DBAPPSecurity 安恒信息

安全通报

本周预警状态为二级：

有一些严重漏洞发布或网络攻击时间有增多迹象。需对网络和主机进行必要的监控和升级。

2015年5月第1周

安恒信息

信息安全漏洞威胁通报

〔2015 年 04 月 30 日-2015 年 05 月 07 日〕5 月第 1 周

根据中国国家信息安全漏洞库统计，本周共收集、整理信息安全漏洞 102 个，其中高危漏洞 32 个、中危漏洞 59 个、低危漏洞 11 个。上述漏洞中，可利用来实施远程攻击的漏洞有 89 个。本周收录的漏洞中，已有 87 个漏洞由厂商提供了修补方案，建议用户及时下载补丁更新程序，避免遭受网络攻击。其中互联网上出现“WordPress 插件 TheCartPress 本地 PHP 文件包含漏洞”、“ProFTPd (mod_copy)远程命令执行漏洞”等零日攻击代码，请使用相关产品的用户注意加强防范。

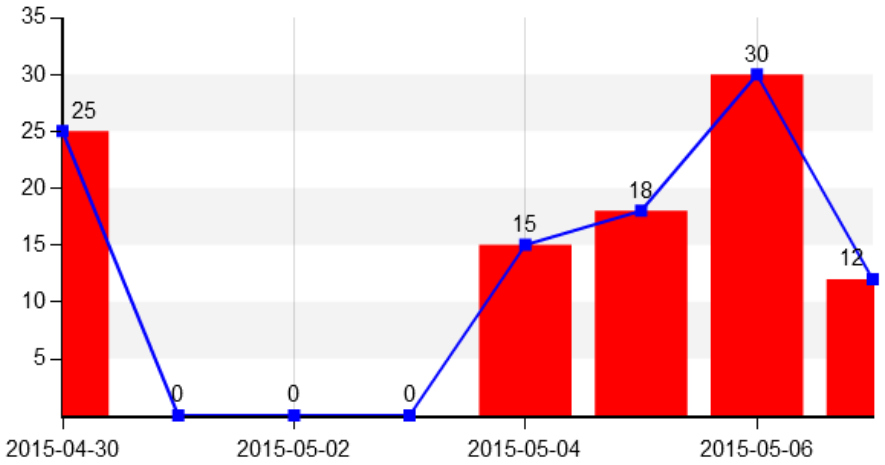
二〇一五年五月七日

目录

注：本通报根据安恒信息风暴中心和国内各大信息安全机构、网站整理分析而成。

1 漏洞预警

1.1 漏洞概况

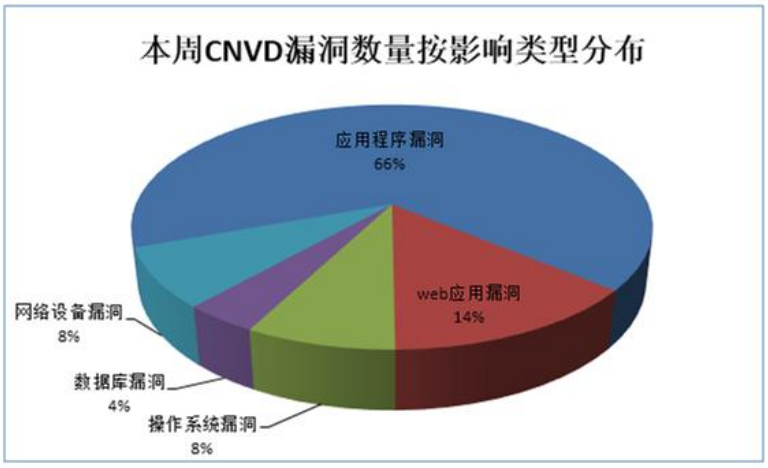


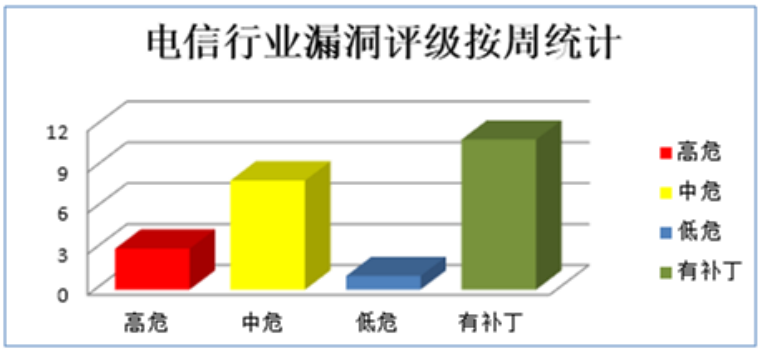
本周漏洞趋势图

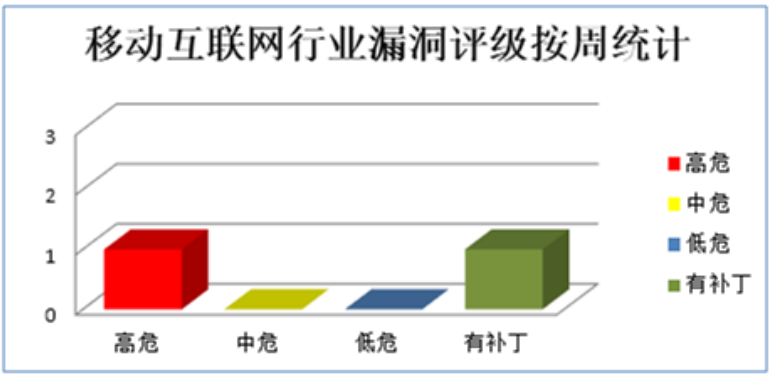
本周，中国国家信息安全漏洞库收录了 102 个漏洞。其中应用程序漏洞 68 个，WEB 应用漏洞 14 个，操作系统漏洞 8 个，网络设备漏洞 8 个，数据库漏洞 4 个。

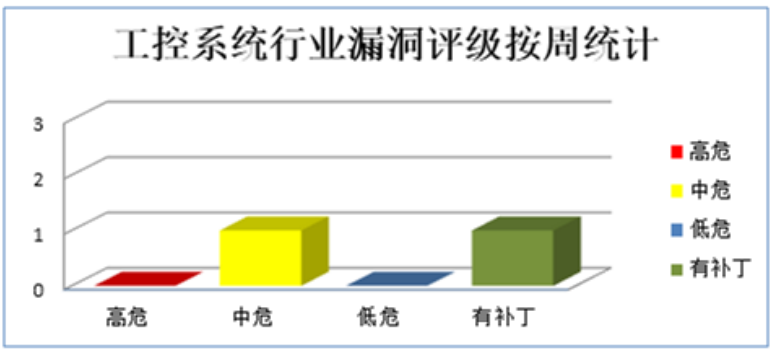
漏洞影响对象类型	漏洞数量
应用程序漏洞	68
WEB 应用漏洞	14
操作系统漏洞	8
网络设备漏洞	8
数据库漏洞	4

漏洞预警


本周CNVD漏洞数量按影响类型分布
应用程序漏洞
66%
web应用漏洞
14%
网络设备漏洞
8%
数据库漏洞
4%
操作系统漏洞
8%


电信行业漏洞评级按周统计
12
9
6
3
0
高危
中危
低危
有补丁
高危
中危
低危
有补丁


移动互联网行业漏洞评级按周统计
3
2
1
0
高危
中危
低危
有补丁
高危
中危
低危
有补丁


工控系统行业漏洞评级按周统计
3
2
1
0
高危
中危
低危
有补丁
高危
中危
低危
有补丁

1.2 漏洞预警

1.2.1 Apache Xerces-C XML Parser internal/XMLReader.cpp 拒绝服务漏洞

发布时间：	2015-05-05
更新时间：	2015-05-05
漏洞编号：	CVE ID:CVE-2015-0252 CNCVE ID：CNCVE-20150252
受影响系统：	Apache Group Xerces C++ < 3.1.2
不受影响系统：	
攻击所需条件：	攻击者必须访问 Apache Xerces。
漏洞描述：	Xerces 是由 Apache 组织所推动的一项 XML 文档解析开源项目。 Apache Xerces-C internal/XMLReader.cpp 不正确处理 XML 数据,远程攻击者通过特制的 XML 数据,对应用进行拒绝服务攻击。
安全建议：	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞： http://svn.apache.org/viewvc?view=revision&revision=1667870

1.2.2 Apache Tomcat 信任请求拒绝服务漏洞

发布时间：	2015-05-05
更新时间：	2015-05-05
漏洞编号：	CVE ID:CVE-2014-0230 CNCVE ID：CNCVE-20140230
受影响系统：	Apache Group Tomcat 8.0.0-RC1 - 8.0.8 Apache Group Tomcat 7.0.0 - 7.0.54 Apache Group Tomcat 6.0.0 - 6.0.43
不受影响系统：	
攻击所需条件：	攻击者必须访问 Apache Group Tomcat。
漏洞描述：	Apache Tomcat 是一个流行的开源 JSP 应用服务器程序。 在完全读取请求正文之前，就把该请求的响应返回给用户代理，默认 Tomcat 会信任剩下的请求正文，因此链接上德下一个请求也会接着处理。Tomcat 对信任的请求正文大小没有限制，会不关闭链接，正在处理的线程会继续保持连接，可导致有限的拒绝服务。
安全建议：	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞： http://tomcat.apache.org/security-8.html

	http://tomcat.apache.org/security-7.html http://tomcat.apache.org/security-6.html

1.2.3 Citrix NetScaler ADC/NetScaler Gateway 拒绝服务漏洞

发布时间：	2015-05-05
更新时间：	2015-05-05
漏洞编号：	CVE ID:CVE-2015-2829 CNCVE ID：CNCVE-20152829
受影响系统：	Citrix NetScaler ADC 10.5.e Build 53-9010.e Citrix NetScaler ADC 10.5
不受影响系统：	
攻击所需条件：	攻击者必须访问 Citrix NetScaler ADC。
漏洞描述：	Citrix NetScaler ADC 是应用交付控制器，可以优化企业服务交付。Citrix Access Gateway 是一款通用的 SSL VPN 设备。 Citrix NetScaler ADC/NetScaler Gateway 存在未明安全漏洞，允许未验证的远程攻击者利用此漏洞使设备重启。
安全建议：	目前没有详细解决方案提供： https://www.citrix.com/downloads/netscaler-

	adc/firmware.html?_ga=1.72013715.1435020893.1430884337

1.2.4 Nagios Business Process Intelligence (BPI) index.php 未明跨站脚本漏洞

发布时间：	2015-05-05
更新时间：	2015-05-05
漏洞编号：	CVE ID:CVE-2015-3618 CNCVE ID：CNCVE-20153618
受影响系统：	Nagios Business Process Intelligence
不受影响系统：	
攻击所需条件：	攻击者必须访问 Nagios Business Process Intelligence。
漏洞描述：	Nagios 是一款开源的免费网络监视工具,能有效监控 Windows、Linux 和 Unix 的主机状态,交换机路由器等网络设置,打印机等。 Nagios Business Process Intelligence index.php 存在跨站脚本漏洞，允许远程攻击者利用漏洞注入恶意脚本或 HTML 代码，当恶意数据被查看时，可获取敏感信息或劫持用户会话。

安全建议：	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞： http://nagios.org/

1.2.5 WordPress 4.2 存储型 XSS 漏洞

发布时间：	2015-05-05
更新时间：	2015-05-05
漏洞编号：	CVE ID:CVE-2015-3440 CNCVE ID：CNCVE-20153440
受影响系统：	WordPress < 4.2.1 WordPress < 3.9.6
不受影响系统：	
攻击所需条件：	攻击者必须访问 WordPress。
漏洞描述：	WordPress 是一种使用 PHP 语言开发的博客平台，用户可以在支持 PHP 和 MySQL 数据库的服务器上架设自己的网站。 WordPress 没有正确过滤注释内容，允许远程攻击者利用漏洞注入恶意脚本或 HTML 代码，当恶意数据被查看时，可获取敏感信息或劫持用户会话。
安全建议：	用户可参考如下厂商提供的安全补丁以修复该漏

	洞： http://codex.wordpress.org/Version_3.9.6

1.2.6 Apache Portable Runtime 命名管道安全漏洞

发布时间：	2015-05-04
更新时间：	2015-05-04
漏洞编号：	CVE ID:CVE-2015-1829 CNCVE ID：CNCVE-20151829
受影响系统：	Apache Portable Runtime < 1.5.2
不受影响系统：	
攻击所需条件：	攻击者必须访问 Apache Portable Runtime。
漏洞描述：	Apache Portable Runtime 是一个为上层应用程序提供可跨越多个操作系统平台使用的底层支持接口库。 基于 Windows 平台的 Apache Portable Runtime 存在安全漏洞，当程序使用 APR 命名管道支持时，允许远程攻击者实施管道非法占用攻击。
安全建议：	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞： http://www.apache.org/dist/apr/CHANGES-APR-

	1.5

1.2.7 EMC AutoStart ftagent 命令执行漏洞

发布时间：	2015-05-04
更新时间：	2015-05-04
漏洞编号：	CVE ID:CVE-2015-0538 CNCVE ID：CNCVE-20150538
受影响系统：	EMC AutoStart 5.5.0
不受影响系统：	
攻击所需条件：	攻击者必须访问 EMC AutoStart。
漏洞描述：	EMC AutoStart 是一套新一代集群软件。该软件支持双机热备、故障排除和负载均衡等。 EMC AutoStart 程序处理节点间通讯时存在错误，允许远程攻击者可利用漏洞通过发送特制的数据包执行任意命令。
安全建议：	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞： http://www.emc.com/storage/autostart.htm

1.2.8 LibAxl XML 处理未明堆缓冲区溢出漏洞

发布时间：	2015-05-04
更新时间：	2015-05-04
漏洞编号：	CVE ID:CVE-2015-3450 CNCVE ID：CNCVE-20153450
受影响系统：	LibAxl
不受影响系统：	
攻击所需条件：	攻击者必须访问 LibAxl。
漏洞描述：	LibAxl 是一个 XML 1.0 标准规范的有效实施工具。LibAxl 处理 XML 内容存在缓冲区溢出，允许远程攻击者利用漏洞使应用程序崩溃或执行任意代码。
安全建议：	用户可参考如下厂商提供的安全补丁以修复该漏洞： http://www.aspl.es/xml/

1.2.9 多款 F5 产品证书校验伪造欺骗漏洞

发布时间：	2015-05-04
更新时间：	2015-05-04
漏洞编号：	CVE ID:CVE-2014-9326 CNCVE ID：CNCVE-20149326

漏洞预警

受影响系统：	F5 BIG-IP LTM 11.5.011.6.0 BIG-IP AAM 11.5.011.6.0 BIG-IP AFM 11.5.011.6.0 BIG-IP Analytics 11.5.011.6.0 BIG-IP GTM 11.5.011.6.0 BIG_IP Link Controller 11.5.011.6.0 BIG-IP APM 11.3.011.6.0 BIG-IP PEM 11.3.011.6.0 BIG-IP ASM 10.0.0-11.6.0
不受影响系统：	
攻击所需条件：	
漏洞描述：	F5 BIG-IP LTM 是一款本地流量管理器；APM 是一套提供安全统一访问关键业务应用和网络的解决方案。 多款 F5 产品中没有正确验证服务器证书，当程序使用自动签名升级功能时，允许攻击者提供特殊的证书进行中间人攻击，欺骗 F5 升级服务器。
安全建议：	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞： https://support.f5.com/kb/en-us/solutions/public/16000/000/sol16090.html

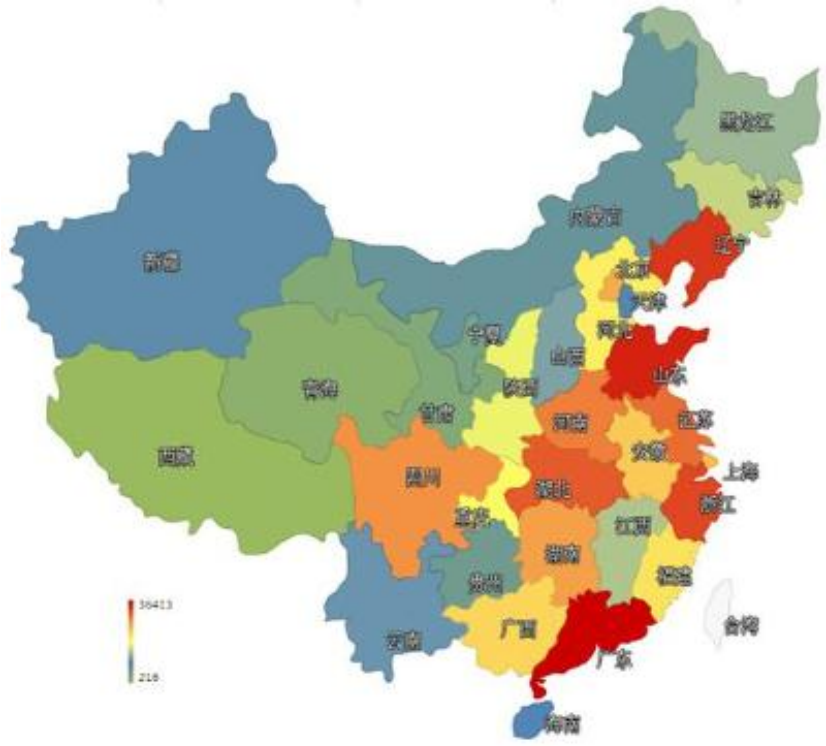
1.2.10 IBM WebSphere Application Server 多个竞争条件权限提升漏洞

发布时间：	2015-04-28
更新时间：	2015-04-28
漏洞编号：	CVE ID:CVE-2015-1882 CNCVE ID：CNCVE-20151882
受影响系统：	IBM WebSphere Application Server 8.5 Liberty Profile
不受影响系统：	
攻击所需条件：	攻击者必须访问 IBM WebSphere Application Server。
漏洞描述：	IBM WebSphere Application Server Liberty Profile 存在安全多个竞争条件漏洞，允许通过验证的用户利用线程冲突导致在 EJB Run-as 用户上下文执行任意 Java 代码并提升权限。
安全建议：	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞： http://www-01.ibm.com/support/docview.wss?uid=swg1PI33357

2 病毒预警

2.1本周网络病毒概况

本周境内感染网络病毒的主机数量约为 43.5 万个，其中包括境内被木马或被僵尸程序控制的主机约 27.8 万以及境内感染飞客（conficker）蠕虫的主机约 15.7 万。



木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区。

排名前三位的分别是广东省、山东省和辽宁省。

2.2本周流行网络病毒预警

2.2.1 Worm.Script.VBS.Agent.ck（木马病毒）

警惕程度 ★★

病毒运行后查找主流杀毒软件进程，并尝试将其结束。同时病毒还将修改用户的注册表，以便实现开机自启动。除此之外，该病毒还在后台连接黑客指定网址，并为恶意网址刷流量，占用大量网络资源。用户一旦中毒，有可能出现网络拥堵等现象。

2.2.2 Trojan.Win32.QQPass.ajz（木马病毒）

警惕程度 ★★

病毒运行后，将利用热键注销当前运行的 QQ，同时伪造登录窗口，并要求重新输入 QQ 账密。用户一旦轻信，QQ 账号信息将被发送至黑客指定服务器，届时用户将面临 QQ 被盗、隐私信息泄露等风险。

2.2.3 Trojan.PSW.Win32.QQPass.fnu（木马病毒）

警惕程度 ★★

该病毒运行后会在后台监视用户的输入，伺机窃取用户的 QQ 号码及密码，并发送给黑客。

2.2.4 Trojan.Win32.KillAV.cyf（木马病毒）

警惕程度 ★★★

病毒运行后，病毒运行后通过内核接口向内核读写数据，修改重要的监控函数，迫使杀毒软件监控瘫痪，并通过释放恶意程序，将恶意代码插入资源管理器的进程中。除此之外，病毒还将后台下载各种恶意软件，并连接远程服务器，等待黑客的后续指令。受到该病毒攻击的用户将面临硬盘数据丢失、隐私信息被盗等威胁。

2.2.5 Trojan.Win32.Generic.182215FF（木马病毒）

警惕程度 ★★★

病毒运行后释放文件 C:\WINDOWS\system32\msnadt.exe 并运行，用病毒程序替换系统程序，后台连接黑客指定地址，下载更多病毒至电脑。电脑一旦中毒，用户将面临隐私信息泄露、网络账号被盗、网银被盗等问题。

2.3病毒防范措施

- 计算机用户在浏览 Web 网页时，务必打开计算机系统中防病毒软件的“网页监控”功能。同时，计算机用户应及时下载安装操作系统已安装应用软件的最新漏洞补丁或新版本，防止恶意木马利用漏洞进行入侵感染操作系统。同时网络管理人员也要定期维护升级网站服务器，检查服务器所存在的漏洞和安全隐患，进行及时地修复和加固。

- 用户使用杀毒软件务必即时、充分升级，每天升级 2 到 3 次以上，以保证病毒库获取最新信息。

- 警惕不明网站、陌生邮件，尤其注意邮件附件。而对于重点网站，或者热门网站，如政府网站和各大媒体网站、论坛，很有可能被利用现有的漏洞进行挂马，或跳转到其他恶意网站。

- 做好系统和重要数据的备份。

- 不浏览不良网站，不随意下载安装可疑插件；不接收 QQ、邮件、微博私信等传来的可疑文件。

3 网站安全

3.1 本周网站安全概况

本周监测发现境内被篡改网站数量为 2543 个；境内被植入后门的网站数量为 1963 个；针对境内网站的仿冒页面数量为 3547。

本周境内被篡改政府网站(GOV 类)数量为 72 个(约占境内 2.8%)，较上周环比下降了 2.7%；境内被植入后门的政府网站(GOV 类)数量为 152 个（约占境内 7.7%），较上周环比下降了 15.1%；针对境内网站的仿冒页面涉及域名 2777 个，IP 地址 630 个，平均每个 IP 地址承载了约 6 个仿冒页面。

3.2 网站安全防护建议

“安恒信息”作为一家致力于 WEB 应用安全的专业产品和服务提供商，建议用户进行以下安全建设，以长期保证用户应用信息系统的安全。

1、定期进行专业的安全评估。

2、针对安全评估结果协调开发团队或厂商进行有效的安全整改和修复。

3、配备专业的 WEB 应用防火墙，针对来自互联网的主流 WEB 应用安全攻击进行安全防护。

4、建立和完善一套有效的安全管理制度，对信息系统的日常维护和使用进行规范。

5、建立起一套完善有效的应急响应预案和流程，并定期进行应急演练，一旦发现发生任何异常状况可及时进行处理和恢复，有效避免网站业务中断带来损失。

6、定期对相关管理人员和技术人员进行安全培训，提高安全技术能力和实际操作能力。

4 安全资讯

4.1 国内安全资讯

4.1.1 CNCERT 发布《2014 年我国互联网网络安全态势报告》

国家互联网应急中心(CNCERT)4 月 30 日发布的《2014 年我国互联网网络安全态势报告》数据显示,中国网络安全形势不容乐观,2014 年 CNCERT 通报的漏洞事件达 9068 起,较 2013 年增长 3 倍。CNCERT 运行部副主任严寒冰介绍,截至 2014 年 12 月底,中国网站总量规模为 364.7 万个,网民规模达 6.49 亿,手机网民规模 5.57 亿,互联网普及率达到 47.9%。随着互联网的迅速发展,相伴产生的新安全问题也层出不穷,基础网络和新型网络产品带来的漏洞风险日益上升。

随着云计算、大数据等新兴技术的应用,互联网金融、游戏、电子商务和电子政务等都在向云服务平台迁移,针对电信企业的网络攻击和安全漏洞正在呈现增长趋势:2014 年,CNCERT 协调处置涉及基础电信企业的漏洞 事件 1578 起,总共发现并通报了 9068 起,均是 2013 年的 3 倍。

严寒冰表示,安全漏洞体现在生活的很多方面,中国数据信息保护面临严 峻挑战。2014 年中国多家知名电商、快递公司、招聘网站、考试报名网站等多次发生数据泄露事件;去年 5 月,某知名手机厂商论坛数据泄露,由于用户管理模 块存在漏洞,导致包括账号、密码

和社交账号等 800 万用户个人信息泄露，用户财产和人身安全受到巨大威胁。

近年来，中国企事业单位已开始重视网络安全防护。抽查数据显示，企业网络或系统的安全漏洞数量较 2013 年下降了 72%；到 2014 年底，抽查企业 80%以上的网络、数据安全漏洞已完成修复。

4.1.2 一季度个人信息泄漏超 11 亿条 你真知道如何保护隐私吗？

日前，国内首个基于大数据的网络犯罪研究报告正式发布。报告显示，中国公民已经泄漏的个人信息多达 11.27 亿条。据了解，这份《2015 年第一季度网络诈骗犯罪数据研究报告》由北京反网络诈骗联盟发布，基于知名 互联网安全中心相关大数据形成。报告中称，在 2015 年第一季度，北京网络安全反诈骗联盟共接到网络诈骗报案 4920 例，报案总金额高达 1772.3 万元。

诈骗短信是导致用户上当的主要原因，其中冒充熟人的诈骗短信最多，占 28.5%，其次是虚假中奖 25.6%，冒充银行 19.9%。

安全专家：至少 11.27 亿条信息被泄露 应随时保持警惕

安全专家裴智勇表示，通过对安全中心大数据的验证，已确认被泄漏的信息至少有 11.27 亿条。

在这些大量被泄漏的信息里，既包括用户的敏感信息，也包括非敏感信息。专家介绍，一个用户的身份证号码、姓名、家庭住址、电话、通讯录等等，这都属于敏感的信息，而个人信息一旦泄漏，很难追回。

对于普通公众如何应对个人信息大量被泄漏，裴智勇提出建议：“在数据已经泄漏的情况下，需要我们个人提高防范意识。即使有人能准确说出你的姓名、家庭住址，甚至是你的银行账号、身份证号，他仍然可能是个骗子，大家需要时刻保持警惕。”

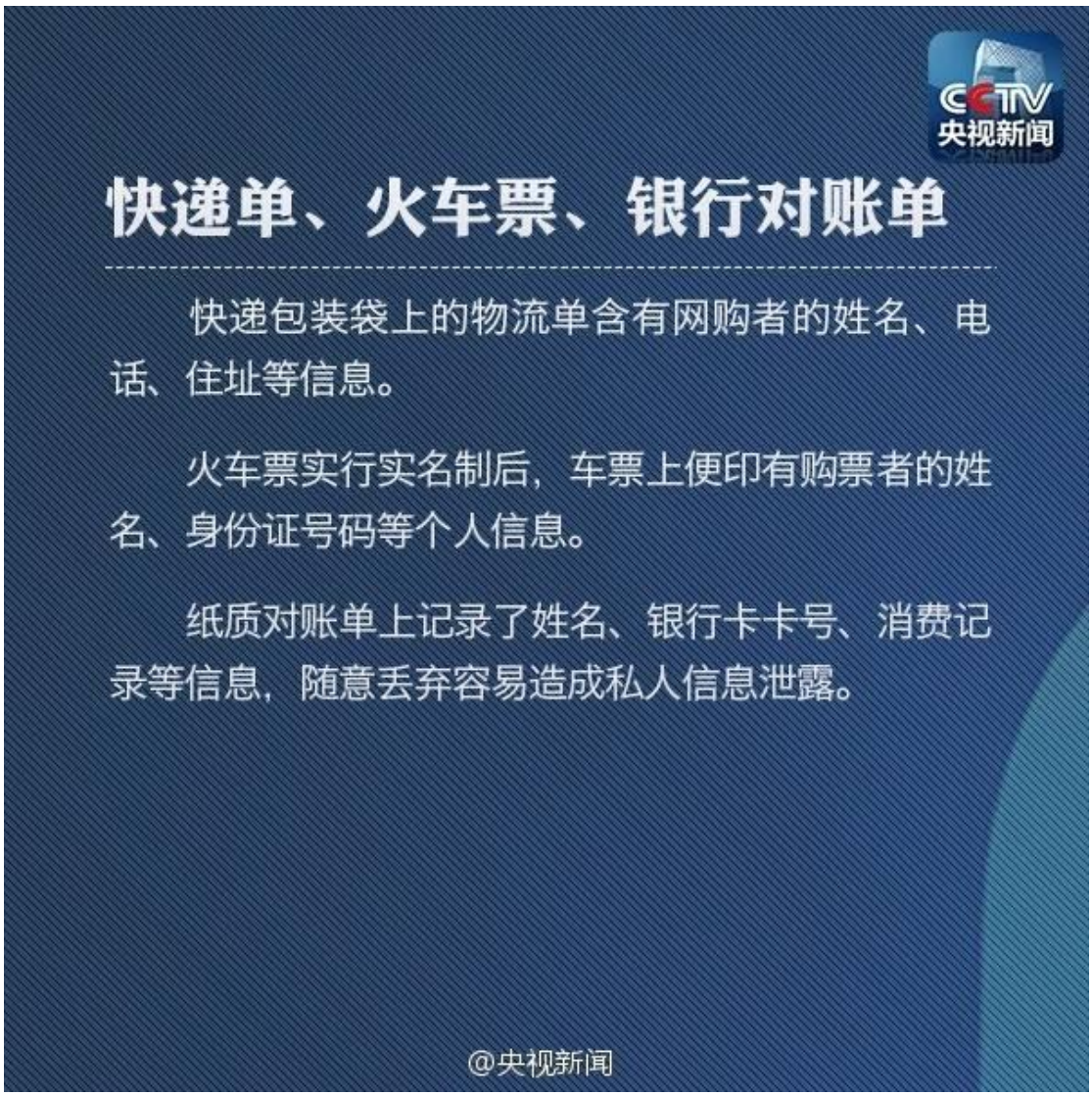
网络搜索能验证个人信息是否泄漏

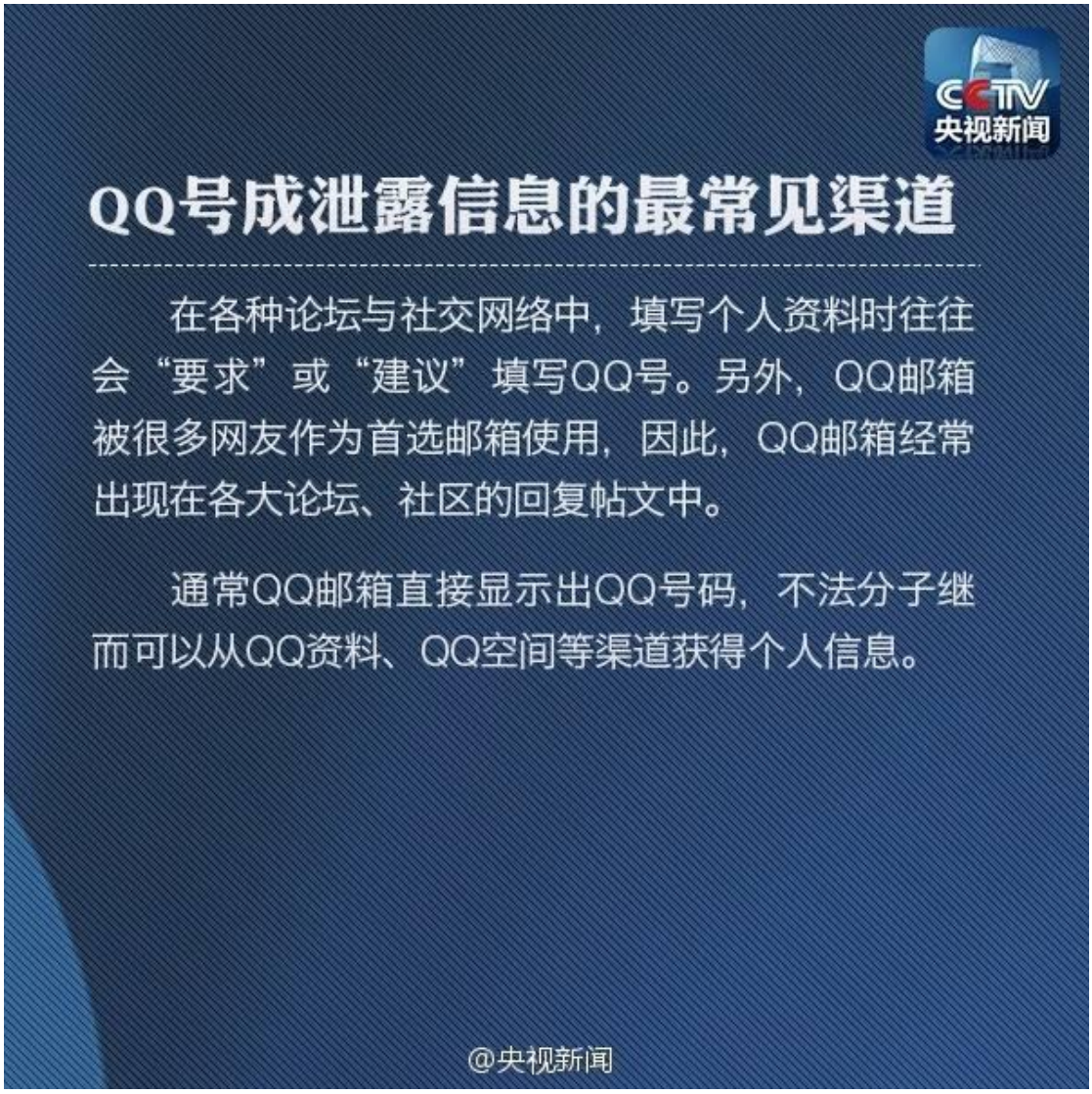
很多用户对自己的个人信息是否泄漏并不清楚，如何验证自己的个人信息是否泄漏？专家提示，可以通过网络搜索进行验证。

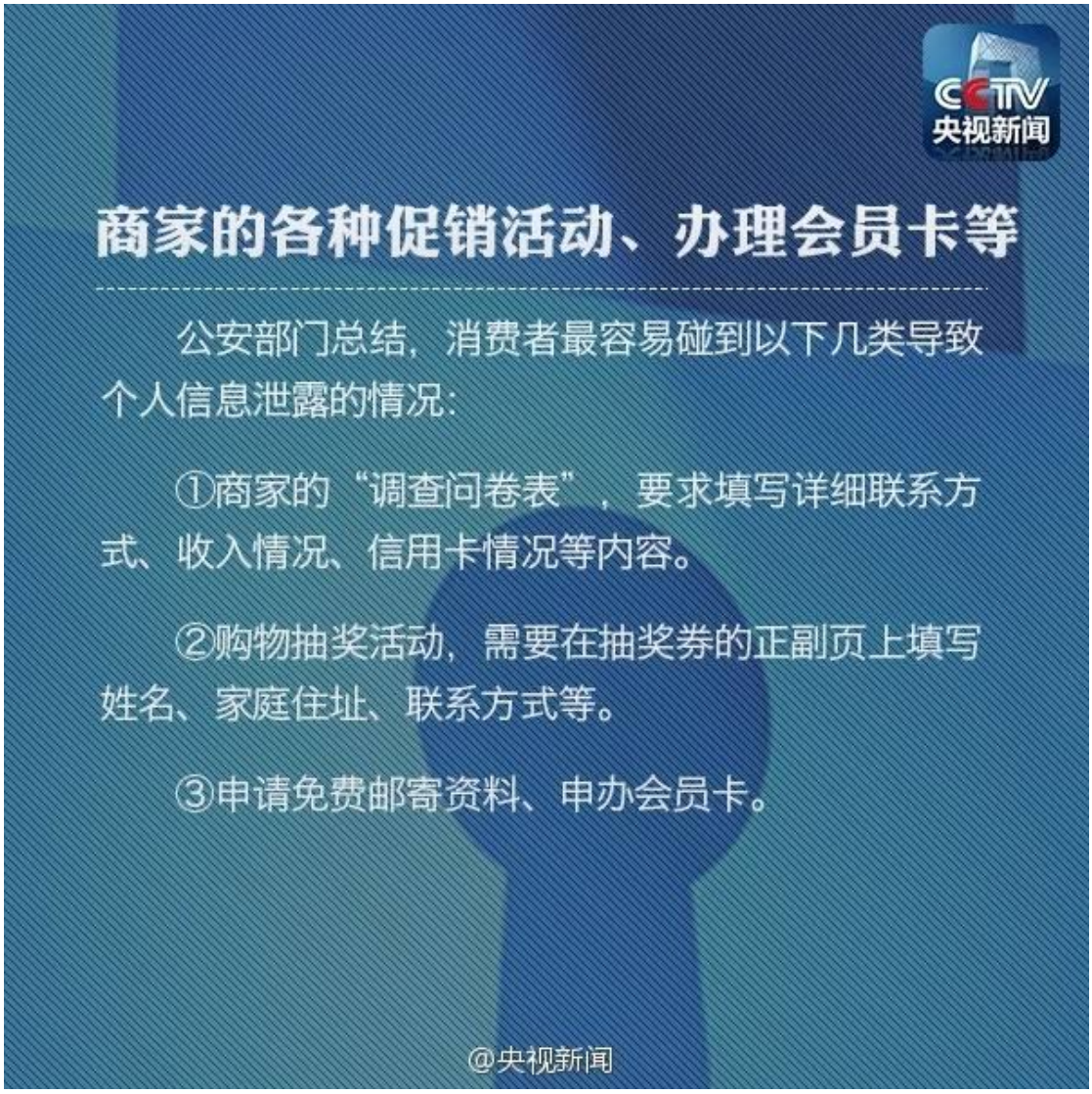
现在很多搜索引擎都提供这样的服务，可以输入自己的电话号码或常用信箱进行搜索。如果搜索结果中，个人相关信息显示得非常正确，则表明个人信息已经泄漏。这时，大家应该及时想办法去弥补，如要求搜索引擎删除相关内容，这样可在一定程度上避免个人信息的长久泄漏。

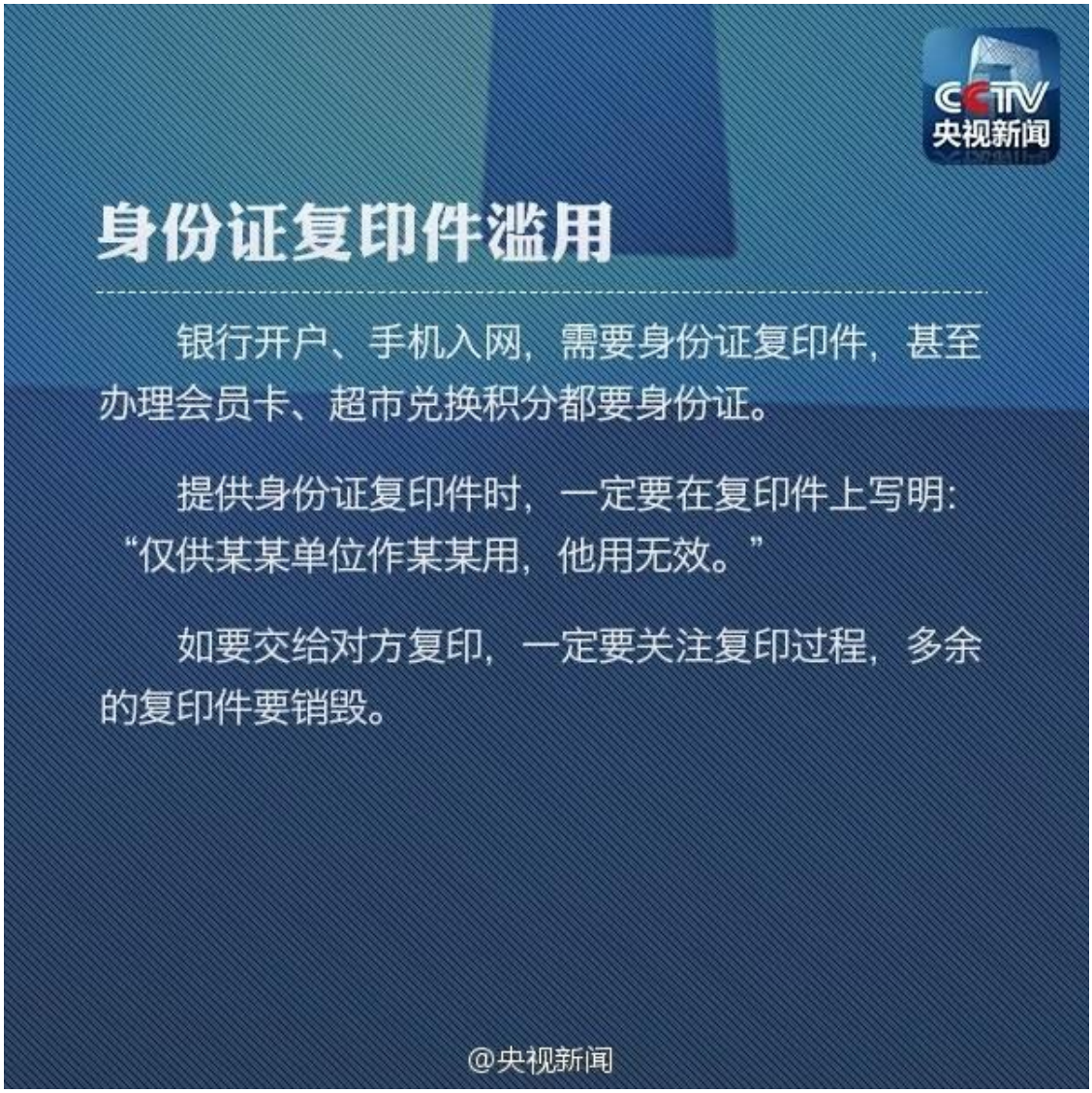
这些途径会泄露个人信息，小心！

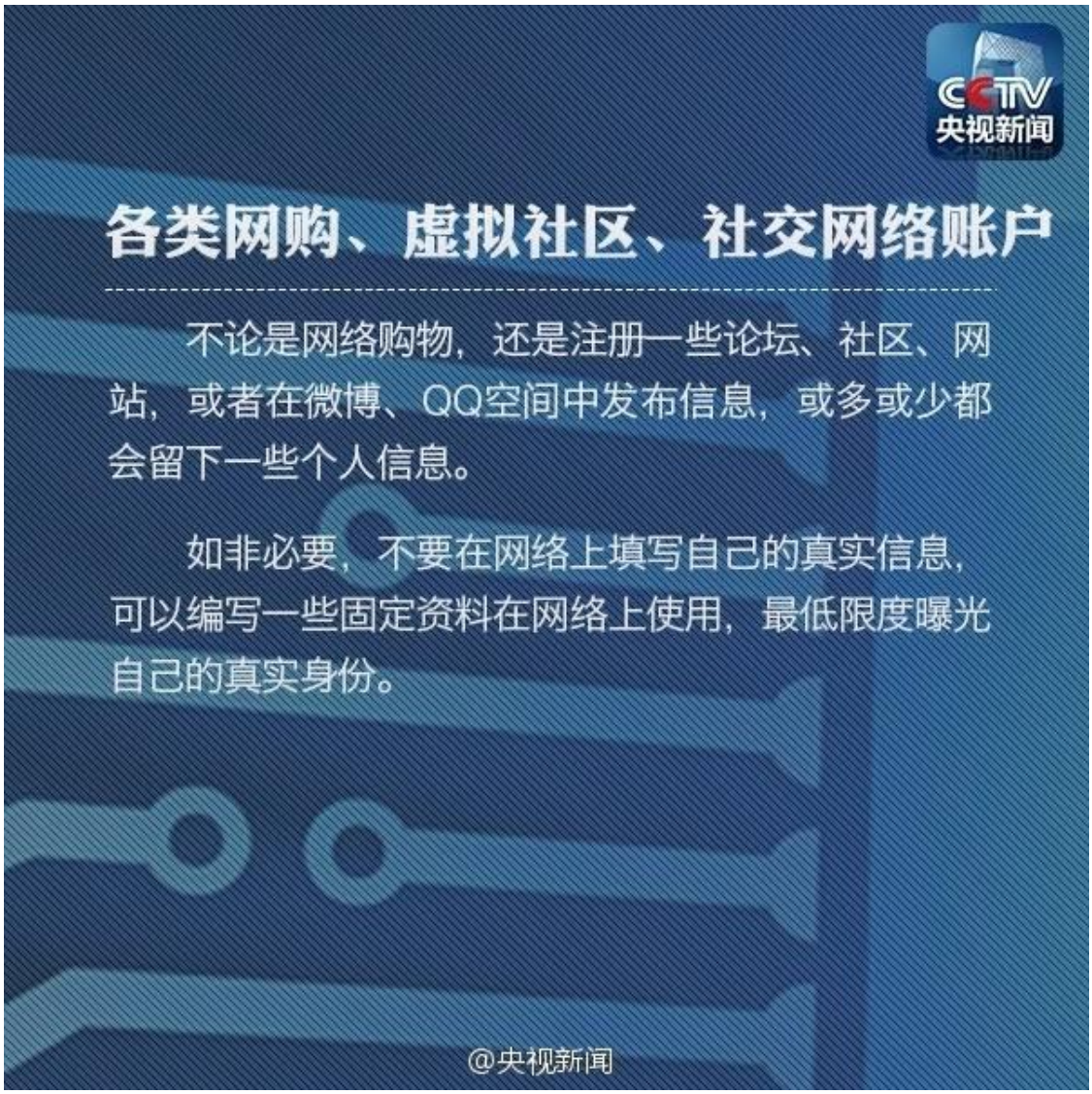
微博、QQ 空间留言互动，参加“有奖问卷调查”，申请免费邮寄资料、申办会员卡，都可能泄露个人资料。有调查报告显示，有近80%的网民手机号遭到过泄露，并有 50%以上的网民因手机号泄露而受到影响。如何有针对性地预防？看图↓↓

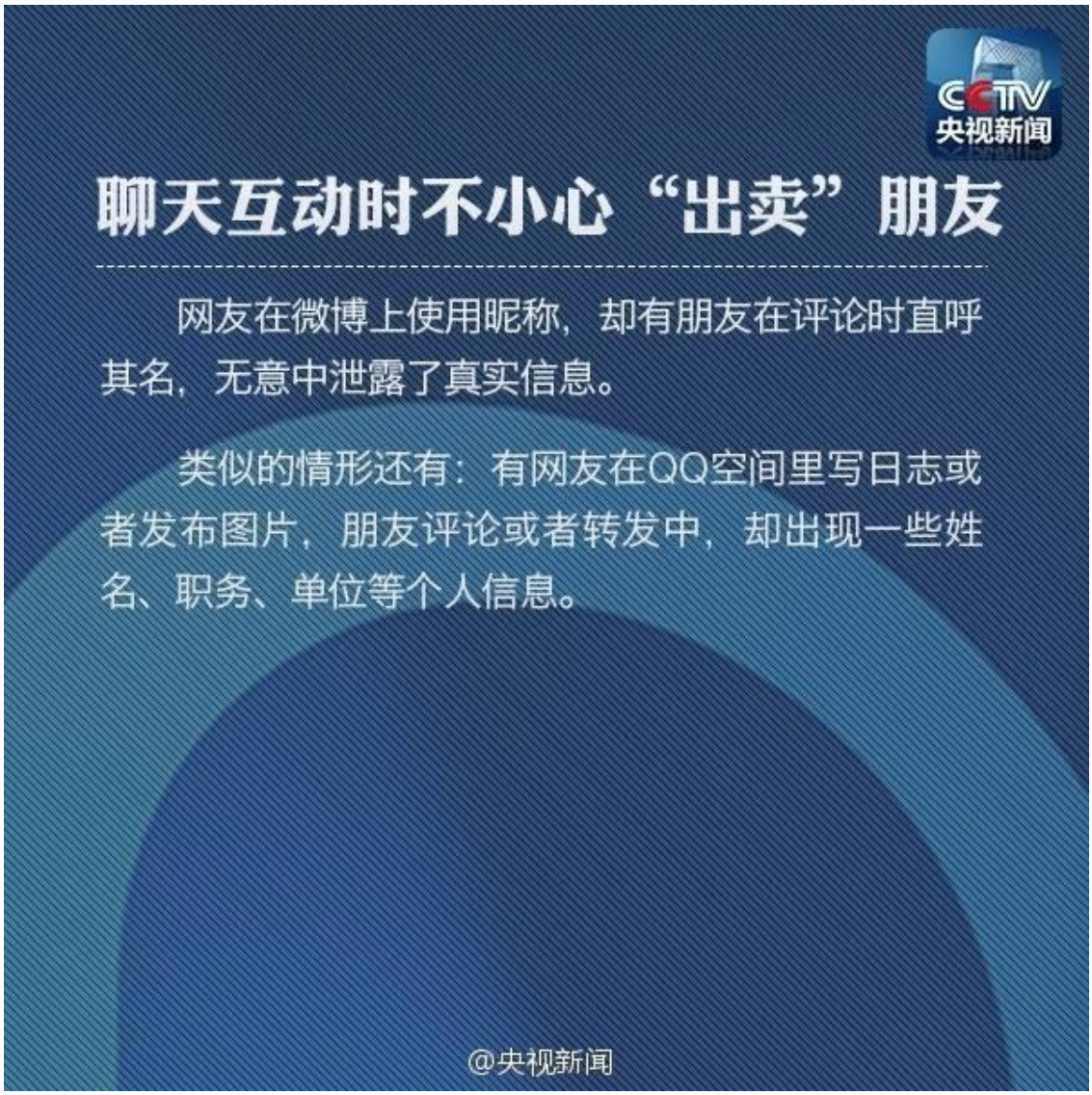


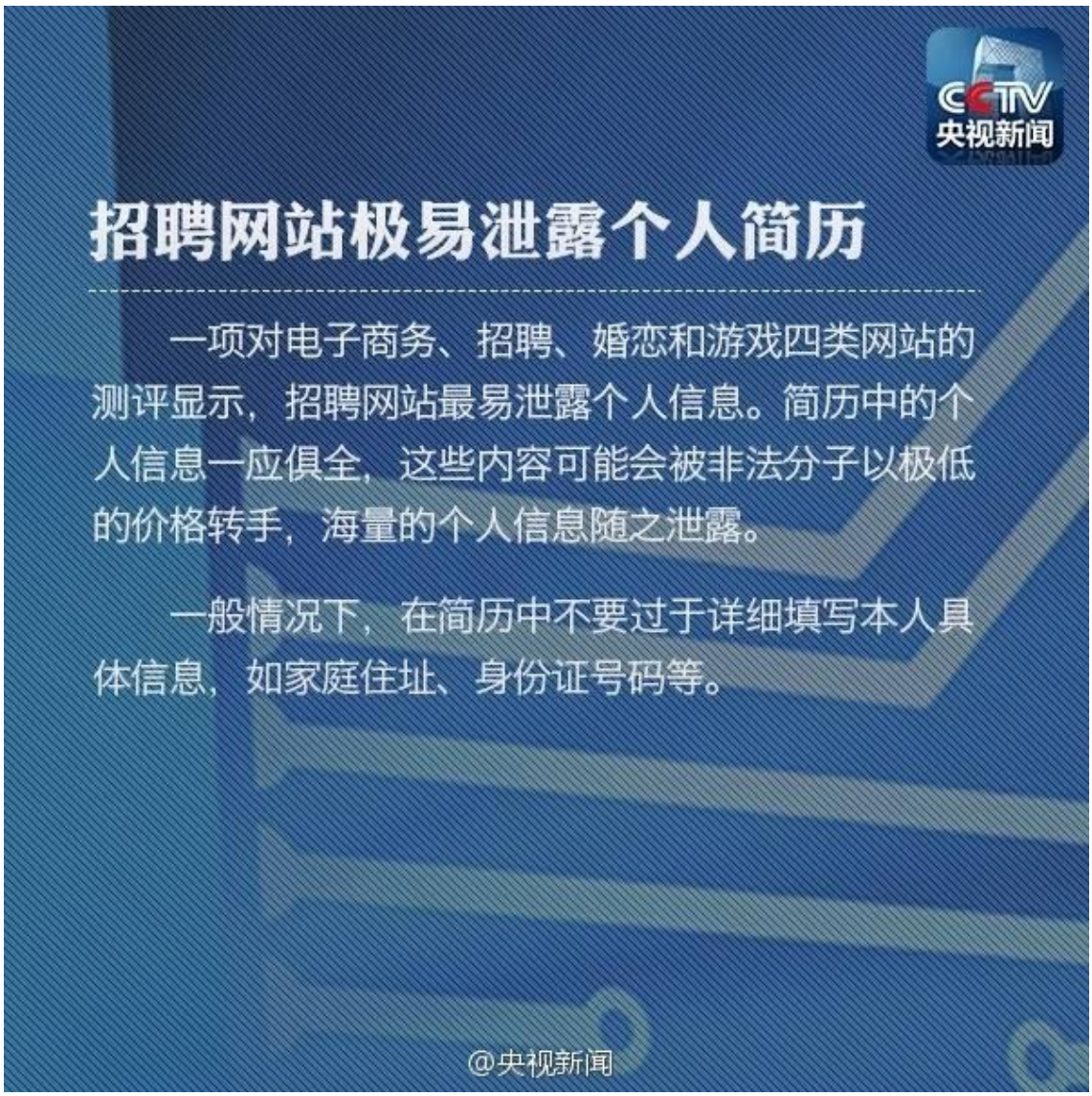

CCTV
央视新闻
QQ号成泄露信息的最常见渠道
在各种论坛与社交网络中，填写个人资料时往往会“要求”或“建议”填写QQ号。另外，QQ邮箱被很多网友作为首选邮箱使用，因此，QQ邮箱经常出现在各大论坛、社区的回复帖文中。
通常QQ邮箱直接显示出QQ号码，不法分子继而可以从QQ资料、QQ空间等渠道获得个人信息。
@央视新闻

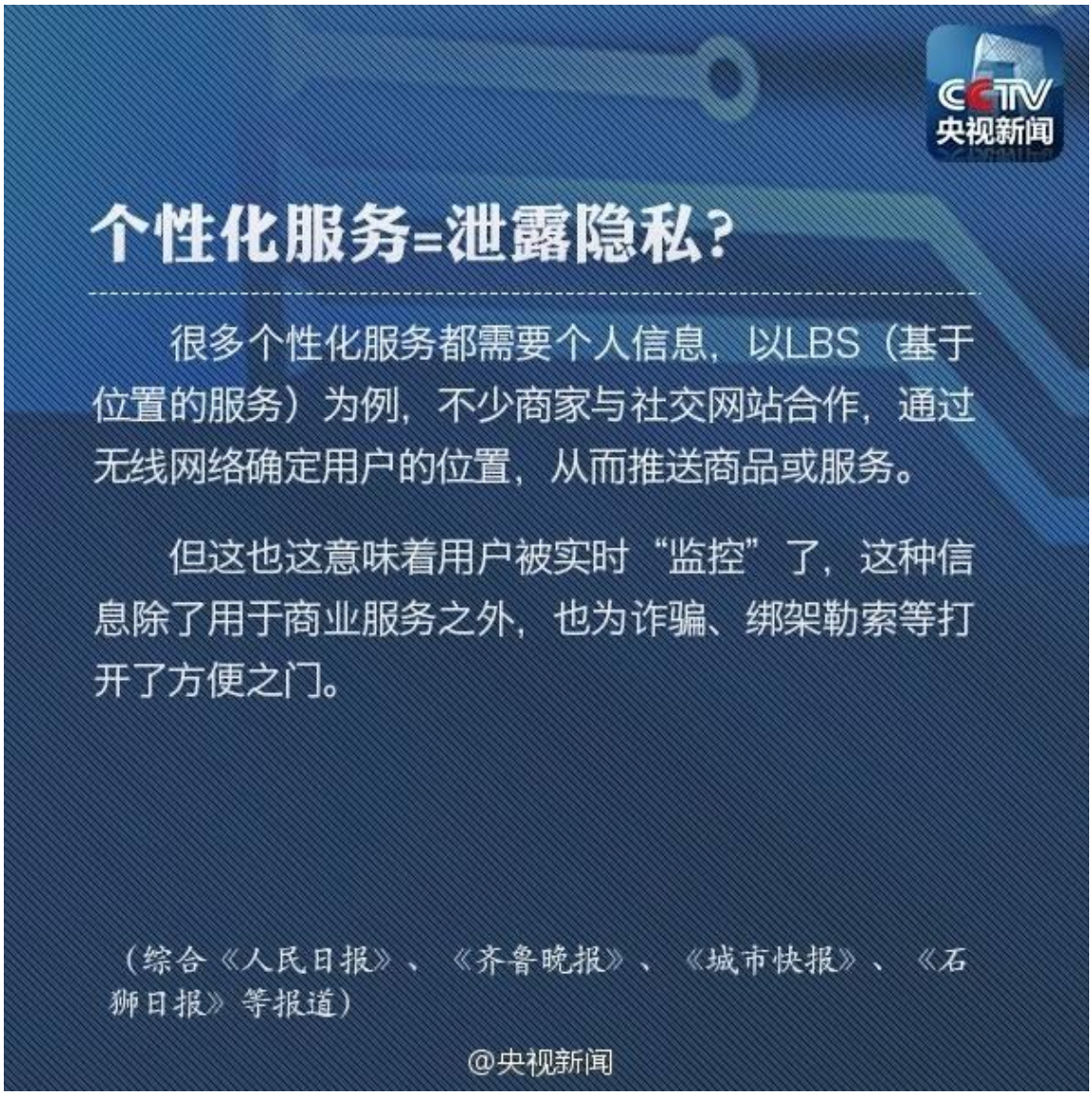

CCTV
央视新闻
商家的各种促销活动、办理会员卡等
公安部门总结，消费者最容易碰到以下几类导致个人信息泄露的情况：
①商家的“调查问卷表”，要求填写详细联系方式、收入情况、信用卡情况等内容。
②购物抽奖活动，需要在抽奖券的正副页上填写姓名、家庭住址、联系方式等。
③申请免费邮寄资料、申办会员卡。
@央视新闻


CCTV
央视新闻
身份证复印件滥用
银行开户、手机入网，需要身份证复印件，甚至办理会员卡、超市兑换积分都要身份证。
提供身份证复印件时，一定要在复印件上写明：“仅供某某单位作某某用，他用无效。”
如要交给对方复印，一定要关注复印过程，多余的复印件要销毁。
@央视新闻


CCTV
央视新闻
各类网购、虚拟社区、社交网络账户
不论是网络购物，还是注册一些论坛、社区、网站，或者在微博、QQ空间中发布信息，或多或少都会留下一些个人信息。
如非必要，不要在网络上填写自己的真实信息，可以编写一些固定资料在网络上使用，最低限度曝光自己的真实身份。
@央视新闻


CCTV
央视新闻
聊天互动时不小心“出卖”朋友
网友在微博上使用昵称，却有朋友在评论时直呼其名，无意中泄露了真实信息。
类似的情形还有：有网友在QQ空间里写日志或者发布图片，朋友评论或者转发中，却出现一些姓名、职务、单位等个人信息。
@央视新闻


CCTV
央视新闻
招聘网站极易泄露个人简历
一项对电子商务、招聘、婚恋和游戏四类网站的测评显示，招聘网站最易泄露个人信息。简历中的个人信息一应俱全，这些内容可能会被非法分子以极低的价格转手，海量的个人信息随之泄露。
一般情况下，在简历中不要过于详细填写本人具体信息，如家庭住址、身份证号码等。
@央视新闻



4.1.3 发布黑客程序 他今年才 15

商报讯 (记者 兰荣江)昨日，记者从铜仁市公安局获悉，印江县一 15 岁少年喜欢电脑游戏和制作软件，12 岁就开始学习编程，近日制作出黑客程序，由于好奇将该程序发布在网络上，被警方依法查处。

据悉，一注册名为“不吃药萌萌哒”的网民日前在百度贴吧发布了一条“本人制作的傻瓜式黑客入侵软件”的信息，并将制作的程序

发到百度网盘，附有软件使用和功能说明。该信息被印江县公安局网安大队民警在互联网巡查时发现，经初步核查，信息中所述的程序是一个计算机黑客程序。

随后，印江县网安民警对此事进行了调查，发现年仅 15 岁的少年张某有重大嫌疑。经传唤，张某在其父亲陪同下到公安机关接受调查。

张某交代了自己 3 年前开始学习编程，并于近日编写了一个黑客程序，其功能主要是让运行程序的计算机死机，远程控制和打开某个网页或程序，并能获取对方 IP、账号和密码。

张某表示其制作该程序只因比较喜欢电脑游戏和制作软件，在好奇心的驱使下，将自己制作的黑客入侵软件发布到了互联网上，并没有想要达到其他目的。

根据国家相关规定，制作、传播计算机病毒等破坏性程序属于违法行为，任何单位和个人不得制作、传播计算机病毒等破坏性程序，包括故意输入计 算机病毒，提供病毒、木马等恶意代码以及包含有各种恶意代码程序的下载服务，向他人提供含有计算机病毒、木马的软件和媒体，销售、出租、附赠计算机病毒程 序以及含有计算机病毒、木马的软件和媒体，如有违反，公安机关将按照有关法律规定予以查处。

根据治安处罚法相关规定，制作黑客软件并发布到互联网上，应被行政拘留，因张某未满 16 岁，印江警方依法不执行行政处罚。

4.1.4 江苏一年发生网络安全事件 37 亿起

近日，由中国通信企业协会主办的“2015 年（第五届）通信行业网络安全年会”在南京召开。记者了解到，去年，我省发生各类网络安全事件 37.3 亿起，平均每个月，就有近 100 万手机用户感染恶意程序。

去年，我省电信业务收入、电话用户数、互联网用户数、省际出口带宽等指标均居全国第二。省通信管理局局长苏少林介绍，目前全省电话用户总数达 10236.8 万户，电话用户普及率达到 128.9 部/百人；互联网固定宽带用户达到 1895 万户，移动互联网用户数达到 6468.4 万户。

目前，网络窃密、篡改、钓鱼、僵尸木马病毒、手机恶意程序等网络攻击事件频发多发。去年我省发生各类网络安全事件 37.3 亿起，其中网站篡改事 件 1.5 万余起，网站挂马事件 81.5 万起，仿冒官方网站进行钓鱼诈骗事件 2.5 万起，主机感染僵尸木马病毒 1.9 亿起，移动互联网用户感染恶意程序事件 33.5 亿起。仅去年青奥会期间，江苏省通信管理局就拦截 1.2 万多次针对青奥业务系统的网络攻击。

据了解，目前江苏手机网民高达 3740 万人，手机用户也成为恶意程序攻击的重点对象，平均每月江苏感染恶意程序的手机用户接近 100 万。

“几乎所有网站都有大大小小的漏洞，极易遭到黑客攻击。”国家安全中心实验室副主任黄元飞指出，一些政府部门、运营企业安全意识淡漠、管理不善，网站漏洞百出，应急处置不力，各部门在安全防备中各自为政，没有形成合力。

黄元飞坦言，眼下黑客泛滥，传统黑客攻击网站，只是为了炫耀技术、发泄私愤或者恶作剧，但随着互联网经济迅猛发展，攻击目的已经慢慢转变为追求经济利益，并形成了完整的黑色产业链。

来自国家安全中心实验室的一组数据表明，近 5 年来，该中心在全国检测了 3207 个网络单位，其中高危漏洞达 1.8 万多个，重大漏洞达 1.3 万多个。去年，全国有逾 4 万个网站被植入后门。

4.1.5 广州公安局长接到诈骗电话“明天到我办公室”

5 天前，广州市副市长兼广州市公安局局长谢晓丹召开新闻发布会。会上一名与会记者投诉早上收到自称广州市公安局某分局打来的诈骗电话引发戏剧性一幕……

谢晓丹借此自爆料，自己局长办公室的座机也经常接到诈骗电话。据他透露，广州市公安局将出台“一揽子”防诈骗举措，包括开展针对信息诈骗的专项打击 行动；从 4 月 1 日起，110 设防诈骗专线，怀疑是诈骗电话可以通过该专线确认；建立专项奖励金，有效防范电信诈骗，最高奖 5 万元。

公安局长接电：“明天到我办公室”

昨日早上，广州市举行第 32 场市领导新闻发布会，谢晓丹轮值担任主发布人。发布会接近尾声时，中国国际广播电台一位记者起身提问,“我今天早上收到一个自称广州市公安局白云分局打来的电话，我自然知道这是诈骗电话。现在电信诈骗现象十分泛滥，广州市公安局有何举措？”

“现在让大家举手说谁没接到过诈骗电话可能没几个人，”谢晓丹听完问题笑了，“我公安局长的办公室座机电话也经常收到诈骗电话。有一次一个人严肃地 说，明天到我办公室来。我问你是谁啊？对方说，你还听不出我是谁？我是政委啊。还有一个公安局副局长也接到诈骗电话，对方还能叫出我的名字。对方问‘谢晓 丹最近怎么样啊？’”他还列举了几种新型诈骗类型，“有一种改号软件，可以改 110 或者银行的服务号码，而且最近发现骗子推送的信息可以和真的服务号推动 到一个信息平台里，一转账钱就到境外了；还有专门针对领导的，‘某某某，你的那些见不得人的事情我都掌握了，点进

去看一下，’或者‘前两天的工作照片上网 去拿，’给个地址，点进去，手机信息就都被掌握了。然后再根据你的通讯录信息反过来骗你。”

怀疑诈骗电话可拨 110 专线

谢晓丹透露，广州市公安部门前年破获的最大一笔信息诈骗案涉案金额高达 2700 万元。“动辄几十万元，而且犯罪分子越来越倾向于年轻化，有些老年人的棺材本都被骗走了。”他称。

谢晓丹分析，信息诈骗猖獗的原因是犯罪成本低、收益高、打击成本高，既有法律不到位的问题，也有监管盲区，还有市民防范意识薄弱的问题。

他称，公安机关将加强联席会议，跟金融部门、电信部门加强沟通，建立点对点常态管理机制，形成快速联动打击电信诈骗工作格局。今年 4 月 1 日 起，110 设反电信诈骗专线，有疑问打 110，警方可以快速处置。同时，警方还要开展专项打击行动，并建立专项奖励工作机制，扩大奖励范围，调动全社会参与。有效防范电信诈骗的，最高奖 5 万元。

今年，广州警方已经发放了 15 .3 万元奖金，奖励 75 名银行职员等成功阻止诈骗发生的人员。

四大骗术如何防范

利用改号软件或“伪基站”伪装成“10086”发短信

手法：利用改号软件或“伪基站”伪装成 10086，并将“钓鱼”网站链接附在短信内，该链接地址与中国移动官方 网站“www.10086.cn”相似，只是在 10086 后增加了后缀(nss，pry，yyz 等)，短信内容以手机号积分兑换等内容骗取事主的信 任，市民很容易误以为真。一旦市民点击该链接，下载带有病毒的软件，按提示在所谓的客户端页面上填入自己的身份证、银行卡账号和密码等重要信息，不法分子 用事主银行卡号通过电商和支付平台发起购物申请，并利用软件病毒在后台读取事主接收到的短信验证码，盗刷市民的银行卡。

支招：认真甄别来电和接收到的短信息，不要轻易打开来历不明的短信，不要随意下载链接软件，不要轻易提供或录入 银行卡账号、密码等涉及财产安全的重要信息。遇有疑问，应立即拨打官方客服电话或向权威部门询问核实。一旦发现银行卡被盗刷，应立即拨打银行客服电话求 助，并拨打 110 报警。

谎称银行卡涉嫌恶意透支或洗钱贩毒

手法：多人分工，分别假冒银行以及公安局或检察院等单位工作人员，谎称用户的银行卡被复制盗用，涉嫌贩毒、洗 钱、走私等犯

罪，以冻结账户相威胁，以保护用户账户资金安全为由，要求用户将存款存入安全账户。这种类型诈骗手法特征是，重复提醒并劝你转账。犯罪分子的 “升级”做法是，给受害者一个假网站，里面有受害者的个人信息、照片以及涉及的罪名，让受害者害怕，接着再提出通过电脑操作核查受害者的资金，叫受害者在 “钓鱼网站”上输入银行卡号、密码等，此时，骗子便通过远程操作将受害者的钱转走。此骗术近期高发，骗子会对受害者谎称他们的案件涉及国家机密，任何人不 能告诉。因此，很多受害者是在被骗后许多天才发现自己被骗。

支招：目前任何公安局、检察院、法院等国家机关，均未设立“国家安全账户”等名目的银行账户。所以当有人打电话 要求你将存款转存到所谓“安全账户”以便保全资金的，即可认定是诈骗行为。国家机关工作人员履行公务，需要向公民询问情况时，一定会当面询问当事人并制作 相关笔录。所以当有人自称是上述机关工作人员打电话告知你涉嫌某种犯罪，要求你透露银行账户、密码进行“核实”时，即可认定是诈骗行为。

假冒领导身份

手法：骗子假冒领导身份打电话，利用某些基层工作人员唯命是从的心理，以垫付款项等“命令”方式，让受骗人支付款项到指定银行账号。

防范：接到“领导”电话，不要慌张，多重信息再三确认，不要贸然给对方汇款。

“老朋友”口气：猜猜我是谁

手法：骗子冒充熟人，在电话中让被害人猜猜他是谁，当被害人报出相识之人的姓名后即予承认。然后往往隔两天再以出车祸、嫖娼或赌博等被公安机关抓获需付保证金等理由要求汇款。

防范：当接到自称“老朋友”口气“猜猜我是谁”的电话时，要保持高度警惕，注意核实对方身份，不要轻易相信对方的种种理由而给其汇款。

其他骗术也勿掉以轻心

“医保卡故障”：不法分子冒用医保中心的名义向参保人员诈称医保卡发生故障、医保卡欠费封锁、医保卡透支以及涉嫌购买非法药品等虚假信息，要求参保人员提供身份证号码、医保卡号码及密码等个人信息，并要求其对某个银行账户进行转款。

还有一种是，骗子以医保中心或其他机关的名义电话通知事主，医保政策变动、缴费银行发生变动等，并留下咨询电话，事主拨打电话就慢慢陷入圈套。

“刷卡消费”：骗子给用户发送虚假手机短信称银行卡在某地刷卡消费多少元，可致电××××号码咨询，客户一旦拨 打提示电话，对方则自称某某银行的客服中心工作人员，要求客户持银行卡到自动取款机上输入密码，进行所谓的查询、设置“防火墙”保护、开通网上电子银行账 户等操作，诱骗客户将卡里的钱转到骗子的账户。

“邮政包裹”：骗子电话客户有邮政包裹未取。当你询问包裹相关情况，“邮政员工”会找各种借口如谎称包裹里有毒 品、危险化学品等违禁品，或包裹中有一张巨额银行卡，有人以你的名义开户洗黑钱或毒品被公安机关开拆，你得马上到公安机关侦查科报案，之后会给你一个“刑 侦队”或“侦查科”的电话号码。拨打过去，“刑侦队”会以各种理由套出你的账户信息，并以设置防护和安全措施为由，让你去银行取款机上操作。这个过程中， 骗子将账户里的钱全部转走。

“引诱汇款”：收到“请把钱存到××银行，账号××××”、“还未汇款吧，账号已改为××××”、“钱请还至账号××××”等内容短信，被害人误以为是商业伙伴或债权人的短信而按要求汇款。

PS 除了“医保卡故障”这一手法小编还没遇到，其他全部经历无数次！而童鞋们都被“诈”了多少次了？童鞋们一般都是怎么“对付”这些“领导”啊，“朋友”的？有被骗子得逞的冤大头么？

4.1.6 山东菏泽网管自学黑客技术 盗网吧 1.3 万余元

近日，山东省菏泽市东明县一网吧网管通过网络自学黑客技术篡改电脑记账系统，先后进 40 次盗窃网吧营业款现金共计 13750 元，被东明县公安局依法刑事拘留。

4 月 28 日下午，东明县公安局城区派出所接指挥中心警令称，辖区一网吧内有人实施盗窃。接警民警遂迅速赶赴事发网吧，经现场询问，报案人刘某向 民警讲述了事情经过：刘某系该网吧经营主，平常不在网吧看管，由其雇佣的年轻男子陈某和邓某两人作为网管负责网吧的日常经营活动，每月 28 日，刘某会到网 吧收取一个月的营业款。

当天下午，刘某来到网吧收取营业款，偏巧这个月的营业额非常少，刘某便寻思着查看一下经营细目，一条显示为“-200 元”的帐目引起了刘某的注 意。通过仔细检查，刘某发现自己用来监管系统的时间锁被人打开，遂怀疑有人在网吧的账目上做了手脚，便立即按时间顺序一直追查到了 2014 年 12 月份，这 期间的账目负值从 20 元到 400 元不等，合计 13750 元，刘某遂赶忙拨打 110 报警。

根据报案人刘某的详细叙述，民警将怀疑目标锁定在两名网管人员身上，经分别询问，陈某当场交待了其自 2014 年 12 月份开始，陆

续盗窃网吧经营 款的犯罪事实。据陈某交待，2014 年 10 月份，他开始在该网吧做网管，12 月份，陈某从某网络论坛内“学习”了篡改电脑帐目系统的黑客技术，并第一次尝 试着操作套取了 20 元营业款，当月向刘某交账时未被察觉；第二次，陈某又试着套取了 100 元营业款，交账时仍未被刘某察觉，于是，自觉万无一失的陈某开始 频繁地套取营业款，每次从 20 元到 400 元不等，直到事情败露，陈某共作案近 40 次，窃取网吧经营款 13750 元。

目前，该陈某已被东明县公安局依法刑事拘留，案件正在进一步侦办中。

4.2 国际安全资讯

4.2.1 谷歌惊现军用无人机攻击教程

近日，谷歌上出现军用无人机的攻击教程，这可能会导致很严重的安全问题和负面影响，例如一架无人机可能会干扰一架飞机，或者向无人机上添加武器，这些举动都可能会带来严重的后果。

因为各种各样的优点，无人机已经变得越来越受欢迎。同时，由于其通用性、廉价性等优点，以及能够防止士兵伤亡等优势，军队中也开始使用无人机。然 而，除了以上优势以外，无人机同时也具有一些不容忽视的缺点。其中一个主要的缺点就是它们可能会被发现，也可能会被他人攻击。这将带来很严重的安全问题， 试想如果在战争中，你的武器受到敌人攻击并被敌人控制用来对付你，可以想象这将会造成多么严重的后果。

谷歌上出现无人机攻击教程

根据以色列航空工业网络系统主管 Esti Peshin 的消息，利用谷歌搜索，任何人都能轻而易举地从网上收集到有关如何攻击无人机的相关教程信息。

在美国华盛顿举办的防御性网络操作和情报会议上，她对轻易获取这种具有威胁性的教程细节以进行非法活动表示非常担忧。她对这些教程材料进行了如下评论：

“虽然这只是一个 PDF 文件...但从本质上讲，它是黑客的一张攻击蓝图。你可以在谷歌上搜索‘Tippenhauer’、‘无人机攻击’或者‘无人机 GPS 欺骗攻击’，都能过找到有关攻击无人机的教程信息。”

当谈到网络安全措施和相应部门的安全警觉性时，她对此表现出了一些悲观和失望：

“事实上，在安全方面我们一直都慢于网络罪犯，他们能够利用这篇教程来实现一场攻击。其中一件让我夜不能寐的事情就是运营网络的安全性、军事系统和武器系统。”

无人机安全令人担忧

需要指出的一个重要事实是，攻击无人机教程的出现可能与伊朗击下美国中央情报局无人机事件有关。随着无人机在更多场合下的普遍使用，GPS 劫持攻击已成为一 个日益严重的现象，很可能在不久的未来这种技术将会进一步提高。攻击无人机的成本估计在 2000 美元到 3000 美元之间，而这笔数目绝对是黑客能够承受并 愿意做的投资。

有关无人机最令人担忧的问题，就是其功能实现中 所采用的都是已经过时的技术，这就是为什么专家们能够轻易渗透过无人机防护机制的原因。如果考虑到越来越多的人开始使用无人机这样一个事实，那么可以很容 易理解这将带来多大的安全风险。既然黑客已经能够在未授权情况下访问无人机，并已经掌握无人机的工作方式，那么将没有什么能够阻止他们任凭自己的兴趣这么 做。

事实证明，在某些情况下，无人机可能会引起非常严重的问题。例如，一架无人机可能会干扰一架飞机，或者可以向无人机上添加武器，这都可能会带来严重 的后果。然而，无人机制造商对此则有自己的说法，他们还解释说任何滥用无人机的情况都不应该被视为无人机的缺陷，或者作为取消无人机存在的理由。这当然是 一个有争议的问题，并会在接下来的一段时间内引起激烈的争论。

4.2.2 欧洲银行建立网络安全的监测机制 对抗网络攻击

据西班牙媒体 5 月 4 日报道，“你的银行是否已经准备好应对网络攻击？”这是欧洲中央银行上周派发到各大银行调查问卷的主要问题。这次参与调查的对象共有 123 家银行之多。

欧洲银行的监管机制（又称 MUS）已经建立了一个针对网络安全的监测机制，在其银行内部也增强了一个控制的机能，用以对付网络攻 击。根据欧洲中央银行的说法，当下首要需要解决的问题，就是金融行业所面对的巨大风险。能否妥善保存顾客的信息数据，成为对一个银行做风险评估的主要借鉴 依据。

该监管机制的主席丹尼尔坚定地认为，目前的银行系统存在许多的漏洞，使得其暴露于风险之中，而首当其冲受到伤害的就是其顾客的财产和信息安全。

“银行是一个巨大的保密信息容器。它所拥有的信息系统必须能够完美地阻隔一切攻击。”事实证明这是完全有必要的。从 2007 年到 2014 年，试图利用互联网进行银行诈骗犯罪的案例增加了 60 倍。唯一的好消息大概是，尽管互联网犯罪不断激增，但日常诈骗犯罪总数减少了 50%。

欧洲中央银行希望能够避免去年 JP 摩根的事件再度发生，同时也向超过 7600 万的个人和 700 万公司做出安全承诺。同时，农业信贷署也在银行的监督下加强了自身的安全监管。

根据信息显示，这些最强大的黑客攻击分别来自东南亚和南非。

面对着日益严峻的黑客攻击，欧洲中央银行做了一个分析报告，希望各银行可通力合作共同应对。

在具体会谈的过程中他们遇到了一些问题，比如，这些安全系统的监测者是否可以参与银行理事会的决议。这个问题遇到了很大争议，并为 多数银行所拒绝。显然他们并不希望自己的实权落在监测人员手上。然而在其他诸多方面，合作面对安全监测问题还是为各家银行认同的。

4.2.3 法国议会通过新监控法 被指跟 NSA 项目非常相似

据外媒报道，在经过数周的讨论之后，法国议会于日前通过了一项影响范围颇广的监控法，主要用于反恐行为。获悉，该法则是在查理周刊恐怖袭击之后推出，但反对者们认为，该监控法将会严重损害到民众的自由。在新系统下，由法国总理领导的监控行动部门将受一个委员会监管。该委员会拥有 9 名成员，他们并不会推翻总理的决定，而是给他一些建议。

很多隐私倡导组织认为，这套全新的监控法将会导致该国的监控力量变得过分集中化，这是极其危险的行为。

而早在 2013 年的时候，法国《世界报》就曾披露其国内有很多跟 NSA 棱镜项目相类似的监控项目。这些项目被指联合谷歌、微软及其他科技公司大规模收集电话 元数据。对此，法国给予否认。不过考虑到法国不是“五只眼”情报联盟的成员，再加上斯诺登泄露的机密信息也未指出法国参与了美国或英国的情报共享行动，所 以可能此前法国真的没有进行过这样的行动。

但对于这套新通过的监控法，很多人认为当 中采取的许多策略都跟 NAS 非常相似，如大规模收集互联网元数据。总理曼努埃尔·瓦尔斯则表示，两者之间并不存在相似之处，他称“这并不是一个法国

版的 《爱国法案》”，对于这样的答复，隐私倡导机构仍不满意，他们还是认为新法案给了情报机构过大的权利。

4.2.4 斯诺登爆料：NSA 将通话语音转换成文字

本周，The Intercept 网站再次发布了爱德华·斯诺登(Edward Snowden)曝光的美国政府文件。其中显示，美国国家安全局(NSA)在近 10 年的时间里持续将监听的语音通话转换为可搜索的文本文档。长期以 来，NSA 一直监控着全球范围内，尤其是阿富汗和伊拉克等冲突地区的“信号情报”，这也是 NSA 的主要职能。以往，这样的数据收集活动需要人工操作员监听 通话，并进行实时的翻译。

然而最新曝光的文件显示，NSA 开发出了一种被称作“语音版谷歌”的技术。这一自动化系统能提供粗略的、同时可通过关键词进行搜索的语音实录。与此同时，NSA 还开发了数据分析项目和复杂的算法，以标记出需要人工审阅的通话。

此外，这一技术实现了自动化和工业级规模，从而帮助 NSA 监控特定地区的庞大通话流量。这些自动转换的文本十分粗略，但根据来自 NSA 的托马斯·德拉科 (Thomas Drake)的说法，“即使并不是 100%完美，我仍可以获得大量信息。这样的情报更容易读取，我可以进行搜索。真正的突破在于实现了庞大的规模。”

4.2.5 恶意程序被发现会通过破坏硬盘逃避检测

思科 Talos Group 的研究人员报告发现了一个恶意程序会采用多种方式破坏逃避检测，其中包括破坏硬盘和防止虚拟机分析。研究人员将恶意程序命名为 Rombertik，它会不加选择的收集用户在互联网上任何所有的操作，可能是为了收集登录信息和其它敏感数据。它主要是通过邮件的恶意附件安装在用户电脑上。研究人员逆向工程了 Rombertik，发现它采用了多种方法逃避分析。

程序包含了多重混淆和反分析功能，让外人难以一窥内部工作。当程序主要组件检测到它正被安全研究人员或竞争对手仔细分析，它会自毁，同时破坏用户的所有数据。

破坏方法首先是复写主引导记录，如果恶意程序没有权限复写主引导记录，它会用随机生成的密钥加密用户的主文件夹，然后重启。

复写的主引导记录包含了打印文字“Carbon crack attempt, failed”的代码（如图）。为了躲避允许在可控环境下运行的沙盒工具，恶意程序会向内存写入 960 亿次随机数据。

4.2.6 匿名者（Anonymous）攻击世界贸易组织（WTO）网站，内部人员信息泄露

黑客组织匿名者近日入侵了世界贸易组织（WTO）的网站并泄露了大量成员的个人信息。

匿名者又来了

```
FULL NEWS >> https://www.hackread.com/anonymous-world-trade-org-hacked-data-leak/

Target: ecampus.wto.org

We are here to hack and destroy your all systems.
We will not stop.
We will not give up.
We have enough rope to hang you and your puppets.
Expec us.

http://justpaste.it/kuoj
http://justpaste.it/kuou

irc.anonops.com PORTS: 6667 / 6697
webchat.anonops.com
Channel: #operationgreenrights
```

最近，匿名者成员大肆入侵了 WTO 的数据库、攻击以色列武器经销进口商并在#OpIsrael 计划中泄露大量在线客户端登录的数据。据统计，此次的入侵 WTO 事件波及到来自许多国家的成员，其中包括巴西、中国、法国、印度、印度尼西亚、巴基斯坦、俄罗斯、圣多明各、沙特阿拉伯、斯里兰卡、美国以及其他世贸组织网站的人员。

WTO 的无效安保措施

经过了解证实，匿名者通过利用一个简单的 SQL 注入来获取来自世界各地的访问者的个人资料。同时，尽管 WTO 组织认识到他们受到了攻击，但采取的系统安全保护措施却是无效的。

黑客告诉 HackRead：

“今天我已经两次破解并获取了超过 53000 的用户姓名、电话等信息，并且第二次的成功入侵还是在他们发现我攻击而变更系统之后。”

黑客从 ecampus.wto.org 下手，这个网站为世贸组织的国际贸易法律及其他与贸易相关事宜在线课程提供了平台。

irc.anonops.com PORTS: 6667 / 6697
webchat.anonops.com
Channel: #operationgreenrights

ecampus.wto.org

web server operating system: Windows 2008 R2 or 7
web application technology: ASP.NET, Microsoft IIS 7.5, ASP
back-end DBMS: Microsoft SQL Server 2012

database management system users [2]:
[*] sa
[*] usrwto_write

available databases [15]:
[*] distribution
[*] hretraining
[*] master
[*] mcabadge
[*] mcacommon
[*] mcacommon_201309120500
[*] mcamorestricted
[*] mcangopublic
[*] mcangorestricted
[*] mcapresspublic
[*] model
[*] msdb
[*] SSISDB
[*] tempdb
[*] WTO

世贸组织数据库泄露

泄露管理员信息

其中包括了管理员的姓名、电话、号码、传真号码、职务、电子邮件地址以及他们的登录凭据。同时，专家还发现了另外一个存储了大约 34 个管理员信息的数据表。

泄露候选人的信息

80 个候选人的姓名出生年月被曝出。但是专家表示有关于世贸组织挑选候选人（面试或相关活动）的方式尚没有任何消息。

泄露 WTO 内部官员和职员的信息

泄露的文档里包括了他们的全名、身份证、电子邮件、IP 地址、电话号码、职称/职务、国籍、使馆所在官员的姓名、邮政编码、上司姓名、使用语言以及注册号为 2100+官员和工作人员。

这几次由匿名者组织所泄露的的数据让我们看到了目前信息安全所受到的巨大威胁。

4.2.7 俄罗斯歌手上传爱国歌曲被黑客删除

5 月 3 日，俄罗斯人民演员、著名歌手奥列格·加兹马诺夫在 YouTube 上的账号被黑，黑客从他的网页中删除了其为卫国战争胜利 70 周年所作的爱国歌曲《前进，俄罗斯》，这首歌曲放到网上 2 天内就有 15 万人点击。

俄罗斯《共青团真理报》4 日报道，这是歌手加兹马诺夫首次遇到黑客袭击。他接受记者采访时表示：“早上，我的助手给我打电话称，我的网页被黑， 歌曲被删除。黑客攻击的目的就是为了删除这首俄罗斯爱国歌曲。这表明，这首歌曲刺痛了一些人，他们并不希望俄罗斯繁荣昌盛。为了将其献给 70 周年，我用近 3 个月时间写出这首歌曲。这首合唱歌曲呼吁人民团结起来对抗所有困难。‘俄罗斯’这一词语是力量和激情的体现，是对祖国表达的热爱之情。”目前，加兹马诺 夫的网页已经恢复，网民可以继续点击欣赏这一歌曲。

加兹马诺夫同时呼吁自己的粉丝们在社交网上广为传播这一视频，发给自己的朋友，以免再次被黑客删除。加兹马诺夫称自己已经报警，希望警方能够查 明这些黑客。对于这一事件，名为“客人”的网民称：“既然俄罗斯的敌人不喜欢这首歌曲，就表明了这首歌曲的力量。我们的精神力量已让敌人害怕了，希望俄罗斯人能听到更多这样的爱国歌曲。正像歌曲中所唱的，‘前进，俄罗斯!’让我们的国家强大起来。”

4.2.8 供电站爆炸促进能源部与安全企业之间的合作

4 月初，美国马里兰州一个电站发生爆炸，导致白宫、国会大厦和国务院停电。

据美国国家广播公司（NBC）报道，这次影响了 1 到 3 万人的电力中断是由于 230 千伏的输电线从支撑结构中脱落而造成的。事故导致了华盛顿特区的史密森尼博物馆和其他热门旅游景点被迫疏散游客。另外，华盛顿交通系统也在 13 个车站启动了应急照明。

这次使美国一些大型电力中心陷入黑暗的事故，充分表明了输电网络面对多种威胁的脆弱程度，其中就包括网络攻击威胁。电力缺失能在非常短的时间内造成灾难性后果。

过去几年中，很多报告和专家都证实美国电力网络对针对性攻击的敏感性。包括：

- 两位研究员在 2013 年秋天证实：超过 20 家厂商的关键基础设施网络控制产品中存在漏洞。一旦这些漏洞被利用，攻击者将能通过诸如让某变电站主服务器掉线的方法破坏电力输送。
- 2014 年 3 月联邦能源监管委员会（FERC）发布的一份研究报告称，遍布全国的 5.5 万座变电站中，攻击者只需要弄停其中不到 10 座

就能引发可持续 1 个月之久的大面积断电。FERC 在其报告中继续揭示道，目前还没有任何条例规程可以保护这些特殊的关键资产。

- 作为对今年早些时候消费者新闻与商业频道（CNBC）发表的一篇文章的回应，IT 安全公司卡巴斯基首席执行官兼创始人尤金·卡巴斯基阐述说；我们已经看到 对关键基础设施的针对性攻击在增多。他进一步警告道：在不久的将来，在其他目标之中，我们很可能会看到导致电网受到“非常明显的伤害”的事故。
- 最后，由《今日美国》和超过 10 家甘尼特集团（Gannett）旗下遍布全美的报纸和电视台进行的一项调查发现：2011 到 2014 年期间，美国电网经历了 362 次攻击，造成了电力中断和功率失调。大部分攻击案例中，攻击者从未被确认。

美国能源部目前正在努力缓解此类威胁及其他隐患。根据最近福克斯新闻网刊登的一篇文章，国家高级能源官员已斥资 45 亿美元进行美国电力网络现代化改造，其中包括对遭受网络攻击时保证关键电力设施运转正常的 1 亿美元专项拨款。

所有这些努力已经对去年由公共事业部门报告的漏洞数据起到了一些正面影响。

《2015 威瑞森数据泄露调查报告》列出的 2014 年近 8 万起安全事件报告中，公共事业部门仅占 73 起。这一数字的下降很有可能是

因为攻击者通常是奔着钱财进行攻击活动的，比如盗取信用卡数据或是占据关键数据索要赎金。

即使如此，就算利益驱动的黑客没什么动机去攻击关键基础设施，国家操纵的高端黑客组织也会以关键基础设施攻击目标。像电力网络这样的公共事业设施，会被国家黑客和恐怖分子黑客所青睐。

因此，公共设施企业需要承认计算机安全对于防卫关键基础设施的重要性。这意味着要在他们的商业模式中引入一套不同的理念体系。当涉及到工业控制系统，承认网 络安全的重要性日益增加意味着要从以合规为中心积极转变到以安全为中心。安全性是可靠性的一方面，网络安全的缺失将造成同样不利的影响。

企业或机构能够转为以安全为核心的一种方法就是威胁情报。

为防备未来的攻击，公共事业部门应该分析今天的攻击模式，并运用威胁情报技术监测它们怎样随时间变化。不利用威胁情报的组织无异于将巨大的优势交到敌人手里，而这是他们所无法承担的损失。这些公司可以与其他公共事业公司共享自己的分析结果，更普遍地保护能源产业。

而信息安全专业人士应该努力扩展安全技术以支持工业控制系统和它们支撑的基础设施，也应该支持并促进公共设施和其他工业控制系统用户的信息共享工作。

很明显，美国电力网络因为针对性攻击而受到断电的威胁。这一威胁也因此促成了公共事业公司与能源部、与信息安全专家相互之间的合作，以应对明天的安全挑战。

4.2.9 FAA 发警告：波音 787 客机存软件缺陷 可导致飞机失控

联邦航空管理局（FAA）已经向波音的 787 梦想客机发出警告，称飞机系统中的软件错误可能 会引发飞机在半空中关闭所有电源，从而导致飞机失去控制。FAA 警告称:“我们通告了这个适航指令(AD)来防止所有 AC 电源突然失效情况的再次发生，这 可能会导致飞机在飞行过程中失去控制。”

根据实验室测试结果显示，梦想客机的发电机组在每隔 248 天（大约 8 个月）的时候就会失效进入 failsafe 模式，在经过连续多天的持续电力使用之后，客 机上的所有四个发电机就会同时停止运作。如果当时恰好处在飞行状态或者起飞或者降落状态，极有可能会酿成事故。所幸的是解决该问题的临时解决方案就是定期 的关闭电源系统。

4.2.10 垃圾邮件恶意程序已感染数千台 Linux 和 FreeBSD 系统服务器

反病毒提供商 Eset 最新公布的 23 页安全报告中 指出，在过去 7 个月间数千台基于 Linux 和 FreeBSD 操作系统系统的服务器感染了名为 Mumblehard 的恶意程序，并悄悄的利用服务器的部分资源用于发送垃圾邮件。在过去的 7 个月内，在监测的其中一个指令和控制渠道，连接了 8867 个独立的 IP 地址，而其 中 3000 个是在过去三周内添加的。

Mumblehard 是由经验丰富、高度熟练的程序员所开发，包含后门和垃圾邮件的守护进程，通过后台进程发送大批量的垃圾邮件。该恶意程序是通过 Perl 编程语言所编写，有 两个重要组件且都在定制的“包”中进行封装，通过低级编程语言通过自然机器代码来调用硬件资源。安全研究员表示，恶意软件还具有通用代理的 能力，只跟监听套接字上的命令及控制服务器通信。可在一个白名单上添加多个主机。

关于安恒信息

杭州安恒信息技术有限公司(DBAPPSecurity)是由国家千人计划专家范渊先生于 2007 年创办，是国内跻身全球网络安全 500 强仅有的四家企业之一，是中国领先的专注于信息安全产品和服务的解决方案提供商。曾先后为北京奥运会、国庆 60 周年庆典、上海世博会、广州亚运会、深圳大运会、首届世界互联网大会等重大活动提供全方位信息安全保障。

公司主营业务涵盖应用安全，数据库安全以及云计算安全、移动互联网安全、大数据安全等智慧城市安全，包括顶层设计、标准制定、课题和安全技术研究、产品研发、产品及服务综合解决方案提供等。

安恒信息通过“智慧监测、智慧防护、智慧审计、智慧应用”四大产品线形成一整套全生命周期的信息安全支撑体系，成为应用安全、数据库安全以及智慧城市安全市场的绝对领航者。是政府军工、公检法司、运营商、金融能源、财税审计、教育医疗、互联网+等行业信息安全领域最值得信赖的首选品牌！

安恒信息官方微信公众账号

关于安恒信息

您也可以下载中国信息安全测评中心和安恒信息联合开发的 E 安全 app 获得最及时的安全资讯、预警信息及风险威胁指数等等。

E 安全是一款面向安全从业人员和安全技术爱好者提供的免费 APP 内容分发平台，这里有最新的信息安全资讯资讯、最及时的威胁预警、最专业的信息安全课程教学、最全面的信息安全资料分享。以“掌握信息安全的专家”为宗旨，E 安全致力于帮助安全从业人员和安全技术爱好者利用碎片化时间随时在线学习信息安全技术课程，满足多层次的信息安全移动在线培训需求。同时还可以及时获取各类安全威胁预警和全球最新安全动态，为信息安全专业人才的成长提供一个更为便捷和高效的一站式成长平台。

扫描二维码进行下载