电子邮件安全手册

电子邮件安全手册

电子邮件已经成为我们生活工作中必不可少的一部分。但是，随着垃圾邮件，邮件病毒，邮件广告等不速之客大量涌入我们的邮箱，电子邮件变得越来越不安全，越来越令人烦恼了。如何实现电子邮件安全，保护我们的信息？本技术手册将为你介绍电子邮件的安全问题以及如何保护电子邮件安全，并分析了未来电子邮件发展的几种趋势。

几种常见的电子邮件安全问题

邮件的安全问题包含两个方面，一个是邮件可能给系统带来的不安全因素，二是邮件内容本身的隐私性。现在黑客猖獗，他们可以通过攻击电子邮件系统来获得敏感数据，也可以通过电子邮件来传播病毒和恶意软件。无论是哪一种，都将给你和你的企业带来不小的损失。本部分，将为你列举几个常见的电子邮件安全问题。

- ❖实例讲解：欺诈类电子邮件
- ❖AT&T 电子邮件地址安全漏洞：黑客可以跟踪 SIM 卡吗？
- ❖Microsoft Outlook 2007 更新引起电子邮件身份验证问题

实现电子邮件安全的方法

在电子邮件的传输，存储等方面，有许多安全因素需要考虑。如何保证你的电子邮件没被泄漏或窃取？如何确保你收到的邮件是真实的而不是虚假广告或恶意链接？如何防止别人利用

你的邮件身份发送信息？在这一部分中，我们将教你如何确保电子邮件的安全，包括如何防范邮件账号被暴力破解，如如何防止电子邮件欺骗等等。

- ❖如何防范对电子邮件帐号的暴力破解？
- ❖电子邮件、网站和 IP 欺骗：如何防止欺骗攻击
- ❖采用 pdf 附件的电子邮件安全性就高吗？
- ❖如何用电子邮件数字证书来保证信息的安全
- ❖抗击网络钓鱼的关键：电子邮件认证方式

电子邮件发展的新趋势

移动应用和云已经是不可避免的趋势，它们正在发生且会发展的越来越快。电子邮件也乘上了这趟趋势的列车，人们的移动设备终端上装有邮件程序，可以随时随地的收发邮件，云电子邮件服务也被提出来。未来的电子邮件还会有怎样的发展？我们拭目以待。

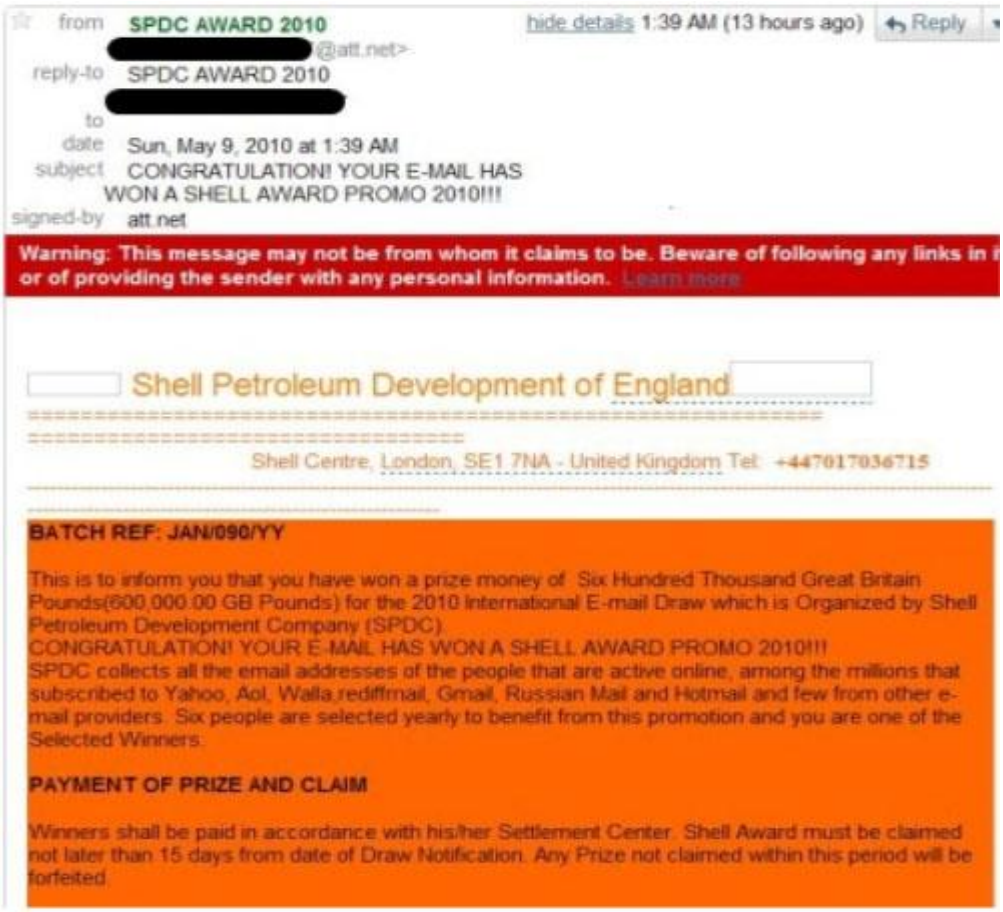
- ❖超越邮件的移动应用之：电子邮件的扩展
- ❖为什么中型企业转向云电子邮件服务

实例讲解：欺诈类电子邮件

最近，我的垃圾邮件过滤器遭遇到了来自不同类型欺诈和网络钓鱼内容电子邮件的轰炸。我发现其中的一些类型非常具有欺骗性，因此，我觉得最好的防御手段就是分享自己的研究结果。这样的话，如果你使用垃圾邮件过滤器，就可以察觉到正在酝酿中的欺骗活动的潜在迹象了。

骗局 1：你获奖了

在最近的一篇文章，我采访了安全顾问谢尔利·黑尔。她提到过一种成功的社会化工程技术，这就是提供奖品或奖励。我不得不承认，当有人告诉你是一名胜利者时的感觉是非常美妙的。60 万英镑看起来非常具有诱惑力：



这种类型的欺诈活动似乎相当普遍。但如果你没有选择进入的话，就不会产生效果。对于骗子来说，这就是最大的问题了。如果你不进入的话，怎么能赢？不论怎么看，这都是非常可疑的。此外，你会发现电子邮件来自 att.net 域，它通常是被互联网服务供应商美国电话电报公司的用户所使用。这也从另一方面暗示出邮件中包含的信息是错误的。

邮件的下一部分内容显示出网络犯罪分子的真实需要。可以在互联网黑市上出售的个人信息：

看完邮件的这部分后，所有的警报都可以响起了。没有诚实的商业或金融机构会要求你通过电子邮件发送个人信息的。

骗局 2：我没有发送该邮件

安全专家们对像 Facebook 和 Twitter 之类的社会化服务网站带来的威胁提出了警告。原因是什么呢？它们的流行导致会员愿意分享自己的个人信息。就在今天，Facebook 董事会的一名投资者自己的帐户就受到了攻击——这可不是好事情。

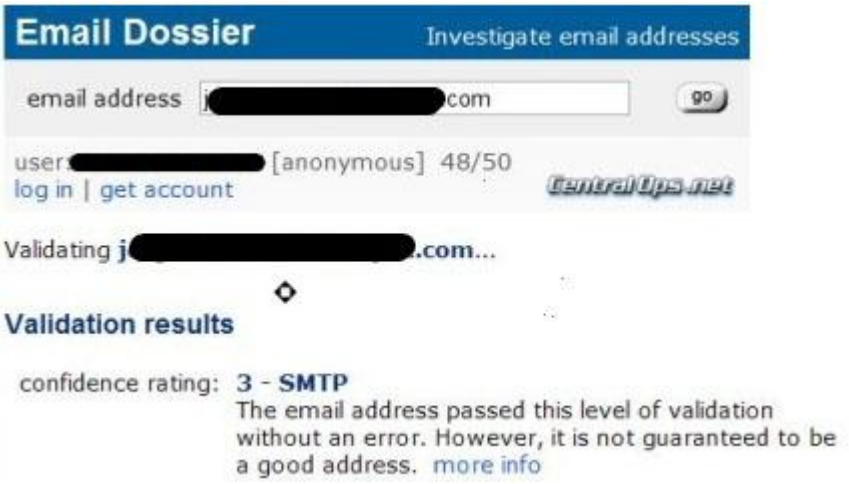
另一个例子是，一封据说是来自 Twitter 如下所示的电子邮件：

表面上来看，这封电子邮件非常像真的。甚至邮件底部的 Twitter 支持链接都是正确的。因此，很多用户会丧失警惕性，准备解决这一问题。

但真正的网络地址是非常危险的。点击后，你会被带到一家网站上，它存在的唯一目的是将恶意软件下载安装到你的计算机上。这样的话，流氓安全软件就可以完全控制计算机，并偷偷地在后台安装键盘记录工具窃取你的个人信息。

更可悲的是，这种类型的欺诈电子邮件还往往具有较高的成功率。相对而言，我属于比较幸运的人，我使用的垃圾邮件过滤服务在检查电子邮件地址时，发现"来自 Twitter 的工程师"这一电子邮件帐户是不合法的：

该电子邮件实际上来自"j??????@icd.????????.com"，一个非常好的地址，但和 Twitter 一点关系都没有：



还有一点我想说一下。我已经收到过来自不同发件人内容相同的电子邮件了。这通常意味着被控制的计算机都属于正在被用来传播这一特定恶意电子邮件的僵尸网络。

网络犯罪分子选择这么做的原因有两个。他们可以防止计算机用户因为电子邮件数量过多而产生怀疑。并且还可以防止跟踪攻击者进行安全分析。

骗局 3：你的邮箱空间已满

下面的欺诈电子邮件就采用了不同的手法。这是相当有效的，因为没有人希望电子邮件丢失：

> 来自：系统管理员＜移除＞
>
> 回复：系统管理员＜移除＞
>
> 到达：
>
> 时间：2010 年 5 月 1 日上午 6 点 20 分，星期六
>
> 主题：最后的提醒！
>
> 你的邮箱占据的容量已经超过了管理员设置的 20GB 存储限额。当前容量为 20.9GB，在重新验证邮箱有效性之前，你可能无法发送或接收新邮件。要重新验证你的邮箱的有效性，请点击下面的链接：
>
> http://（移除）
>
> 如果该链接无法直接工作的话，请将它复制并粘贴到你的网络浏览器窗口中使用。
>
> 谢谢
>
> 系统管理员

在这封电子邮件中，有几条线索让你应该提高警惕：

- 一或两次的预先提醒是通常情况下的处理方式。它给用户一次机会来对邮箱进行清理。
- 电子邮件中提到的存储限制和电子邮件帐户提供的容量是不一样的。
- 这应该属于一条自动发送的信息。而"该链接无法直接工作"这样的语法错误，应该让你对链接的真实性产生怀疑。

如果用户点击了该电子邮件中提供的链接，他们就会被带到一家恶意网站上。同样的事件又一次发生了，任何恶意软件都可以被下载并安装到计算机上。

你可以从这里获得帮助

如果你询问专家的话，他们会告诉你，对于防范欺诈类电子邮件来说，对所有内容保持怀疑态度依然是最好的方法。而且，这并不仅仅是安慰，你会很高兴地发现，还是有一些组织可以提供帮助的。反钓鱼欺诈工作组（APWG）就是一个典型的例子。

APWG 致力于在全球范围内，帮助公司企业和执法机关消除由各种类型的网络钓鱼攻击、网址嫁接行为和电子邮件诈骗活动带来的欺诈和身份盗窃类犯罪。

他们官方网站上提供的一篇文章非常有用。在文章中，它以通俗易懂的方式解释了人们为什么应该提高警惕。我一定会将它发给所有希望了解网络诈骗活动的人。

另一家非常有用的网站是 millersmiles.co.uk。来自微笑米勒的人们和 APWG 一样，致力于清除网络钓鱼和电子邮件欺诈带来的威胁：

“微笑米勒是关于欺诈类电子邮件和网络钓鱼行为信息最重要的信息来源，它包含了来自实际事例中的大量与电子邮件以及伪造的网页内容相关的文字类和图片类资料。”

这就是微笑米勒推出的可以对现有网络钓鱼行为进行搜索的数据库。它非常独特，用户可以通过输入包括邮件主题、邮件内容、公开的发件人地址或网络地址等参数来对可疑的电子邮件进行检查：

最后的思考

除非这一问题已经被解决，否则的话，我们就必须关注诈骗技术的最新发展。在本文中，我给出了几个最近遇到的例子。希望可以为你防范欺诈和网络钓鱼电子邮件的工作提供帮助。

（作者：至顶网　来源：TechTarget 中国）

AT&T 电子邮件地址安全漏洞：黑客可以跟踪 SIM 卡吗？

问：你能解释一下目前关于成千上万个电子邮件地址被破解的事情吗？这是 Apple 的过失还是 AT&T 的过失？用户的本地数据也有被破解的风险吗？

答：目前的 Web 安全攻击有电子邮件地址安全漏洞攻击和 iPad 用户 SIM 卡系列号的破解，这看起来似乎是 AT&T 公司的过失。据 AT&T 首席安全官 Ed Amoroso 说，为了使用户更新更早，AT&T 预组装了具有电子邮件地址的网站。攻击者可能利用了 AT&T 网站中的一个漏洞来提取数据。AT&T 虽然需要对系统的安全负责，但是 Apple 也应该确保其合作伙伴对其客户的敏感数据进行了有效的保护。

名人电子邮件地址的暴露在此次攻击中引起了人们极大的注意。但是 SIM 卡系列号（与蜂窝式系统中所使用的 ICC-ID 和 IMI 号码相关）的泄漏可能更应该引起人们的注意。这些号码是用来确定手机和设备位置的，如果被不认识的人跟踪，手机设备持有人的人身安全将受到威胁。为了跟踪 SIM 卡，攻击者需要访问蜂窝式网络，但是这种访问很容易获取，获得了访问，攻击者就能跟踪个人手机。企业应该确保已经意识到他们用户的物理安全风险（由于这种攻击使其用户暴露），而且还应该警惕用户，如建议高危员工在不使用手机时将手机关机。

（作者：Nick Lewis　译者：曾芸芸　来源：TechTarget 中国）

Microsoft Outlook 2007 更新引起电子邮件身份验证问题

在用户抱怨 Office 2007 严重的连接问题和性能的下降后，Microsoft 推出了无安全性的 Office 2007 更新。

12 月 14 日发布的更新（KB2412171），本是为了提高 Outlook 2007 的稳定性和性能的。但是自动更新后不久，Microsoft 的支持论坛就开始充满了用户对连接到 Microsoft Exchange Server 以及低效的性能问题的抱怨。

一位用户在 Microsoft Answers 支持论坛投诉道，“不仅是打开 Outlook 文件夹很慢，拒绝从 Gmail 下载 POP3 的邮件，而且它居然从别的 POP3 邮件服务器下载邮件。”

这些大量问题的反应都来自用户和小企业，也许他们没有在 Outlook 里配置一个 Microsoft Exchange Server 帐户。

Microsoft 的 Outlook 产品组在上周晚些时候，在一条博客更新中承认了 Outlook 2007 电子邮件身份验证的问题。不定的更新打断了 Outlook 对安全密码验证的支持（Secure Password Authentication），安全密码验证是 Microsoft 确保 Outlook 使用 SMTP，POP 或者 IMAP 验证的一条协议。这个更新还使得文件夹间的切换速度变慢。

“那些使用 Gmail 且选择了 SPA 选项的用户，无法连接到 Gmail，”Outlook 产品组在博客中这样写道。

在一封邮件中，Microsoft 可信赖计算（Trustworthy Computing）的主任 Dave Forstrom 说道，更新应该允许用户选择身份验证扩展保护（Extended Protection for Authentication）。但更新进程没有修改 Outlook 2007 的行为，反而引起了身份验证问题。

Forstrom 表示，“我们没有任何证据证明是更新引起了安全问题。”

更新是为了增加对特定形式攻击的保护，Forstrom 说道。身份验证扩展保护（Extended Protection for Authentication ）确保身份验证需求与产生 Windows 身份验证的服务器的服务主体名称（SPN）以及传输层安全（TLS）通道绑定，Forstrom 解释道。

（作者：Robert Westervelt 译者：Ping 来源：TechTarget 中国）

如何防范对电子邮件帐号的暴力破解？

问：为什么现在对电子邮件帐号的暴力破解成为一种流行的攻击技术？这种攻击是如何完成的？那么我们又能做些什么防范措施以在企业级别上去防止这种暴力攻击呢？

答：这是问题问得很好。对于基于网页的电子邮件帐号进行暴力破解变得非常流行，因为这种技术是如此的简单易行。当前的用于暴力猜测密码的工具现在比比皆是，并且只需要掌握很少量的技术就可以很熟练的去应用这些工具，比如像“Brutus”就属于一种这样的工具。你只需要给 Brutus 一个由单词组成的列表（也就是一个词典），这个列表的内容将被作为用户名和密码。Brutus 将从列表中取出任何可能的用户名，密码组合去猜测帐号，直到某一种组合起作用。某些工具可能还会尝试每个密码的一些简单变形（比如”“fluffy8”，“fluffy9”，等等）。这些攻击工具是如此简单以至于一个十几岁的孩子都可以通过简单的点击动作去完成对基于网页的电子邮件帐号的暴力破解的工作。

好消息是我们有许多有效的方法来防止这种针对企业的基于网页的电子邮箱的帐号暴力攻击。也许这当中最直接的策略是使用双因素认证。我们都知道通常有三种形式的认证：

1. 你拥有什么？（比如一张借记卡）

2. 你知道什么？（比如一个密码）

3. 你的东西是什么？（比如你的指纹）

由密码所保护的基于网页的电子邮件帐号就是一种典型的单因素认证机制（即，你知道什么）。由于密码经常会被远程猜测出来或者被盗窃，所以对于限制访问的需求来说这种认证机制是一种非常低安全度的方法。

对于基于网页的电子邮件系统，我建议使用至少两个认证因素，比如使用 RSA 信息安全公司的硬件 SecurID 令牌。这些令牌就如您的手掌大小，便于携带，同时他们能在您每次登录的时候显示一个不同的登录密码。这个密码永远不会重复，而能达到与某个密码有效期间同步地进行密码猜测的几率是相当的小的。这个令牌（你拥有的）和这个个人身份号码（你知道的）结合起来之后，您只需要如通常那样输入这个个人密码即可。当然，还有很多其他的方式去实现这种双因素认证机制，比如基于软件的认证者或者基于手机的一些认证系统。

另一方面，您也可以通过限制登录尝试的次数来降低网页电子邮件帐号被暴力破解的危险（比如，在一分钟之内三次登录失败将会导致一次十五分钟的系统锁定）。这种方式可以有效地限制一个攻击者进行攻击时的猜测次数。同时，您还需要确保您拥有一个强口令规则，使得在这个规则下的密码都很难通过一般的方法被猜测到进而被检测到帐号信息。最后，如果您的系统存在一个密码复位机制，还需要确保复位密码时所使用的问题的答案的安全，即，它不应该很容易就能够通过一些公开的信息或者社会网络来获得。

（作者：Sherri Davidoff　译者：行久　来源：TechTarget 中国）

电子邮件、网站和 IP 欺骗：如何防止欺骗攻击

有一位读者问我们的威胁专家 Nick Lewis：您能解释一下什么是欺骗攻击吗？有没有什么方法可以让组织免受这一新的威胁呢？

Nick Lewis：有几种不同类型的欺骗攻击，攻击者可能会利用伪造的 IP 数据包源、电子邮件或者网站来欺骗受害者接收恶意数据。从历史上看，IP 欺骗流行于二十世纪九十年代。电子邮件伪造需要黑客伪造一个电子邮件的不同字段。网站欺骗是指攻击者制作一个看起来合法的网站使受害者输入他们的信用卡号码或其他类型的个人信息。要防止 IP 欺骗攻击，需遵循 1995 年的 CERT 建议：“防止 IP 欺骗的最佳方法是安装过滤路由器，限制你的外部界面的输入，如果数据包中有你内部网络的源地址，则不允许数据包通过。此外，你还应该过滤掉源地址与你内部网络不一致的传出数据包，从而防止源 IP 欺骗攻击来自您的网站。”

为了保证数据包的保护措施到位，您可能还需要检查您的 ISP。如果攻击者不能发送伪造的 IP 数据包，他们可能会尝试进行拒绝服务攻击或攻击外部主机，从而使攻击看起来像来自不同的网络（这样就更难停止攻击）。

若要防范电子邮件欺骗或伪造，你可以使用反垃圾邮件软件，并且培训你的用户查看电子邮件标头，以识别可疑的信息，也可以在电子邮件中添加签名，以便接收方知道是谁发送的。关于电子邮件欺骗，CERT 也有较好的建议。

要防范网站欺骗，请确保你访问的是通过 SSL/TLS 的网站。非 SSL/TLS 网站为黑客提供了大量的欺骗机会，所以如果您希望避免这种情况，请确保访问的网站是 SSL/TLS。

但是，即使使用 SSL/TLS 也存在威胁。因为可能会发生中间人攻击，它是一种欺骗攻击，它会使 DNS 和 SSL/TLS 连接或路线中毒，并将你定向到恶意站点。要抵御这类攻击，您需要确保你在具有最新更新（更新中间人漏洞）的软件上运行，并使用信任的网络（具有网络级别保护）。

（作者：Nick Lewis　译者：曾芸芸　来源：TechTarget 中国）

采用 pdf 附件的电子邮件安全性就高吗？

问：用电子邮件发送包含敏感信息的 pdf 附件安全吗？

答：首先，我们必须明确，单纯发送一封电子邮件或者发送带 pdf 格式附件的电子邮件并不会感染病毒或者恶意软件，但我想这并不是你真正想问的问题。通过电子邮件或者附件的方式发送敏感信息都是不安全的，并且，鉴于您所在企业的安全政策，这可能使你陷入很多麻烦之中。原因如下。

发送一封电子邮件就好像发送一张明信片：每个处理这封电子邮件的人或者系统都可以阅读和记录邮件的内容。当然，如果内容无利可图或者一点也不重要，这倒没有什么问题，然而，如果内容包含银行资料、网络密码或者其他类型的敏感数据，这将是一个很大的问题，包含明确禁止的反动言论也是一样。如果您通过电子邮件发送包含公司安全策略明文禁止的数据或者内容，你会因此招致麻烦。绝大多数具备安全意识的公司都会有涵盖敏感信息传输的政策和准则：哪些数据可以通过电子邮件发送，哪些必须被加密，等等。为了不冒犯这些政策，您应该与 IT 部门确认如何区分发送不同敏感等级的信息。

仅仅将敏感信息转换为 pdf 格式的文件来替代邮件正文并不能保护信息，除非使用 Adobe 的加密选项。文件必须签署数字标识并应用安全证书。Adobe Acrobat 允许创建自我签名的数字标识，在大多数情况下就足够安全了。

最安全的发送信息和附件的方式是在发送前将它们加密。除了在传输过程中保护附件，而且不管是存储在 PC 上，还是它通过的任意邮件服务器，或者最终到达收件者的机器上，文件加密都将为存储提供保护。在为他人提供可读的 pdf 文件之前，应考虑移除显示文档历史或者包含个人信息的内容，如将您的姓名列为作者的元数据。

另外，我建议在加密重要文件的同时对这些文件进行签名，这样收件人可以确信文件是由您发出的。如果收件人也有数字证书，您可以签署和加密信息，确保它不能被预期收件人以外的人更改或者阅读。作为一个良好的习惯做法，我总是将电子邮件写成明信片而不是信的格式，在电子邮件的正文添加致敬、数据和时间确保电子邮件的内容明确。发送出去的电子邮件或者附件可能被有意或无意的转发给许多其他人阅读。即使加密了电子邮件的内容或者 pdf 文档属性禁止打印或复印，但是没有什么可以阻止人们对内容显示屏拍照。

最近 pdf 文档中出现不少安全漏洞，因此如果你需要交流 pdf 文档，请确保计算机保持最新的补丁更新。确保计算机上安装、更新和运行了防病毒和反间谍软件，在打开电子邮件和文档前扫描它们。

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

如何用电子邮件数字证书来保证信息的安全

问：我刚刚收到同事的一封电子邮件（关于我们在一些国家的疟疾救援方案）。奇怪的是，邮件文本中几乎所有的国家名字都被移除/删除了。我们注意到，受到干扰的似乎只是那些国家名字，别的内容没有问题。这种干扰一定是在电子邮件传送过程中发生的。这种情况已经不是第一次发生了。您认为这其中可能的原因是什么呢？

答：尽管你的电子邮件中丢失了数据，但是如果不是敏感信息或者有价值的信息受到干扰的话，这种情况不太可能是恶意攻击。有可能是格式问题——你的电子邮件程序没有正确地处理或者显示了来自另一种电子邮件程序的内容。为了解决这类问题，你应该检查电子邮件程序的选项。比如，如果你使用的是 Microsoft Outlook，那么点击工具—选项，点击首选参数按钮。在这里你可以改变消息的外观显示，并改变处理它们的方式。

如果这样还不能解决你的问题，而且你确定你的电子邮件在传输过程中被拦截，或受到干扰，那么你和你的同事需要使用电子邮件数字证书对电子邮件进行签名和加密。数字证书将保证只有收件人才可以阅读邮件，而且收件人能够验证邮件是否被篡改。

数字证书包括一个私有密钥（存储在发件人的计算机中）和一个含有相关公共密钥的证书。你可以从 Certification Authority（CA 认证机构）那里获得数字证书，比如 VeriSign 公司。VeriSign 公司的电子邮件加密传送（Secure Email）产品——1 级数字标识（Class 1 Digital ID），价格为 19.95 美元。这些数字证书以及其他的证书能与那些遵从 S/MIME 协议的电子邮件客户端（比如，Microsoft Outlook、Outlook Express、 Mozilla Thunderbird，或者 Apple Safari 等等）相兼容。

对电子邮件进行签名和加密的数字证书是绑定在你的有效电子邮件地址上的。通过它，你的邮件收件人知道消息来自你的电子邮件地址，而且从你发送电子邮件到他们收到电子邮件这段时间内消息是保密的，没有被修改过。签名的电子邮件还可以提供所谓的不可否认的证据，可以防止发件人后来否认他/她发过这个邮件。

如果你想通过电子邮件给同事发送机密信息，你需要有他们的数字证书的副本，获得他们的证书其实很简单。当有人给你发送带有数字签名的消息时，电子邮件程序都会附带发件人的数字证书，其中含有所发送消息的公共密钥。这样做的话收件人就能够验证发件人的签名是否正确，并且可以确认该消息是否被篡改。你的同事给你发送了带有他签名的电子邮件之后，你

可以把他的证书保存在你的电脑上，然后用他的公共密钥来加密回复给他的信息，反之亦然。这样，你的加密消息只有你的同事才能阅读，别人不可以。VeriSign 公司有许多不错的关于电子邮件加密的手册，可以很好地指导大家如何进行数字签名以及怎样使用各种邮件程序对电子邮件消息进行加密。

当然，你一定要考虑信息发送给同事之后的安全性问题。一旦收件人解密并且阅读了你发送的信息，别人就可以无限制的复印或者打印那些信息，所以在发送邮件之前一定要考虑邮件内容的性质和敏感性。你还必须要保护好与数字证书相关的私有密钥，因为它实际上就是你的数字身份识别码。

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

抗击网络钓鱼的关键：电子邮件认证方式

在旧金山召开的 2010 RSA 会议中，安全专家们在周三的一次小组讨论中提到，越来越多的公司需要采取电子邮件认证方式来有效阻截越发频繁和复杂的网络钓鱼及垃圾邮件问题。

“以前拼写和语法错误曾是垃圾邮件的特征之一，现在这种情况正在渐渐消失。” Todd Inskeep 这样说道，他是美国银行的资深副总裁，他的工作内容专注于认证，客户保护和社会空间方面。

“由于现在坏人们变得越来越老练，我们真的需要技术解决方案来保护我们所有的客户，这个问题非常紧迫。”他在一个关于如何通过对抗网络钓鱼和欺诈以保护电子邮件安全的小组上这样说道。

“很多用户的电脑系统受网络钓鱼的攻击感染病毒，这使得降低非法邮件数量这个问题变得非常紧迫。”Paul Smocer 这样说道，他是 BITS 的安全副总裁，BITS 是金融服务业论坛的一个部门，是一个关注最佳实践和技术基础结构的金融服务领导人的论坛。他另外补充道，由于网络钓鱼现象的存在，金融产业由于品牌信誉受损而遭到沉重打击。从声誉的角度来看，存在这样的情况对我们的产业一点好处也没有。

小组成员说，电子邮件认证方式和协议在对抗网络钓鱼问题上还有很长的路要走，去年，BITS 发表了一篇用于实施 DKIM 和 SPF（通过域钥鉴别的邮件和发送者策略框架）的指导性文章。SPF 的目标是通过提供一个可供邮件发送者认证的框架来防止邮件的滥发，DKIM 允许组织对外发的邮件的邮件头上增加上一个加密的签名，以证明这封邮件是从这个域中发送出来的。

从小组讨论中所给出的统计数据来看，从 18 个月前只有 20%的邮件带有 SPF 记录，到现在已经有 51%的邮件带有 SPF 记录。在相同时期，通过 DKIM 认证的邮件比例从 2%上升到 16%。

雅虎邮件的资深产品管理总监 Mark Risher 说：“我们希望鼓励更多的公司来认证他们的邮件，那样他们就不会成为薄弱环节。”

Smocer 说，如果将电子邮件认证和信任推进到一个更高的阶段，那将允许金融机构使用电子邮件来为客户提供更多的服务，而不只是提供警报。如果我们可以保证安全问题，那么将有很多机会可以用来加强金融机构通过电子邮件可以提供的服务。

但是小组成员说，电子邮件认证方式和技术是有限制的。Smocer 说，拥有多种业务的大机构经常会有超过几十个并没有通过中央管理的域。同时，小机构可能缺乏擅长电子邮件认证的人员。还存在制定机构和多家 ISP 在他们所创建的关于 SPF 和 DKIM 的规则集上达成一致的问题。

Smocer 说，“我们正在尝试创建一个核心服务，它可以提供一个流程，通过这个流程金融机构可以创建他们自己的规则集，而且 ISP 们可以对它们进行检查。”

Inskeep 说，“同样，问题也存在于发送邮件的商业合伙人上，美国银行有很多合伙人，他们会以美国银行的名义发送电子邮件，所以很紧迫的一点是，要和你的商业合伙人建立一个联盟，并把他们包括进来。”

Steve Jones 是美国银行的副总裁兼架构师/战略家，他说：“实施电子邮件认证的第一步是建立从所有业务线上买进的策略，你需要全组织的支持。”

小组成员注意到电子邮件认证并不是最终的解决方案，而只是一层安全保护。CISCO 公司的首席安全研究员，讨论会的主持人 Patrick Peterson 表示：“即使它通过了认证，也并不意味着它是可信赖的。”但随着行业推进电子邮件认证进程的深入，以及大公司越来越多地鼓励厂商去支持这样的协议，那么对于小公司来说，就更容易采取这样的解决方案。

Smocer 说：“你可以从对你来说最重要的区域开始着手。”另外他补充道：“欺骗性电子邮件问题将会随着电子邮件认证在整个行业的采用而得到解决。”

（作者：Marcia Savage　译者：陈运栋　来源：TechTarget 中国）

超越邮件的移动应用之：电子邮件的扩展

很多公司都采用了某种形式的移动电子邮件，这是他们跨入无线应用的第一步。但是有的企业仍然在是否采用连接到后端办公系统的应用上犹豫不决。尽管在邮件的配置已经成熟并获得了成功，企业仍然在更复杂的应用上非常不放心。他们担心在小型设备上工作的复杂性、配置成本、安全性和用户不愿应用等问题，还有如果在早期的实施上有了不成功的经历，他们也会在再次配置的时候畏手畏脚。 但是不愿意配置应用已经是过时的思想了。意识超前的公司都在短期内配置成本合理的移动应用，而且通常都是在现有的基础架构上。而且他们在终端用户生产力和业务效率上都有重大的收获。

希望给员工配置移动解决方案的企业应该在开始的时候制定战略规划，关注点应该是用户完成工作的需求、已有而且可用的基础架构的类型、以及在以后的几年中业务需求将发生什么样的变化。移动策略的最后一部分特别重要，因为它将决定现在要实施什么，而且也决定了以后提高和改善业务所要求得灵活程度。如果没能考虑到业务的长期需求，那么就意味着移动方案将会是一个不能随着业务变化或增长的方案，也不能代表不够好的投资策略，而且可能要求短期内方案的裂缝和替换。

电子邮件的扩展

大部分开发了简单移动应用的企业都可以利用这些应用包含用户和企业更广泛的需求。例如，配置了无线邮件方案的企业可以把应用的核心的功能扩展到向用户交付推送双向的数据，这可以通过在后端办公方案中包含目标连接实现的，特别是在交互行为包含在基础形式的应用中的时候。大部分现代的移动方案，包括所有无线邮件系统，都可以提供这样的应用扩展机制。

当然，设备的限制也需要考虑到，而且很复杂，实际上不活跃的应用最好保持在高端的设备上（例如，笔记本电脑）。但是移动员工的很大一部分可以获得授权连接到使用现有基础架构的简单应用上，这可以通过 XML 或者其他基于 Web 的方式和使用已有的可见应用开发工具实现。虽然不适合所用的情况，但是这些相对轻松的配置和低成本让这种扩展方案深受各种业务需求的吸引。

（作者：TechTarget　译者：Tina　Guo　来源：TechTarget 中国）

为什么中型企业转向云电子邮件服务

Erik Dubovik 是波士顿的私募股权公司 Audax Group LP 的信息技术副总裁，最近 TechTarget 就中型企业转向云计算服务的趋势对其进行了采访。在采访中 Dubovik 主要谈及了以下内容：云电子邮件在中型企业得以大规模应用的原因、为什么 IT 经理们会觉得无法说清楚什么是云、他如何被管理层问及云服务相关的问题。Audax Group 管理着约 30 家公司的 40 亿美元资金。

为什么 IT 经理对云计算服务以及其使用的看法会有如此大的不同？

Dubovik：部分原因是由于云被过分渲染了——大家都听到了太多云的前景描述，但是对于我们公司来说，云计算只在相当有限的范围内适用。

对我来说把任何应用放到云里是不可能的，对于存储需求来说也是一样。从理论上说我可以从 Amazon 购买弹性计算能力和存储，或者从 Saleforce.com 购买 CRM 服务，甚至有很多可以为小企业所用的免费 SaaS 服务。但是，魔鬼隐藏在细节里，有很多细节使得现实情况完全不一样，比如购买存储，如果是用于归档的单向（unidirectional）存储，那么云存储是非常不错的，价格便宜而且你只需把信息发送出去就行。如果是双向存储，则意味着既有发送也有取回数据的过程，这类云存储服务和传统的存储产品相比未必便宜，尤其是在目前存储价格下滑较快的情况下。

贵公司的高管们就云计算服务向你询问了哪些问题？

Dubovik：他们的问题主要集中在两个方面：基于云的电子邮件和 CRM 服务会带来哪些好处？关于后一点主要是因为 Salesforce.com 不止能提供 CRM 服务，还能通过其应用和开发平台（Force.com）提供基于云的业务扩展。

高管们可能从同行那里听说了云电子邮件，因此他们想知道这东西是否能为我们带来更低成本的解决方案。此外，他们还想知道迁移到云的深远意义，以及我们是否需要制定一个云战略。

那么你是怎么回答的呢？

Dubovik：我的回答是我们还需要继续调研。任何一个 IT 类工作都需要不断地了解和评估相关技术。我们正在和咨询公司以及业界同行一起调查研究云计算能在本行业的哪些具体领域内实现成本降低或效率提升。

你认为是什么原因导致云电子邮件成为一个热点的？

Dubovik：对于小企业来说，这样就无需为电子邮件建设基础设施了，通过云电子邮件服务就可以获得邮件归档、邮件托管、垃圾邮件过滤甚至通过移动设备访问等功能。我认为在今后两到三年内会有大量中型企业采用基于云的电子邮件及归档服务。

为什么会有这种大规模的迁移趋势呢？

Dubovik：云电子邮件已经发展得比较成熟了，而且从基础架构的角度看电子邮件系统相对简单。比如微软的 Exchange 和 Exchange 服务器，可以为其配置相应的计算能力、本地存储、备份策略、业务连续性和灾备流程。电子邮件系统在基础架构方面有明确清晰的定义，可以相对容易地转向到云服务或者高级托管服务。

大量的中型企业拥有 Exchange Server 2003 或者更老的硬件设施，而现在 Exchange 2010 已经发布了两个版本，其甚至相对于 2007 版都具有更出色的 I/O 性能，可以说 Exchange 2010 在性能和高可用性方面都有较大进展。于是你将面临这样的选择：是将有限资源投入到电子邮件系统还是投入到业务系统中？而后者对提高收入和削减成本有直接作用，再加上更新硬件、构建高可用系统以及归档的成本，那么很显然，把电子邮件相关的基础设施和管理放到企业外部是很现实的考虑。

还有其他因素导致中型企业采用云电子邮件吗？

Dubovik：Gmail 提供 2G 的起始容量和搜索等功能，在不知不觉中使终端用户对企业邮箱的期望值大大提高了，这对于那些无法拥有相应设施甚至存储的中小企业是很大的挑战。

因此，转折点来临了 -- 面对新版本 Exchange 的发布，IT 团队列出了 2010 版的改进，而业务团队负责做出抉择：用 4 个礼拜时间来升级电子邮件系统然后进行监控？还是把这些事情干脆抛开？

你是如何考虑本公司在云电子邮件方面的举措？

Dubovik：对于我们 IT 团队来说，通过电子邮件系统来测试和了解软件即服务（SaaS）或者云计算是相对安全的，可以为今后采用其他的云服务做好准备。

（作者：Christina Torode　译者：木易　来源：TechTarget 中国）