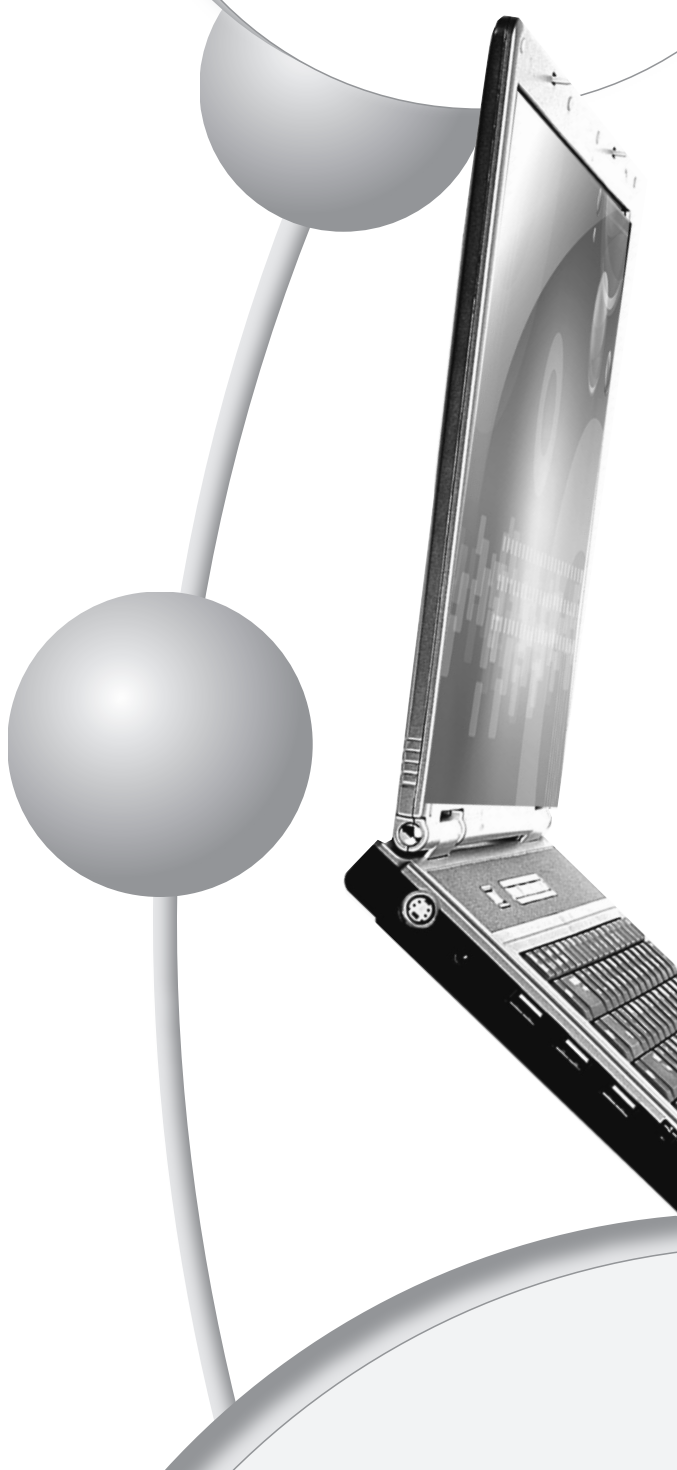
■ 本版撰文 本报记者 徐 淼 霍玉菡 杨 颖

编者按：近几天，细心的用户可以发现，不论是打开邮箱、微博，还是登录社交网站、聊天工具，总会出现更改密码或者增加密码安全设置的提示，这是各网络运营商对自己网站安全漏洞的一次全力补救，也是互联网安全攻防进步的一个契机。2011年年底出现的“泄密门”事件让各界对网络安全的重要性有了一个全新的认识。

在互联网时代，各种账号不仅是用户进入相关网站的钥匙，也与用户的生活息息相关，甚至在一定程度上捆绑着用户的财产安全。保护各种账号已经成为维护互联网安全的重要组成部分，网站、用户、监管机构均有责任。



“泄密门”暴露网络安全隐患 网民直呼“伤不起”

近日，让互联网裸奔的“CSDN泄密门”事件传出最新消息，两名涉案黑客已经被公安部门抓获。不过，由于仍有部分人员尚未落网，北京市公安局外宣处工作人员表示，具体案情尚不便向外界透露。至此，该信息泄露事件终于“拨云见日”。

据悉，自2011年12月21日技术网站CSDN上600万用户资料被公开开始，大量网站陆续被曝出存在用户数据泄露问题，事态蔓延极其迅速，影响甚广。来自国家互联网应急中心（CNCERT）的统计数据显示，截至2011年12月29日，被外界怀疑泄露的数据库已达26个，涉及账号、密码2.78亿条。

尽管各相关网站在事后纷纷出面澄清，但网民还是担心数据泄露会让用户个人信息、社交生活、财务资料全部暴露。而此后，“你的密码改了吗？”也成为岁末年初网民间最流行的问候语。

明文密码引发危机？

去年12月21日，CSDN在公告中表示，泄露密码库系2009年CSDN作为备份所用，目前，尚未查明泄露原因，已向公安机关报案，公安机关也正在调查相关线索。不过，不少网民却对此表示质疑，其中，最大的疑问源于CSDN明文存储密码的做法。

一些网友表示，如今，互联网账户中所包含的信息已经越来越重要，不少信息甚至涉及用户个人财富安全，然而，由于大部分互联网企业对用户信息保护比较轻视，相关信息并没有得到很好的保护。这次CSDN数据泄露事件固然有黑客之过，但没有对用户信息安全进行加密设置的网站，也难逃干系。

“网站只有明文密码不设置二层保护，就意味着只要能打开数据库文件，用户信息就唾手可得。”中投顾问IT行业研究员王宁远表示，“明文密码泄密确实可以说是导致此次密码泄密案件的主导因素。”

近年来，随着中国互联网经济的快速发展，争夺用户已经成为各网站的重要竞争内容。为了节省用户时间，让用户体验更为顺畅，许多网站都简化了注册和登录过程。然而，在大方招揽用户上门的同时，各网站的用户数据保护工作却进展甚微。王宁远认为，部分互联网企业在安全防范问题上过度松懈，确实使黑客有机可乘，客观上为偷窃者提供了便利。互联网泄密应直接追究相关企业的责任。

业内人士透露，互联网企业要建立自己的安全运营团队，必须投入大量资金。据介绍，一个大型B2C购物网站每年的安全投入高达千万元。因此，对于一些企业来说，用户安全是花钱但不产生收入的“亏本”买卖。此次“泄密门”事件的发生，也算是为中国的互联网企业敲响了警钟。

王宁远指出，目前，除了密码问题外，钓鱼网站、虚假广告、关联搜索真实性、网站木马、不正确的价值观导向、网络管理盲点等，均是中国互联网产业需要注意的问题。互联网市场要想求得长远发展，必须加强机制监管与企业监管力度。

网民唏嘘

“CSDN泄密门”事件被曝出至今，已经过去20多天了，到底这场“泄密风暴”波及多少网民的利益，目前无法确切统计，但泄密事件还是让不少网民唏嘘不已。一些网友指出，“泄密门”给了我们一个警告，那就是，不仅要关好家里的门，更要为自己的网络加上“防盗门”。

此后，网上也掀起了一场密码设定方法的大讨论，一些网友还晒出了自己的密码设置技巧。其中，网友“怎样科学养猪”的密码设置方法十分有趣。该网友调侃称，自己看似复杂的密码“ppnn13%dkstFeb.1st”，其实很简单，只要记住密码谐音“娉娉袅袅十三余，豆蔻梢头二月初”就能轻松“hold ”住。

不过，巧妙的密码设置只是用户维护自身网络安全的途径之一。王宁远提醒，个人用户还应该尽量减少设置重复密码。此外，虚拟不重要的个人信息等行为也能够在一定程度上有效降低个人信息泄密的风险。

易观分析师张萌则建议，网络支付用户还应该提高风险防范意识，养成良好的电脑和网络使用习惯。用户在使用电脑的过程中，应安装必要的杀毒软件并对系统定期升级，在网购过程中也要提高警惕，做到不轻易接收和点击陌生人发送的图片和链接。

网站反省

当然，除了网友要加强“防盗”意识，各网站也必须承担起保护用户信息的重任。王宁远告诉记者，由于企业的防范方法存在问题而导致用户个人信息泄露，企业也将承担相关风险。保证客户资料安全是互联网企业必须达到的运营要求。

据业内人士介绍，只要网站增加验证码流程就可以在一定程度上提升网站的安全性，但这会影响用户体验，可能会流失部分潜在用户。所以，很多中小网站，甚至一些大中型网站，都不重视网站安全。但实践证明，随着网络技术发展的不断深入，网络信息安全对市场的持续发展将起到越来越重要的作用。

虽然国家互联网应急中心的通报表示，此前能够确认的数据泄露情况只发生于CSDN与天涯两个网站，其他数据库被公布的“泄露信息”只有部分属实，但“泄密门”也为公众网络信息安全防护敲响了警钟。专家指出，由于行业准则缺失，大部分企业需要从最基本的信息加密、长期安全保护做起，逐渐达到保护用户信息安全的目的。

“从企业来看，应做好安全保护和信息安全技术共享措施，再辅以建立安全保护联盟，巩固安全防卫手段，不断降低泄密风险。”王宁远说。

张萌也提出，第三方支付厂商应该加强安全生态产业链合作，培养用户对网络支付安全的信心。“第三方支付厂商在网络支付安全建设过程中，应最大范围地加强与安全生态系统厂商间的合作，并从安全宣传、安全承诺等方面增强用户的网络支付安全信心，以促进整个第三方网络支付行业的发展。”他说。

新商业模式或将出现

据报道，“泄密门”发生后，已经有不少网站开始主动联络安全厂商，讨论提高网站安全防护能力等问题，这对中国互联网市场来说，无疑是一个良好的信号。

经过此次事件，各方对网络安全将有更深刻的认识，未来，无论是信息安全投入，还是行业自律、流程规范，都将得到强化，互联网信息安全也将有机会随之提高，更多提升用户信息安全的新商业模式将陆续出现。

据报道，目前，新浪、腾讯、支付宝等大网站都已经在各自联合大量合作伙伴推广OPEN ID。通过这一服务，用户只需要记住一个统一的账号和密码，就可以同时登录多家网站，但是其账号、密码等信息，只存储于核心企业的数据库中，这既减少了用户记忆密码的难度，也因为可以集中保护，降低了数据泄露的风险。

而在2011年8月，金山网络也推出了新的业务“网购敢赔”，承诺只要金山毒霸2012用户开启网购“敢赔模式”，如果网购仍感染木马或登录钓鱼网站遭遇财产被盗，金山网络将进行上限500元的现金赔付。

这些商业模式的出现是相关企业对保障用户信息安全的探索。未来，相关企业对安全防护业务的投入将不断加大，相信，这也将催生更多新的商业模式，用户将享受到更加完善的服务，整个互联网产业的信息安全状况也将大大提升。

谁动了我的网络财产？

在银行设置密码，在家里安装防盗门、防盗窗，甚至动用保险柜来保证财产安全，你的财产就能真正安全了吗？

现在，几乎每个人都有大把的账号，并通过其进行工作和情感交流、购物，甚至是缴纳一些费用。这些账号一旦被盗用，其损失将难以用金钱衡量。

设想一下，如果有一天，喜欢上网聊天的你，再也登录不上QQ账号，联系不上好友，花费很长时间得到的“小太阳”也付之东流，你会有多抓狂？据了解，不少网友都有过账号被盗的经历。看到自己的账号变成黑客敛财的工具，网友都相当气愤，先不说存不存在财产损失，个人信息泄露带来的问题就有一箩筐。

或许，你还喜欢玩网游。可是，如果某一天，当你发现之前纠集众多好友、“牺牲”数次才从BOSS手中得到的终极装备被别人高价卖出时，你会有多纠结？

近年来，网络游戏产业高速发展。网络游戏蕴含的巨大利润，不仅成就了陈天桥、史玉柱的事业传奇，同样也成就了黑客的庞大帝国。如今，网络游戏已经成为黑客和病毒侵害的重灾区。基于网游虚拟市场的暴利诱惑，网游中的盗号行为日益猖獗，盗号灰色产业链已初步形成。

近年来，虚拟交易日益频繁，公民财产也不再具象化。如何保护个人网络财产，已经成为各界必须关注的重要问题。

业内人士指出，未来，各网站应该在保护用户网络安全上投入更多精力。而第三方网络支付的安全建设经验很值得相关企业学习。根据易观智库最新发布的《中国第三方网络支付安全调研报告》显示，第三方支付厂商重视支付安全建设，整体安全情况良好。“以支付宝为例，其良好的安全状况得益于银行、IT安全厂商、商户等网络支付安全生态系统各环节的共同努力，其在加强安全产业合作方面的经验值得业内厂商借鉴。”易观分析师张萌说：“同时，支付宝针对网络支付安全提出的‘快捷支付72小时全额赔付’承诺，也在一定程度上增强了用户对网络支付安全的信心，值得其他支付厂商学习。”

此外，此次“泄密门”事件也提醒我们，国内相关法律法规还不够完善。国家应尽快立法，从权利保护、责任认定、责任追究和法律保障上对个人信息安全予以保护，将个人、网站和监管机构应当承担的责任、义务厘清。与此同时，个人用户也要自觉提升网络安全意识。与其担心隐私被泄露，不如趁早下手，养成良好的上网习惯，要明白只有重视虚拟财产及隐私，才能保障网络财产安全。

2011年，中国互联网以“泄密门”作为终结，2012年，我们希望中国网络能够找到可靠的“门卫”。