

# 17 Tips for Avoiding Spyware

## MicroData Technical Brief

---

### Abstract

*October 27, 2005* – This brief is intended to give users some practical tips for avoiding spyware. These tips are general recommendations only and users should make sure their systems always have anti-spyware and anti-virus software installed and that they follow their organization's anti-spyware policies and procedures.

### Seventeen Tips for Avoiding Spyware

Users must always exercise care because spyware comes from a variety of sources: it can come from e-mail, from downloading software, or by simply clicking a link in an unsafe website or ad.

There are ways to fight these menaces, however. Here are some tips to help avoid spam, viruses, spyware, adware and malware:

#### Be careful with the spam you receive

1. Don't buy anything promoted in a spam message.
2. Don't reply to spam, click on its "unsubscribe" link, or click on a hyperlink in a message. Those actions inform the sender that your e-mail address is valid or may initiate installing an application. If the sender appears legitimate and you want to follow a hyperlink, copy the hyperlink into a new browser window rather than click on it.
3. If your e-mail program has a preview pane, disable it to prevent the spam from reporting back to its sender.
4. Use one e-mail address for family and friends, another for everyone else. When an address attracts too much spam, abandon it for a new one. Select an address with embedded digits, such as jane8doe2@isp.com.
5. If you get lots of spam, check your Internet service provider's filtering features and compare them with those of competitors.

6. Don't post your e-mail address in its normal form on a publicly accessible Web page. Post it in a form, such as "Jane AT isp DOT com," that can't be easily read by harvesting software.

### **Beware of viruses and hackers**

7. Don't open an e-mail attachment unless you were expecting it.
8. Use anti-virus software and keep it updated.
9. Install and use a firewall. In a corporate environment, it will usually be provided by your company. For home users, Windows XP has a built-in firewall. Make sure it is active and working.
10. Regularly update your operating system, Web browser and other major software.
11. Use passwords that are at least eight characters long that include at least one numeral and one symbol. Never disclose a password online.

### **Beware of New Software Downloads**

12. Download and install software only from trusted sources.
13. Never download 'free' utilities such as weather add-ins, smileys for your e-mail, or browser tools bars (Google and Yahoo are OK). These 'free' applications are just ploys to get you to initiate an installation procedure. Spyware will get installed along with whatever the 'free' application is.
14. Close windows containing pop-up ads or unexpected warnings by closing the entire window, not by clicking within the window.
15. Never click on a link promising something like a 'free PC tune-up' or 'virus scan'. These are usually associated with spyware and your clicking on the link is effectively allowing them to install onto your computer.
16. Adjust your Web browser's security settings. If you use Microsoft Internet Explorer 6, keep its security level at medium or higher to block Web sites from downloading a file without your authorization.
17. Use updated anti-spyware software to scan your hard drive regularly. Always download it from a trusted site. Microsoft provides free anti-spyware software for all Windows users.