

By Steven Warren, MCSE, MCDBA

Some computer users (and even some IT professionals) have been confused about the definition of a "phishing" attack. What exactly is a phishing attack? A phishing attack is when you receive an official-looking e-mail from an online banking or financial institution – it could even be eBay or PayPal, or any other service that deals with money. The e-mail states that you should click a link and confirm your login and password to this particular institution (or enter your account number or credit card number).

As soon as you click on the link, you are sent to a Web page that looks remarkably similar to the company's real Web site, but it's not the company's real Web site. What is happening is that you are sent to a fake page that is controlled by the criminal who is behind the phishing scheme. As soon as you type your login\password or account information or credit card number, the thieves or hackers capture the information and then commit identity theft by using your credit card or stealing money from your account. Below are 12 steps that users can take to keep from being victimized by phishing scams. And after that are some examples of phishing scams.

**1 Keep antivirus up to date** – One of the most important things you can do to avoid phishing attacks is keep your antivirus software up-to-date because most antivirus vendors have signatures that protect against some common technology exploits. This can prevent things such as a Trojan disguising your Web address bar or mimicking an https secure link. If your antivirus software is *not* up-to-date, you are usually more susceptible to attacks that can hijack your Web browser and put you at risk for phishing attacks.

**2 Do not click on hyperlinks in e-mails** – It is never a good idea to click on any hyperlink in an e-mail, especially from unknown sources. You never know where the link is going to really take you or whether it will trigger malicious code. Some hyperlinks can take you to a fake HTML page that may try to scam you into typing sensitive information. If you really want to check out the link, manually retype it into a Web browser.

**3 Take advantage of anti-spam software** – Anti-spam software can help keep phishing attacks at a minimum. A lot of attacks come in the form of spam. By using anti-spam software such as [Qurb](#), you can reduce many types of phishing attacks because the messages will never end up in the mailboxes of end users.

**4 Verify https (SSL)** – Whenever you are passing sensitive information such as credit cards or bank information, make sure the address bar shows "https://" rather than just "http://" and that you have a secure lock icon at the bottom right hand corner of your Web browser. You can also double-click the lock to guarantee the third-party SSL certificate that provides the https service. Many types of attacks are not encrypted but mimic an encrypted page. Always look to make sure the Web page is truly encrypted.

**5 Use anti-spyware software** – Keep [spyware](#) down to a minimum by installing an active spyware solution such as [Microsoft Antispyware](#) and also scanning with a passive solution such as [Spybot](#). If for some reason your browser is hijacked, anti-spyware software can often detect the problem and provide a fix.

**6 Get educated** – Educate yourself on how to prevent these types of attacks. A little research on the Internet may save you a great deal of pain if you are ever the victim of identity theft. You can report any suspicious activity to the FTC (in the U.S.). If you get spam that is phishing for information, forward it to [spam@uce.gov](mailto:spam@uce.gov). You can also file a phishing complaint at [www.ftc.gov](http://www.ftc.gov). Another great resource is the [FTC's identity theft page](#) to learn how to minimize your risk of damage from ID theft. Visit the [FTC's spam page](#) to learn other ways to avoid e-mail scams and deal with deceptive spam.

**7 Use the Microsoft Baseline Security Analyzer (MBSA)** – You can use the MBSA to make sure you have all of your patches up to date. You can [download](#) this free tool from Microsoft's web site. By keeping your computer patched, you will protect your systems against known exploits in Internet Explorer and Outlook (and Outlook Express) that can be used in phishing attacks.

8

**Firewall** – Use a desktop (software) and network (hardware) firewall. On the desktop, you can use a software firewall such as [Zone Alarm](#) or use Microsoft's built-in software firewall in Windows XP. The incorporation of a firewall can also prevent malicious code from entering your computer and hijacking your browser.

9

**Use backup system images** – Keep a backup copy or image of all systems in case of foul play. You can then revert back to a pure system state if you suspect that a phishing attack, spyware, or malware has compromised the system. Tools such as [Symantec Ghost](#) and [Acronis True Image](#) are perfect for this.

10

**Don't enter sensitive or financial information into pop-up windows** - A common phishing technique is to launch a bogus pop-up window when someone clicks on a link in a phishing e-mail message. This window may even be positioned directly over a window you trust. Even if the pop-up window looks official or claims to be secure, you should avoid entering sensitive information because there is no way to check the security certificate. Close pop-up windows by clicking on the X in the top-right corner. Clicking cancel may send you to another link or download malicious code.

11

**Secure the hosts file** – A hacker can compromise the hosts file on desktop system and send a user to a fraudulent site. Configuring the host file to read-only may alleviate the problem, but complete protection will depend on having a good desktop firewall such as Zone Alarm that protect against tampering by outside attackers and keep browsing safe.

12

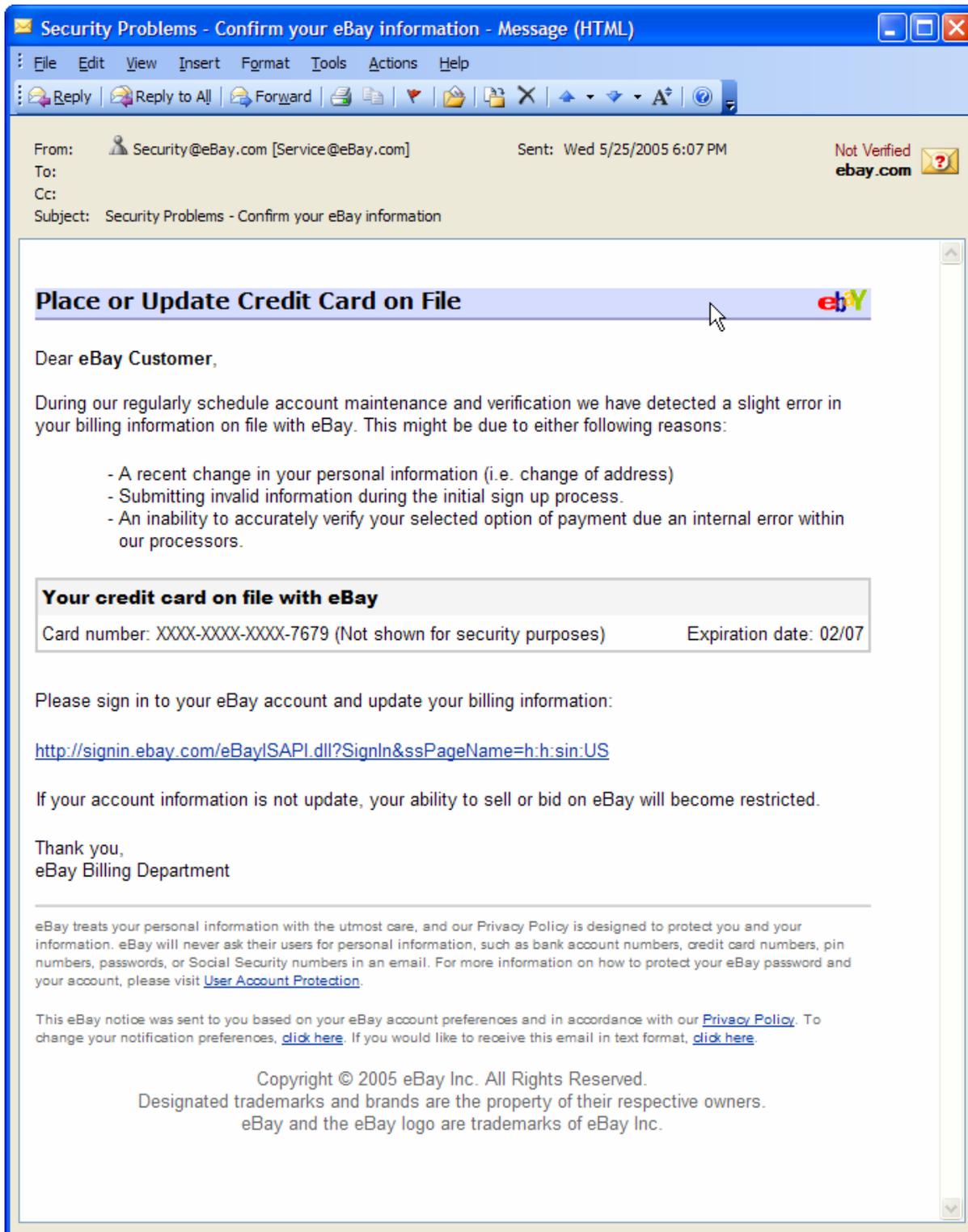
**Protect against DNS pharming attacks** – This is a new type of phishing attack that doesn't spam you with e-mails but poisons your local DNS server to redirect your Web requests to a different Web site that looks similar to a company Web site (e.g. eBay or PayPal). For example, the user types in eBay's Web address but the poisoned DNS server redirects the user to a fraudulent site. This is what I consider new age phishing. This needs to be handled by an administrator who can use modern security techniques to lock down the company's DNS servers.

## What does a phishing e-mail scam look like?

As the technologies gets better and better, the people behind the phishing scams also become more devious. They now use pop-up windows, official logos, and mock-secure connections copied from actual Web sites.

**Figure A** shows an example of a fishing scam e-mail I received the other day.

Figure A



The link in this e-mail, which purportedly goes to eBay, actually goes somewhere else. When I mouse over it, you can see that this text is actually masking a link to another site (66.246.90.60), as shown in the close up in **Figure B**. Also, note that the original link text does not have an "https://" secure address, but if a link like this read "https://" you might think it was safe while it could actually be masking a fake, non-secure URL.

**Figure B**

<http://signin.ebay.com/eBay!SAPL.dll?SignIn&ssPageName=h.h.sin:US>

If your account information is not <http://66.246.90.60/~testing/ebay/secupdate.html> become restricted.

Thank you,  
eBay Billing Department

## What does a hijacked browser scam look like?

When your browser is hijacked in a phishing attack, the real address bar is suppressed and is spoofed using Javascript and frames, as shown in **Figure C**.

**Figure C**



When the user enters a URL into the address bar (**Figure D**), the frame retains control and the hacker can gain information from you (notice the funny-looking URL). A simple pop-up blocker will keep this attack from working or from closing the current session of your browser.

**Figure D**



## Additional resources

- Sign up for our [Downloads Weekly Update](#), delivered on Mondays
- Check out all of [TechRepublic's newsletter offerings](#).
- [E-mail infrastructure: Lock it down in 10 steps](#) (TechRepublic)
- [Exchange Server: Lock it down in 10 steps](#) (TechRepublic)
- [Information Security Policy](#) (TechRepublic)

## Version history

**Version:** 1.0

**Published:** June 3, 2005

## Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to [drop us a line](#) and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team