



[Site Search Tool](#)

Phishing - 5 Tips To Protect Yourself!

Sign-up free!



Phishing Tips Overview

POPULAR XP NEWSLETTER

Claim Your FREE

Guides!



[Subscribe Now!](#)

[Current Issue](#)

[Issue Archive](#)

1. Never respond to requests for personal information via e-mail.
2. Visit Web sites by typing the URL into your address bar.
3. Check to make sure the Web site is using encryption.
4. Routinely review your credit card and bank statements.
5. Report suspected abuses to the proper authorities..

Download this page as a PDF file here: [Phishing Tips](#)

What is phishing?

* [What's RSS?](#) *

Phishing is a type of deception designed to steal your identity. In a phishing scam, a malicious person tries to get information like credit card numbers, passwords, account information, or other personal information from you by convincing you to give it to them under false pretences. Phishing schemes usually come via spam e-mail or pop-up windows.

[RSS Newsletter](#)

[Website RSS Feed](#)

How does phishing work?

[RSS Podcast](#)
Coming Soon!

A phishing scam begins with a malicious user who sends out millions of fraudulent e-mail messages that appear to come from popular Web sites or from sites that you trust, like your bank or credit card company. The e-mail messages, and the Web sites they often send you to, look official enough that they deceive many people into believing that they're legitimate. Believing that these e-mails are legitimate, unsuspecting people too often respond to the e-mail's requests for their credit card numbers, passwords, account information, or other personal information.

POPULAR ARTICLES

[FREE Stuff](#)

[Codecs for WMP9](#)

[SHERLOCK Codec Utility](#)

[Online Data Storage](#)

A scam artist might put a link in a fake e-mail that appears to go to the legitimate Web site, but actually takes you to a scam site or even a pop-up window that looks exactly like the official site. These copies are often called spoofed Web sites. Once you're at one of these spoofed sites or pop-up windows you might unwittingly enter even more personal information that will be transmitted directly to the person who created the spoofed site. That person can then use this information to purchase goods, apply for a new credit card, or steal your identity.

5 ways to help protect yourself from phishing

[WMP and DVD](#)

Just as they do in the physical world, scam artists will continue to develop new and more sinister ways to trick you online. But following these five steps can help you protect your personal information.

[Cryptographic Service](#)

1. Never respond to requests for personal information via e-mail or in a pop-up window. If in doubt, call the institution that claims to be the sender of the e-mail or pop-up window.

[Microsoft Photo Story 3](#)

[Scannow sfc](#)

2. Visit Web sites by typing the URL into your address bar.

[Download IE6](#)

3. Check to make sure the Web site is using encryption.

[Logon XP Tips](#)

4. Routinely review your credit card and bank statements.

[Windows File Protection](#)

5. Report suspected abuses of your personal information to the proper authorities.

[Computer Workstation Ergonomics](#)

Step 1: Never respond to requests for personal information via e-mail

[Anti Virus Free Trial](#)

Microsoft and most legitimate businesses will never ask for passwords, credit card numbers, or other personal information in an e-mail. If you do receive an e-mail requesting this kind of information, don't respond. If you think the e-mail is legitimate, contact the company by phone or through their Web site to confirm. See Step 2 for the best ways to get to a Web site if you think you've been targeted by a phishing scam.

[WinTasks 5 Professional](#)

For a list of sample phishing scam e-mails that people have received, check the [Anti-Phishing Working Group Phishing Archive](#).

[Windows XP Task manager](#)

Step 2: Visit Web sites by typing the URL into your address bar

[Stop Messages](#)

If you suspect that an e-mail from your credit card company, bank, online payment service, or other Web site you do business with is not legitimate, don't follow the links to the Web site from an e-mail message. Those links may take you to a spoofed site that might send all the information you enter to the scam artist who created the site.

COMMON ERRORS

[C00D11CD](#)

Even if the address bar displays the correct address, don't risk being fooled. There are several ways for hackers to display a fake URL in the address bar on your browser. Newer versions of Internet Explorer make it more difficult to spoof the address bar, so it's a good idea to visit [Windows Update](#) on a regular basis and update your software. If you don't think you'll remember to update or if you prefer to have the updates downloaded automatically, you may be able to configure your computer for Automatic Updates. [Windows Automatic Updates](#).

[0x800A138F](#)

[0x8007007E](#)

[0x80072EE2](#)

[0x80072EFD](#)

Step 3: Check to make sure the Web site is using encryption

[800C0008](#)

If you can't trust a Web site by the address bar, how do you know it's likely to be secure? There are a few different ways. First, before you enter any personal information, check to see if the Web site uses encryption to transmit your personal information. In Internet Explorer you can do this by checking the yellow lock icon on the status bar as shown in the following illustration.

[0x8DDD0018](#)

[0xc00d1199](#)

[c00d11ba](#)

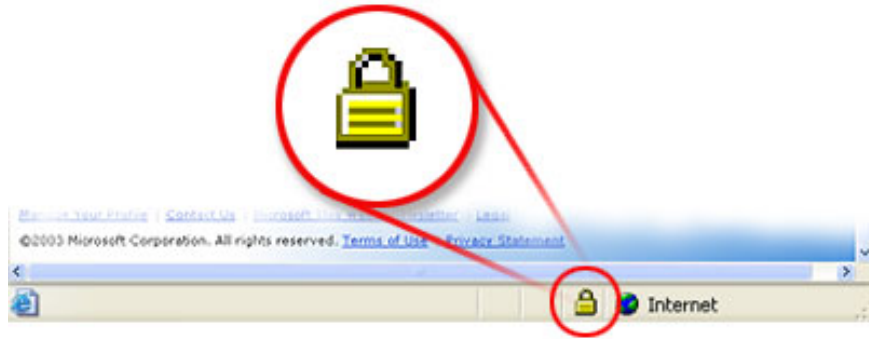
[0x800B0004](#)

[wmpdxm-dll](#)

[wmp-dll](#)

[rstrui entry point](#)

**DIGITAL
MEDIA**



[Codec SVCD](#)

Secure site lock icon. If the lock is closed, then the site uses encryption.

[Divx & WMP](#)

This symbol signifies that the Web site uses encryption to help protect any sensitive personal information-credit card number, Social Security number, payment details-that you enter.

[Windows XP
Codecs](#)

Double-click the lock icon to display the security certificate for the site. The name following Issued to should match the site you think you're on. If the name differs, you may be on a spoofed site. If you're not sure whether a certificate is legitimate, don't enter any personal information. Play it safe and leave the Web site.

**TRIAL
SOFTWARE**

To find out more ways to determine if a site is safe, read [How Internet Explorer Keeps Your Data Safe](#).

[WinTasks Pro
15 Day Trial](#)

*"Master the
processes
running on
your PC!"*

Step 4: Routinely review your credit card and bank statements

Even if you follow the three steps above, you may still become a victim of identity theft. If you review your bank statement and credit card statements at least monthly, you may be able to catch a scam artist and stop them before they cause significant damage.

[SpeedUpMyPC
15 Day Trial](#)

*"Take control
of your PC's
speed and
memory!"*

Step 5: Report suspected abuses of your personal information to the proper authorities

If you feel you have been a victim of a phishing scam, you should:

[Spy Sweeper
30 Day Trial](#)

*"Don't get
caught by
harmful
spyware!"*

Immediately report the scam to the company that's being spoofed. If you're unsure how to contact the company, visit the company's Web site to get the correct contact information. The company may have a special e-mail address to report such abuse. Remember not to follow any links in the phishing e-mail you received. You should type the known Web site address for the company directly into the address bar in your Internet browser.

[Site
Search
Tool](#)

Was this article on *phishing* useful?

Have you signed up for my popular [Windows XP Newsletter](#) below?

Enjoy the rest of site and remember if you have a query about this site or a comment to make then drop me a line at the [Contact Page](#)

Kind Regards



Marc Liron - [Bio](#)
Microsoft Digital Media MVP
Your Guide to using Windows XP
A Unique Windows XP Newsletter? [Sign Up Now!](#)
- **Make sure you get your FREE tips and advice...**

Finally a quality XP Newsletter!

Sign-up free!



First name

E-mail address

Subscribe **Unsubscribe**

I HATE SPAM AS MUCH AS YOU DO!

That is why you'll get none from me...

My [Privacy Policy](#)

Find out more here: [XP Newsletter](#)

*"Hey Marc! I signed up to your newsletter on **Fred Langa's** recommendation. After a quick lurk, I am glad I did - you appear to be doing us all a big favour - for which I am grateful . . ."*

Charlie - Carmel, Indiana US

Can I Show You How To Use RSS?

The Multimedia Course Is FREE!

<http://www.rss-lessons.com>

The views on this website are my own and **NOT that of Microsoft!**

I am not responsible for the content of any sites linked to.

ALL Trademarks are freely acknowledged

ALL information is provided "**As Is**"

This page was last updated 20th April 2005

[Home Page](#) | [Privacy Policy](#) | [About Me](#) | [Contact Me](#)

A page about phishing