Internet Explorer Security

SURF THE WEB SAFELY AND SECURELY. BY RUSSELL SHAW

According to the market-research firm OneStat, 93.9 percent of the world's Internet users surf the Web using Microsoft's Internet Explorer. Is it any wonder, then, that the most common online privacy and security violations occur via IE? We'll show you how to button down your browser, so you don't become a victim.

There's no shortage of businesses—large and small—who would like to know which Websites you frequent, and who are keen to find out where you live. If you don't configure and use Internet Explorer properly, you could be giving up this information—and exposing yourself to even more serious trouble—without even knowing it.

Certificates can verify an individual's identity, assure a Website's security arrangements, and protect your PC from unsafe software.

The reasons for these companies' abiding curiosity are most often not sinister; more typically, they lust after this information so they can target you for their sales pitches. Most—but certainly not all—of these operations are legitimate, and their practices are often entirely legal. In some cases, you might even find that you're interested in purchasing the goods and services they have to offer.

Most of the time, however, you'll just get annoyed at the constant intrusions. After all, you have an inalienable right to be left alone. If you're interested in a Las Vegas vacation package, a cut-rate re-fi, or prescriptions for little blue pills, wouldn't you rather seek out the information when you're ready, as opposed to having it shoved in your face all day long?

Although relatively minor annoyances, such as spam and pop-up ads, greatly outnumber more egregious problems, such as violations of privacy and outright Web thievery, serious crimes such as these do happen. Making an online purchase during an unprotected Internet Explorer session, for example, could lay bare your credit-card number to even the most inexperienced hacker. Unprotected Web browsing could also roll out the red carpet for a viral invasion of your PC.

But you needn't make it so easy for unscrupulous advertisers and ne'er-do-wells to cause you trouble.

SECURITY CERTIFICATES

One way to maintain your online privacy and security is to make use of security certificates. These statements can verify an individual's identity, assure a Website's security arrangements, and protect your PC from unsafe software (such as viruses, spyware, and worse).

A personal certificate serves as a digital verification that you are who you say you are. These come into play whenever you conduct a transaction with Websites that requires you to prove your identity. A Website certificate affirms to visitors that a given Website is secure and genuine. Website certificates don't vouch for the quality of goods, services, or information that might be available

on that site, they only provide an assurance that the Website is what it claims to be.

In the end, it's up to you to decide if you trust any given Website; however, sites that possess these certificates are far less likely to secretly download harmful or annoying software onto your PC, and they're unlikely to collect and sell your personal information to third parties without your consent.

Security certificates are based on n encryption/decryption concept volving public and private keys eys are numbers derived from a athematical algorithm applied to a domly chosen number).

nyone possessing your public key n use it to encrypt (scramble) data d send it to you over the Internet. at data, however, can only be crypted (unscrambled) using your vate key. As long as you keep your vate key private, it doesn't matter o has possession of your public key, cause no one can read encrypted essages without your private key.

The merchant, bank, or any her party on the other side of the ansaction will also have a public nd private key. They'll provide you ith their public key, which IE will use encrypt the information you send to them. They, in turn, will use their private key to decrypt the information when they receive it.

Most of this activity will take place behind the scenes, and you won't even be aware that it's happening. In some cases—such as online banking and with some online merchants—confidential transactions are handled using a technology known as Secure Sockets Layer (SSL).

You'll establish a user-name and password with the other party and provide that information whenever you sign onto their Website. As soon as the Website verifies your identity, the website transfers you to a secure area where any information you send or receive is encrypted.

DIAL "S" FOR SECURITY

You can verify that you're on a secure Website by looking at the address in IE's Address bar: Instead of reading "http://www..." it will read "https://www..." The presence of that "s" tells you that the information passing between your computer and that Website is encrypted.

Digital certificates are granted by certification authorities. Most often, these are commercial entities that have gone through a rigorous vetting process and have been approved by Microsoft and other companies with an interest on online security. According to Microsoft, certification authorities empowered with granting digital certificates to Websites must have the capability and the willingness to:

- Issue, renew, and revoke certificates.
- Authenticate the identities of individuals and organizations.
- Verify the registrations of individuals and organizations.
- Publish and maintain a Certificate Revocation List (CRL) of all certificates that the certification authority has revoked.
- Handle legal and liability issues related to security.

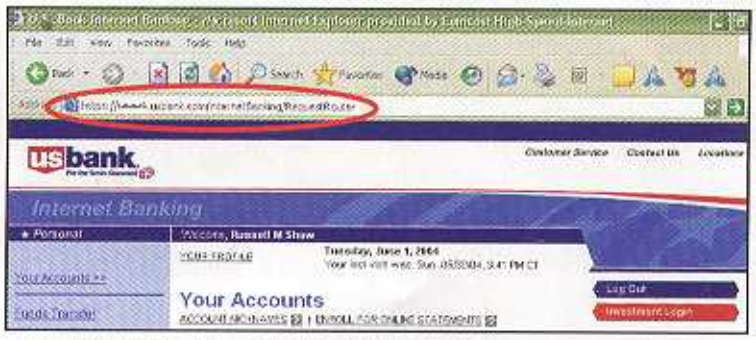
WANNA COOKIE?

Another way to ensure your privacy is to control whether or not Websites can place "cookies" on your computer.

Cookies are small text files that are sometimes useful—and sometimes not. If you're interested in seeing weather reports for your hometown, for example, you'd likely visit a Website—say, www.weather.com—that specializes in weather forecasts. Supply the Website with your zip code once, and Weather.com will store your zip-code information in a cookie on your computer's hard drive. The next time you visit Weather.com, the site will automatically retrieve that cookie and present you with a custom weather report based on your zip code.

An unscrupulous Website operator, however, might take advantage of cookies to place code on your computer that tracks and reports on your Web travels. Cookies can also be used to determine personal information about you, for the purposes of targeting you for spam—or worse.

You have an inalienable right to be left alone. Don't allow advertisers to shove their messages in your face.



In this Website address, the "https" indicates that a secure connection has been established, and that any data exchanged between your PC and the Website will be encrypted during transit.

IN THE ZONE

Internet Explorer bases its privacy safeguards on a concept called "Content Zones." These zones are not geographical, but pertain to the types of Websites you visit and how much you trust the business, organization, or person running that Website. IE classifies each Website into one of four zones, each of which has a default security level associated with it. The security level determines which privileges the site is granted, which in turn controls how your computer behaves at that site.

INTERNET ZONE Unless you specify otherwise, most of the Websites you visit will fall into this zone. By default, IE's security and privacy controls are set to Medium for any Websites in this zone.

LOCAL INTRANET ZONE Intranets are internal Websites that are closed to the outside world. The most typical example is a company Website used to post proprietary information. Here again, IE's security and privacy controls default to Medium for any Websites in this zone.

TRUSTED SITES ZONE You can place any public Websites that you feel absolutely comfortable with in this zone. By default, IE's privacy and security controls are set to Low for any Websites in this zone.

RESTRICTED SITES ZONE Place any Websites you visit that you decide you're not entirely comfortable with in this zone. By default, IE's privacy and security controls are set to High for any Websites in this zone.

IE uses Content Zones to manage what the Websites you visit are permitted to do with your computer. Most public sites fall into the Internet Zone by default.

Changing Zones and Settings

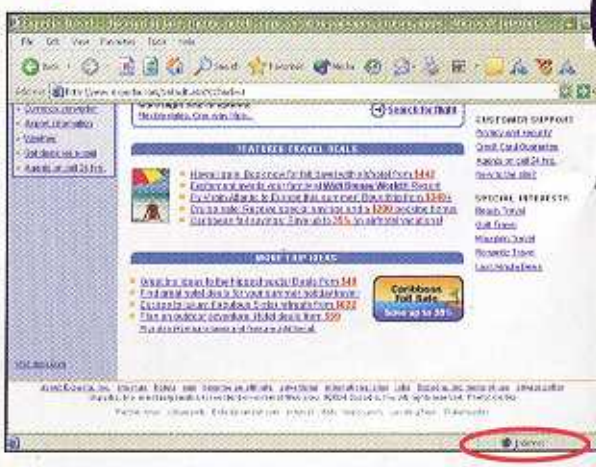
As described above, Internet Explorer will place all the Websites you visit in the Internet Zone unless you tell it otherwise. You can easily designate which zone any given site is placed in. If you've established a high degree of trust with a particular site—your bank, for example—you might want to move that site from the Internet Zone, with its default Medium security setting, to the Trusted Zone, with its default Low security setting.

Here's how to move a Website from one Internet Zone to another:

1. Launch Internet Explorer, click on the Tools menu, and choose Internet Options.
2. Click on the Security tab within the Internet Options box.
3. Click on the icon representing the Content Zone you want to place this site in.
4. Click on the Sites button, enter the address of the Website you wish to place in this Content Zone, and click OK.

You can change the default security levels for each of the Content Zones just as easily:

1. Launch Internet Explorer, click on the Tools menu, and choose Internet Options.
2. Click on the Security tab within the Internet Options box.
3. Click on the icon for the Content Zone whose settings you'd like to change.



If you have Internet Explorer's Status bar activated, it will display which Security Zone you've placed the current Website in.

4. The Internet Zone has a slider that you can use to adjust an array of security settings. (Click on the Default Level button to return them to their original values.)
5. Click on the Custom Level button, and you can tweak several dozen security settings. (To return these settings to their default values, click the Reset button.)
6. Click OK when you're finished.

Looking in the Cookie Jar

As we've described, some cookies are useful, some are useless, and still others are downright harmful. You can configure Internet Explorer to accept or reject a broad range of cookie types for all sites you've listed in the Internet Zone, or you can configure it to handle them on a site-by-site basis.

If you'd like to change how IE handles cookies, launch it, click on the Tools menu, and choose Internet Options. Click on the Privacy tab and move the slider control up and down. At the highest privacy setting, E will block all new cookies, and Websites won't be able to read any existing cookies stored on your computer.

Although this setting provides the absolute highest degree of curity, it's not all that useful because it doesn't discriminate tween beneficial and harmful cookies. We recommend you set IE's vacy setting to either Medium (the default) or Medium High.

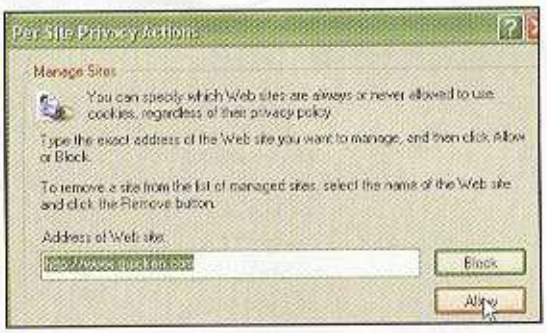
y of IE's privacy settings other than High will also enable u to configure IE to accept cookies from some Websites, and ect them from others. Here's how:

1. Launch Internet Explorer, click on the Tools menu, and choose Internet Options.
2. Click on the Privacy tab within the Internet Options box.
3. Click on the Edit button.
4. In the Per Site Privacy Actions box that opens, enter the address for the Website you're interested in customizing.
5. Click on the Block button to always prohibit that site from placing cookies on your PC, or click on the Allow button to ways allow it.

en if you configure IE to reject cookies from Websites, prevent Websites from reading cookies already your computer, neither of these actions will remove *existing* cookies. Here's how to do that:

1. Launch Internet Explorer, click on the Tools menu, and choose Internet Options.
2. Click on the General tab within the Internet Options box.
3. Click on the Settings button.
4. Click on the View Files button.
5. Click on any files you want to delete (hold down the Ctrl key to select multiple files).
6. Click on "Delete this item" in the left-hand window pane.

The author has allowed the travel Website Expedia to place a cookie on his computer. As a result, he's automatically "recognized" whenever he visits the site using his computer.



Internet Explorer gives you the power to accept or block all cookies from any particular Website regardless of the site's privacy policy or which Content Zone you've placed it in.

A Balancing Act

The biggest danger in publishing stories like this are that we go over the top and frighten readers into thinking danger lurks around every corner of the World Wide Web. Don't worry; it doesn't. But anything as sensitive as your personal privacy is worth guarding, and Internet Explorer doesn't always do a good job of that right out of the box.

What we've tried to do here, then, is to show you how IE works, and how you can use its tools to at least better secure your privacy rights. We would also recommend against using IE's tools exclusively. You'll find a number of other products discussed in this issue that will go even further, and you'll find several products—both trialware and fully functional programs—on the enclosed disc. In the end, you'll discover that protecting your privacy while getting the most out of the Internet and the World Wide Web is something of a balancing act.