# LESSON 20

# Using Netscape® Security

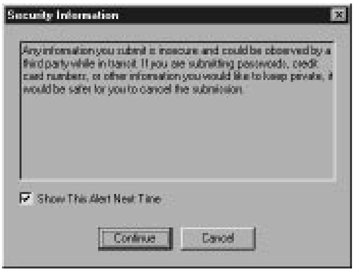
*In this lesson, you learn about security issues on the Internet and how Netscape can help you keep your data secure.*

## What About Netscape Security?

Internet security is a big topic these days. Computer hackers, crackers, and online crime are rapidly becoming weekly items in the news. Because the Internet has opened all kinds of doors to online shopping and information exchange, security is a big issue. While much of the Internet is relatively safe, there are some things you want to watch out for to keep yourself and your data protected.

**Hacker and Cracker** These are terms used to describe computer users with considerable expertise who break into other computer systems. The term “hackers” is commonly used to describe those who merely break in and look around in other computer systems. The term “cracker” is commonly used to describe those who break in and steal information, destroy files, or commit some degree of malicious mayhem in other computer systems.

Netscape Communicator comes with some built-in security options you can apply. For example, whenever you enter information onto an electronic form, Netscape displays a warning dialog box similar to the one shown in Figure 20.1. With most of the forms you encounter on the Web, you won’t be inserting sensitive information, however, Netscape warns you just the same.



Any information you submit is insecure and could be observed by a third party while in transit. If you are submitting passwords, credit card numbers, or other information you would like to keep private, it would be safer for you to cancel the submission.

FIGURE 20.1 Netscape warns you when you encounter an unsecured form.

One of the biggest concerns users have is giving out their credit card numbers online. Keep in mind that the Internet was not designed for secure communications. Since it's an open system, the data exchanged goes through numerous computer systems, risking interception by outsiders. However, you face the same potential security risk every time you hand your credit card to a waiter in a restaurant or give your number over the telephone when ordering merchandise.

Netscape uses a protocol, called *Secure Sockets Layer* (SSL), to encrypt the data you send over the Internet. When you connect to a server using this protocol, the data is less likely to be intercepted. Unfortunately, you're at the mercy of the server you're connecting to. If it doesn't use an SSL protocol, your data won't be secure.

In this lesson, you learn some tips for applying security measures to your own Internet and World Wide Web travels.

TIP **Don't Catch a Virus!** A computer virus can be contracted by downloading infected files. While most Web servers have administrators and personnel who check all files that are uploaded onto their computers, that does not mean you should feel safe. Always check the data you download by using an anti-virus program. (You learn more about viruses later in this lesson.)

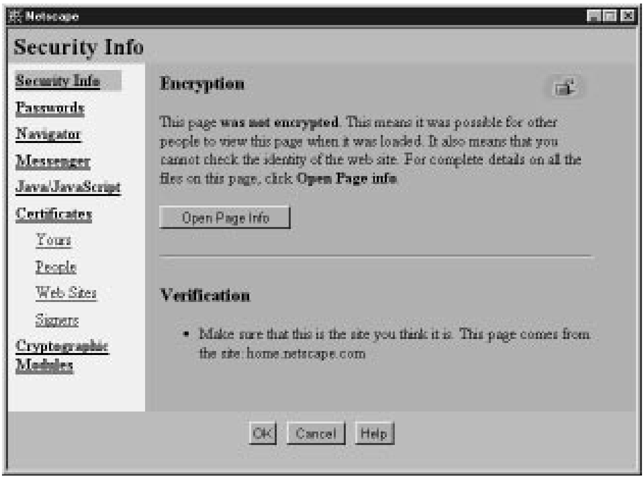
## SETTING SECURITY PREFERENCES

Netscape's security options can be found in the Security Preferences dialog box. The following list describes each of the warning options you may choose from:

> Entering a Secure Document Space (Server) A notification appears whenever you encounter a Web site that uses the latest security standards.
>
> Leaving a Secure Document Space (Server) A notification that indicates when you're leaving a secure site.
>
> Viewing a Document with a Secure/Insecure Mix Notifies you of a mixed security site. If it's mixed, you probably can't send secure information.
>
> Submitting a Form Insecurely When replying to a Web page form, a message appears to warn you that the data is unsecured.
>
> Enable SSL v2 Turns on data encryption for Web sites using version 2 of the SSL protocol.
>
> Enable SSL v3 Turns on data encryption for Web sites using version 3 of the SSL protocol.

Make sure Netscape's security warnings are turned on. To do so, follow these steps:

1. Click the Security icon on the Navigation toolbar. This opens the Security Preferences dialog box (see Figure 20.2).
2. Select SSL Browsing under Applications and make sure the security options are turned on by clicking the appropriate check boxes for the options you want to enable.
3. To exit the dialog box and apply the settings, click OK.



Encryption

This page **was not encrypted**. This means it was possible for other people to view this page when it was loaded. It also means that you cannot check the identity of the web site. For complete details on all the files on this page, click **Open Page info**.

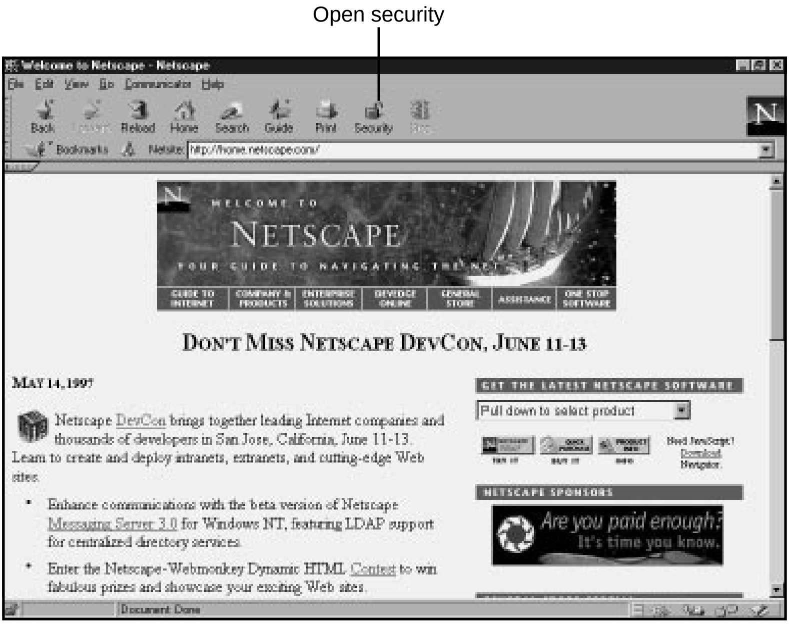
Verification

- Make sure that this is the site you think it is. This page comes from the site: home.netscape.com

FIGURE 20.2 The Security Preferences dialog box.

## SECURITY DOS AND DON'TS

There are tips you can follow when you encounter security concerns on the Web. When you come to a document form that asks for personal information, to a check the page's security status by glancing at the security icon on the Netscape toolbar (see Figure 20.3). If the key icon appears as an opened lock, the site is not secure and neither is the data you fill in on the form. In such a case, it's not a good idea to enter any data you would consider personal.


Open security
Welcome to Netscape - Netscape
File Edit View Go Communicator Help
Back
Forward
Reload
Home
Search
Guide
Print
Security
Stop
Bookmarks
Netsite: http://home.netscape.com/
WELCOME TO
NETSCAPE
YOUR GUIDE TO NAVIGATING THE NET
GUIDE TO INTERNET
COMPANY & PRODUCTS
ENTERPRISE SOLUTIONS
DEVEDGE ONLINE
GENERAL STORE
ASSISTANCE
ONE STOP SOFTWARE
GET THE LATEST NETSCAPE SOFTWARE
Pull down to select product
TRY IT
BUY IT
INFO
Need JavaScript1 Download Navigator.
NETSCAPE SPONSORS
Are you paid enough? It's time you know.
Document: Done

DON'T MISS NETSCAPE DEVCON, JUNE 11-13

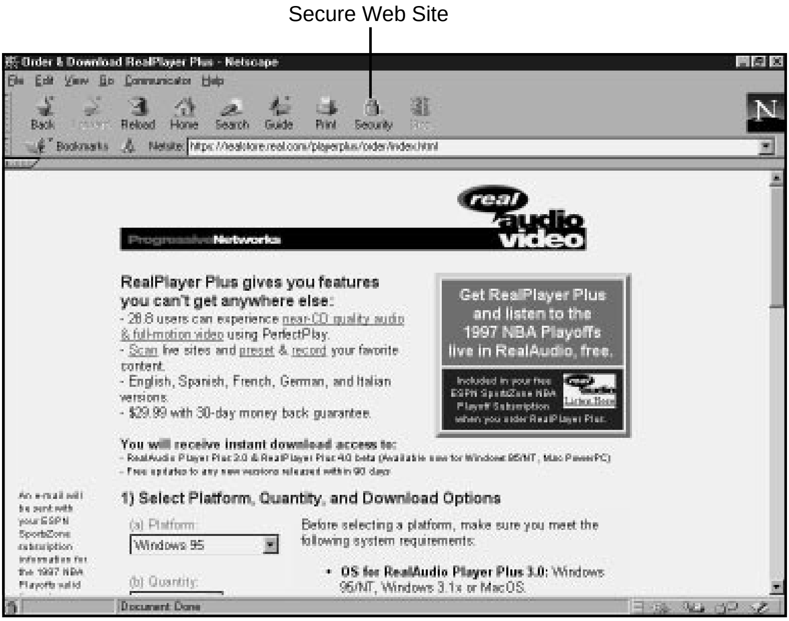
MAY 14, 1997

Netscape DevCon brings together leading Internet companies and thousands of developers in San Jose, California, June 11-13. Learn to create and deploy intranets, extranets, and cutting-edge Web sites.

- Enhance communications with the beta version of Netscape Messaging Server 3.0 for Windows NT, featuring LDAP support for centralized directory services.
- Enter the Netscape-Webmonkey Dynamic HTML Contest to win fabulous prizes and showcase your exciting Web sites.

FIGURE 20.3 Beware of open security icons.

If the security icon is closed or locked, the information you type will be encrypted. An https:// prefix indicates that the Web server you're in contact with is using a secure protocol (see Figure 20.4).


Secure Web Site
Order & Download RealPlayer Plus - Netscape
File Edit View Go Communicator Help
Back
Reload
Home
Search
Guide
Print
Security
Bookmarks
Netsite:
https://realstore.real.com/playerplus/order/index.html
ProgressiveNetworks
real audio video
Document: Done

RealPlayer Plus gives you features you can't get anywhere else:
- 28.8 users can experience near-CD quality audio & full-motion video using PerfectPlay.
- Scan live sites and preset & record your favorite content.
- English, Spanish, French, German, and Italian versions.
- $29.99 with 30-day money back guarantee.

Get RealPlayer Plus and listen to the 1997 NBA Playoffs live in RealAudio, free.

Included in your free ESPN SportsZone NBA Playoff Subscription when you order RealPlayer Plus.

You will receive instant download access to:
- RealAudio Player Plus 3.0 & RealPlayer Plus 4.0 beta (Available now for Windows 95/NT, Mac PowerPC)
- Free updates to any new versions released within 90 days

An e-mail will be sent with your ESPN SportsZone subscription information for the 1997 NBA Playoffs valid

1) Select Platform, Quantity, and Download Options

(a) Platform:
Windows 95

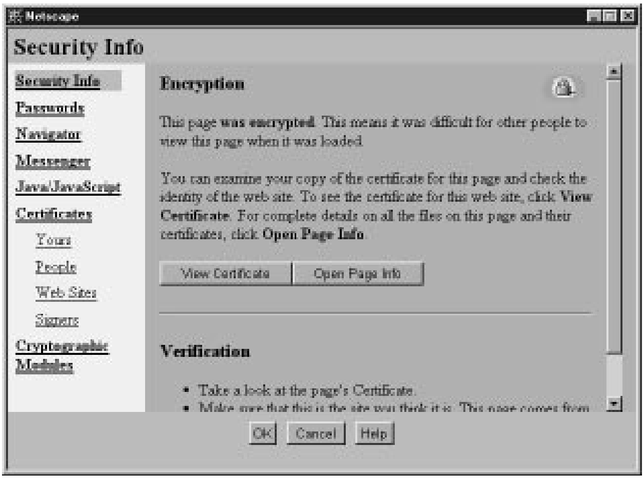
(b) Quantity:

Before selecting a platform, make sure you meet the following system requirements:

- **OS for RealAudio Player Plus 3.0:** Windows 95/NT, Windows 3.1x or MacOS.

FIGURE 20.4 There are certain things you can look for on a secure Web site.

To find out what kind of security protocol is activated, click the Security icon. This displays the Security Information dialog box, similar to the one shown in Figure 20.5, which offers details about the security measures in effect. To find out more, click the Security Info link.



**Encryption**

This page **was encrypted**. This means it was difficult for other people to view this page when it was loaded.

You can examine your copy of the certificate for this page and check the identity of the web site. To see the certificate for this web site, click **View Certificate**. For complete details on all the files on this page and their certificates, click **Open Page Info**.

**Verification**

- Take a look at the page's Certificate.
- Make sure that this is the site you think it is. This page comes from

FIGURE 20.5 Use the Security Info dialog box to see what type of security is being used.

If you intend to conduct business over the Web with a select amount of clients, you may want to check with your service provider to see if they offer *Electronic Data Interchange* (EDI). EDI uses an e-mail program that sets up a special mailbox on the service provider's computer. The special mailbox is exclusively for e-mail you and your clients exchange; the messages are automatically encrypted for you. You and your clients must both have the special software program needed to decrypt the messages. EDI is not cheap. However, if privacy concerns you, it is to your advantage to look into EDI.

## SHOPPING ON THE INTERNET

Another area of concern is online shopping. Many Internet users fear giving out their credit card numbers to pay for items found on Web sites and in online catalogs. Keep in mind, the Internet was not designed for secure communications of any kind. If possible, you should always try to find the online company's phone number or address to arrange payment for the items you want to buy.

But sometimes you may find something you can't resist. When this happens, you may want to look into *e-cash* (electronic cash). Innovative companies, such as DigiCash, are starting to offer various forms of e-cash for personal transactions conducted over the Internet. With e-cash, you set up an account with a bank and the bank sends you e-cash as encrypted e-mail. The encrypted e-cash consists of unique 64-bit numbers that cannot be copied. When you find something online you want to buy, you can use your e-cash to make the purchase. The company or person receiving your e-cash forwards it back to the bank for verification. If the numbers are accurate and enough cash is in your account, the e-cash transfers to the merchant.

CyberCash is another company offering innovative online transaction software. When you find an item you want to buy, request an electronic invoice from the merchant. You can then fill out the invoice by using CyberCash's software to encrypt your credit card number. When you send it back to the merchant for confirmation, he or she forwards the invoice to a CyberCash server to decrypt the number and process the purchase through a banking system, similar to a regular credit card purchase.

You'll see more innovations regarding online purchasing in the future. In the meantime, just use common sense and caution whenever making an online purchase. You may want to make sure that the company you are dealing with is a legitimate business before you divulge credit card information over the Net. When in doubt, look for companies that also give you the option of placing orders by using an 800 or 888 number.

## WORKING WITH COOKIES

Some Web pages you visit hand out *cookies*. Cookies are electronic tokens that Netscape keeps track of so the server can easily identify you the next time you visit. Cookies are also common among the Web's shopping pages. For example, each time you add an item to your electronic shopping cart, the server gives you a cookie marking the page where you found the item. When you check out, the server knows from the assigned cookies which items you want to buy.

Cookies enable the Web server you're visiting to write information onto your Netscape Navigator program. Any time another computer system writes information onto your computer system, there are some security risks. If this worries you, open the Edit menu and select Preferences. Choose the Advanced category. Select how or whether to accept cookies. Click OK to exit the dialog box.

If the information content of a cookie rattles your curiosity, you can open the COOKIES.TXT file and examine its contents. If a remote site storing its information onto your computer concerns you, you can safely delete the COOKIES.TXT file after you leave Netscape Communicator. The next time you start up the program, you will have a freshly baked cookie file.

## USING DIGITAL CERTIFICATES

Some of the Web sites you visit may assign you a user name and password that enable you greater access to the information stored there. In some cases, the additional privileges cost a small fee or require subscribing to the service.

Keeping track of the many user names and passwords needed to visit Web sites can be difficult. To solve the problem, you can use digital certificates or digital passports. With a digital certificate, you enter information about yourself the first time you connect to a site. When you connect to the site later, Netscape automatically identifies you to the server by sending your digital certificate. Therefore, you don't have to remember your user name and password because Netscape does it for you.

Digital certificates usually cost a small fee. Not many places on the Web offer digital certificates. VeriSign is one of few and can be found at http://digitalid.verisign.com/. Upon filling out an application and billing information, VeriSign will issue you a temporary certificate. The permanent one arrives via e-mail.

Netscape displays a dialog box that lets you assign a password to the certificate, if needed. Netscape also prompts you to enter a nickname to identify the certificate. When you're finished setting up the certificate, you can check it by clicking the Security icon on the toolbar. This opens the Security dialog box. Select Certificates Yours.

## WATCHING FOR VIRUSES

Computer viruses are a terrible thing, and there's good reason to be cautious. A virus is a program designed to interrupt your computer system or destroy data. A virus often hides itself in another file and passes innocently from one computer user to another. Once the virus is passed to you, it attaches itself to your system and can do damage to your data. Depending on the type of virus, the damage may be minimal, such as an annoying screen message; other times it's deadly, resulting in a total loss of important data. A virus may take action immediately when it enters your system, or it may lie in wait.

Viruses themselves are usually written for fun by programming pranksters. The more serious viruses, the ones that destroy data, are not designed in the spirit of fun, but in maliciousness. You will definitely want to avoid viruses, regardless of the spirit in which they were created.

Since the only way viruses can enter your computer system is through another file, you should take precautions when working with computer files. Here are some rules you can apply:

- Always download files into a temporary directory and run a virus detection program to check them.

- Invest in a good virus-protection program, particularly one that runs behind the scenes at all times to keep things secure, such as Norton Anti-Virus or McAfee. In addition, many of the better anti-virus programs scan compressed files before you decompress their contents.
- Make sure to backup your computer data often, especially your important files.
- Don't leave floppy disks in your disk drives. If you turn off the computer and an infected disk remains in the drive, the virus can infiltrate your system the next time you boot up your computer.
- Write-protect your floppy disks so foreign data cannot be copied onto the disks. To write-protect a floppy disk, slide the tab in the upper-left corner (with the label facing away from you) to open the tab.

There are many good virus-protection programs you can use today to keep your system secure. There are also anti-virus programs available on the Internet. Use a Web search engine to find out more about them.

**I Think I Have a Virus!** If you suspect your system has contracted a virus, use an anti-virus program to eradicate the virus then use your backup disks to restore your damaged data. Consult with a computer guru for help or check with a computer expert at your office.

Congratulations! You have made it through the last lesson in this book. You now possess the skills to surf the Web as an experienced Netscape user. But, don't put Que's *10 Minute Guide to Netscape Communicator 4* on the shelf yet. Keep it near your computer as a quick reference whenever you have trouble remembering any of the commands and options covered in these lessons.