



## *internet help site*

HEALTH ADVICE FOR YOUR COMPUTER

---

### How to use Email safely

#### 13 top tips and secrets that every user must know

- 1) Free email addresses like Hotmail may be convenient in some circumstances, but they're targets for spam. If you want to access your email anywhere, you're better off using the webmail service provided by your ISP.
- 2) If you frequent forums and chat rooms take precautions. These addresses get farmed by spammers, so expect to get targeted. Here you could use a Hotmail address or create a special address for that purpose or even multiple addresses for all the different things that you do.
- 3) For the same reason, be wary of subscribing to online newsletters. Choose carefully.
- 4) Don't forward Chain Emails (just like chain letters). Thousands of people will have **your address** and you don't know who's got it. These addresses may also get farmed by spammers.
- 5) Don't use CC (carbon copy) in your emails. Same reason as above. If you have to forward something, delete all the addresses or use BCC (blind carbon copy). There's nothing worse than receiving an email with half a page of email addresses on it before you get to the point.
- 6) Beware of what you put into your emails. If it contains, images, photos, icons, media files, ads or html code, it may get filtered by the recipient's or even their ISP's spam filter. It may be wise to call up and check to see if they actually received your email and ask if they use any filtering software. They may not even know!

7) These days, many people won't open attachments. If you have to send one, send them an email beforehand, letting them know that they'll receive an attachment from you or give them a call.

8) Don't send junk to every one in your address book. Not every one appreciates it. Sure, some of it's funny, but you're better off asking permission first. This can be classed as spam also.

9) Be wary if someone tells you that you sent them an infected message especially if you know you didn't send it. You may be infected or you may not. Your name is probably in someone's address book and some clever malware is spoofing the "from address". Somebody is infected but who? Don't forward any of these types of messages.

### 10) Potentially unsafe filename extensions (do not open):

.ade .adp .asx .bas .bat .chm .cmd .com .cpl .crt .exe  
.hlp .hta .inf .ins .isp .js .jse .lnk .mda .mdb .mde  
.mdt .mdw .mdz .msc .msi .msp .mst .ops .pcd .pif .prf  
.reg .scf .scr .sct .shb .shs .url .vb .vbe .vbs .wsc  
.wsf .wsh

Normally a file will end in something familiar eg; .txt .doc .xls .ppt .pdf .wpd .jpg

### **Check the filename extensions of your attachments every time!**

Do not open these: .scr (screens saver) .pif (program information file)

If you get two file extensions such as \_\_\_\_.*doc.vbs* or \_\_\_\_.*jpg.bat* or the file ends in one of the above, watch out!

Also if you get a zip file as an attachment (it ends in .zip and .sit) and it's from an unknown source, watch out!

Most of these zip files have two file extensions but you can't see the second one because the display column is too narrow. The second extension sits way over to the right and becomes invisible to the user. Here's an example.

( Information.zip .exe)

**Remember:** don't open *anything* unless you're *expecting it* and you know *who sent it!*

## 11) Disposable email address

As the name implies, disposable email addresses ("DEAs") are those you can throw away at any time. They're similar to "aliases" which may be provided by your ISP. They're especially useful for testing newsletter vendors, personal info requests, downloads and chat rooms or forums. It is not uncommon for companies to sell email addresses or give them to spammers (companies that send you unsolicited email).

DEAs are not "fake" addresses. Mail sent to them will be forwarded to a Real Email Address ("REA") of your choosing (such as `whatever@whatever.com`). After you "turn off" a DEA, however, mail sent to that DEA will bounce back to the sender.

## 12) Phishing, Spoofing and Pharming!

Phishing isn't really new -- it's a type of scam that has been around for years and in fact predates computers. Scam artists did it over the phone for years and called it social engineering. What is new is its modern day delivery vehicle -- spam and faked Web pages.

"Spoofing" attempts to make surfers believe that they are receiving e-mail from a trusted source, or that they are securely connected to a trusted web site, when that's not the case. Spoofing is generally used as a means to convince people to give out personal or financial information by deception.

In "E-mail spoofing", the header of an e-mail appears to have originated from someone or somewhere other than the actual source. Spammers and criminals often use spoofing in an attempt to get recipients to open and possibly even respond to their emails.

"Page Spoofing" involves altering the return address in a web page so that it goes to the hacker's site rather than the legitimate site. This is accomplished by adding the hacker's address before the actual address in any e-mail, or page that has a request going back to the original site, often with a form that looks identical to the legitimate site.

*A page spoof might look something like this:*

`http://www.paypal.com@thespiesdomain.com/index.html`. The actual domain address is AFTER the @ sign. If you were to surf to this web address and submit any information via a form it would go to the spy and not to PayPal.

### **TIP:**

**Get into the habit of visually inspecting addresses in your browser's address location bar.**

## ***Phishing:***

Many of these schemes use 'spoofed' e-mails to lead consumers to counterfeit websites designed to trick people into divulging financial information such as credit card numbers, account usernames, passwords and social security numbers. By hijacking the brand name banks, e-retailers and credit card companies, such as Citibank, eBay, PayPal, AOL, MSN, Yahoo and EarthLink and Best Buy, phishers often convince people to respond because they look like the "real deal".

Others plant spyware onto PCs to steal credentials directly, often using Trojans and keyloggers. Pharming crimeware directs users to fraudulent sites or proxy servers. The number and sophistication of phishing scams sent out to consumers is continuing to increase dramatically.

While online banking and e-commerce is generally very safe, be careful of giving out your personal financial information over the Internet. Banks don't ask for your secret details via email.

The Anti-Phishing Working Group has compiled a list of recommendations below that you can use to avoid becoming a victim of these scams.

- Firstly, download the latest Internet Explorer 7. It's got upgraded security and a built in Phishing Filter. I suggest you do not disable it
- Be suspicious of any email with urgent requests for personal financial information. Unless the email is digitally signed, you can't be sure it wasn't forged or 'spoofed'. Phishers, typically include upsetting or exciting (but false) statements in their emails to get people to react immediately. They ask for information such as usernames, passwords, credit card numbers, social security numbers, etc.
- Phisher emails are typically NOT personalized, while valid messages from your bank or e-commerce company generally are.
- Don't use the links in an email to get to any web page. If you suspect the message might not be authentic, call the company on the telephone, or log onto the website directly by typing in the Web address in your browser.
- Avoid filling out forms in email messages that ask for personal financial information. You should only communicate information such as credit card numbers or account information via a secure website or the telephone. Always ensure that you're using a secure website when submitting credit card or other sensitive information via your Web browser.
- To make sure you're on a secure Web server, check the beginning of the Web address in your browsers address bar - it should be "https://" rather than just "http://"

- Consider installing a Web browser tool bar to help protect you from known phishing fraud websites. This is also being incorporated into some security packages.
- You can get the EarthLink ScamBlocker which is part of a free browser toolbar that alerts you before you visit a page that's on Earthlink's list of known fraudulent phisher Web sites.

It's free to all Internet users - download at <http://www.earthlink.net/earthlinktoolbar>  
The down side is, it may contain adware or some sort of browser tracking like most toolbars.

- Regularly log into your online accounts. Don't leave it for as long as a month before you check each account. Regularly check your bank, credit and debit card statements to ensure that all transactions are legitimate. If anything is suspicious, contact your bank and all card issuers.
- Ensure that your browser is up to date and that security patches are applied. In particular, people who use the Microsoft Internet Explorer browser, should go to the Microsoft Security home page – <http://www.microsoft.com/security/> to download a special patch relating to certain phishing schemes.
- Report "phishing" or "spoofed" e-mails to the following groups or similar government organizations in your country:

Forward the email to [reportphishing@antiphishing.com](mailto:reportphishing@antiphishing.com).

Forward the email to the Federal Trade Commission at [spam@uce.gov](mailto:spam@uce.gov) .

Forward the email to the "abuse" email address at the company that is being spoofed (e.g. "spoof@ebay.com")

When forwarding spoofed messages, always include the entire original email with its original header information intact.

Notify the Internet Fraud Complaint Center of the FBI by filing a complaint on their website: <http://www.ic3.gov/>

---

The information contained here is published by

[www.internethelpsite.com](http://www.internethelpsite.com)

*Copyright © 2005-2007 Joe Jutrisa - All Rights Reserved*

This is a free report.

Please feel free to pass it on, or refer your friends to the above site for more free information.

If you found these tips helpful and you would like to know more about protecting yourself, your family and your business, just click below to get your own copy of the book, "Internet Security Secrets". It's jam-packed full of information, tips and secrets and is available now at a special introductory price.

[www.internetsecuritysecrets.com](http://www.internetsecuritysecrets.com)

