实战讲解防范网络钓鱼技术大全

实战讲解防范网络钓鱼技术大全，此文是笔者为 CCIDNET 写的一篇约稿，希望指正。原文链接：转自：http://tech.ccidnet.com/art/302/20060106/408699_1.html

作者：曹江华

网络钓鱼(Phishing)一词，是“Fishing”和“Phone”的综合体，由于黑客始祖起初是以电话作案，所以用“Ph”来取代“F”，创造了”Phishing”,Phishing 发音与 Fishing 相同。“网络钓鱼”就其本身来说，称不上是一种独立的攻击手段，更多的只是诈骗方法，就像现实社会中的一些诈骗一样。攻击者利用欺骗性的电子邮件和伪造的 Web 站点来进行诈骗活动，诱骗访问者提供一些个人信息，如信用卡号、账户用和口令、社保编号等内容（通常主要是那些和财务，账号有关的信息，以获取不正当利益），受骗者往往会泄露自己的财务数据。诈骗者通常会将自己伪装成知名银行、在线零售商和信用卡公司等可信的品牌，因此来说，网络钓鱼的受害者往往也都是那些和电子商务有关的服务商和使用者。

一、网络钓鱼工作原理图

现在网络钓鱼的技术手段越来越复杂，比如隐藏在图片中的恶意代码、键盘记录程序，当然还有和合法网站外观完全一样的虚假网站，这些虚假网站甚至连浏览器下方的锁形安全标记都能显示出来。网络钓鱼的手段越来越狡猾，这里首先介绍一下网络钓鱼的工作流程。通常有五个阶段：

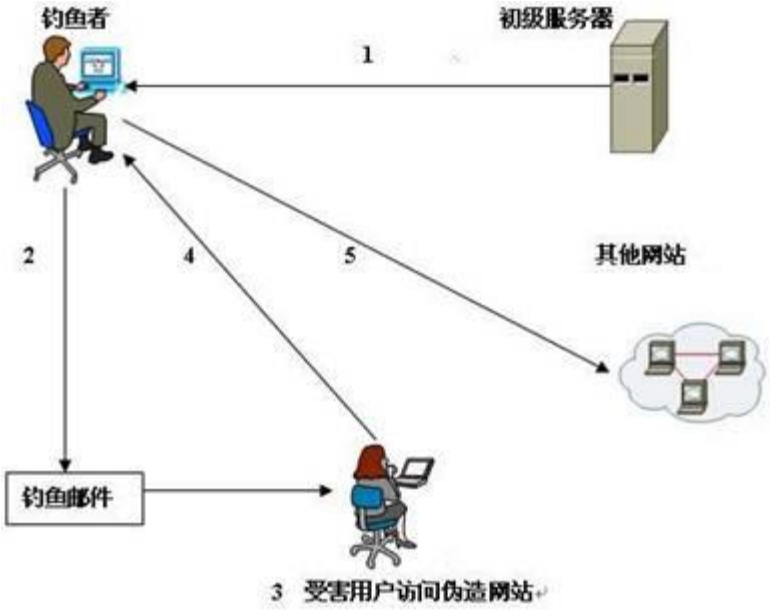

图 1 网络钓鱼的工作原理

1. 钓鱼者入侵初级服务器，窃取用户的名字和邮件地址

早期的网络钓鱼者利用垃圾邮件将受害者引向伪造的互联网站点，这些站点由他们自己设计，看上去和合法的商业网站极其相似。很多人都曾收到过来自网络钓鱼者的所谓“紧急邮件”，他们自称是某个购物网站的客户代表，威胁说如果用户不登录他们所提供的某个伪造的网站并提供自己的个人信息，这位用户在购物网站的账号就有可能被封掉，当然很多用户都能识破这种骗局。现在网络钓鱼者往往通过远程攻击一些防护薄弱的服务器，获取客户名称的数据库。然后通过钓鱼邮件投送给明确的目标。

2. 钓鱼者发送有针对性质的邮件

现在钓鱼者发送的钓鱼邮件不是随机的垃圾邮件。他们在邮件中会写出用户名称，而不是以往的“尊敬的客户”之类。这样就更加有欺骗性，容易获取客户的信任。这种针对性很强的攻击更加有效地利用了社会工程学原理。很多用户已经能够识破普通的以垃圾邮件形式出现的钓鱼邮件，但是他们仍然可能上这种邮件的当，因为他们往往没有料到这种邮件会专门针对自己公司或者组织。根据来自 IBM 全球安全指南(Global Security Index)的报告，被截获的钓鱼事件从 2005 年一月份的 56 起爆炸性地增长到了六月份的 60 万起。

3. 受害用户访问假冒网址

受害用户被钓鱼邮件引导访问假冒网址。主要手段是

(1）IP 地址欺骗。主要是利用一串十进制格式，通过不知所云的数字麻痹用户，例如 IP 地址 202.106.185.75，将这个 IP 地址换算成十进制后就是 3395991883，Ping 这个数字后，我们会发现，居然可以 Ping 通，这就是十进制 IP 地址的解析，它们是等价的。

（2）链接文字欺骗。我们知道，链接文字本身并不要求与实际网址相同，那么你可不能只看链接的文字，而应该多注意一下浏览器状态栏的实际网址了。如果该网页屏蔽了在状态栏提示的实际网址，你还可以在链接上按右键，查看链接的“属性”。

（3）Unicode 编码欺骗。Unicode 编码有安全性的漏洞，这种编码本身也给识别网址带来了不便，面对“%21%32”这样的天书，很少有人能看出它真正的内容。

4. 受害用户提供秘密和用户信息被钓鱼者取得

一旦受害用户被钓鱼邮件引导访问假冒网址，钓鱼者可以通过技术手段让不知情的用户输入了自己的“User Name”和“Password”，然后，通过表单机制，让用户输入姓名、城市等一般信息。填写完毕。他现在要用户填写的是信用卡信息和密码。一旦获得用户的帐户信息，攻击者就会找个理由来欺骗用户说“您的信息更新成功！”，让用户感觉很“心满意足”。 这是比较常见的一种欺骗方式，有些攻击者甚至编造公司信息和认证标志，其隐蔽性更强。一般来说，默认情况下我们所使用的 HTTP 协议是没有任何加密措施的。不过，现在所有的消息全部都是以明文形式在网络上传送的，恶意的攻击者可以通过安装监听程序来获得我们和服务器之间的通讯内容。

5. 钓鱼者使用受害用户的身份进入其他网络服务器

下面钓鱼者就会使用受害用户的身份进入其他网络服务器（比如购物网站）进行消费或者在网络上发送反动、黄色信息。

二、Linux 用户对网络钓鱼的防范

Linux 用户访问互联网的两个主要工具是浏览器和电子邮件。下面就从这两个方面作起。

1.电子邮件防范网络钓鱼的设置

Linux 下电子邮件软件很多，其中 Mozilla 基金会的雷鸟（Thunderbird）是比较常用和安全的。

(1)升级电子邮件软件雷鸟到 1.1 以上。

首先建议您将电子邮件软件雷鸟（Thunderbird）到 1.1 以上，在雷鸟 1.1 版本中实现的新功能包括实现了防止网钓（phishing）攻击警告系统。在新的 Thunderbird 功能里，当使用者点选电子邮件里疑似网钓的 URL （网址）时，侦测器会在网页打开之前以对话框

提醒使用者，Gemal 写道。当网址内有数字型的 IP 位址而不是用域名名（domain name），或者 URL 和文字链结里所显示的网络地址不一样时，侦测器就会启动。见面见图 2。

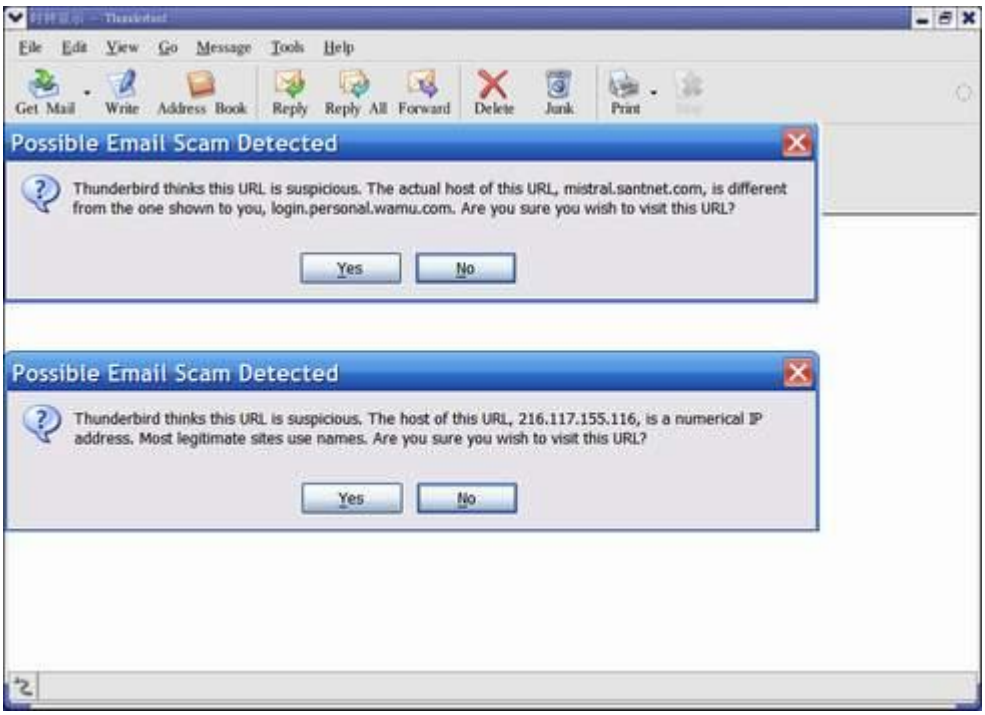

图 2 1.1 版本以上的雷鸟可以防范网络钓鱼

另外也可以通过一个 SPF 插件防范网络钓鱼，下载链接：http://taubz.for.net/code/spf/thunderbird-sve.tgz 。安装 SPF 插件后当用户点击网络钓鱼邮件中的链接时，雷鸟的 SPF 插件将检测这一地址或者链接文字与实际地址不相符时都将发出警告，并弹出警告对话框提醒用户。工作界面见图 3。

图 3 使用 SPF 插件防范网络钓鱼

（2）关闭雷鸟的预览面板

许多网络钓鱼邮件只需要在电子邮件收发程序的预览面板中显示就能侵入你的计算机。因此我们建议用户关闭收件箱的预览面板。在 Mozilla 雷鸟中，打开“Layout ” ->，清除“ “Messages pane”复选框(或者使用“F8”快捷键关闭预览面板)，见图 4。

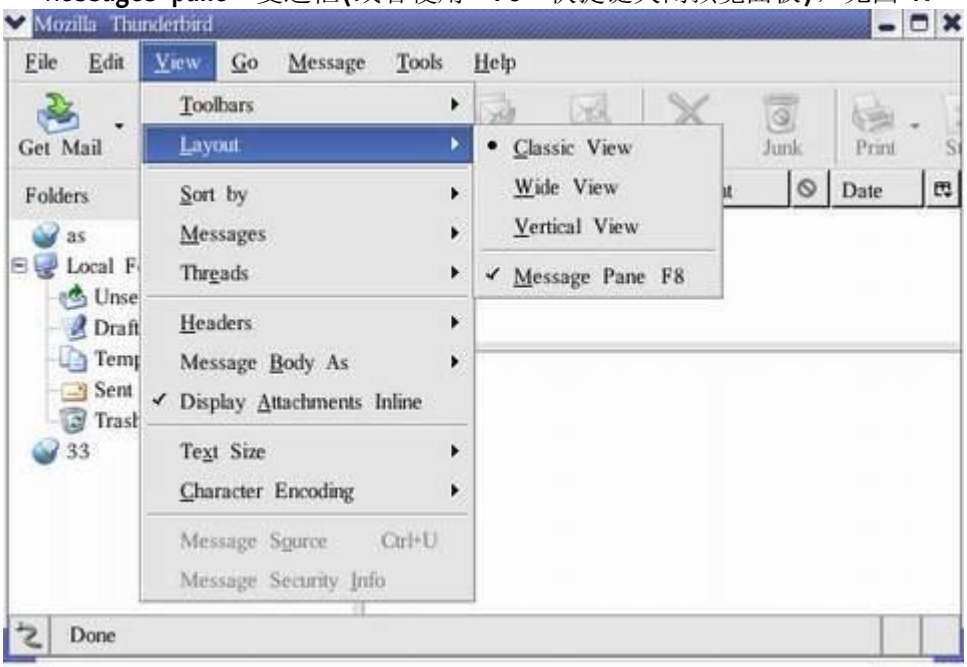

图 4 关闭雷鸟的预览面板

（3）以纯文本方式阅读电子邮件

许多网络钓鱼邮件都是通过 HTML 代码来达到其不可告人的目的，因此如果你以纯文本方式阅读这些邮件就会让它们无计可施。在 Mozilla 雷鸟中，选择“view” ->“Message body As” -> “Plain text”复选框。见图 5。

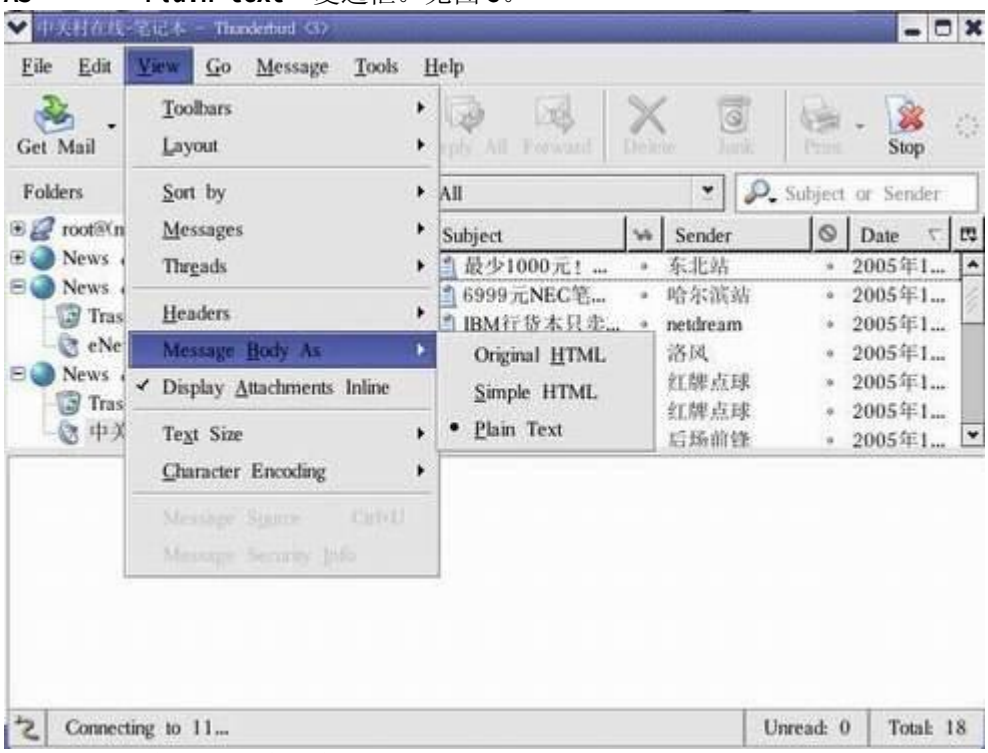

图 5 以纯文本方式阅读雷鸟电子邮件

（4）不要把字符 Unicode 编码

Unicode 编码有安全性的漏洞，这种编码本身也给识别网址带来了不便，所以不要把雷鸟的字符集设置为 Unicode 编码。

2.浏览器防范网络钓鱼的设置

（1）增强火狐（Firefox）的安全性。

火狐是 Linux 下最佳浏览器，当然火狐也存在一些安全隐患。丹麦安全产品开发商 Secunia 于 7 月 30 日公开了 Web 浏览器“Mozilla”与“Mozilla Firefox”的安全漏洞。如果恶意使用安全漏洞，可以伪装地址栏、工具栏、SSL 对话框等用户界面。可伪装的不仅是地址栏，还有工具栏、表示进行 SSL 通信的加密标记等，甚至可以伪装点击加密标记后所显示的数字证书。

Secunia 提出的对策是“不要点击不可靠的网站链接”，“不要随便输入个人信息”，一定要记住：眼见不一定为实。升级到最新版本可以消除这些安全隐患。另外，将 JavaScript 设为无效也可防止伪装。另外网络钓鱼者在用户输入数据后，还可以通过巧妙的 Javascript 脚本来迷惑用户。仿冒的站点提供了很多银行的连接，这样就给人以可信的感觉，实际上也是一种社会工程学的暗示。用户输入账号信息后，钓鱼者可能就在后面窃喜了，因为，网站早已通过巧妙的脚本设计，使用户相信自己的数据确实得到了更新。要想对网站禁用 Javascript，必须下载并安装插件 NoScript，它由 Giorgio Maone 开发。用 Firefox 浏览网页时，如果页面中使用了 Javascript，NoScript 将会在 Web 页面下方显示一个警告栏。单击这个警告栏可以对这个网站上的脚本进行控制，既可以是暂时的也可以是永久的，另外还能对脚本进行禁用或者其他操作。这个程序还可以禁用 Flash 动画或者其他 Firefox 插件。NoScript 是免费软件，官方网站是：http://www.noscript.net 。下载链接：http://releases.mozilla.org/pub/mozilla.org/extensions/noscript/noscript-1.1.3.4-fx+fl+mz.xpi ，NoScript 配置界面见图 6。

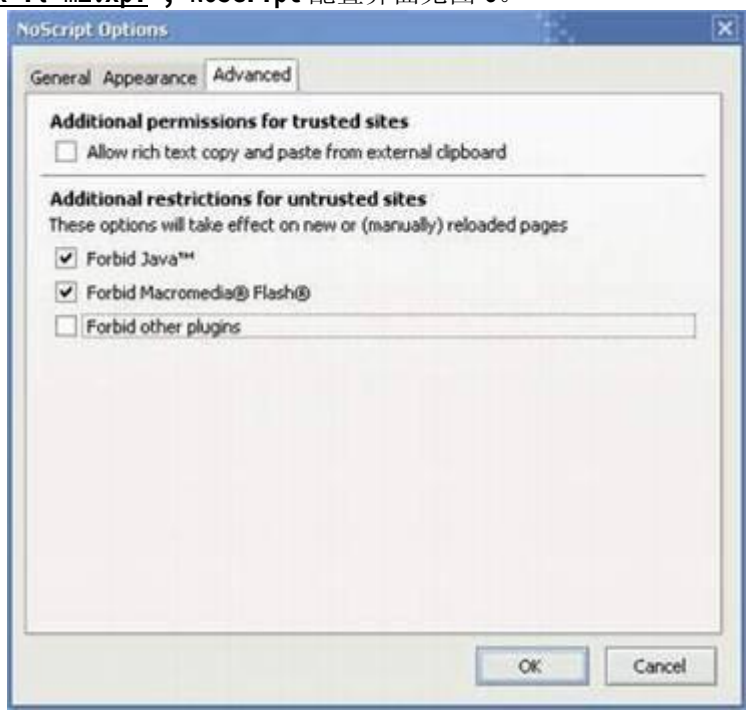

图 6 NoScript 配置界面

（2）安装 Netcraft Toolbar

2004 年互联网服务厂商 Netcraft 已经发布了它自己的火狐安全工具插件。这款插件能够帮助 Firefox 用户免受钓鱼式欺诈攻击。Netcraft Toolbar 能够封杀由其他用户报告的钓鱼式欺诈网站。Netcraft 去年 12 月份发布了的 Netcraft Toolbar 目前，被发现和封杀的钓鱼式欺诈攻击网站达到了 7000 多个。除了封杀钓鱼式攻击网站外，Netcraft Toolbar 还包括能够帮助用户在上网时更注重安全的其它功能。例如，它能够对网站的危险性“打分”，显示有关网站的访问量和网站所在国家的信息。 Netcraft Toolbar 还能够根据使用的字符“诱捕”可疑的网站，强制显示浏览器的导航按钮，打击企图隐藏这些按钮的弹出式窗口。

Netcraft Toolbar 能够在火狐支持的所有操作系统（Linux、BSD、Windows、MaC）上运行，用户可以免费从 Netcraft 的网站上下载这款工具条。 官方网址是：http://www.noscript.net ，下载链接：http://freebsd.ntu.edu.tw/mozilla/extensions/netcrafttoolbar/netcrafttoolbar-1.1.1.1-fx.xpi ，Netcraft Toolbar 安装文件是：netcrafttoolbar-1.1.1.1.xpi。在浏览器的菜单中选择文件－打开文件－然后选择你要安装的 XPI 扩展插件文件。稍后就可以看到浏览器会询问你是否要安装这个插件,点击“是”即可，这样做是为了安全，因为默认情况下，你无法从任何网站安装插件。另外注意新安装的插件必须在重启浏览器后才能生效（关闭所有的浏览器窗口，包括扩展，主题等窗口）。Netcraft Toolbar 工作界面见图 7。

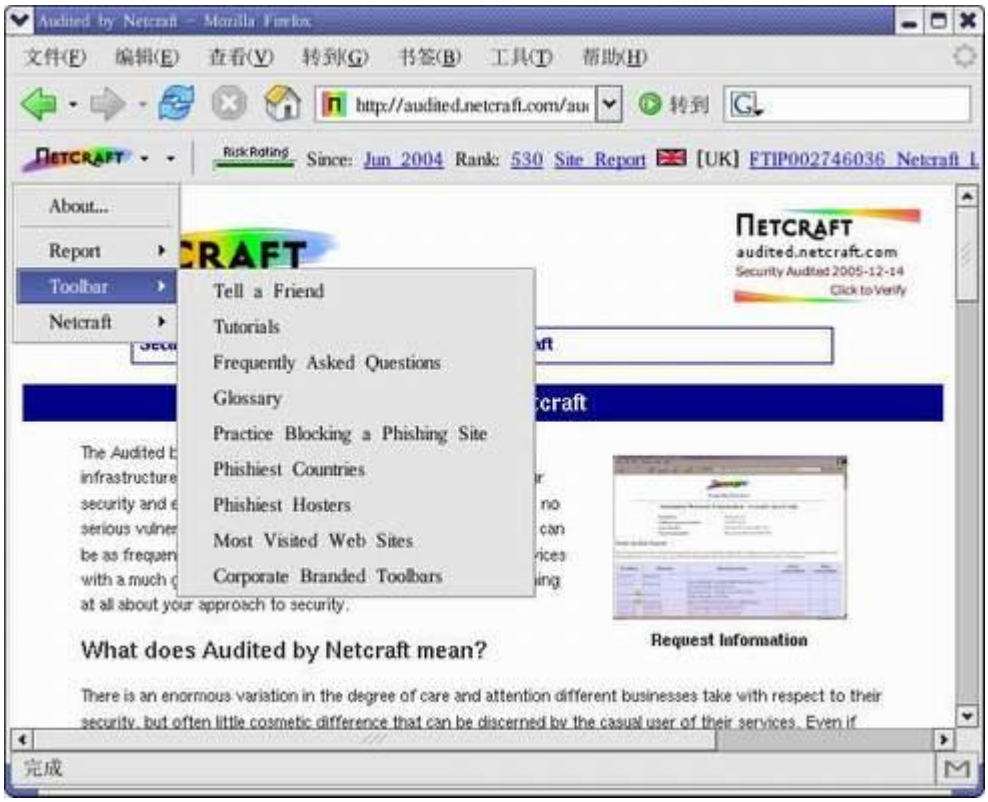

图 7 Netcraft Toolbar 工作界面

三、其他方面

1.个人的责任

针对网络钓鱼的性质，往往是为了获取和电子商务有关的账号密码，进而获取一些经济利益，因此我们应该从 3 个方面养成一个良好的习惯。

（1）妥善选择和保管密码

密码应避免与个人资料有关系，不要选用诸如身份证号码、出生日期、电话号码等作为密码。建议选用字母、数字混合的方式，以提高密码破解难度。尽量避免在不同的操作系统使用同一密码，否则密码一旦遗失，后果将不堪设想。黑客们经常用一些常用字来破解密码。曾经有一位美国黑客表示，只要用“password”这个字，就可以打开全美多数的计算机。其它常用的单词还有：account、ald、alpha、beta、computer、dead、demo、dollar、games、bod、hello、help、intro、kill、love、no、ok、okay、please、sex、secret、superuser、system、test、work、yes 等。密码设置和原则：

1.足够长，指头只要多动一下为密码加一位，就可以让攻击者的辛苦增加十倍；

2. 不要用完整的单词，尽可能包括数字、标点符号和特殊字符等；

3.混用大小写字符；

（2）做好交易记录

客户应对网上银行办理的转账和支付等业务做好记录，定期查看“历史交易明细”、定

期打印网上银行业务对账单，如发现异常交易或账务差错，立即与银行联系，避免损失。

（3）管好数字证书

网上银行用户应避免在公用的计算机上使用网上银行，以防数字证书等机密资料落入他人之手，从而使网上身份识别系统被攻破，网上账户遭盗用。

2.企业领导和网络管理员的责任

当被问及如何防范网络钓鱼时，安全专家立刻会说加强对用户的教育。很多人要通过专门学习之后才知道电子邮件的附件不可以随便打开。常识无法“升级”，智力不能“安装”，在网络安全这根链条上，人总是最薄弱的环节。仅仅告诫人们网络钓鱼的危害是不够的，安全专家敦促企业不要发送包含网络链接的电子邮件。企业不应当在电子邮件中包含链接，并且要确保用户清楚这一点，另外网络钓鱼利用人类常见的各种感情，如信任、恐惧、贪婪、善良，几乎所有的网络钓鱼都涉及社会工程学的技巧。最近常见的手法比如让收到邮件的用户填写一个表单，以便得到职位、奖金或者礼物。在节日临近时，钓鱼者发出很多钓鱼邮件。不断进行用户教育是必需的。另外不同的企业应该共享网络钓鱼信息，建立联盟。为了防范那些利用仿冒网址而危及用户利益的事件发生，在美国和英国已经成立了专门反假冒网址等网络诈骗的组织，比如 **2003** 年 **11** 月成立的 **APWG(Anti-Phishing Working Group)**和 **2004** 年 **6** 月成立的 **TECF(Trusted Electronic Communications Forum)**。一些国外公司的主页底部也设有明显链接，以提醒用户注意有关 **E-mail** 诈骗的问题。而国内许多公司的主页似乎还没有这种安全防范意识，同时也没有类似的组织去专门研究这方面的应对之策。

另外对于 Linux 网络管理员要为 Apache 服务器配置 SSL。SSL 可以用于在线交易时保护信用卡号、股票交易明细、账户信息等。当具有 SSL 功能的浏览器与 WEB 服务器(Apache)通信时，它们利用数字证书确认对方的身份。数字证书是由可信赖的第三方发放的，并被用于生成公共密钥。因此，采用了安全服务器证书的网站都会受 SSL 保护，其网页地址都具有“https”前缀，而非标准的“http”前缀。从目前钓鱼式攻击者的实践来看，大多没有这个标志，即使有，也可能是仿冒的比较容易识别，从而也这就进一步揭穿了他们的把戏。通常现在网络钓鱼者往往通过远程攻击一些防护薄弱的服务器，攻击手段是网络嗅探，注意如果您确信有人接了嗅探器到自己的网络上，可以去找一些进行验证的工具。这种工具称为时域反射计量器(Time Domain Reflectometer，TDR)。TDR 对电磁波的传播和变化进行测量。将一个 TDR 连接到网络上，能够检测到未授权的获取网络数据的设备。对于防范嗅探器的攻击最好的方法是：

（1）安全的拓扑结构。

（2）会话加密。

（3）用静态的 ARP 或者 IP－MAC 对应表代替动态的 ARP 或者 IP－MAC 对应表

（4）使用专用硬件仪器。

3. 勤打补丁

无论是网络管理员还是个人用户都应该经常到你所安装的系统发行商的主页上去找最新的补丁。操作系统是计算机系统灵魂，维护着系统的底层，对内存、进程等子系统进行管理和调度。如果操作系统本身出现了漏洞，其影响将会是致命的。操作系统的内核，对于网络安全是至关重要的。目前，内核的维护主要分两种模式：对于私有操作系统，如 **Windows/Solaris** 等，由于个人用户不能直接接触其源代码，其代码由公司内部开发人员维护，其安全性由同样的团队保证，内核的修正与其他应用程序一样，以 **patch/SP** 包的方式发布。对于 **Linux** 这样的开放式系统，是一种开放的结构。应该说，开放的模式是双刃剑。本文介绍的雷鸟和火狐等都是开源软件，而且都在不停升级，稳定版和测试版交替出现。在 **http://www. Mozilla.org/**上最新的 **ChangeLog** 中都写着：**bug fix, security bug fix** 的字样。所以要经常的关注相关网站的 **bug fix** 和升级，及时升级或添加补丁。

四. Windows 用户对网络钓鱼的防范

Windows 用户访问互联网的两个主要工具是浏览器和电子邮件。下面就从这两个方面作起。

1.电子邮件防范网络钓鱼的设置

Windows 下电子邮件软件很多，其中 Mozilla 基金会的雷鸟（Thunderbird）和 Outlook 2003 以及 Outlook Express 6 是比较常用。雷鸟设置方法查看前文，这里介绍后两者。

（1）关闭预览面板

一些钓鱼邮件只需要在电子邮件收发程序的预览面板中显示就能侵入你的计算机。因此我们建议用户关闭收件箱的预览面板。在微软 Outlook 2003，打开菜单“视图”，清除“自动预览”复选框。在 Outlook Express 6 中，打开“视图->布局”，清除“显示预览面板”复选框。

（2）以纯文本方式阅读电子邮件

许多恶意邮件都是通过 HTML 代码达到其不可告人的目的，因此如果你以纯文本方式阅读这些邮件就会让它们无计可施。在 Outlook 2003 中，打开“工具->选项->设置->电子邮件选项”，选中“以纯文本方式显示所有电子邮件”复选框。在 Outlook Express 6 种，打开“工具->选项->阅读”，选中“明文阅读所有信息”复选框。见图 8。

图 8 以纯文本方式阅读电子邮件

（3）小心处理电子邮件链接

钓鱼者攻击计算机的一条重要渠道是通过电子邮件。为了减小因为电子邮件而感染病毒的风险，在可疑电子邮件中不要点击链接，邮件中显示的文字往往会掩盖真实的 Web 地址。正确的做法是，在浏览器的地址栏中手工输入 URL，或者到网站的首页，然后再找到需要浏览的页面。

（4）不要把字符 Unicode 编码

Unicode 编码有安全性的漏洞，这种编码本身也给识别网址带来了不便，所以不要把字符集设置为 Unicode 编码。

2.IE 浏览器防范网络钓鱼的设置

（1）增强 IE 的安全性

将 IE 的安全级别设置为“中级”时，对 ActiveX 控件、小程序以及脚本的监控过于宽松。一些 Web 应用，比如在线购物的表单程序以及安全扫描程序需要 ActiveX 以及 Javascript 才能正常运行，但是打开这些功能也为恶意代码和黑客打开了方便之门。要想让 IE 更加安全，在 IE 中打开“工具->Internet 选项->安全->自定义级别”，在“安全设置”对话框下方展开下拉列表选择“高”，然后单击“重置”按钮。但是将 IE 安全级别设置为“高”之后，浏览器在访问网站时会不断弹出警告窗口。解决这个问题的方法是，将需要经常访问的网站添加到 IE 的“受信任的站点”列表中：选择命令“工具->Internet 选项->安全”，单击“受信任的站点”图标，然后单击“站点”按钮。输入网站地址，单击“添加”按钮。如果需要添加更多网站可以重复该操作。注意要清除“对该区域中的所有站点要求服务器验证(https:)”复选框。完成设置后，单击两次“确定”按钮。

（2）安装 Netcraft Toolbar

2004 年互联网服务厂商 Netcraft 已经发布了它自己的 IE 安全工具插件。这款插件能够帮助 IE 用户免受钓鱼式欺诈攻击。Netcraft Toolbar 能够封杀由其他用户报告的钓鱼式欺诈网站。Netcraft 去年 12 月份发布了的 Netcraft Toolbar 目前，被发现和封杀的钓鱼式欺诈攻击网站达到了 7000 多个。除了封杀钓鱼式攻击网站外，Netcraft Toolbar 还包括能够帮助用户在上网时更注重安全的其它功能。例如它能够对网站的危险性“打分”，显示有关网站的访问量和网站所在国家的信息。 Netcraft Toolbar 还能够根据使用的字符“诱捕”可疑的网站，强制显示浏览器的导航按钮，打击企图隐藏这些按钮的弹出式窗口。用户可以免费从官方网址是：http://www.netcraft.com/的网站上下载这款工具条。下载链接：http://dlc.pconline.com.cn/filedown.jsp?id=56955&dltypeid=1 ， Netcraft Toolbar 安装文件是：NetcraftToolbar.msi。Netcraft Toolbar 工作界面见图 9。

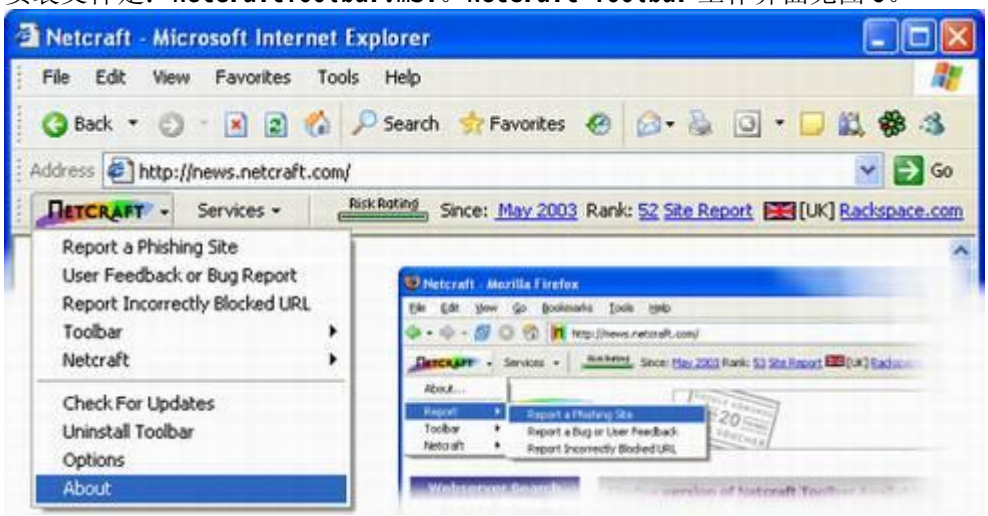

图 9 IE 浏览器的 Netcraft Toolbar 工作界面

（3）禁用 WSH

针对改写和重指向威胁，这种手段利用了 Windows 脚本，不需要用户点击电子邮件中的链接，只要邮件一打开，一段脚本就会被执行。这些代码将会改写受感染计算机的主机文件。如果修改成功，当用户登录网络银行时，他实际上会被指向伪造的网站。这个伪造的网站会收集用户输入的账号、密码以及其他个人信息。所以禁用 WSH 是一种选择。

（4）升级 IE 版本到 7.0

IE7 中内嵌的钓鱼欺诈过滤器主要是为了保护用户远离钓鱼欺诈网站，保护隐私，并且整个过程做到透明和灵活。微软会提供选择用或是不用的自由，所有发往反欺诈服务器的请求都将使用 SSL 进行加密。这就是钓鱼欺诈过滤器的设计原则。IE7 采用向反钓鱼欺诈服务器实时查询的方式，而不是像一些反间谍软件那样定时下载一份站点列表文件，选择实时查询的原因有二，一是它能比使用静态站点列表方式提供更好的保护；二是可以避免给网络增加过重的负载。欺诈过滤器确实可以定时下载一份已知为安全的站点列表，但钓鱼欺诈攻击可以在 24～48 个小时内转移到新的地址，这比发布站点列表要更快。另外如果要求用户不

断地下载站点列表还要考虑网络负载因素，目前可能用于发动钓鱼欺诈攻击的计算机数量要远远超过间谍软件的数量，每小时都去下载新的黑名单列表将会严重影响网络的正常流量。IE7 是利用以下经过欺诈过滤器的数据的，

- 如果你不亲自启动这项功能，过滤器将不会连接到反欺诈服务器，不会检查任何站点；
- 只有当一个站点不在 IE 所下载的“已知为安全”的站点列表里时，过滤器才会对其进行检查；
- 像 URL 中的查询字符串等潜在的敏感数据在被送到反欺诈服务器进行检查之前将被全部删除。其他和网络浏览相关的数据如 http cookies 等不会被送到微软那里；
- 通过使用加密的 SSL 连接，URL 将被安全地送到服务器中以保护隐私信息。

（5）其他

打开 Windows 的自动更新功能，在 Windows XP 中，打开“开始->控制面板->安全设置(在分类视图中)->自动更新”。在 Windows 2000 中，打开“开始->设置->控制面板->自动更新”。不管是哪个版本的 Windows 操作系统，确保选中“自动更新(推荐)”选项。另外，你还可以让 Windows 开始下载更新文件的时候通知你，或者进行手工更新。Windows XP Service Pack 2 中最受欢迎的新功能就是 Windows 安全中心，当计算机中的防火墙或反病毒软件没有打开或者没有及时更新时，安全中心会提出警告。Windows XP 自带的防火墙只能抵御一些外来的入侵行为，但是无法预防一些可疑的对外连接。我们推荐用户关闭 Windows XP 自带的防火墙，安装 Zone Labs 的 ZoneAlarm 或者其他第三方防火墙工具，这样才能有效地同时预防这两种安全威胁。

3.定期对 Windows 体检

无论是网络管理员还是个人用户都应该经常到你所安装的系统发行商的主页上去找最新的补丁。推荐使用微软发布的 MBSA1.2 来实现全方面检查 Windows 系统和应用软件的漏洞。Microsoft Baseline Security Analyzer（MBSA）工具允许用户扫描一台或多台基于 Windows 操作系统的计算机，以发现常见的安全方面的配置错误。MBSA 将扫描基于 Windows 的计算机，并检查操作系统和已安装的其他组件（如 IIS 和 SQL Server），以发现安全方面的配置错误，并及时通过推荐的安全更新进行修补。首先要把 Windows 2000 的浏览器升级到 IE5.01 以上，并且安装 MSXML Parser 3.0 以上版本（下载链接：http://download.microsoft.com/download/d/9/8/d9886528-6438-4828-9094-697103203a32/msxml3usa.msi ）这是因为 MBSA 检查报告存储格式是 XML，所以需要使用微软的 MSXML 解析器读取 XML 文档。http://download.microsoft.com/download/d/7/5/d757ff81-4f97-4a6d-a9d8-edea72363aa8/MBSASetup-en.msi 最新版本 1.23361.2。 安装 MBSA1.2 后在桌面上找到该工具的快捷方式。工作界面见图 10。

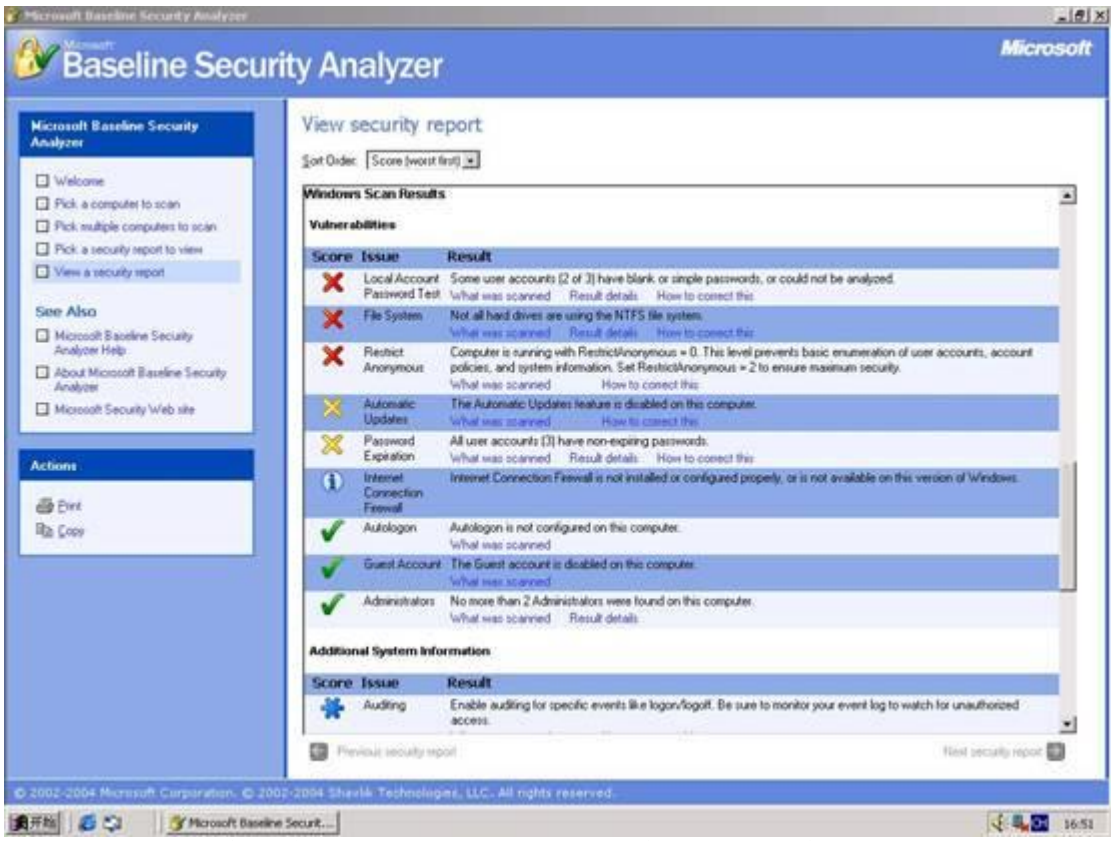

图 10 以不同颜色的符号，显示系统漏洞。如：绿色的“√”图标表示该项目已经通过检测。红颜色的“×”表明不安全的因素，黄颜色的“×”表明 MBSA 无法确认其安全性，二者（红色或黄色）的图标表示该项目没有通过检测，即存在漏洞或安全隐患。蓝色的“*”图标表示该项目虽然通过了检测但可以进行优化，或者是由于某种原因 MBSA 跳过了其中的某项检测。白色的“i”图标表示该项目虽然没有通过检测，但问题不很严重，只要进行简单的修改即可。对于第一个系统漏洞“Password test”的详细情况，点击“Result Details”可以看到它的详细解释。下面点击“How to correct this”可以得到如何修补这个漏洞的方法和建议以及下载补丁的网址。MBSA 是面向 Windows NT 4、Windows 2000、Windows XP 和 Windows Server 2003 系统的安全评估工具，MBSA1.2 不但能为我们找到系统需要的补丁,并且介绍给我们如何去做。

总结：

网络钓鱼之所以如此猖獗并且能够频频得手，最大的原因就是利用了人们疏于防范的心理以及“贪小便宜”和“贪图便利”的弱点。网络钓鱼投下足够吸引猎物上钩的“美味鱼饵”或恐吓，或诱惑，用户的防线在这些因素的干扰下彻底崩溃而咬住了钩子。这是任何软件也无法解决的，因为毒在心，而非工具软件。当然这些骗术也涉及了一些技术手段，但是社会工程学的影响却成了最大的干扰。