电子邮件安全

电子邮件安全

近年来，作为一种通讯方式,电子邮件不断快速发展。电子邮件用户和公司所面临的安全性风险也变得日益严重。病毒、蠕虫、垃圾邮件、网页仿冒欺诈、间谍软件和一系列更新、更复杂的攻击方法，使得电子邮件通信和电子邮件基础结构的管理成为了一种更加具有风险的行为。电子邮件的安全越来越受到重视。

电子邮件安全现状

垃圾邮件对电子邮件的效用造成了严重影响。垃圾邮件泛滥程度不仅广泛，而且引发的损失可谓惨重。例如美国民主党总统候选人奥巴马和希拉里也被滥用于一些垃圾邮件中，以欺骗人们泄露他们的私人信息、购买药品股份和哄抬股票价格。但是一些用户把大多数反垃圾邮件技术评定为失败这种等级。

- 恶意垃圾邮件汹涌 Srizbi 僵尸网络作怪
- Gmail 验证程序遭破解 垃圾邮件汹涌
- 最新垃圾邮件利用 Google Docs
- PDF 垃圾邮件隐身半年 再度出现！
- 垃圾邮件无孔不入：奥巴马、希拉里被利用
- 垃圾邮件及网络钓鱼攻击手段越来越高明
- 垃圾邮件日趋复杂 雇员错误继续增长
- 用户对大多数反垃圾邮件技术都不满意

电子邮件安全保护技术和策略

针对日益泛滥的垃圾邮件，可以使用“鸡尾酒”疗法；那么针对病毒、蠕虫、网页仿冒欺诈、间谍软件等一系列更新、更复杂的攻击方法，电子邮件的安全应该如何保障呢？

- 垃圾邮件的“鸡尾酒”疗法
- 网络邮件安全:保护数据的最佳做法
- 内部邮件如何通过企业防火墙
- 如何配置具有 SSL 保护的 FTP 服务器？
- 网络配置：IIS SMTP 邮件中继服务

电子邮件加密

除了上述的方法，加密也是保护电子邮件安全的一种手段。尤其在企业中，通过加密包含公司机密的电子邮件，就不用担心机密信息被拦截以及数据被窃取的可能了，来自竞争对手的风险也会减小。另外，在一个这样的时代，顾客们同样希望自己的私人资料受到保护，而加密通信就能确保客户的私人数据不被窃取。电子邮件加密不是万能药，然而它有能力保护关键数据的安全性。

- 五个步骤成功加密电子邮件
- 通过 SSL 发送的电子邮件是否需要加密？
- 最差做法 加密失误

恶意垃圾邮件汹涌 Srizbi 僵尸网络作怪

Marshal 的研究人员说，这个月恶意垃圾邮件急剧上升可以归因于 Srizbi 僵尸网络。垃圾邮件中对用户电脑的影响的恶意软件是过去一周的三倍，从六月初的 3%提高到接下来几个星期的 9。9%。

Marshal 称，Srizbi 僵尸网络目前正在产生垃圾邮件，企图欺骗用户点击邮件主题中邮件地址的第一部分，这一部分暗示他们可以看到愚蠢的视频。它还欺骗 Classmate.com 服务，主要是通过利用邮件中 Classmate.com 的错误网页的链接，引导他们运行 Flash 视频播放器。当用户点击链接的时候，就会提示他们下载会影响到计算机的可执行文件。

Marshal 的 TRACE 团队的威胁首要分析师 Phil Hay 把 Srizbi 僵尸网络称为“今天对互联网用户最大的威胁之一”。Marsha 说僵尸网络应该对 46%的垃圾邮件负责任。

(作者：Marcia Savage 译者：Tina 来源：TechTarget 中国)

Gmail 验证程序遭破解 垃圾邮件汹涌

安全厂商 MessageLabs 的一份报告称，黑客利注册了大量随机 Gmail 帐号，并利用这些帐号通过绕过谷歌防止恶意注册验证程序大肆向用户发送垃圾邮件。

MessageLab 二月底监视了谷歌 Gmail 中大量的垃圾邮件。该公司的高级反垃圾邮件技术专家 Matt Sergeant 说，垃圾邮件的大量增加说明黑客们已经发现了绕过 CAPTCHAS (Completely Automated Public Turing Test To Tell Computers and Humans Apart)验证程序的方法，CAPTCHAS 验证程序时为了确认自动登录信箱时确实有人申请使用帐户。

Sergeant 说，雅虎和 hotmail 等也在使用 CAPTCHA 验证程序，如果黑客确实找到了破解这一程序的办法，那就意味着整个互联网的一次危机。

他说：“如果黑客解决了 CAPTCHA 验证程序的问题，事情就糟糕了，因为很多的站点都使用它来抵制垃圾邮件保护站点安全，”另为值得注意的是很多恶意人士喜欢把 google 这样的大公司当作保护伞，他补充说：“不能把 Gmail 或者 hotmail 放入黑名单，因为还有那么多合法邮件都是通过他们的。如果这些他们的油箱被禁用了，大家都会很困扰，所以现在大家不得不过滤邮件内容，而这要比禁用一个 IP 地址难得多。”

他们又两个绕过 CAPTCHA 验证程序的办法。黑客可以利用 mechanical turks 的服务，这些人可以手动创建帐户或者利用一个软件界面来破解 CAPTCHA 验证程序。或者这些恶意人士可以编造一个自动寻找 CAPTCHA 验证程序漏洞的算法。Sergeant 说，一旦获得了合理的准确度，以算法为基础的攻击就是可以扩展的。

MessageLabs 的研究表明，这些算法的成功率在 20%到 30%。把这些算法和僵尸网络的计算功率结合在一起，黑客就可以随心所欲的创建 email 帐户。他们还可以利用 mechanical Turks 把不同的方法结合在一起，在扩展数据库时首先破解 CAPTCHA 验证程

序，并且解决发展中算法的培训、测试和调节问题。随着成功率的上升，黑客可以减少或者降低利用昂贵的 mechanical Turks 的利用，转向以僵尸网络为动力的操作。

最新分析表明，上个月，使用雅、Hotmail、MSN 和谷歌的网络邮件为基础的服务发送的垃圾邮件占所有垃圾邮件的 4.2%，比一月份降低了 1.5%。在这组数据中，雅虎被滥用最严重，但是研究院也发现从一月到二月谷歌的垃圾邮件也翻倍了。这些垃圾邮件的进一步分析表明这些垃圾邮件都连接到成人娱乐内容网站。

Sergeant 说，他的公司一直都和大型搜索引擎保持联系。“谷歌非常重视这件事，并且正在研究。” 他说，“如果检测到可疑内容，他们可以尽快禁用这些账户，但是僵尸网络、垃圾邮件可疑从不同的地方登录，这个问题比较难解决。”

谷歌的发言人 Megan Lamb 在一封邮件中说：“在我们的服务项目中，使用 Gmail 发送垃圾邮件违背了程序政策。我们立即禁用了这些账户，如果他们继续扩散，我们还会这么做。”

(作者：Bill Brenner 译者：Tina 来源：TechTarget 中国)

最新垃圾邮件利用 Google Docs

垃圾邮件研究人员发现利用 Google 基于 Web 的文字处理器的不必要信息的运行，这些信息甚至使用 Google 的分析工具测试他们的行为。

信息试验室发言人 Matt Sergeant 说，这些信息都成功的通过了大部分企业的邮件过滤器。这些信息不包含内容，只有一个链接，把收件人带到 Google Docs 文件。一旦打开文件，就会有大量太过熟悉的内容欺骗进入垃圾邮件的活动。

Sergeant 说：“这是垃圾邮件发送者发现的影响经过基本加固的站点另外一种方法，”

Google 已经标出了显示为垃圾邮件的主机文件。Sergeant 对 TechTarget 中国的特约记者说，有个好消息是，Google Docs 仍然处于幼年期，所以在企业中使用的人数还不多。

到现在为止，这些信息的数量还不多，但是也足够引起信息试验室的警惕了。

（作者：Robert Westervelt 译者：Tina TechTarget 中国）

PDF 垃圾邮件隐身半年 再度出现！

有些安全研究人员还正为去年夏天 PDF 垃圾邮件几乎销声匿迹而纳闷。不过现在，至少有一家公司 MX Logic 称它正在追踪这种不请自来重新出现的垃圾邮件。

MX Logic 公司的威胁管理总监 Sam Masiello 说，PDF 垃圾邮件占上周全球垃圾邮件的比例不到 0.5%。但是，他说 PDF 垃圾邮件的重新出现，意味着制造垃圾邮件者可能正努力测试该文件格式能否逃过某些垃圾邮件过滤器的检查。MX Logic 位于美国科罗拉多，是一家反垃圾邮件和运营管理服务的厂商。

“这可能是有的人在测试市场，或者是暴风雨之前的平静，”Masiello 说，“通常而言，较小的本地化攻击被检测到的可能性比较小，但是，现在这种情况，很明显邮件的主题就很可疑。”

根据一些安全研究人员的看法，去年七月份出现的 PDF 垃圾邮件是 Storm 木马的一种变种。PDF 文件格式在企业中广泛应用，所以，这一新方式的出现，引起了安全研究人员的关注。垃圾邮件过滤厂商快速地开发了一种检测不想要消息的方法，帮助决定什么是合法的 PDF 文件。在发现 PDF 垃圾邮件的一个月内，安全公司说该文件格式的垃圾邮件几乎销声匿迹。

之前的 PDF 垃圾邮件包含炒股诈骗的内容。上周发现的 PDF 垃圾邮件很容易检测到，因为多数垃圾消息里通常包含各种药物的广告。多数公司判断该 PDF 文件是否合法，不存在困难，Masiello 说。

Masiello 认为，除了 PDF 垃圾邮件，Storm 仍然继续占领大部分的不想要消息市场。两周前出现的 Storm 变种“情人节”攻击收件箱。Storm 的情人节消息包括一个恶意 URL。SANS 互联网风暴中心的研究人员称，如果收件人点击 URL，就会下载一个可执行文件并受到感染。

Masiello 说，垃圾制造者同时也转向更为隐秘的感染方式。这个月早些时候安全研究人员发现 MBR（主引导记录）rootkit，据称它通过运行自己的代码悄悄地改写 MBR 来获得系统的控制权。主引导记录是电脑硬盘上分区存储的一个重要部分。

Masiello 说，2008 年通过垃圾邮件发出的恶意代码，较早地显示了攻击者除了利用 Zombie machinesPill 垃圾邮件、病毒和股票欺诈，还利用混合型威胁，诱骗并感染不加防范受害者的进一步趋势。

“我想，这种混合型的模式部分还在萌芽期，因为人们受到感染的方式仍然继续在发展中，”Masiello 说，“现在，用户无需访问恶意网站，或者打开文件附件，就会被感染。”

相关介绍：来自 Storm 木马的“情人节快乐’

情人节虽然未到，但这丝毫阻止不了 Storm 木马利用节日主题诱骗用户下载恶意软件的行为。

SANS 互联网风暴中心的网站介绍了 Storm 电子邮件的另一波攻击，邮件的主题设计尽量吸引收件人的注意，邮件的内容只有一个包括 IP 地址的 URL。只要用户访问这个网站，就会看到一个漂亮的页面以及一个下载可执行文件的链接。类似下图：

Your download should begin shortly. If your download does not start in 10-20 seconds, you can click here to launch the download and then press Run. Enjoy!

TT 中国专家建议一如既往：不要点击来自你不熟悉和不信任的 URL 和邮件附件！

（作者： Robert Westervelt,Bill Brenner 译者：Shirley 来源：TechTarget 中国）

垃圾邮件无孔不入：奥巴马、希拉里被利用

最近，民主党总统候选人奥巴马和希拉里被滥用于一些垃圾邮件中，以欺骗人们泄露他们的私人信息、购买药品股份和哄抬股票价格。

“总统侯选人本身就是一个众所周知的品牌。很多人都收到了这些合法的电子邮件，”赛门铁克的反垃圾邮件工程组分析师 Dermot Harnett 说：“这样，受害者将更可能会打开这些邮件并点击链接。”

2 月份，垃圾邮件发送者散发虚假链接希拉里•克林顿视频，其中隐藏着恶意特洛伊木马。赛门铁克还称，含有希拉里名字的网址也被用于淫秽和“伟哥”的垃圾邮件。

共和党竞争者也未能避免这一现象。最近已退出竞选的迈克•哈克比和麦凯恩也一直是某些垃圾邮件的利用对象。但是 Harnett 说，垃圾邮件发送者主要利用的是奥巴马和希拉利之间的激烈竞争。

垃圾邮件活动过去是商家垃圾邮件报告的一部分，现在受到了赛门铁克的追踪。赛门铁克公司表示，过去的两个月内垃圾邮件率总体稳定在 78.5%，与 2007 年上半年的 61%相比，还是呈上升趋势。

假期是购物的高峰季节，通常垃圾邮件也会达到高峰，这段时间过后垃圾邮件率会稳定下来。Harnett 说，垃圾邮件活动也会达到市场饱和状态。

他还说到：“尽管垃圾邮件率已经稳定下来，但是巨大数量的垃圾邮件还是会给系统资源带来很大压力。”

由于总统候选人本身就是品牌，垃圾邮件发送者也抓住这些传统的名字不放。美国西南航空公司最近就遭遇了品牌抢夺。赛门铁克公司称，他们已追踪了相当数量的垃圾邮件。在这些邮件里，如果注册成功并完成一份调查问卷就送两张机票。

“这些邮件的目的是收集私人信息，这种方法很成功。” Harnett 说，“垃圾邮件发送者们屡试不爽。”

垃圾邮件发送者还会不断试用不同的手段去欺骗安全厂商的反垃圾邮件引擎。据反垃圾邮件管理服务供应商 MX Logic 公司透露，PDF 格式的垃圾邮件似乎在 1 月份再次出现。赛门铁克公司表示他们将继续追踪 PDF 格式的垃圾邮件，不过只是在很低水平上的追踪，这可能标明垃圾邮件发送者在探查反垃圾邮件厂商侦测虚假信息的能力。

“我们通常所看到的只是垃圾邮件爆发前的一个小测试，接着才会是铺天盖地的垃圾邮件，”Harnett 说，“现在我们有适当的措施阻止这些信息。”

今年二月，赛门铁克启动了反垃圾邮件网站，反垃圾邮件工程师将会在网站上共享他们进行的研究并报告他们的新发现。

(作者：Robert Westervelt 译者：涂凡才　来源：TechTarget 中国)

垃圾邮件及网络钓鱼攻击手段越来越高明

虽然 Botnet 在最近几个月引发了大量的垃圾邮件，但是，安全研究人员更警惕的是垃圾邮件的高级水平。安全人员警告说，有针对性的钓鱼攻击正在进入企业电子邮件服务器。

纽约 MessageLabs 公司的首席安全分析师 Mark Sunner 说，垃圾邮件已经达到了我们通常所说的商业级产品的水平。我们已经看到了这种活动的变化。现在，Botnet 发出大量单独的垃圾邮件。

根据 MessageLabs 的统计，去年 11 月份全球垃圾邮件的通信量已经增长到了占全球电子邮件通信量的 90%。这个百分比预计在今年 12 月份将继续保持下去。此外，这家公司报道说，在 200 封电子邮件中有一封电子邮件包含钓鱼攻击的内容。MessageLabs 指出，最近拦截的恶意电子邮件中，有 68%以上的恶意邮件是钓鱼攻击邮件，比过去的几个月增长了。

安全研究人员预计，2007 年将是攻击的高级程度发展到惊人的水平的一年。Sunner 说，坏分子将搜索 MySpace 等社交网络网站，窃取地址、地区号码和其他身份数据以便使钓鱼攻击电子邮件让受害者看起来像真的一样。

Sunner 说，在许多情况下，坏分子可能使用银行的地址，让受害者以为电子邮件是从银行发出来的，从而使钓鱼攻击获得成功。这些坏分子将抢劫大型社交网络团体的数据库，利用垃圾邮件成功地实施攻击。

安全公司赛门铁克的高级工程经理 Alfred Huger 说，每一天发生的钓鱼攻击的企图高达 700 多万起。他说，不成熟的钓鱼攻击已经显著增加到了每天 900 起以上。

Huger 说，攻击者将从住在同一个地区的人们那里收集电子邮件地址。然后，攻击者向受害者发出一封钓鱼攻击电子邮件。这种电子邮件表面上看好像是从那个地区的银行或者其它金融机构那里发来的。进入到 2007 年，Huger 预测，钓鱼攻击将变得更加有针对性并且更难发现其欺骗性。

Huger 说，可信赖的因素非常高，人们更容易成为这种攻击的猎物，因为人们想不到自己的银行会参与这种事情。

Huger 表示，随着具有电子邮件和其它消息功能的手机的应用，使用短信实施的钓鱼攻击在 2007 年也将增长。他说，我们的手机现在已经成为微型的计算机，任何在台式电脑上发生的事情都可能对我们的手机产生影响。一些企业已经开始制定有关移动设备使用的政策，还有一些企业没有制定这种政策。中间地带并不大。

企业和消费者能够采取基本的措施进行反击。金融机构将改善身份识别功能和加强教育的努力，以便帮助客户理解他们的银行什么时候将与他们进行合法的联系。消费者可以向赛门铁克反钓鱼攻击网站举报钓鱼网站以便与网络诈骗作斗争。

Rootkit 在增长

攻击者在 2006 年更广泛地应用 rootkit 技术。这种技术的应用在 2007 年将继续增长。rootkit 是一种软件工具集，能够让网络管理员访问一台计算机或者一个网络。一旦安装了 rootkit，攻击者就可以把自己隐藏起来，在用户计算机中安装间谍软件和其它监视敲击键盘以及修改记录文件的软件。虽然微软发布的 Vista 操作系统能够减少某些 rootkit 的应用，但是，rootkit 的使用在 2007 年将成为标准。据赛门铁克称，用户模式 rootkit 策略目前已经非常普遍。内核模式 rootkit 的使用也在增长。

Huger 说，rootkit 是一种功能更强大的工具。我们将看到更多的 rootkit，因为安全产品正在变得越来越强大，攻击者不得不提高赌注。

(作者：Robert Westervelt 来源：TechTarget 中国)

垃圾邮件日趋复杂 雇员错误继续增长

Michael Kessler 目睹了网络犯罪的最差状态。这位计算机取证专家及会计舞弊调查员帮助研究各种案例，反对儿童色情作品，并揭露令人震惊的会计实务背后的故事。

但是，让 Kessler 晚上睡不着的并非那些典型的罪犯。

像其它拥有远程雇员和大量垃圾邮件的公司一样，Kessler 尽力阻止恶意软件感染系统。他说，他的网站 investigation.com 经常遭受攻击。他最近购买了一份保险，希望能够在经济上分担数据安全泄露带来的风险。

Kessler 说：“你可能拥有合适的最佳方案，但我们在很多案子中发现引起你今天所见问题的不是计算机错误，而是人为错误。”

Kessler 见证了计算机犯罪 35 年以上的发展历程。Kessler 曾担任纽约市财税部门的主调查官，随后于 1998 年创立了自己的计算机调查公司 Kessler International。他还担任过纽约市税务犯罪局的主管，纽约大都会捷运局的副检查官，以及纽约州特别检查官的助理审计员和调查员。

Kessler 认为，现在几乎每个人都会受网络犯罪的影响。有一项最新报告支持 Kessler 的论断。根据 Cisco 公司旗下 Ironport Systems 的最新报告，07 年全球垃圾邮件的数量成倍增加，达到了每天 1200 亿封。随着垃圾邮件制造者开始给雇员发送看似合法实际旨在传播恶意软件、窃取敏感信息的邮件，这些邮件变得越来越先进。

Ironport 产品部经理 David Mayer 说：“我们曾认为，垃圾邮件制造者一个个都是爱因斯坦，因为他们采用不同的方法，仅运用一种文件类型来包装他们的信息，不过从六月份开始，他们从一种文件类型转向三至四种不同文件类型。”

Kessler 认为，只要有利可图，垃圾邮件永远不可能完全受到控制。

“这是一场猫和老鼠的游戏。” Kessler 说，“只要供应商研制出合适的技术，这些坏家伙就能将它找出来，同时想出破坏这种技术的方法，或者只是简单地开发出一种技术，用以反对生产商。他们总是能够领先一步。”

为保护 Microsoft Outlook Web Access 免受黑客攻击，Kessler 采用了总部位于加拿大安大略省的 Messageware 公司的技术，以保护知识产权，终止非活动进程。但是他采用的一些技巧技术性不强。例如，他利用企业内部软件拦截垃圾邮件，然后一名员工每天负责从清除邮件中挑出合法邮件。

“在我们公司，需要谨慎选择我们拦截垃圾邮件的方法，” Kessler 说，“我们经常与贷款公司做生意，并处理儿童色情事件，所以我们不能仅仅根据指定单词判断邮件，这样的话可能许多合法邮件也会遭到拦截。”

Messageware 公司总裁兼 CEO Mark Rotman 认为，电子邮件信息传递导致敏感数据丢失的风险在大大增加。Rotman 说：“我认为你得先看看现在的邮件内容——如果你是 CFO，你会收到别人发给你的财务初稿；如果你在法律公司上班，你就会得到案子相关信息；如果是一个发展团队就可能获得下一代产品的计划。现在，邮件是一种商业活动，你必须认真对待。”

位于密歇根州 Elk Rapids 的 Ponemon 研究机构发表了一项最新报告，报告发现数据损坏成本已增长到每条记录 197 美元，分别比 2006 年和 2005 年增长了 8%和 43%。数据泄漏的风险增长如此之多，以致于 Kessler 购买了保险，希望能支付数据通告和诉讼案件的成本。

“像我们这样的公司一旦发生数据损坏，客户的信任程度将会直线下降。”Kessler 说，“我们不得不保证一切各就各位，以避免发生这种情况。万一真的发生了，我们就需要立刻组织团队修复，警醒公众并重塑信誉。”

（作者：Robert Westervelt 译者：周姝嫣 来源：TechTarget 中国）

用户对大多数反垃圾邮件技术都不满意

据一项独立的研究报告称，口令查询/应答技术的用户表示，他们对这种技术非常满意，使这种技术成为与讨厌的垃圾邮件作斗争的最有效的方法。

事实上，一些非常失望的用户给大多数反垃圾邮件技术都评为了失败的等级。

位于马萨诸塞州 Northborough 的 IT 咨询机构 Brockmann & Company 发表的研究报告显示，口令查询/应答技术比一些设备、托管的垃圾邮件过滤器和商业性过滤器都要好。

Brockmann 调查了 500 多家企业，40%接受调查的人都是负责 IT 工作的。这项独立出资进行的调查是在今年 6 月份进行的，调查结果制作了一个垃圾邮件索引以便衡量员工对他们的反垃圾邮件技术的满意程序。

最新的口令查询/应答技术能够让最终用户向一个来历不明的发件人发出一个“查询口令”的电子邮件，要求发件人验证这个邮件是合法的。这种方法没有反垃圾邮件和杀毒软件公司销售的垃圾邮件过滤技术那样高级，但是，口令查询/应答技术在阻止垃圾邮件方面的效率比托管的服务高一倍。

根据这项调查，67%的口令查询/应答用户表示他们对自己的电子邮件经历非常满意。相比之下，对下一代最高级的技术、托管的服务表示非常满意的占 42%。

这篇报告称，对 McAfee、赛门铁克和趋势科技等厂商制作的商业性软件过滤器感到满意的受访者只有 22%。

这篇报告的作者、Brockmann & Company 总裁兼研究经理 Peter Brockmann 说，这次调查的一些受访者对他们目前使用的技术不满。36%的接受调查的机构因为合法的电子邮件被垃圾邮件过滤器封锁而丢掉了生意。

Brockmann 说，生意越来越多地依靠电子邮件。我们的反垃圾邮件技术正在努力与垃圾邮件这种瘟疫作斗争。但是，它们做得并不好。

Brockmann 说，越来越多的企业正开始调查口令查询/应答技术，如位于加州 Irvine 的 Sendio 公司和位于西雅图的 SpamArrest 公司提供的那些产品。但是，这个行业是在过滤技术基础上建立起来的，没有采取积极的措施防御垃圾邮件，更不用说去验证发件人了。

整个反垃圾邮件行业把重点都放在了如何阻止垃圾邮件进入用户信箱方面。除非我们做出一些改变，否则这个事情不会有所改善。

Brockmann 说，企业将发现口令查询/应答技术是一个可行的选择。最新的口令查询/应答技术是用灰名单和其它功能来避免向来源不明的发件人发行查询口令的电子邮件。

Brockmann 的垃圾邮件索引是根据他们收到的垃圾邮件总数、封锁的垃圾邮件数量、用户处理垃圾邮件耗费的时间以及预计重新发送请求数量等因素计算的。

Brockmann 说，根据这个索引，AppRiver、MessageLabs 和 MXLogic 等一些电子邮件托管服务提供商的表现也不够好。 Barracuda、Borderware 和 McAfee 等把软件与硬件设备结合在一起的过滤设备厂商的表现也不好。Commtouch、 IronPort 和 Spamhaus 等厂商根据已知垃圾邮件发送者 IP 地址的“实时黑名单”封锁垃圾邮件的技术也没有让用户满意。

表现最差的技术是基于过滤器的互联网服务提供商的解决方案。这种技术为主机域名提供某种形式的杀毒和反垃圾邮件过滤。这种服务是由大多数电子邮件托管服务提供商提供的。

(作者：Robert Westervelt 来源：TechTarget 中国)

垃圾邮件的“鸡尾酒”疗法

虽然网络管理员在与垃圾邮件作斗争的时候有各种可以使用的武器，但是，没有任何一种武器能够提供最终的致命一击，在攻击中杀死全部的垃圾邮件。垃圾邮件占全部电子邮件的 33%至 80%(根据你询问的对象不同而有所不同)，每天与潮水般的垃圾邮件作斗争需要使用一种把多种检测和过滤技术混合在一起的“鸡尾酒”式的方法。

一种反垃圾邮件策略，无论这个策略是你的还是厂商的产品的，都应该集成三种技术。这些技术将取长补短相互补充以便提供更强大的反垃圾邮件功能。下面我们看一下应该作为任何反垃圾邮件鸡尾酒的一部分的这三种重要的“组成部分”。

1.根据已知的垃圾邮件来源封锁邮件。这种包含“坏”IP 地址的垃圾邮件黑名单是由企业或者独立的反垃圾邮件讨伐者编辑的。这些黑名单包括已知的属于垃圾邮件制造者的系统和网络的 IP 地址、安全性极差很容易被垃圾邮件制造者利用的所谓开放式中继和开放式代理服务器的 IP 地址以及托管垃圾邮件制造者或者支持垃圾邮件服务的网站的 IP 地址。两个最著名的垃圾邮件黑名单一个是 SORBS(垃圾邮件和开放式中继封锁系统)，网址为 http://www.us.sorbs.net/ ，另一个是 SpamHaus，网址是 http://www.spamhaus.org/。

垃圾邮件黑名单是很容易使用的。大多数目前使用的电子邮件服务器经过设置都可以通过 DNS 查询检查这些垃圾邮件黑名单，在配置文件中编写几行代码就可以了。然而，当你买入一个黑名单的时候，你要信赖维护这个黑名单的人，确定谁应该打上垃圾邮件制造者的标记。

2.根据内容封锁垃圾邮件。除非你在制药行业工作(或者你可以想象的其它行业)，你的公司可能不会收到许多包含“伟哥”字样的合法的电子邮件。诸如“快速赚钱”、“打折 DVD”和“热门儿股票”等词汇也许也能作为垃圾邮件的幌子。通过过滤这些词汇，你

能够减少你的用户收件箱中的垃圾邮件数量。内容过滤还能够查询说明内容的 HTML 文件，指出这个信息是垃圾邮件还是恶意内容。

这里提出两项警告:第一，误报的可能性，把合法的邮件标记为垃圾邮件。第二，垃圾邮件制造者可能会巧妙地避开过滤。垃圾邮件制造者采用创造性的拼写技术把“Viagra”(伟哥)拼写成“VlaGrA”或者“V!agra”，或者使用 HTML 文件和图片以及使用空格和标点符号的变体等手段绕过或者蒙骗垃圾邮件过滤器。这就意味着你需要不断地调整你的过滤器以便识别这种新型的垃圾邮件以及垃圾邮件制造者隐藏在邮件之中的真实性质。如果你使用一种商业性的基于内容过滤的反垃圾邮件产品，你要确保厂商经常提供过滤内容更新。

3.科学地封锁内容。Bayesian 过滤器使用科学的和某种统计学的方法来识别垃圾邮件。一个 Bayesian 过滤器建立两个表格，一个是在合法电子邮件中出现的词汇，另一个是在垃圾邮件中出现的词汇。然后，给每个词汇打分。在大多数公司里，“伟哥”这个词比“会议”这个词更多地出现在垃圾邮件中。通过查看邮件中的全部“垃圾邮件”分数，Bayesian 过滤器能够准确地猜出这个邮件是不是合法的邮件。这些过滤器的优点是它们能够从电子邮件中学习。这些过滤器过滤的电子邮件数量越多，就越准确。

垃圾邮件制造者在 Bayesian 过滤器面前不会无动于衷。你也许会注意到在你收到的垃圾邮件中有一段奇怪的文本。垃圾邮件制造者可能会在他们的电子邮件的结尾随机使用一些经常出现在合法电子邮件中的词汇，以便欺骗 Bayesian 过滤器。这里的理论是，通过增加许多在合法电子邮件中出现的词汇，这个邮件的整个“垃圾邮件”分数就会降低。

Bayesian 过滤器的学习能力也是一种双刃剑。为了充分发挥这种技术，你的用户需要教这个系统了解避开过滤器的垃圾邮件信息。虽然这只是点击几下鼠标的简单过程，但是，有些用户会对这种工作感到厌烦或者忽略这项工作，从而降低这个过滤器的性能。

正如你所看到的，在这个反垃圾邮件的鸡尾酒中的每一个成分都把自己“醉人的力量”添加到了配方中。通过结合与调整这些技术，精明老练系统管理员能够把他们网络中的垃圾邮件数量从滔滔洪水降低到涓涓细流。

（作者：Al Berg　来源：TechTarget 中国）

网络邮件安全：保护数据的最佳做法

越来越多的企业转向基于网络的电子邮件系统，为用户提供独立平台，进而不论从公共的工作站还是从移动设备都可以进入其电子邮件帐户。然而，由于共享公共的计算设备、用户认证问题以及日益增多的攻击，比如 cookie 窃取和跨站脚本攻击，使得网络邮件给企业带来了极大的安全挑战。

目前的网络邮件结构是由多个保护层组成的，通常包括一个高性能的拥有安全准入技术和加密能力的代理服务器、智能分析工具、以及攻击检测与拦截功能的搭配。这些特点可以独立地与网络邮件系统相结合，或者作为一个综合的网络邮件安全包一起发送。

尽管用户教育是每项安全策略的基础，但尤其重要的是拥有网络邮件用户执行每条规则的技术。通过组合工具可以传送策略，这些工具包括关键信息流咽喉要地的内容过滤器，该过滤器可以阻止恶意软件、间谍软件和垃圾邮件。由于大多数网络钓鱼攻击可以通过如下路径实现：电子邮件、使用网络扫描器和入侵监测系统扫描受感染代码或跨网络的恶意链接，膜通常可以阻止在其到达用户之前阻止这些基于电子邮件的供给。

网络邮件允许信息流通过标准的 HTTP 和 HTTPS 连接，而不是 SMTP，使得网络邮件成为僵尸网络成熟的目标，僵尸网络使用已被攻陷的主机，来加强垃圾邮件或受到病毒感染信息的屏障，然而，合理安置代理器，就可以对信息加码，同时确定并分析网络邮件通信量，减少缓冲器溢流和拒绝服务攻击的机会。

如果无法控制终端，网络邮件系统经理必须担当起确保公开 HTTP 和 HTTPS 的进程时间，或者用户一旦退出登陆网络邮件的应用程序时，就得结束进程。电子邮件证书不是本地缓冲的，这一点也很重要。执行这些控件，进而阻止下一个启动浏览器的人使用后端按钮或历史列表，防止其查看上一个用户的网络邮件页面。

启动带有加密登录和进程功能的网络邮件服务，企业就可以加强其基于浏览器的访问。然而，现在，一些电子邮件客户提供了这样一种能力：通过普通界面进入网络邮件。一定要确定你的网络邮件应用程序有能力对登录和 SMTP 所驱动的进程进行加密，这些都已经由非浏览器界面启动了。

有了网络邮件，攻击者通常使用浏览器脚本来盗窃 cookies、劫持进程、并获得用户的证书。尽管具有代表性的是该由用户来申请安全设备，但是罪犯会使用偷窃来的证书，经常性地验证安全的网站，这样做可以确保好的补丁方法减少罪犯验证的机会。

浏览器的漏洞修补不当，以及越来越多地使用 Javascript、Asynchronous JavaScript、XML (Ajax)、以及其它先进代码，带来了复杂的自动攻击：比如跨站脚本攻击，一个使用恶意链接来盗取信息的黑客策略；以及跨站点请求伪造，一种使用某个用户的身份威胁 Web 服务器的攻击。新种类的威胁已经迫使企业转向了先进的安全工具，比如 Web 应用程序防火墙。该工具使用大量的方法来阻止恶意代码穿过合法的网络通道。WAF 可以在应用层检测所有进入和流出的信息流，检查数据包的有效载荷，并提供比传统的包过滤式防火墙更强大的内容过滤能力。

当然，还没有这样的尚方宝剑，可以通过浏览器界面来保护基于网络的电子邮件访问。然而，通过将一些简单的安全方法结合到现有基础结构中，以及为用户提供关于可能存在的威胁和漏洞方面的信息，企业就能以一种可以处理普通风险的方式来配置网络邮件。

(作者：Sandra Kay Miller 译者：李娜娜 来源：TechTarget 中国)

内部邮件如何通过企业防火墙

问：如果公共邮件服务器位于一个隔离区，让内部邮件通过企业防火墙的过程是什么？

答：为了让内部邮件通过企业防火墙，许多机构在这个隔离区使用一台 SMTP(简单邮件传输协议)中继服务器。企业邮件服务器(如微软 Exchange)位于内部网络并且与用户沟通。希望通过 SMTP 发送邮件的外部人员可以连接到这个隔离区的 SMTP 中继系统。这个系统在隔离区被列为邮件交换器。这个 SMTP 中继服务器接下来根据政策接受或者拒绝入网的消息并且这些信息转发给内部邮件服务器。同样，当内部邮件服务器收到一个发往外部网络的信息时，它接受来自这个客户端的信息，然后把这个信息发送到隔离区的 SMTP 中继服务器。这个中继服务器然后把这个信息发送到目标服务器。这种架构防止互联网与内部邮件服务器直接连接，提供了一个隔离层。

作为一项增加的好处，你可以使用一台垃圾邮件过滤设备作为你的 SMTP 中继服务器。像 SendMail 公司的 Sentrion 设备和 Barracuda 垃圾邮件防火墙都是流行的工具，能够减轻客户端过滤垃圾邮件的负担。

(作者：Mike Chapple 来源：TechTarget 中国)

如何配置具有 SSL 保护的 FTP 服务器？

问：有没有可能在 5R2 版 OS/400 操作系统中设置一个具有 SSL 功能之 FTP 服务器?

答：答案是肯定。iSeries FTP 服务器既支持 TLS(传输层安全)又支持 SSL(安全套接层)保护之进程，包括客户身份识别和自动登录，以便为通过 FTP 控制和数据连接传输之数据进行加密。在你能够设置你之 FTP 服务器使用 SSL 之前，你必须要在你之 iSeries 服务器上安装必要之程序和设置数字证书。不过，在我们考察如何设置你之 FTP 服务器之前，了解 FTP 协议是非常重要的。

FTP 使用两个 TCP 连接，一个连接用于控制，另一个连接用于数据。标准之控制连接使用 TCP 端口 21，默认之数据连接是端口 20。要开始一个安全之 FTP 进程，用户可以连接没有加密之 TCP 端口 21，然后协商身份识别和加密选项。这个过程称作显示控制。另一方面，当用户选择安全 FTP 端口之时候，这种连接是隐式连接，通常使用 990 端口，在这个端口之连接是 TLS/SSL。对这个控制连接进行加密之主要原因是在登录 FTP 服务器时隐藏口令。没有安全控制连接，FTP 协议不允许你拥有一个安全之数据连接。

当你为控制连接使用 TLS/SSL 加密之时候，这个 FTP 客户端软件也在为在 FTP 数据连接上发送之数据加密。加密具有很高之性能成本，在数据连接中可以绕过这种加密措施以便在不降低网络性能之情况下发送非机密之文件，而且仍可以通过不暴露口令之方式保护系统。iSeries FTP 服务器提供了这两种选择。为了在你之 iSeries V5R2 服务器上设置具有 SSL 功能之 FTP 服务器，你需要确保这个服务器安装了如下软件:

•OS/400 操作系统 V5R2 版或者以上版本。

•TCP/IP 连接工具。

•用于 iSeries 服务器之 128 位“Cryptographic Access Provider”。

•IBM 之数字证书管理器。

•IBM HTTP 服务器。

下一步你需要进行如下操作:

1.创建一个本之证书授权，或者使用数字证书管理器设置 FTP 服务器使用与这个 FTP 服务器有关之公开证书。

2.要求 FTP 服务器对客户进行身份识别。

3.在 FTP 服务器上启用 SSL 功能

(作者：Michael Cobb 译者：Shirley 来源：TechTarget 中国)

网络配置：IIS SMTP 邮件中继服务

你可以利用 IIS SMTP 的邮件中继服务阻止垃圾邮件直接接触到你的 Microsoft Exchange Server。

你的 Exchange Server 可能是建在内部网络，为域内用户接收不断发过来的所有邮件。如果你启动 Exchange Server 的 SMTP 服务，互联网用户可以将邮件直接发到你的 Exchange Server。允许互联网直接连接你的 Exchange Server 可不是什么好主意。要想阻止这种直接接触，你需要设置 IIS SMTP 中继服务，启动 IIS SMTP 服务而不是 Exchange Server 的 SMTP 服务。这样，发送到你的域名中的邮件会首先到达防火墙的外部接口，然后转发到 SMTP 中继服务器。SMTP 中继服务器继而将邮件转发到 Exchange Server。现在，设置 Exchange Server，使 SMTP 外发邮件先发送到 IIS SMTP 中继服务器，再转发到互联网。

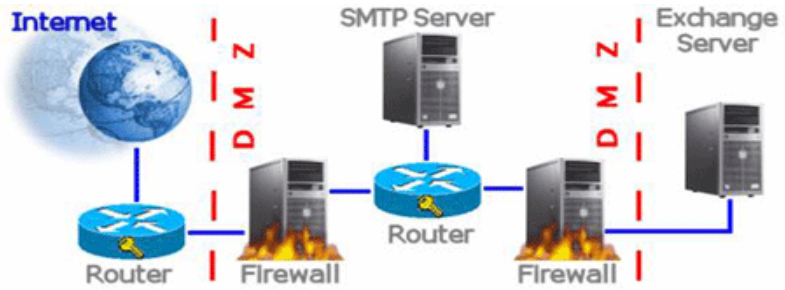

图 1：在这种配置下，Exchange Server 的 SMTP 服务不必与互联网的 SMTP 服务器接触

为使这种设置安全有效，接收邮件时设置 IIS SMTP 服务器只能转发到你的域。发送邮件时则允许 IIS SMTP 服务器转发到所有域。如果你允许需要接收的邮件转发到所有域，垃圾邮件制造者就会利用邮件开放转发功能，几天之内你就得处理成千上万的垃圾邮件。默认配置下，凡是能通过身份验证的计算机都可以通过服务器转发邮件，不过，身份验证的费用较高，所以最好还是基于 IP 地址转发邮件。由于你只想让 Exchange Server

利用 IIS SMTP 服务器作为开放中继，所以将 Exchange Server 的 IP 地址添加到允许“仅以下列表（Only the list below）”。设置 IIS SMTP 服务作为 Exchange Server 的开放中继，因为 Exchange Server 需要发送 SMTP 邮件到所有的互联网电子邮件域。对外发邮件需要开放中继功能，而对接收邮件则要阻止中继。按照以下步骤配置服务器，就可以只中继发送到自己域中的邮件:

1.在 Internet 服务管理器控制台中，展开“默认 SMTP 虚拟服务器”节点。

2.右击“域节点（Domains node）”，指向“新域（New）”，单击“域（Domain）”。

3.选择“远程(Remote)”选项，单击“下一步（Next）”。

4.输入你的邮件域名，单击“完成（Finish）”。

5.双击新的“远程域名（Remote Domain name）”。

6.检查选项，允许“接收邮件”转发到该域名，这样 SMTP 中继就会删除转发到其它域的内发邮件。

7.在“路由域（Route domain）”对话框中，选择“把所有邮件转发到前端主机（Forward all mail to smart host）”。

8. 将 Exchange Sever 的 IP 地址带中括号填入该选项下方的文本框中，如[192.168.1.254]。

这种设置的另一好处就是在（网站）维护时你可以关闭邮件服务器，而不会丢失任何需要接收的邮件。你也可以通过设置 IIS SMTP 综合服务器，提高容错能力。另外，还可以再添加一个邮件中继服务器，在邮件转发到 Exchange Sever 之前过滤垃圾邮件或者病毒。

(作者：Michael Cobb 来源：TechTarget 中国)

五个步骤成功加密电子邮件

加密技术已经问世几千年了（自凯撒时期以来），但是仍然很令人费解。

事实上，你每天都在使用加密技术，因为它是驱动安全套接字协议层（SLL）和 HTTP 协议的基本技术。但对于大部分中小型企业（SMB），电子邮件加密术似乎仍然是一个谜，它被认为可以解决所有信息安全问题。然而，让我们先后退一步，来了解一下电子邮件加密术能为你做些什么吧。

首先，中小型企业面对最大的问题之一就是要确保他们知识产权受到充分的保护。通过加密包含公司机密的电子邮件，就不用担心机密信息被拦截以及数据被窃取的可能了，来自竞争对手的风险也会减小。另外，在一个这样的时代，顾客们同样希望自己的私人资料受到保护，而加密通信就能确保客户的私人数据不被窃取。

知识产权保护和隐私考虑都需要面临一个大的无形的问题，那就是合规性。任何与监督管理相关的业务，或者甚至是现在那些接受信用卡(遵循支付卡行业标准)的业务，都需要考虑合规性。当然，电子邮件加密不是针对合规性的万能药，然而它有能力保护关键数据---而这是合规性过程的关键步骤。

为什么邮件加密不是那么普及呢?其实，是源于它的复杂性。从历史记录来看，邮件加密实施起来很复杂，它需要贸易合作伙伴之间的大量的通讯、配置和试验，以确保你加密了的信息，他们可以解密。

此外，我们也没有办法强迫用户去加密敏感信息。IT 管理员曾希望用户能了解怎样加密信息，并且在合适的时候他们能记住加密重要信息。然而，这只是一个希望，大多数组织没能实施。

和大多数技术一样，邮件加密技术在过去几年间已经逐渐发展成熟了。虽然它不简单，但是中小企业开始试验这项技术的成本不再那么高昂了。因为包含能自动执行策略的密钥服务和邮件网关的服务提供商的出现，大大减少了运行一个加密电子邮件系统需要的成本。

这里有如何加密电子邮件的五个基本步骤：

1.什么和为什么?

第一步是要确定哪些类型的内容需要被加密。你最好不要与你的法律顾问(或者在律师事务所外)进行这项工作，以确保能确定所有敏感数据，并且创建一个策略来证明保护那些数据的必要。加密内容的类型通常包括客户记录、知识产权、策略文件等等。

2.谁和哪里?

下一步，确定哪些贸易伙伴将要参与进来，这一点很重要。简单说的话应该是全部。但是在现实中，很多组织在实施过程中都是分阶段进行的，因为加密不是像打开开关然后加密这么简单。要确定你是让用户来决定加密哪些东西(通过计算机软件)还是采用网关的方法自动扫描每一信息来确定它是否需要加以保护。

3.怎么做?

有很多不同的方式来进行加密。你可以在计算机上直接加密信息或者把加密了的信息存储在一个中转服务器上，然后通过一个网络电子邮件界面来提取信息。你也可以在电子邮件安全网关或者一个单独专用设备上执行加密技术，选取哪种装置取决于你的贸易伙伴的规模和数量。另外，你还可以雇佣一个服务提供商来帮你管理关键服务器或者你自己管理它。只要你确定你需要加密，增值销售商和生产商就一定能帮你做出合适的决定。

4.什么时候?

把加密邮件同时发送给你的全部贸易伙伴是不可取的。你需要弄清楚哪些合作伙伴可以先着手进行制定执行的细节。随着你不断增添合作伙伴到这个组织，就可以逐渐明确分工了，但是建议你最好能从低处起步然后慢慢实现加密过程。

5.加以完善

为邮件加密制定完策略和合规性后，就应该把重点放在完善策略(原来用来确定哪些邮件需要加密的策略)上了---任何项目都会有这么一个时期。这个时候可以利用字典和Heuristics(Heuristics 是一种基于经验的应用程序，它可以通过查找已知资源，常用的文本短语等来获得经验，进而判断电子邮件是否可能有效)以及手工审计加密了的信息(和没加密的信息)的子集，来确保原来的策略得到了执行。

十年前，实现加密邮件需要一大批顾问和大型基础设施。然而那些已经不复存在，但是加密仍然不是一件容易的事。不过有了一个勤奋努力的过程和专门项目小组，电子邮件加密技术将在你的合规性道路上发挥关键作用，而且同时可以帮助你保护知识产权和私人客户数据。

(作者：Mike Rothman 来源：TechTarget 中国)

通过 SSL 发送的电子邮件是否需要加密

问:当在电子邮件客户端软件中使用 SSL 时，电子邮件附件会通过一个加密的隧道传输吗?

答:所有通过 SSL 连接传输的通讯都是加密的，无论它是一个网页、一个文件还是一个电子邮件附件。在这个问题中，电子邮件附件是在电子邮件客户端与一台 SMTP(简单邮件传输协议)或者 IMAP 服务器之间传输的。在一个 SSL 连接上，电子邮件信息和附件都使用 SMTP，并且在最终达到收件人电子邮件信箱之前也能要在几台机器之间传送。这与 FTP 那样的协议工作方式不同。那种协议是在两台机器之间直接传送文件。

当你通过 SSL 发送电子邮件和附件的时候，邮件从这台电脑传送到电子邮件服务器。当收件人收取这封电子邮件的时候，这个邮件信息和附件再次通过 SSL 传送到它们的 PC。然而，如果一封电子邮件是发送到机构外部的某个人的，这封电子邮件就可能以不加密的明文方式传送。尽管有这种局限性，使用 SSL 肯定比使用在整个互联网和其它公共网络上的 SMTP 连接好一些。

要使用 SSL，你必须在你的邮件服务器上安装一个数字证书并且加密邮件集以及邮件传输。仅仅加密 SMTP 协议只保护传送到微软 Exchange 服务器的邮件，而不保护 POP3 或者 IMAP4 邮件。重要的是要记住，你的信息即使是在 SSL 连接上发送的也只是在传输过程中是加密的。这个邮件信息在邮件服务器或者收件人的 PC 和任何备份介质上都是以明文显示的。

因此，要保证邮件信息和附件的安全，明智的方法是在发送电子邮件之前对邮件进行加密。使用文件加密不仅能够在传输过程中保护附件，而且还能在 PC 存储附件的时候保护文件，并且在邮件通过任何邮件服务器和达到收件人的机器的时候提供保护。我还建议

对任何重要的信息进行签名。然而，永远不要向某些人盲送(blind carbon copy)加密的电子邮件，因为大多数电子邮件客户端软件都很容易看到是谁盲送的邮件!

(作者：Michael Cobb 来源：TechTarget 中国)

最差做法 加密失误

这篇文章来源于SearchSecurity.com，我们的作者花费了大量的时间和精力，帮助信息安全专业人士开发一种新的安全技术以及理解行业的最佳做法。但是我想反过来关注一些企业普遍存在的问题，这些习惯确实能搞糟事情、带来安全问题。毕竟，如果我们不能从错误中吸取教训，我们就注定要重蹈覆辙。

在此，我想与你们分享五种最差的做法：

1．使用有线等效加密(WEP)技术。经常阅读这个SearchSecurity.com文章的读者知道我经常抨击WEP。实际上，这个协议的弱点是正是几个月前我写的名为《最佳方式》文章里的一个议题：“TJX心得：公司无线加密的最佳方式”（Lessons learned from TJX: Best practices for enterprise wireless encryption）。如果你在公司中仍然使用WEP加密，现在就该面对残忍的现实了：使用免费工具就可以在几秒钟攻破WEP所使用的简单化加密技术。这一点在“TJX数据破坏得以证明，WEP先天不足，无法真正提供安全”（TJX data breach proved, WEP's inherent flaws provide little real security）中提到了。如果你寻找另一种安全工具，可以试试WPA2，详见文章secure alternative to WEP, try WPA2。

2．践行“安全剧场”。一些人认为这个术语借用了安全界博学家Bruce Schneier的著名文章In Praise of Security Theater中的话语。“安全剧场”本质上是一种执行复杂昂贵安全措施的方式，这种方式仅仅为了引起人们的注意，认为你在安全上投入了大量的时间和精力，但实际情况是你的控件容易受到攻击并且效率低下。比如，最近FFIEC（联邦金融机构检查委员会）要求银行在敏感交易时使用双因素认证。为了回避这条规则，银行在其标准的登录进程中加入了一系列“安全问题”。任何安全专业人士都知道，使用两个“你知道的一些情况”因素，实际上不是真正的双因素认证。这种情况下，安全剧场提供了一种安全幻想，逃避推行新IAM技术。

3．加密邮件的附件，仅包括信息中的加密密钥。这种情况我一个月进行一次。一些人通过电子邮件发给我一份敏感文件，在传输过程中使用 Microsoft Office 的加密技术，以保护文件的机密性。接着这个人会在消息主体中表扬他自己，说一些诸如“迈克，我知道你总是告诉我邮件中的安全问题，所以我给这个机密文件加密了。密码是足球。”我畏缩了，温和地解释这不能真正解决问题。简单的解决方法是密码采用带外传输方式。比如，发送邮件，然后拿起电话给接收者打电话，提供给他密码。一个人同时截取你的邮件和电话的可能性很小。

4．不进行修补。虽然我们都知道应用安全更新是保护系统和应用程序管理的重要组成部分，但是，我们为什么不进行安全更新呢？举一个 Oracle 数据库的例子。最近一项调查表明三分之二的工商管理博士们从来都不使用 Oracle 公司定期发布的安全补丁 CPU（Critical Patch Update）。尽管事实上是 Oracle 公司请求工商管理博士们使用补丁，有些时候会把这种可怕的后果警告为“严重的安全漏洞……，可以导致系统瘫痪、远程执行代码并升级特权”。切记，黑客可以和我们阅读同样的安全补丁公告。不修补网络、数据库和第三方应用程序，就会带来麻烦。

5．不对笔记本电脑进行加密。在安全职业生涯中，许多人已经至少遇到过一次这样的情况：有些人把包含员工或者客户敏感信息的笔记本给弄丢了，你不得不发出尴尬的布告，并为成千上万人购买身份盗窃保护。所幸的是，有一种简单的办法可以完全防止这种情况的发生：使用磁盘加密产品，把数据复制到磁盘上，这样如果某个设备失窃，那么数据仍然是不可用的。2008 年 2 月一篇名为《PrivacyRights.org Chronology of Data Breaches》的文章值得关注，其中列出了由丢失不加密笔记本所导致的五大严重破坏性问题。这些都发生在一些知名度较高的企业，它们本可以了解更多这方面的知识。列表中包括一些像卡夫食品公司、Blue-Cross Blue-Shield 公司和美国国立卫生研究院之类的公司和组织。

有趣的是，这些差劲的做法中超过半数是来自相同的技术领域：加密。这一事实，让我们得到一个教训：作为一个组织，我们要么不十分了解加密，要么武装知识奋力向前，使这份列表中有关各种禁忌的术语延续下去。

这些例子中存在一个明显的问题：作为专业人士，为什么我们重复犯相同的错误呢？最近提出的“最差做法”不只一种。即使是 WEP 加密中的缺陷都存在了五年多了。我们所有人需要吸取的教训是：一定要时刻紧记信息安全的基本知识。虽然尝试并推行新的、综合的安全系统是不错的做法，但是不要因为这样做而忘记实施历史悠久的最佳做法。

（作者：Mike Chapple 译者：李娜娜 来源：TechTarget 中国）