽、危害不断增大。

本文通过梳理通讯信息诈骗的演化发展过程，详细分析了移动场景下通讯信息诈骗的特点并提出了防范打击通讯信息诈骗的相关应对策略。

通讯信息诈骗的演化发展过程

通讯信息诈骗是犯罪分子以非法占有为目的，借助移动手机、固定电话、互联网等现代通信技术，采取远程、非接触等方式，通过虚构事实等手段诱使受害人往指定金融账号打款转账，骗取财物的一种犯罪行为。

从诈骗类型上来看，相关组织机构筛选出了通讯信息诈骗的十大典型案例，即冒充公检法诈骗案、代考改分诈骗案、网络购退款诈骗案、娱乐节目中奖诈骗案、救助助学诈骗案、冒充QQ与微信好友诈骗案、医保社保诈骗案、钓鱼网站诈骗案、订票诈骗案、贷款诈骗案。

从通讯信息诈骗发展过程进行总结分析，其主要历经了3个阶段的演变进化。第一阶段为固

定电话与普通功能电话时代，诈骗者主要依靠给受害人打电话实施电信诈骗，以办案需要、电话欠费、朋友借钱、索要赎金等借口进行诈骗，成功概率较低；第二阶段是随着互联网的发展普及，诈骗者综合利用拨打电话、网络钓鱼和远控木马等方式实施网络诈骗，成功概率相对提高；第三阶段是移动互联网的全面发展及“互联网+”与各行业的融合应用，移动智能终端设备呈现泛在普及之势，个人信息资源和个人财富资产亦不断向移动端聚合，牵引诈骗分子盯准“新兴市场”，诈骗平台快速由PC端向移动端过渡转移，移动场景下诈骗的智能化、科技化、专业化水平不断提升，危害迅速升级。

移动场景下通讯信息诈骗特点分析

相较于传统电信诈骗，移动场景下通讯信息诈骗手法变得更加灵活和强大，本文主要梳理移动场景下通讯信息诈骗的一般流程并分析其主要特点。

1.一般诈骗流程

移动场景下通讯信息诈骗的主要诈骗手法和流程大体包含6个步骤。第一步，对已获取的用户数据进行分析以瞄准诈骗目标，通过冒充公检法等方式拨打诈骗电话给受害者，如通报其涉嫌“某某案件”需冻结资金；第二步，诈骗者再次给受害者打电话，并发送包含Android木马下载链接的钓鱼网站给受害者，诱导其打开链接下载木马；第三步，进一步诱导受害者输入银行账户信息，如伪造“最高检刑事逮捕令”恐吓受害人，诱导其进行银行帐户，继而获取用户帐户信息；第四步，依据所获取账户信息，利用网银远程发起转账汇款；第五步，利用Android木马拦截回传银行发送给用户的短信验证码；第六步，使用验证码完成转账。

2.主要诈骗特点

移动场景下通讯信息诈骗的威胁性日益凸显，不法分子以移动终端为载体，其隐私窃取和远程控制能力显著增强，逐步形成了一套成熟的诈骗体系，总体来看主要具有2个特点。

一是移动场景下用户隐私信息泄露诱发“精准诈骗”。电信诈骗以非法获取公民用户数据信息为前提，低成本、高收益是其高发频发的重要驱动力。随着用户个人信息资源不断向移动端聚合，以移动应用为入口的隐私信息泄露途径拓宽。其一，钓鱼应用软件登堂入室肆意窃取用户信息，此类仿冒应用软件在用户安装后，恶意诱导用户输入全面精准的个人信息；其二，移动应用权限申请过度索取用户隐私，大量应用软件在安装时，均要求用户开放各式权限，涉及通讯录、短信、相册、地理位置等用户隐私信息，加大个人信息泄露安全风险；其三，移动恶意应用软件泛滥成灾，在后台盗取用户个人信息，隐私窃取类恶意程序在用户毫不知情的情况下，可后台监控用户行为、盗取用户信息。此外，诈骗组织通过将互联网数据与移动平台隐私信息进行大数据关联分析，更深入地建立受害者档案画像，对目标

进行“瞄准攻击”，诱发“精准诈骗”。

二是移动端木马病毒升级演变助推“自助诈骗”。在用户个人信息资源不断向移动端汇聚的同时，用户个人财富资产亦存相同趋势，移动终端对用户资产逐步拥有一定“控制权”。其一，隐私窃取类、远程控制类木马可获取与用户资金、生活密切相关的短信等数据信息，甚至控制受害人手机的短信收发动作以及通话行为；其二，移动场景下的支付类木马，可协助诈骗者在受害人不知情的情况下完成远程转账。上述两大类木马病毒的升级演变和融合应用极大促使了“自助诈骗”模式的产生和发展。

应对策略

防范打击通讯信息诈骗是切实维护人民群众合法权益和服务社会民生的重要举措，相关公安、电信、金融等主管部门高度重视，大力遏制通讯信息诈骗犯罪蔓延趋势。但当前通讯信息诈骗高发、频发的态势依然严峻，且其涉及面广、链条长、手段多、花样新，因此防范打击通讯信息诈骗是一项系统工程，亟需在总结分析移动场景下的通讯信息诈骗特点基础上，以预防为主，多措并举，不断强化防范打击力度。

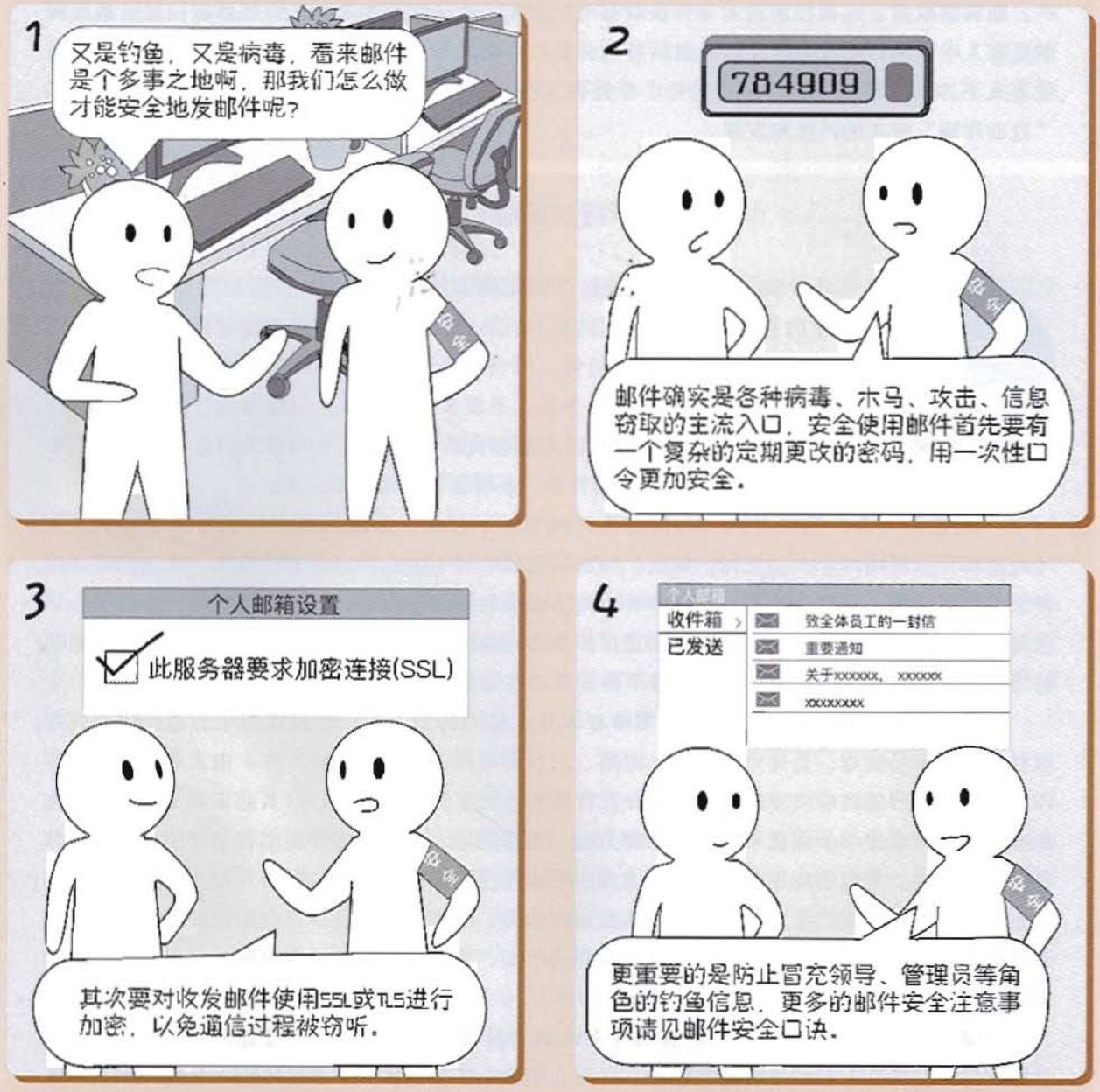
一是追本溯源，强化用户个人信息保护机制。一方面，应深入贯彻落实《网络安全法》《电信和互联网用户个人信息保护规定》等法律法规中对于个人信息保护的要求，并积极推动用户个人信息收集、存储、处理、删除等环节具体标准的细化与制定；另一方面，加快推进个人信息保护法的立法进程，强化公民个人信息保护立法与执法保护，减少侵害公民个人信息违法犯罪行为的生存空间，从而切断电信诈骗等下游犯罪的实施条件。

二是狠抓落实，持续推动恶意应用治理工作。移动场景下通讯信息诈骗中的恶意仿冒应用软件及支付木马病毒，是导致用户隐私泄露、后台转账行为成功的关键所在。由工业和信息化部印发的《移动智能终端应用软件预置和分发管理暂行规定》于2017年7月1日起正式生效，应以此为契机，一方面进一步强化平台监测治理力度，要求网站、应用商店等提供移动智能终端应用软件下载、安装、升级的应用软件平台加大对应用软件进行审核及安全、服务等相关检测的力度，在审核和检测中发现的恶意应用软件等违法违规软件，应严肃处理且不得向用户提供下载违法违规软件渠道；另一方面大力督促企业相关责任的落实，强化责任倒查追究机制，确保恶意程序治理成效。

三是加强防范，不断引导用户提高安全意识。通讯信息诈骗频发，与受害者个人信息保护意识和对诈骗的防范意识薄弱息息相关。一是在用户个人信息保护方面，电信、金融等相关行业主管部门和组织机构应定期发布个人信息泄露风险提示、组织宣传典型案例等活动，提升全社会个人信息保护意识；二是随着不法份子诈骗手法不断翻新，诈骗技术不断升级，导致用户防不胜防，公安、电信、金融等机构在发现新型电信诈骗作案方法手段后，应及时利用纸媒、电视媒体、互联网平台等更新防诈骗提示，在全社会范围内进行“地毯式”宣传，全面提高民众的防范意识。END

信息安全意识漫谈——邮件安全篇

◆ 总结篇



◆ 邮件安全口诀

- 邮件传输要加密，黑客截获难破译
- 各种附件谨慎点，可执行文件风险高
- 默认浏览器非IE，陌生链接勿点击
- 遇事冷静莫慌张，电话确认是法宝

下期将为您继续介绍信息安全常识，希望您继续关注！END（绿盟科技供稿）

信息安全小百科

《碟中谍》背后暗藏的身份识别技术

在汤姆·克鲁斯主演的系列片《碟中谍》中有一个不可或缺的元素，就是炫酷的暗黑科技产品。这些高科技产品总会瞬间逆转，成功拯救人类。随着互联网以及智能城市、智慧家居的发展，曾经在科幻电影里看到的画面已不只处于想象之中了。影片中暗黑高科技里暗藏哪些玄机？本文要给大家揭秘其中的身份识别技术。

身份识别技术

身份识别（Identification，ID）是指能够识别本人身份的凭证，如我们每天使用邮箱的密码口令、安检出示的身份证、出入境的护照及指纹锁等。这些ID形式主要有以下特征：根据你所知道的信息来识别你的身份（What You Know，你知道什么），比如邮箱私有秘密口令；根据你所拥有的东西来识别你的身份（What You Have，你有什么），比如身份证、护照；直接根据独一无二的身体特征来识别你的身份（Who You Are，你是谁），比如指纹、面貌、DNA等。

ID除了上面所列举的技术外，还利用静态密码、短信密码、动态口令、生物识别等技术。生物识别技术是指通过可测量的身体或行为等生物特征进行身份识别。生物特征是指唯一的可以测量或可自动识别和验证的生理特征或行为方式。

身份识别与信息安全

随着信息技术的不断发展，一些传统的ID技术已不能满足人们对个人身份识别在安全性、灵活性和准确性方面的更高要求。在生物识别技术日趋成熟的时代，ID技术呈现出了多样性发展趋势。

尽管生物特征很难伪造，仍有黑客通过信息技术手段破解部分ID技术。例如，黑客恶意收录用户声音样本，通过合成后的声音重复使用可达到破解声纹识别的效果；指纹识别技术早已被破解，黑客通过用户接触过的物体，甚至根据照片，都可提取出可用于ID的指纹，然后通过3D打印技术打印出手套或指纹用于伪造用户信息。此外，目前流行的虹膜识别也存在风险。

为进一步加强ID的安全性，单一依靠某一种ID技术已难以胜任“不可能完成的任务”了。在未来，两种及以上的ID技术相结合使用将成为趋势，也就是《碟中谍》中所展现的多模态生物识别技术，即根据应用场景、用户条件、安全等级等选择两种以上的识别技术进行匹配。将不同识别精度、采集距离、设备成本、防盗防伪、简单易用等特征融为一体，这比任何单一ID技术更安全可靠，可全面提升应用系统的安全性，确保用户信息的安全。END

（康双勇/国家保密科技测评中心）

（栏目编辑：郝君妤）

要 闻

工信部关于印发《公共互联网网络安全威胁监测与处置办法》

为加强和规范公共互联网网络安全威胁监测与处置工作，消除安全隐患，制止攻击行为，避免危害发生，降低安全风险，维护网络秩序和公共利益，保护公民、法人和其他组织的合法权益，9月13日，工信部发布了《公共互联网网络安全威胁监测与处置办法》，界定了公共互联网网络安全威胁及其监测与处置机制，提出工信部将建立网络安全威胁信息共享平台，委托国家计算机网络应急技术处理协调中心、中国信息通信研究院等机构认定网络安全威胁信息并提出处置建议。

（http://www.cac.gov.cn）

2017年国家网络安全宣传周于9月16—24日举行

2017年国家网络安全宣传周于9月16—24日在全国范围内统一举行，主题是“网络安全为人民，网络安全靠人民”，由中央宣传部、中央网信办、教育部、工业和信息化部、公安部、中国人民银行、新闻出版广电总局、全国总工会、共青团中央九部门共同举办。宣传周活动主要内容包括：举办网络安全博览会暨网络安全成就展，举办网络安全技术高峰论坛，举办主题日活动，首次开展一流网络安全学院示范高校评选活动，表彰网络安全先进典型。

（http://www.cac.gov.cn）

国家网络安全宣传周
China Cybersecurity Week

首项由我国主导的物联网标识国际标准发布

近日，安全研究组（ITU-TSG17）全会及各工作组会议在瑞士日内瓦召开。由中国电子技术标准化研究院、中兴通讯股份有限公司联合提出并牵头研制的国际标准提案ITU-T X.oid-iot《OID在物联网中的应用指南》通过了ITU-TSG17全会批准，成为正式发布的国际标准文件。该标准作为首项由我国提出的物联网标识领域的国际标准提案，规范了基于物联网域名（Object Identifier，OID）的物联网标识体系建设方法，涵盖标识机制设计、解析系统建设部署、运营规程建设等内容，不仅有助于指导在全球范围内采用OID技术快速建立物联网标识体系，而且对我国建设工业互联网、智能制造标识解析体系，深化各行业OID标识应用具有重要意义。

（http://www.cnii.com.cn）

数 字

75%

近期，市场研究公司Gartner完成的一项全球调查结果显示，75%的企业、机构愿意为5G移动通信技术支付更多的费用。

6年

近日，德国软件开发商称，早在2011年被发现的PDF解析库中的隐蔽漏洞，6年后再次出现，几近全部PDF阅读器中招。

8项

安全研究人员日前发现8项安全漏洞（统一代号为BlueBorne），表示其将影响超53亿台启用蓝牙功能的各类设备。

技 术

北斗系统首次实现7000公里长基线时间比对

近日，中国科学院国家授时中心在国际上首次实现了基于北斗导航卫星的7000公里长基线国际时间比对，对于北斗系统走向国际拓展应用具有重要价值和里程碑意义。该次远距离国际时间比对，授时中心时间基准实验室基于我国时间基准UTC（NTSC）系统，采用北斗共视（Beidou Common-view）法，通过与瑞典国家技术研究中心（RISE）所保持的瑞典国家标准时间UTC（SP）来进行比对试验。该次试验实现2.25纳秒的比对精度，在北斗系统星座还不完善的情况下（目前在欧洲只能观测到四颗卫星），其远距离比对性能指标与美国GPS共视比对精度相当。此次亚欧国际时间比对，为北斗比对正式纳入国际原子时TAI归算比对链路做了技术准备，对北斗迈向国际应用具有重要的意义。

（http://www.huanqiu.com）

瑞士开发网络攻击快速监测工具

瑞士国防部所属的国防装备科技中心与瑞士苏黎世联邦理工大学信息安全研究中心（ZISC）联合开发出一种新型网络安全工具，可快速监测网络恶意攻击行为，为实施《瑞士防范数字风险国家战略》提供技术支撑。据介绍，瑞士开发的这种新型网络安全工具能及时监测到感染病毒计算机中的恶意攻击软件与实施网络攻击行为的外部远程控制服务器之间的信息传递，并在数小时内确定超文本传输协议（HTTP）网络环境下它们之间的信息沟通路径（APT C&C-Channel）。

（http://www.most.gov.cn）

阿里云发布异构计算产品可将深度学习成本缩减一半

近日，阿里云宣布推出全新一代异构加速平台，这也是继企业级ECS家族全线升级后，阿里云再次在企业级市场推出专业服务，将异构计算的使用领域从人工智能扩大到更广的计算需求领域。资料显示，异构计算是一种特殊形式的并行和分布式计算，它能协调地使用性能、结构各异的机器以满足不同的计算需求，并使代码（或代码段）能以获取最大总体性能方式来执行。新品具备更强的并行能力和多场景支持，不仅全力支撑人工智能计算力升级需求，也为图形计算、生命科学、材料力学、分子动力学等科研计算领域提供普惠计算能力，特别是在人工智能领域，可将深度学习成本缩减一半。

（http://www.ifeng.com）

（本栏目数据内容摘自相关媒体、网站）

48小时

9月12—13日，我国首个48小时黑客马拉松破解大奖赛成功举办，吸引了来自全国的20名顶尖白帽参加。

46.5万

近日，有46.5万台美国老牌心律调节器被曝出存在安全漏洞，这可能导致装置的设定被修改。

165万

2017年1月1日至今，卡巴斯基共检测到165万台被恶意软件感染进而安装货币挖矿软件的设备。

威 胁

微软办公软件也不安全了？研究人员发现Excel安全漏洞或遭跳板攻击

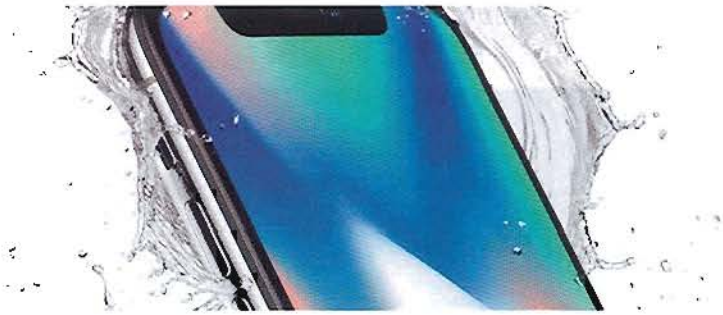
安全研究人员研究发现，微软旗下的Microsoft Excel的默认启动与访问权限存在安全漏洞，那些基于宏发动的攻击完全不需要和受害者交互就能够利用这个漏洞发动跳板攻击，以此对网络中的其他系统进行入侵。由于Microsoft Excel当中没有设置明确的启动或访问权限，因此攻击者可以通过其他方式发动攻击，且Microsoft Office的宏安全机制是无法阻止此类攻击的。这个漏洞使得攻击者还可以利用这次入侵为跳板，转而发动对其他计算的攻势。虽然这种攻击受限于拥有管理员权限的用户，但是其攻击后果往往非常严重，局域网内的电脑都无法幸免。在公司中，这个安全问题将被无限放大。

（http://www.secdoctor.com）

斯诺登评苹果Face ID：我更担心隐私安全

苹果已推出名为Face ID的面部识别技术作为解锁iPhone X的新式生物识别方法。这套系统利用手机前置摄像头扫描和登记用户面部结构特征作为密码，省去了输入键盘密码或扫描指纹环节。不过，设备安全似乎并不是美国中央情报局（CIA）前雇员爱德华·斯诺登（Edward Snowden）的主要担忧。他更担心隐私安全问题，与科技界的许多人一样，斯诺登把注意力转向了苹果的Face ID，并在Twitter上对其生物识别系统进行了总体上的正面评价，尽管如此，他还是谨慎地指出，面部扫描技术成为常态可能导致被滥用。

（http://www.163.com）



最新人工智能机器人配备自主模块，机器人危机来临

随着智能技术的发展，智能机器人已具备超越虚构的能力，马上就要进入我们的生活。研究人员已实现机器人的自主模块化，意思就是机器人具有了控制自身的能力。机器人不再依照写好的代码来进行机械动作，而是有着自主编写、自主更新、自主学习和交流的能力。布鲁塞尔大学人工智能实验室的首席研究员Marco Dorigo表示，在不久的将来，机器人将具备自主合作的能力，也许众多科幻大片中的机器人危机，也将来到我们身边。

（http://www.sina.com.cn）

数 字

（本栏目数据内容摘自相关媒体、网站）

1100万

9月12日，《法律视角下的全球网安态势及对策报告》（2017年篇）在京发布。《报告》指出经评估全国约有1100万个高危企业邮箱。

30亿

Google宣布防钓鱼工具已累计为超过30亿台设备（涵盖智能手机、笔记本和桌面PC）提供安全防护，相比2016年多出10亿台。

1.8万亿

全球移动通信系统协会（GSMA）的最新数据显示，到2026年，物联网将为移动运营商提供高达1.8万亿美元的收入机遇。

（栏目编辑：郝君婷）