Help safeguard your personal information online

Published: December 12, 2003 | Updated: October 11, 2005

Many Web sites today offer features and services customized to your individual preferences based on personal information that you supply. For example, some shopping sites save you time by retaining your shipping and billing information, and some news sites offer you the headlines you're most likely to be interested in.

Related Links

- How to limit your personal data in online directories
- Protect your privacy with online payment services
- How to shop online more safely

Unfortunately, not all sites can be trusted to use your personally identifiable information the way you want or expect. Some malicious individuals employ what's known as a phishing scam to set up a convincing-looking spoof of a legitimate Web site. They then try to trick you into visiting this Web site and disclosing personal information, such your credit card number.

Fortunately, there are several steps you can take to help protect yourself from these and other types of attacks.

What can happen and how to avoid it

Several types of attacks are used to steal information and other assets on the Web. The most common ones include:

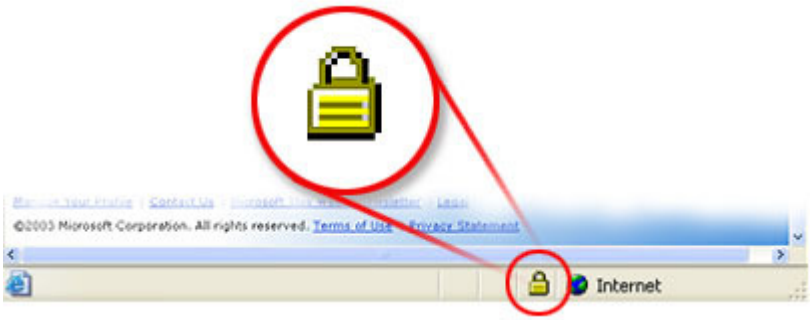
Phishing attacks

Phishing is the act of luring someone to a spoofed Web site. One common method is to send an e-mail that looks like it came from a trusted source but that contains a link to a malicious site. The malicious site is designed to look like the legitimate site in an effort to trick you into revealing personal information or downloading a virus.

Spoofing attacks

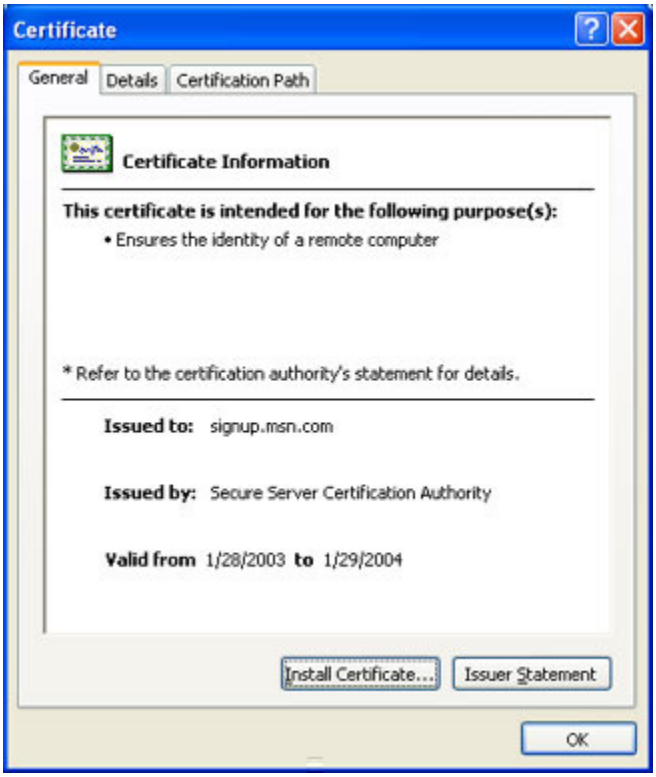
Spoofing attacks are commonly used in conjunction with phishing. The spoofed site is usually designed to look like the legitimate site, sometimes using components from the legitimate site. The best way to verify whether you are at a spoofed site is to verify the certificate. Keep in mind that there are several ways to get the address bar in a browser to display something other than the site you are on. Therefore, do not rely on the text in the address bar as an indication that you are at the site you think you are.

Always verify the security certificate issued to a site before submitting any personal information. Before submitting any personal information, ensure that you are indeed on the website you intend to be on. In Microsoft® Internet Explorer, you can do this by checking the yellow lock icon on the status bar. This symbol signifies that the website uses encryption to help protect any sensitive personal information—credit card number, Social Security number, payment details—that you enter.



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

to display the security certificate for the site. This certificate is proof of the identity for the site. When you check the certificate, the name following **Issued to** should match the site you think you are on. If the name differs, you may be on a spoofed site. If you are not sure whether a certificate is legitimate, do not enter any personal information. Play it safe and leave the Web site.



Legitimate certificate. When new subscribers sign up for MSN® services, they can match the **Issued to** domain name (msn.com) to the Web site domain name (also msn.com). Also, be cautious about clicking links in e-mail messages or in online ads from retailers you don't recognize or trust. If you have any doubt about a link, do not click it. Instead, type the Web site address into the address bar of your Web browser, or try to confirm that the link is legitimate. Remember, if an offer sounds too good to be true, it probably is.

Viruses

Viruses are malicious programs that attackers can use for a variety of purposes, none of them good. These uses include stealing personal information on your computer, destroying all of your data, and turning your computer into a spam-spewing zombie without you even realizing it. Viruses are a traditional problem in computer security. You can help protect your computer against viruses and other malicious programs:

- Learn how to take steps to protect your PC

Top of page

For Technical Assistance

If you need assistance with identifying or removing a virus, please contact your antivirus software vendor. If you need more help with virus-related issues, or if you think you have a different security-related problem, please contact Microsoft Product Support Services.

- For Microsoft Product Support Services within the United States and Canada, call toll-free (866) PCSAFETY (727-2338).
- For worldwide support, find contact information for Microsoft subsidiaries

Top of page

Was This Information Useful?

Yes No

Printer-Friendly Version Send This Page Add to Favorites