# WEB SECURITY


By Dr. V. DEEPIKA

# Unit - II

## Privacy and Security for Users

- The Web's War on Your Privacy
- Privacy-Protecting Techniques
- Privacy-Protecting Technologies
- Backups and Antitheft

## Web Server Security

- Physical Security for Servers
- Host Security for Servers
- Securing Web Applications

# 1. The Web’s War on Your Privacy

“Understanding Online Privacy, Data Collection, and Tracking”

- Web activity is continuously monitored
- Every page visit is recorded by computers
- Browsing builds user interest profiles
- Registration leads to marketing emails & offers
- Privacy loss is often invisible to users

# Web Opportunities vs Privacy Costs

- Web enables:
  - Consumer convenience
  - Global access
- Also empowers:
  - Marketers
  - Sales organizations
  - Criminals
- Web ads collect:
  - Location
  - Browsing history
  - Internet access type
- **More data = less privacy**

# Technology and Privacy

- Internet designed for data transfer, not privacy
- Multiple web technologies enable tracking
- Privacy risks are built into the system
- Later chapters discuss privacy protection tools

# Understanding Privacy

- Privacy definitions vary.
- Merriam-Webster defines privacy as:
  - Being apart from observation
- Freedom from unauthorized intrusion

# The Tort of Privacy

- Introduced in 1890
- **Authors**:
  - Samuel Warren
  - Louis Brandeis
- Privacy **protects**:
  - Personal life
  - Against unwanted publicity
- Truth and lack of malice are not defenses

# Four Privacy Torts

1. **Privacy intrusion**
   - Intruding into a private sphere.
2. **Disclosure of private facts**
   - Publishing private information with no public interest.
3. **Portrayal of information in false light**
   - True or false information that misleads.
4. **Appropriation**
   - Using a person's name or likeness commercially without permission.

# Informational Privacy (Westin)

- Defined in 1967
- Control over:
  - When data is shared
  - How data is shared
  - To what extent
- Most web privacy violations fall here

# Types of Information

- **Personal information**
  - Name, birth date, education, family.
- **Private information**
  - Personal information not generally known.
  - Some protected by law (education records, bank records).
  - Privacy depends on context.
- **Personally Identifiable Information (PII)**
  - Data that reveals identity (name, account number).
- **Anonymized information**
  - Modified so identities cannot be discerned.
- **Aggregate information**
  - Statistical summaries (e.g., Census tract data).

# Triangulation

- Combining anonymized or aggregate data can reveal identities.
- Example: Zip code + birthday can uniquely identify individuals.
- Even “aggregate” questions may request PII unintentionally.

# User-Provided Information

- Users willingly provide:
  - Names
  - Addresses
  - Credit card details
- Accounts enable:
  - Purchase tracking
  - Long-term profiling

# User-Provided Information

- Figures 8-1 and 8-2: registration & security questions

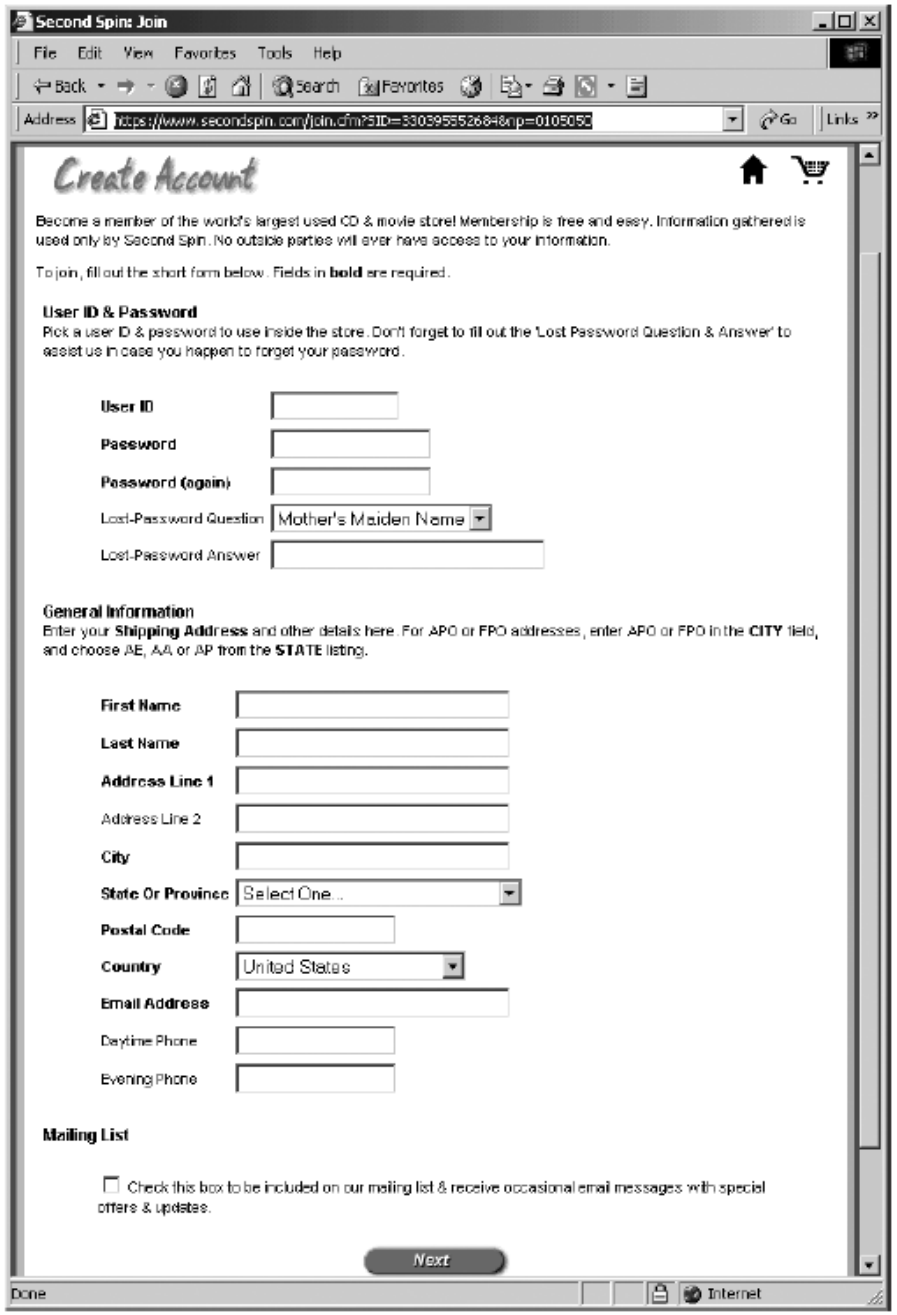


*Figure 8-1. By far, the greatest kind of personal information on the Web today is the information provided by consumers when they register at web sites.*

# User-Provided Information

- Figures 8-1 and 8-2: registration & security questions

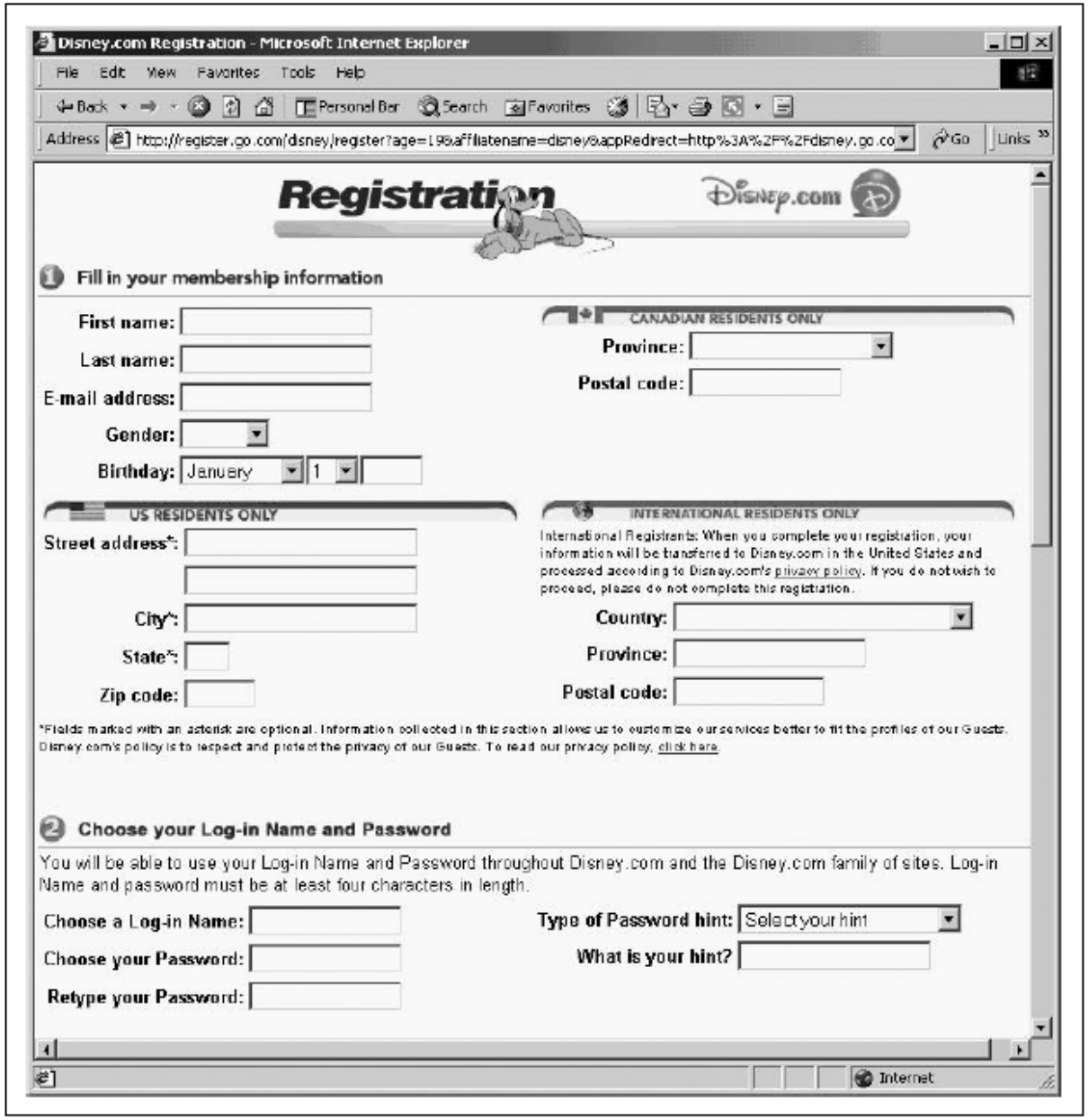


*Figure 8-2. Disney's registration page for adults asks for name, email address, gender, and birthday, in addition to mailing address. Many people are surprised how identifying even simple demographic information can be. For example, in many cases a person can be uniquely identified by day of birth (without the year) and Zip code.*

# Log Files

- Log files record network and user activity.
- Created for:
  - Debugging
  - Maintenance
  - Marketing
  - Government investigations
- Users usually unaware of logs

# Retention and Rotation

- **Rotation**: automatic deletion of old logs.
- Some systems retain logs until manually deleted.
- Backup systems (e.g., magnetic tape) may preserve logs for years.
- **Example** web server logs show:
  - access_log
  - access_log.1
  - access_log.2.gz
- These indicate **compressed and rotated logs**.

# Web Logs

- Each page request generates entries on:
  - Web servers
  - Databases
  - Firewalls
  - Proxies
- Logs can be subpoenaed or misused.
- Most logs are never reviewed, yet store extensive data

# What's in a Web Log?

- IP address and hostname
- Timestamp
- Requested URL
- Browser type
- Refer link
- Errors
- Authentication usernames
- Logs can be cross-correlated to identify users.

# What's in a Web Log?

- **Example 8-1**
- Shows a **typical web server log**
- Demonstrates:
  - IP tracking
  - Browser identification
  - Refer links

*Example 8-1. A sample web server log*

```
free-dial-77.freeport.mwci.net - - [09/Mar/1997:00:04:11 -0500] "GET /awa/issue2/
    Woodstock.gif HTTP/1.0" 200 26385
"http://www.vineyard.net/awa/issue2/Wood.html" "Mozilla/2.0 (compatible; MSIE 3.01;
    Windows 95)" ""
free-dial-77.freeport.mwci.net - - [09/Mar/1997:00:04:27 -0500] "GET /awa/issue2/
    WoodstockWoodcut.gif HTTP/1.0" 200 54467
"http://www.vineyard.net/awa/issue2/Wood.html" "Mozilla/2.0 (compatible; MSIE 3.01;
    Windows 95)" ""
crawl4.atext.com - - [09/Mar/1997:00:04:30 -0500] "GET /org/mvcc/ HTTP/1.0" 200 10768 "-"
    "ArchitextSpider" ""
www-as6.proxy.aol.com - - [09/Mar/1997:00:04:34 -0500] "GET /cgi-bin/imagemap/mvol/cat2.
    map?31,39 HTTP/1.0" 302 - "http://www.mvol.com/" "Mozilla/2.0 (Compatible; AOL-IWENG
    3.0; Win16)" ""
www-as6.proxy.aol.com - - [09/Mar/1997:00:04:40 -0500] "GET /mvol/photo.html HTTP/1.0" 200
    6801
"http://www.mvol.com/" "Mozilla/2.0 (Compatible; AOL-IWENG 3.0; Win16)" ""
www-as6.proxy.aol.com - - [09/Mar/1997:00:04:48 -0500] "GET /mvol/photo2.gif HTTP/1.0" 200
    12748
"http://www.mvol.com/" "Mozilla/2.0 (Compatible; AOL-IWENG 3.0; Win16)" ""
free-dial-77.freeport.mwci.net - - [09/Mar/1997:00:05:07 -0500] "GET /awa/issue2/Wood.html
    HTTP/1.0" 200 37016
"http://www.altavista.digital.com/cgi-bin/query?pg=q&what=web&fmt=.&q=woodstock" "Mozilla/
    2.0 (compatible; MSIE 3.01; Windows 95)" ""
free-dial-77.freeport.mwci.net - - [09/Mar/1997:00:05:07 -0500] "GET /awa/issue2/
    Sprocket1.gif HTTP/1.0" 200 4648
"http://www.vineyard.net/awa/issue2/Wood.html" "Mozilla/2.0 (compatible; MSIE 3.01;
    Windows 95)" ""
free-dial-77.freeport.mwci.net - - [09/Mar/1997:00:05:08 -0500] "GET /awa/issue2/
    Sprocket2.gif HTTP/1.0" 200 5506
"http://www.vineyard.net/awa/issue2/Wood.html" "Mozilla/2.0 (compatible; MSIE 3.01;
    Windows 95)" ""
www-as6.proxy.aol.com - - [09/Mar/1997:00:05:09 -0500] "GET /mvol/peter/index.html HTTP/1.
    0" 200 891 "http://www.vineyard.net/mvol/photo.html" "Mozilla/2.0 (Compatible; AOL-
    IWENG 3.0; Win16)" ""
```

# The Refer Link Field

- Automatically sends the **previous URL.**
- Used to:
  - Measure advertisement effectiveness
  - Track navigation paths
- Can leak:
  - Search queries
  - Form data
- GET vs POST:
  - GET embeds data in URLs → higher privacy risk

# Obscuring Web Logs

- Proxy servers hide user IP addresses.
- Proxies do not guarantee anonymity.
- Proxy logs can still identify users.

# RADIUS Logs

- RADIUS authenticates dial-up users.
- Logs include:
  - Username
  - IP address
  - Session time
  - CALLER-ID
- Played a key role in identifying the **Melissa worm author**.

# Mail Logs

- Track:
  - Sender and recipient
  - Time
  - Message ID
- Content usually not logged.
- Useful for identifying:
  - Communication patterns
  - Mailing list membership

# DNS Logs

- DNS servers can log every query.
- Reveal:
  - Websites accessed
  - User behavior patterns
- Useful for maintenance and surveillance.

# Understanding Cookies

- Cookies = small ASCII text blocks
- Stored by browsers
- Sent with every request
- Enable session tracking

# The Cookie Protocol

- Cookies are set using Set-Cookie headers.
- Key attributes:
  - expires
  - domain
  - path
  - secure
- Cookies are sent back via HTTP headers.

# The Cookie Protocol

## Example Cookies

- HotBot sends multiple cookies (Table 8-1).
- Includes third-party cookies (e.g., .lycos.com).
- Cookies used for:
  - Tracking
  - Visitor counting
  - Advertising profiles

*Table 8-1. Cookies sent by www.hotbot.com at 8:10 a.m. EST on April 21, 2001*

| Cookie # | Content | Domain | Expires | Path |
|---|---|---|---|---|
| 1 | lubid=01000008C73351C5086C3AE177A40000351200000000 | *.lycos.com* | 18-Jan-2038 08:00:00 GMT | / |
| 2 | p_uniqid=aD3QMJX/K93Z | | 21-Dec-2012 08:00:00 GMT | / |
| 3 | remotehost=secondary=chi%2Emegapath&top=net | | 21-May-2001 07:00:00 | / |
| 4 | HB%5FSESSION=BT=lowend&BA=false&VE=&PL=Unknown&MI=u&BR=Unknown&MA=0&BC=1 | | | / |

# Cookie Uses

- Store user data directly
- Or store identifiers linked to databases
- Widely used for advertising analytics

# Cookies and Privacy

- Cookies can:
  - Weaken privacy (profiling, tracking)
  - Improve privacy (store preferences locally)
- Example privacy-protecting cookie:
- DigiCrime virus counter

# Cookie Jars

- Cookies stored:
  - In memory
  - On disk if persistent
- Netscape:
  - cookies.txt (Example 8-2)

*Example 8-2. A sample Netscape cookies file*

```
# Netscape HTTP Cookie File
# http://www.netscape.com/newsref/std/cookie_spec.html
# This is a generated file!  Do not edit.
.techweb.com     TRUE  /wire/news FALSE 942169160 TechWeb 204.31.228.79.852255600 path=/
.hotwired.com    TRUE  /   FALSE 946684799 p_uniqid  yQ63oN3ALxO1a73pNB
.talk.com        TRUE  /   FALSE 946684799 p_uniqid  y46RXMoBwFwD16ZFTA
.packet.com      TRUE  /   FALSE 946684799 p_uniqid  y86ijMoA9MhsGhluvB
.boston.com      TRUE  /   FALSE 946684799 INTERSE   stl-mo8-10.ix.netcom.
com20748850376179639
.netscape.com    TRUE  /   FALSE 1609372800 MOZILLA  MOZ-ID=DFJAKGLKKJRPMNX[-]MOZ_VERS=1.
    2[-]MOZ_FLAG=2[-]MOZ_TYPE=5[-]MOZ_CK=AJpz085+6OjN_Ao1[-]
.netscape.com    TRUE  /    FALSE 1609372800 NS_IBD   IBD_
    SUBSCRIPTIONS=INC005|INC010|INC017|INC018|INC020|INC021|INC022|INC034|INC046
www.xmission.com   FALSE  /  FALSE  946511999  RoxenUserID  0x7398
ad.doubleclick.net FALSE  /  FALSE  942191940  IAF  22348bb
.focalink.com     TRUE    /  FALSE  946641600  SB_ID  ads01.28425853273216764786
gtplacer.globaltrack.com  FALSE  /  FALSE 942105660  gtzopyid  85317245
.netscape.com     TRUE    /  FALSE  1585744496  REG_DATA  C_DATE_REG=13:06:51.304128 01/
    17/97[-]C_ATP=1[-]C_NUM=0[-]
www.digicrime.com   FALSE    FALSE  942189160  DigiCrime  virus=1
```

# Cookie Jars

- Internet Explorer:
- Individual files (Figure 8-3, Example 8-3)

*Example 8-3. The contents of an Internet Explorer Cookies file.*

```
SITESERVER
ID=94e349397f0ba875c43fac4e1497ed69
caregroup.org/
0
642859008
31887777
514252192
29395648
*
```

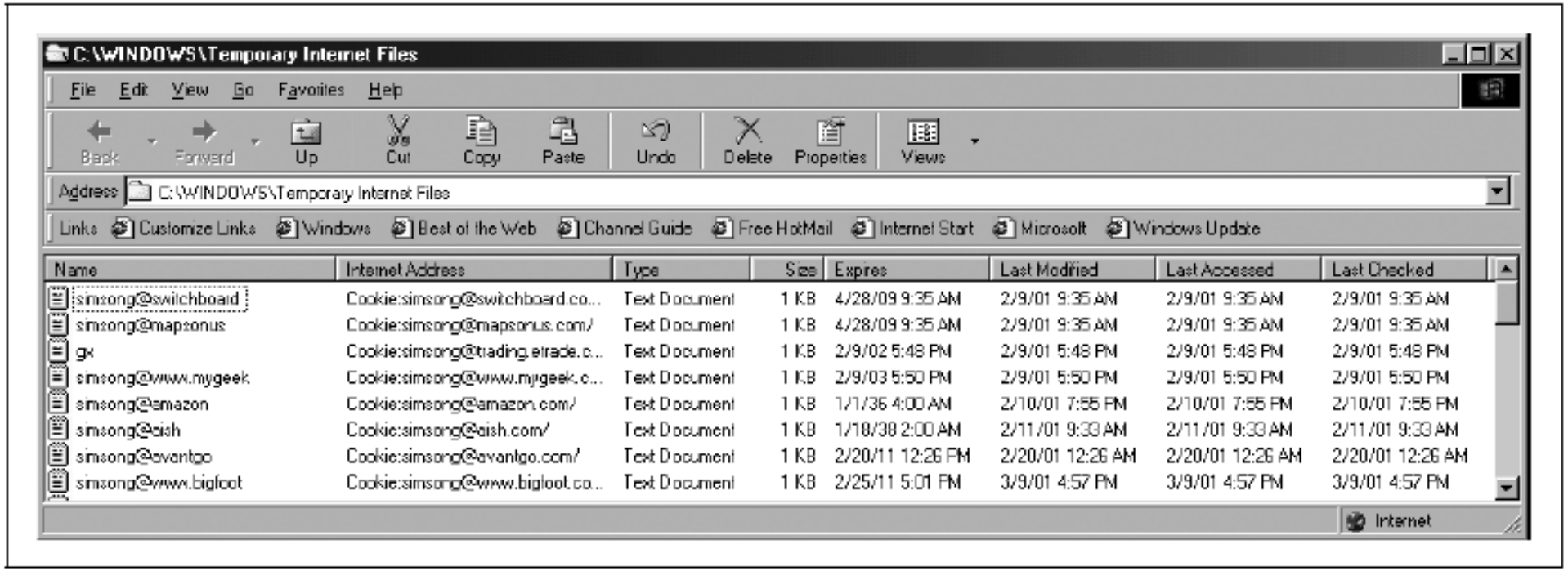


*Figure 8-3. Internet Explorer stores cookies in files in the Cookies directory. You can delete a cookie by clicking on the cookie with the mouse and hitting the "Delete" key.*

# Cookie Security

- Cookies can be edited by users.
- Secure cookies use:
  - Random IDs
  - Cryptographic MACs
- Examples compare insecure vs more secure cookies.

# Disabling Cookies

- Browsers allow:
  - Accept all
  - Reject all
  - Prompt user
- Cookies already accepted cannot be selectively blocked.
- Advanced techniques include:
  - File permission tricks
  - Proxy filters

# Disabling Cookies

- Figure 8-4 shows cookie management interface.

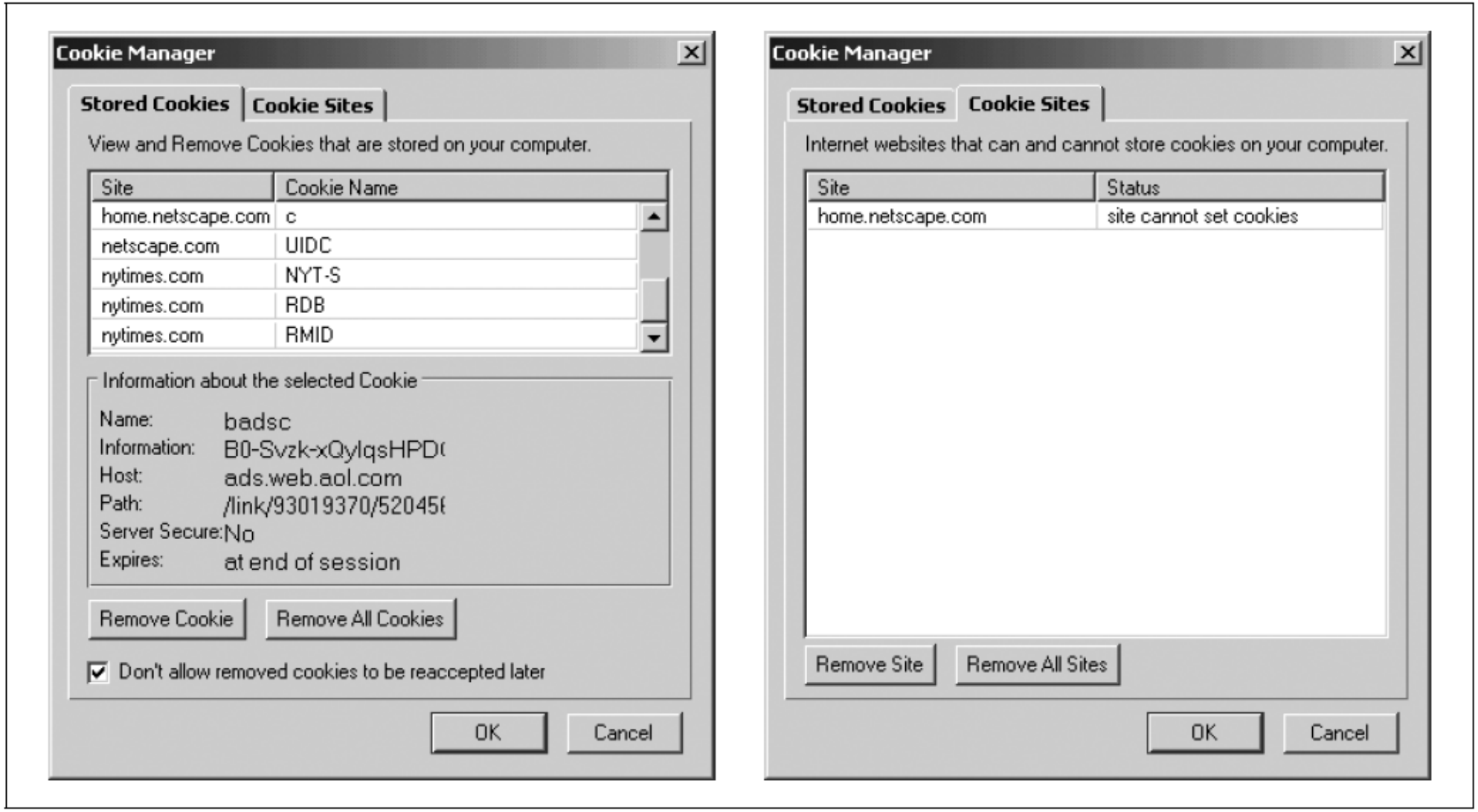


*Figure 8-4. Netscape 6.0's Cookie Manager allows cookies to be controlled on a site-by-site basis*

# Web Bugs

- Introduced publicly in 2000 by the Privacy Foundation.
- Small invisible images (1×1 GIF).
- Also called:
  - Clear GIFs
- Beacon GIFs

# Web Bugs on Web Pages

- Example bugs from Quicken.COM:
  - Doubleclick
  - MatchLogic
- Enable third-party tracking without ads.
- Allow cross-database correlation.
- Figure 8-5 shows web bug in Yahoo Profile.

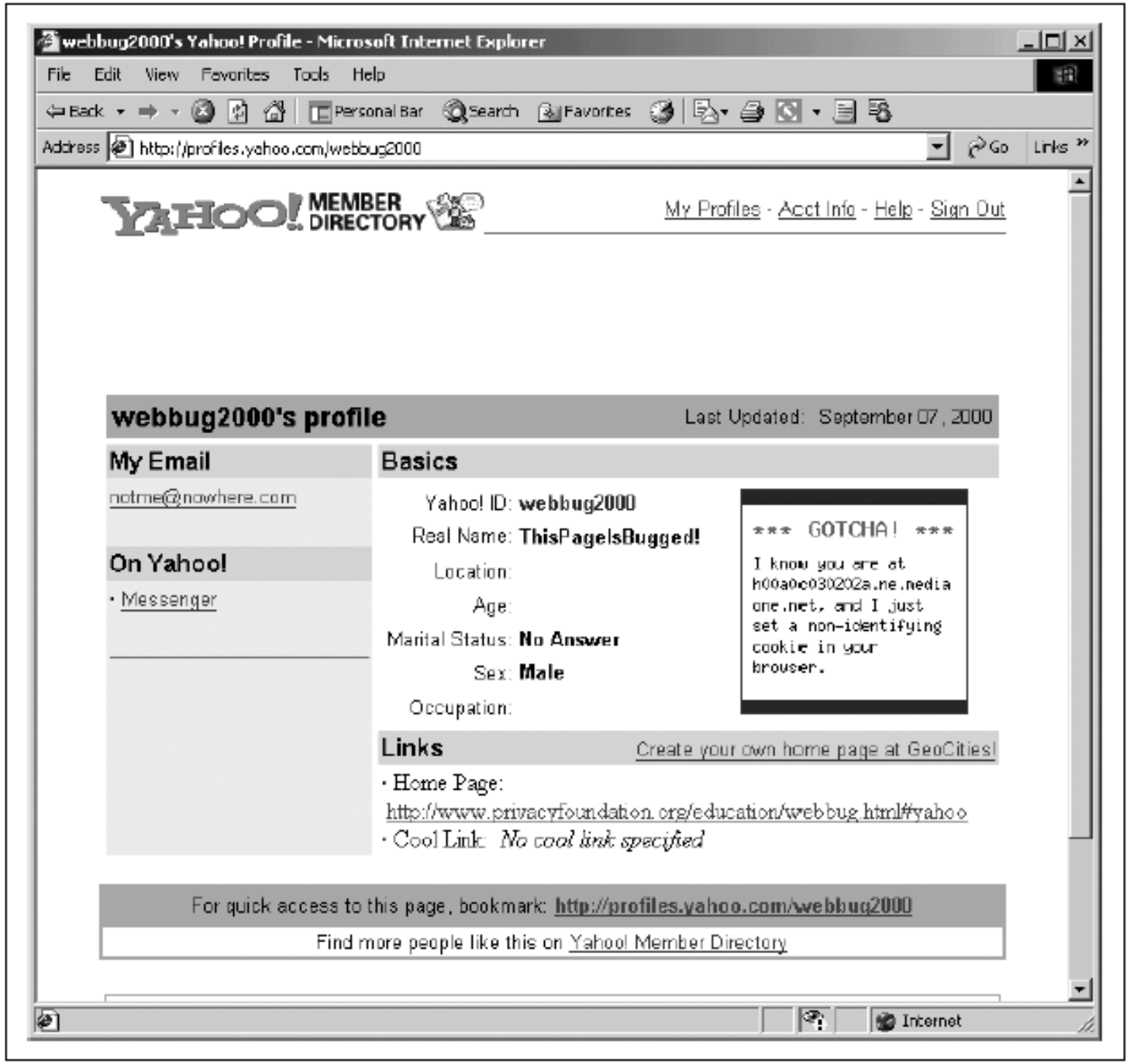


*Figure 8-5. A Yahoo profile that was bugged with a web bug by the Privacy Foundation*

# Web Bugs in Email Messages and Word Files

- Used to detect:
  - Email reading
  - Forwarding
- Can be embedded in:
  - HTML email
  - Usenet messages
  - Microsoft Word documents

# Uses of Web Bugs

- Usage statistics
- Cross-site tracking
- User profiling
- Cookie synchronization
- Ad verification
- Email tracking
- Detecting copyright infringement

# 2. Privacy-Protecting Techniques

- The Internet allows extensive **collection of personal information**.
- This chapter focuses on **practical techniques** to protect privacy.
- Techniques are mostly:
  - Simple
  - Common-sense
  - Immediately applicable
- Key areas covered:
  - Choosing a good service provider
  - Using strong passwords
  - Cleaning online traces
  - Avoiding spam and junk email
  - Protecting against identity theft

# Choosing a Good Service Provider

- The **most important privacy decision** is selecting a trustworthy ISP.
- ISPs can monitor:
  - Every website visited
  - Emails sent and received
  - Online behavior patterns
- Dial-up ISPs can infer:
  - When you are home
  - Travel or vacation periods
- ISPs may learn:
  - Workplace location (via email access)
  - User demographics

# ISP Monitoring Practices

- ISPs may monitor for:
  - Maintenance
  - Research
  - Marketing
- Some ISPs sell user data
- Monitoring may be:
  - Disclosed
  - Or hidden
- New tools allow ad replacement and profiling

# ISP Privacy Policies

- Some ISPs enforce strict data-access rules.
- Others have **no privacy policies**.
- Many policies state:
  - "We can monitor anything we want."
- Privacy policies may use **vague legal language**.
- Some ISPs provide **no privacy policy at all.**
- Legal protections are limited; ISPs hold significant power.

# Picking a Great Password

- Passwords are the **simplest form of authentication**.
- A password is **a shared secret** between user and computer.
- Strong passwords are a **first line of privacy defense**.
- Risks:
  - Easy-to-guess passwords
  - Reusing passwords across services

# Why Use Passwords?

- Early personal computers:
  - Used by one person
  - Rarely required passwords
- Internet use introduced:
  - Email account passwords
  - Website account passwords
- Passwords prevent:
  - Unauthorized access
  - Viewing personal data
- Modern operating systems:
  - Windows
  - Macintosh
  - Unix
- Passwords control limited access to personal data.
- Users often receive **poor guidance** on password selection.

# Bad Passwords: Open Doors

- Bad passwords are easy to guess.
- Crackers use:
  - Automated password-guessing programs
  - Lists of common passwords
- Weak passwords include:
  - Names (self, family, pets)
  - Dictionary words
  - Short passwords
  - Common substitutions (l → 1, E → 3)
  - Words backwards
- Examples of weak choices:
  - Movie characters
  - Landmarks
  - Phone numbers
  - Famous computer scientists
- Web-based services are more vulnerable due to:
  - High-speed guessing attempts
- Password rules vary widely across services.

# Smoking Joes

- “Joe accounts”:
  - Username and password are identical
- Extremely easy for attackers to exploit.
- Crackers often check for Joe accounts first.
- Making username lists public increases risk.

# Good Passwords: Locked Doors

- Strong passwords:
  - Use uppercase and lowercase letters
  - Include digits and punctuation
  - Are at least 7–8 characters long
  - Are easy to remember
  - Can be typed quickly
- Suggested techniques:
  - Combine words with symbols (robot4my)
  - Use personal acronyms
- Once published, examples become **bad passwords**.

# Bad Passwords

- Avoid:
  - Names (yours or others')
  - Birthdates
  - Social Security numbers
  - Usernames
  - Dictionary words
  - Keyboard patterns (qwerty)
  - Single-digit variations
- Eight-character random passwords provide:
  - Billions of combinations
  - Protection against brute-force attacks
- Longer passwords often fail due to:
  - System truncation at 8 characters

# Writing Down Passwords

- Written passwords can be stolen
- Complex written passwords may be safer
- If written:
  - Don’t label as passwords
  - Don’t include account names
  - Don’t keep near computer
- Password-keeping programs (Table 9-1)

# Writing Down Passwords

*Table 9-1. Recommended password keeper programs*

| Platform | Program | Location |
|---|---|---|
| PalmOS | GNU keyring | *http://gnukeyring.sourceforge.net/* |
| PalmOS | Strip | *http://www.zetetic.net* |
| Windows | Password Keeper 2000 | *http://www.gregorybraun.com/PassKeep.html* |
| Windows | Password Safe | *http://www.counterpane.com/passsafe.html* |
| Macintosh 8.x, 9.x | Mac OS Keychain | Built in; see the Keychain Access control panel |

# Strategies for Managing Multiple Usernames and Passwords

- Reusing passwords increases risk:
  - One breach compromises many accounts
- System administrators may access stored passwords.
- Password restrictions differ by system.

- Password Classes
- Password Bases
- Password Rotation
- Password Keepers

# Strategies for Managing Multiple Usernames and Passwords (cont..)

**Password Classes**

- Divide passwords by security level:
  - Banking
  - Email
  - Low-security sites

**Password Bases**

- Modify a base password per service.
- Avoid obvious patterns.

**Password Rotation**

- Change passwords periodically.
- Can become confusing over time.

**Password Keepers**

- Store passwords securely in encrypted form.
- Built into browsers (Netscape, Internet Explorer).
- Available as:
  - Wallet programs
  - Stand-alone software
- PGP can be used to create a custom password safe

# Sharing Passwords

- Sharing passwords gives others:
  - Access to personal data
  - Ability to impersonate you
- Treat passwords like house keys.
- Best practices:
  - Share discreetly
  - Never email plaintext passwords
  - Change passwords after sharing ends

# Resist Social Engineering Attacks

- Attackers trick users into revealing passwords.
- Common methods:
  - Fake ISP emails
  - Phone calls posing as IT staff
  - Requests to reset passwords
- Attacks succeed due to:
  - Desire to be helpful
  - Lack of security awareness

# Beware of Password Sniffers and Stealers

**Password Sniffers**

- Capture unencrypted passwords in transit.
- Target protocols:
  - FTP
  - HTTP
  - POP
  - TELNET
  - RLOGIN
- Sniffers have been found on:
  - University networks
  - Corporate systems
  - ISP backbones
- Use encrypted protocols to reduce risk.

# Beware of Password Sniffers and Stealers (cont..)

**Keystroke Recorders and Keyboard Sniffers**

- Record everything typed.
- Can be:
  - Software-based
  - Hardware-based
- Figure 9-1: KeyKatch device
  - Small hardware keystroke recorder
  - Undetectable without physical inspection
- Screen recorders capture display content.
- Programs like Back Orifice 2000 enable remote spying.

# Beware of Password Sniffers and Stealers (cont..)


*Figure 9-1. The KeyKatch is a small device that attaches between a keyboard and a desktop computer and can record more than two million keystrokes (reprinted with permission)*

# Beware of Password Sniffers and Stealers (cont..)

**Beware of Public Terminals**

- Higher risk of spyware.
- Precautions:
  - Avoid confidential access
  - Use temporary webmail accounts

# Cleaning Up After Yourself

- Internet use leaves electronic footprints.
- Computer forensics can reveal:
  - Visited websites
  - Downloaded data
- Cleanup reduces privacy risk.
- Automatic cleanup tools

# Browser Cache

- Cache stores previously visited pages.
- Improves speed but reduces privacy.
- Privacy protection methods:
  - Disable caching for SSL pages
  - Disable caching entirely
  - Manually delete cache

# Browser Cache:

## Managing Cache with Internet Explorer

- Use Internet Properties panel.
- Options:
  - Delete Files
  - View cached files
- Figure 9-2: Internet Properties panel
- Figure 9-3: Cache directory view
- Figure 9-4: ActiveX objects list

# Browser Cache:
# Managing Cache with Internet Explorer

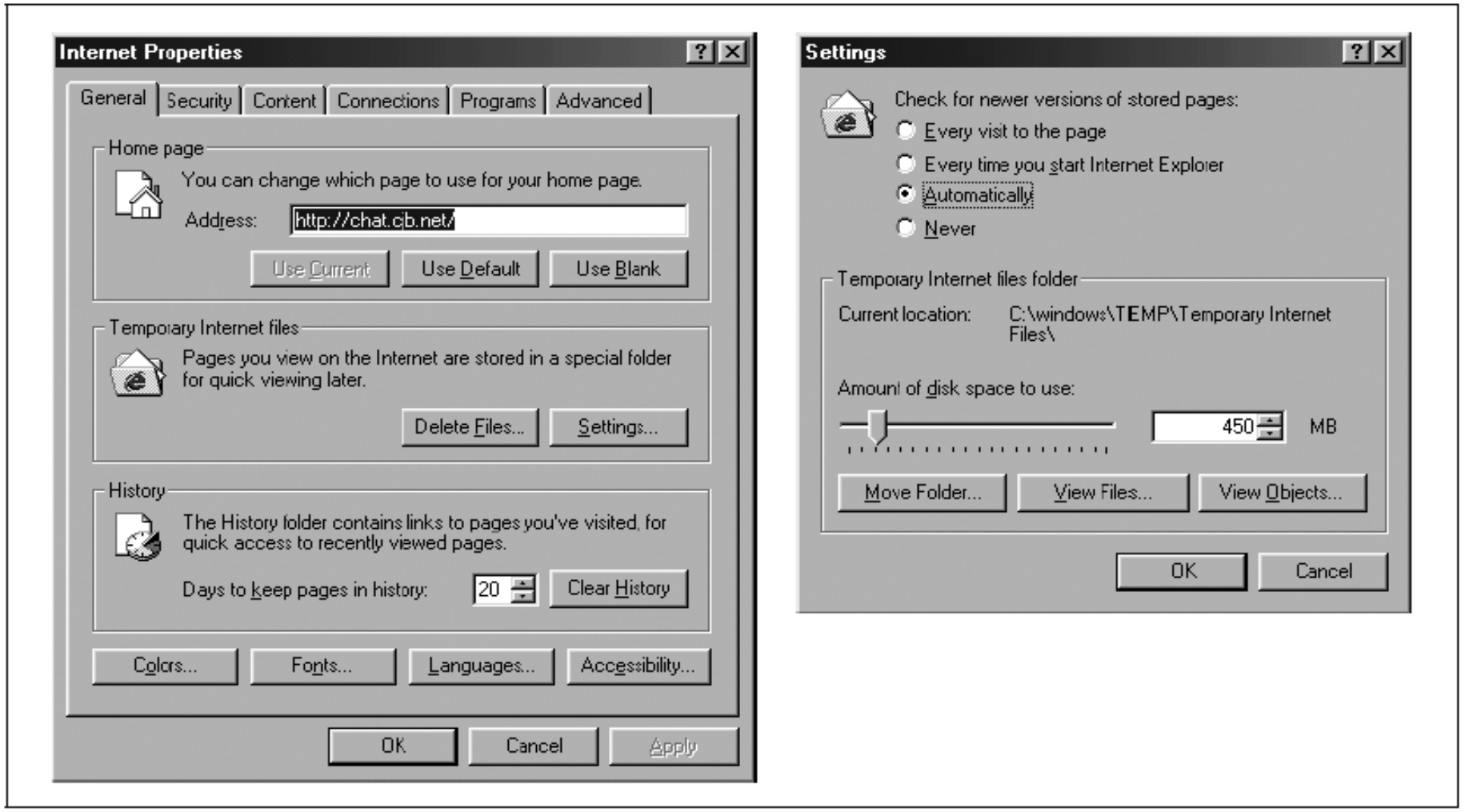


*Figure 9-2. With the Internet Explorer "Internet Properties" control panel, you can control the browser's cache by clicking on the "Delete Files . . . " and "Settings . . . " buttons. If you click the "Settings . . . " button, the Settings panel will appear. Click the "View Files . . . " button to display the directory containing cookies and browser cache.*

# Browser Cache:
# Managing Cache with Internet Explorer

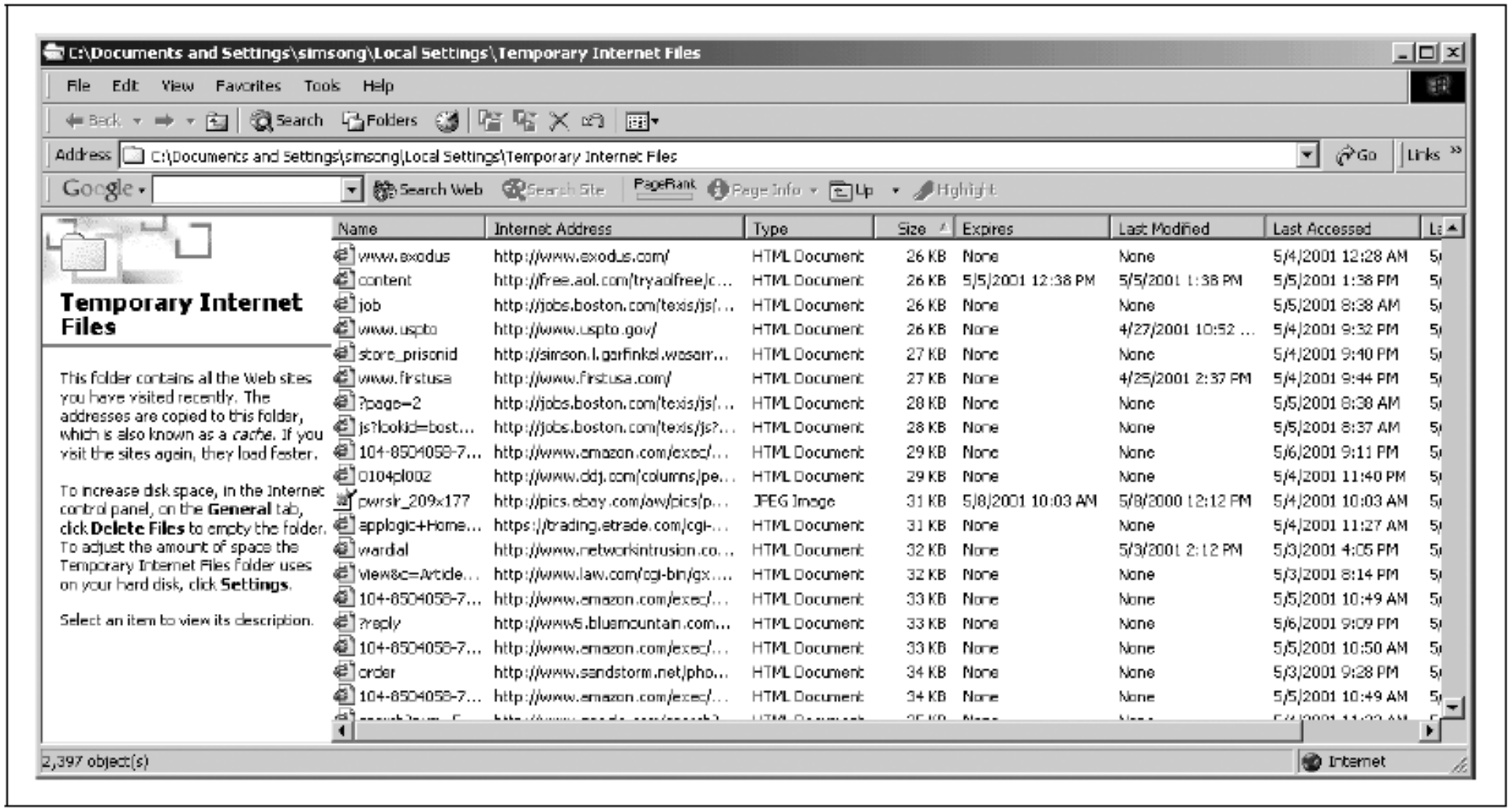


*Figure 9-3. When you click on the View Files button, Internet Explorer opens up the Temporary Internet Files folder. This folder can contain cookies, JPEG files, and HTML documents. You can delete them as you wish without damaging your computer.*

# Browser Cache:
# Managing Cache with Internet Explorer

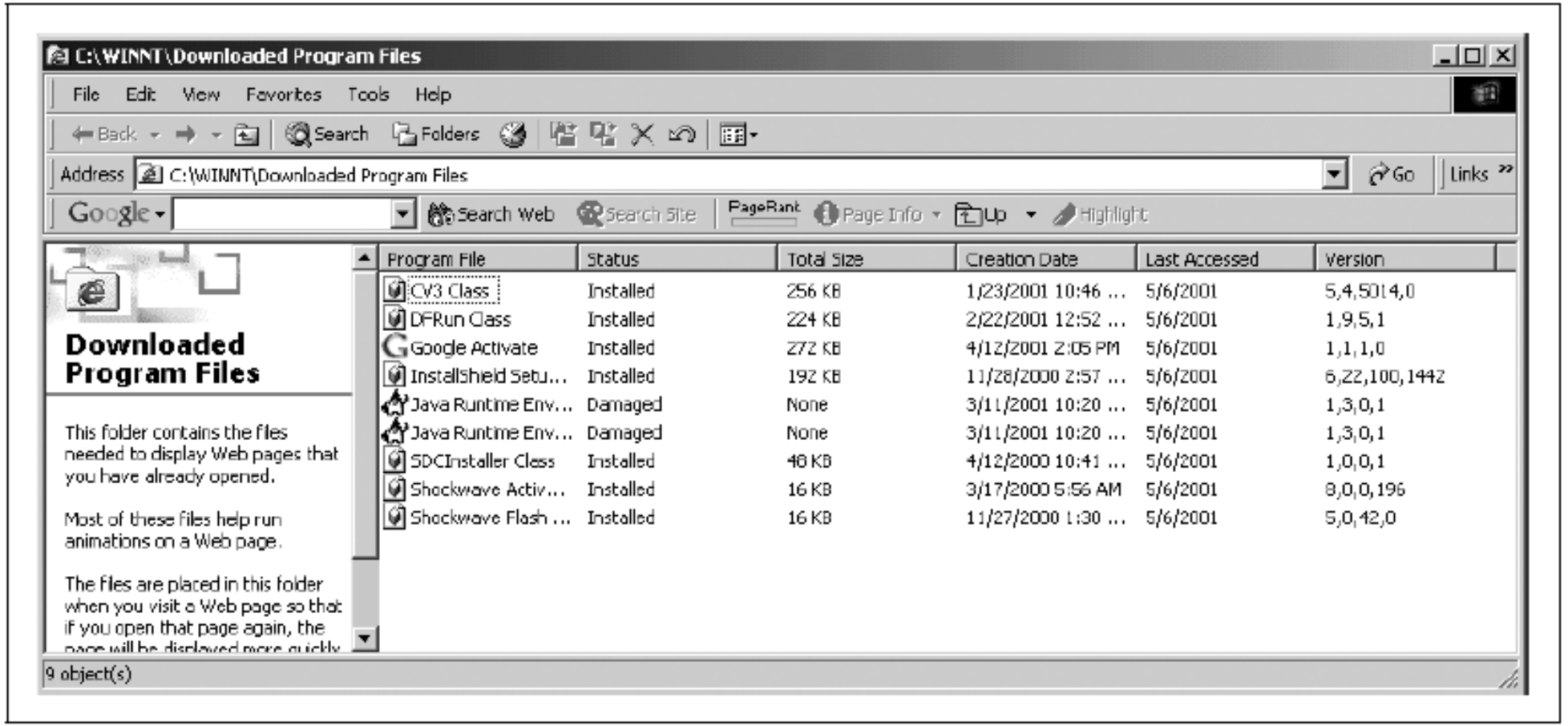


*Figure 9-4. When you click the "View Objects..." button, Internet Explorer opens up the Downloaded Program Files folder. This folder will show you the ActiveX components that have been downloaded. In this example, components for several third-party programs have been downloaded. All except the Java runtime components are active.*

# Browser Cache:
# Managing Cache with Internet Explorer

- Preferences → Advanced → Cache
- Clear disk and memory cache
- Figure 9-5: Netscape cache settings

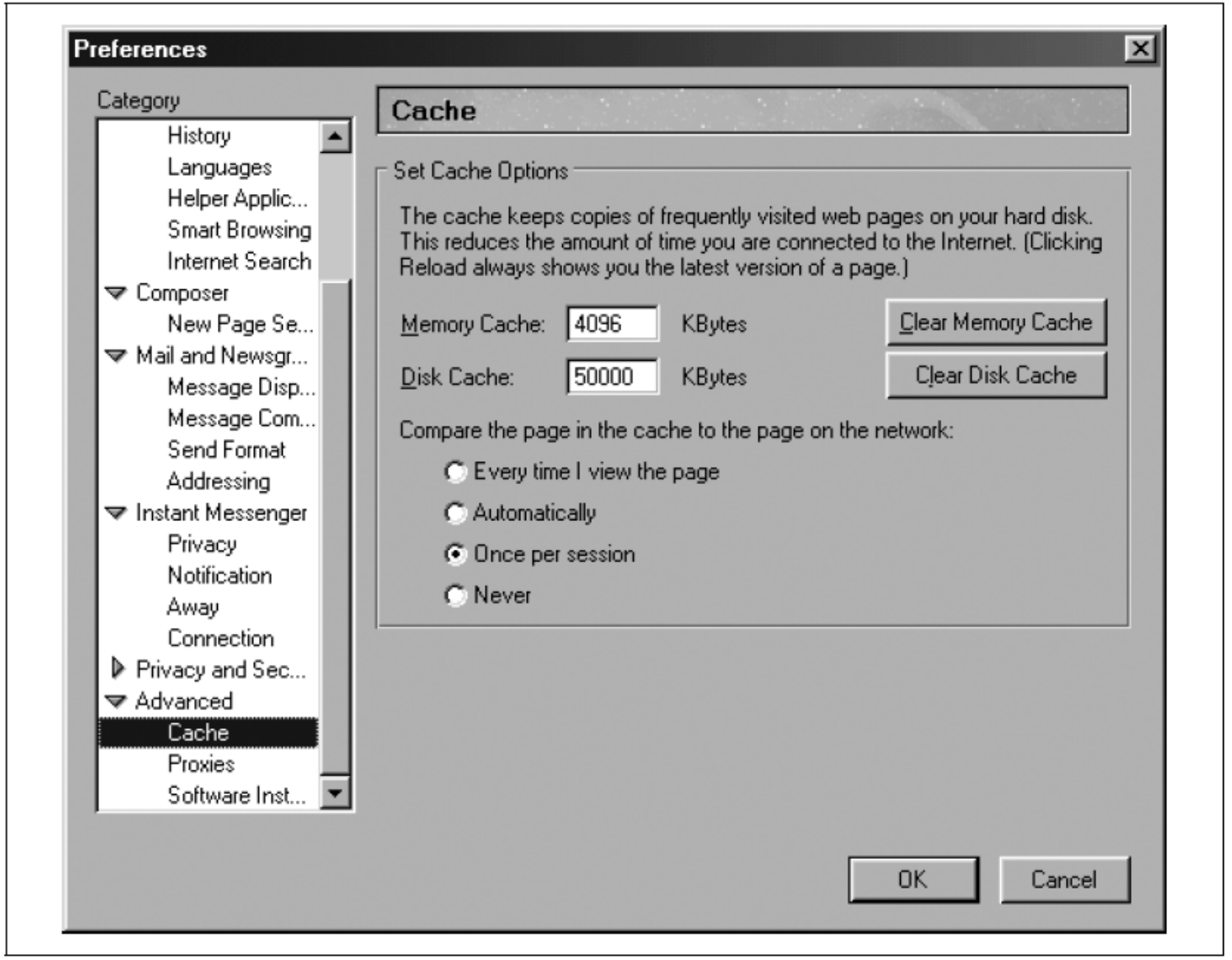


*Figure 9-5. Buttons on Netscape Preferences panel allow you to clear the cache*

# Cookies

- Cookies store session and tracking data.
- Can expose personal information.

**Crushing Internet Explorer's Cookies**

- Cookies stored in History directory.
- Can be manually deleted.

**Crushing Netscape's Cookies**

- Stored in cookies.txt.
- Managed via Cookie Manager.
- Figure 9-6: Cookie Manager menu
- Figure 9-7: Stored cookies view

# Cookies

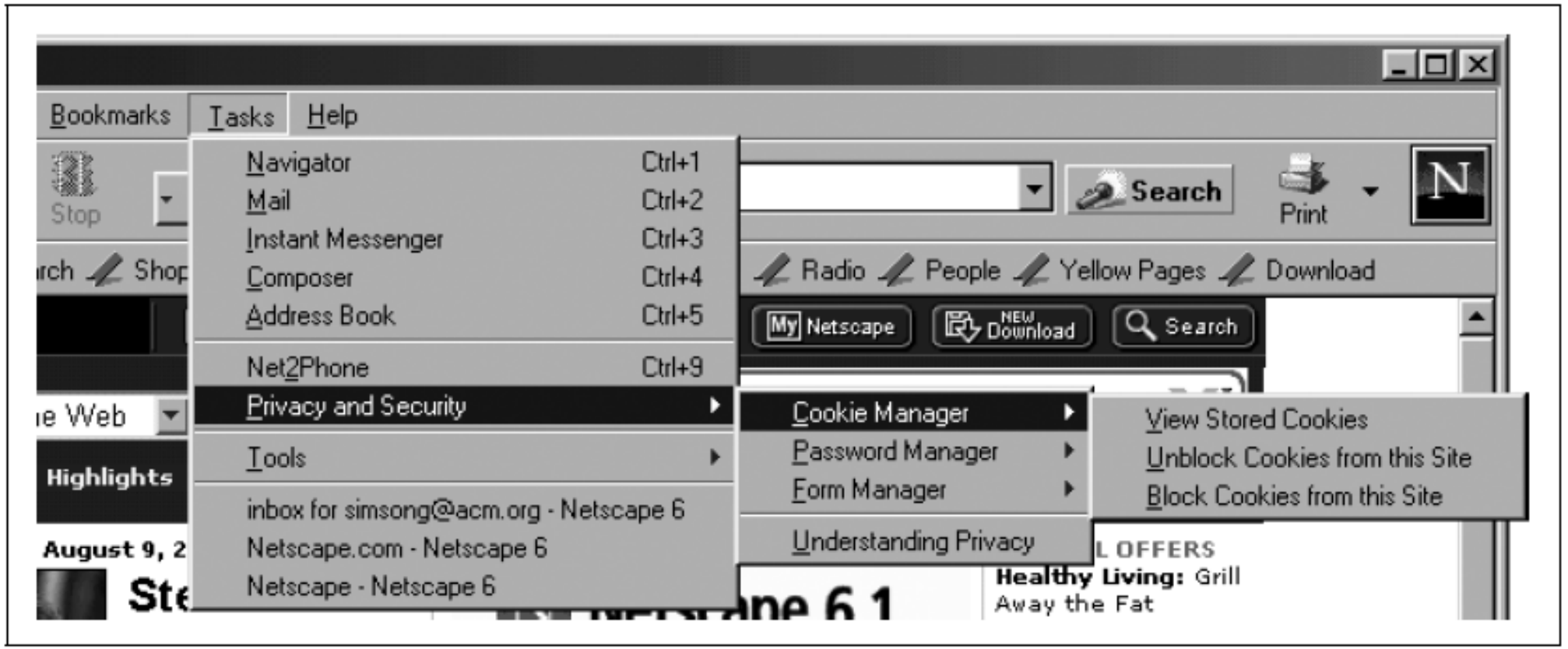


*Figure 9-6. Netscape's Cookie Manager is accessed through the "Privacy and Security" submenu of the Tasks menu.*

# Cookies

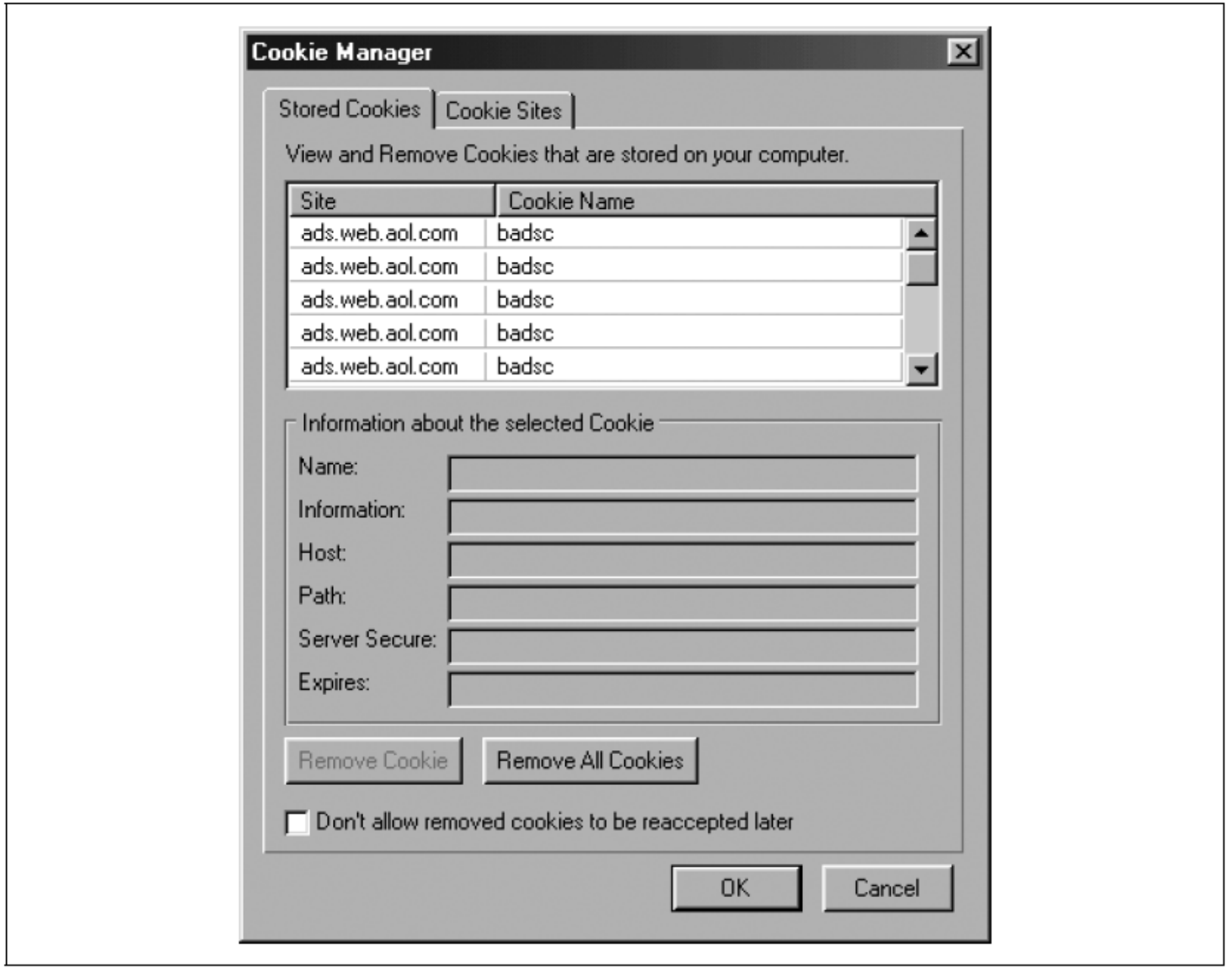


*Figure 9-7. The Netscape Cookie Manager shows you which cookies have been accepted from which site. It allows you to block individual cookies, to delete a cookie, or to remove all cookies.*

# Browser History

- Browsers store visited URLs.
- Can reveal sensitive activity.
- Clearing history is recommended.

**Clearing Internet Explorer's Browser History**

- Stored in index.dat.
- Viewed as databases in Explorer.
- Figure 9-8: History database view
- Figure 9-9: Typed URLs registry

**Clearing Netscape Navigator's Browser History**

- Preferences → Navigator → History

# Browser History

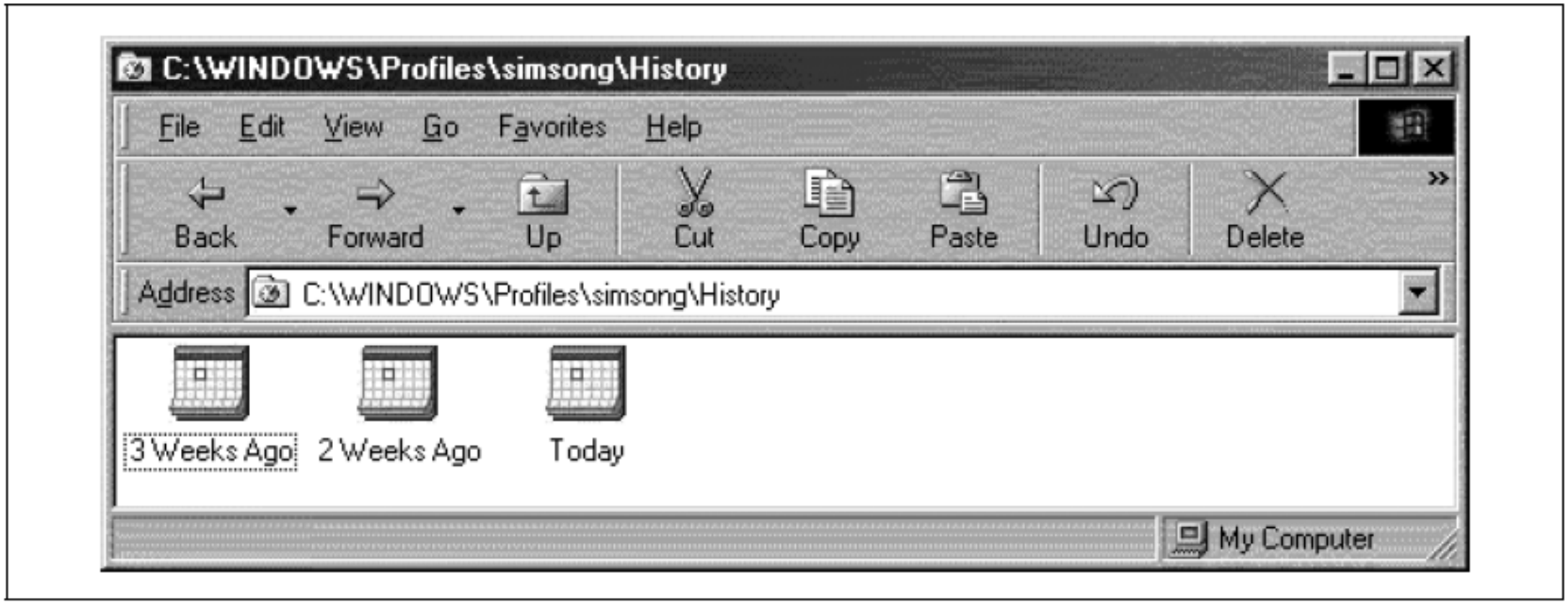


*Figure 9-8. Internet Explorer has a shell extension that makes the file index.dat in the History folder appear as a set of tiny calendars. If you double-click on one of the little calendar icons, you will see the individual history records that it contains.*

# Browser History

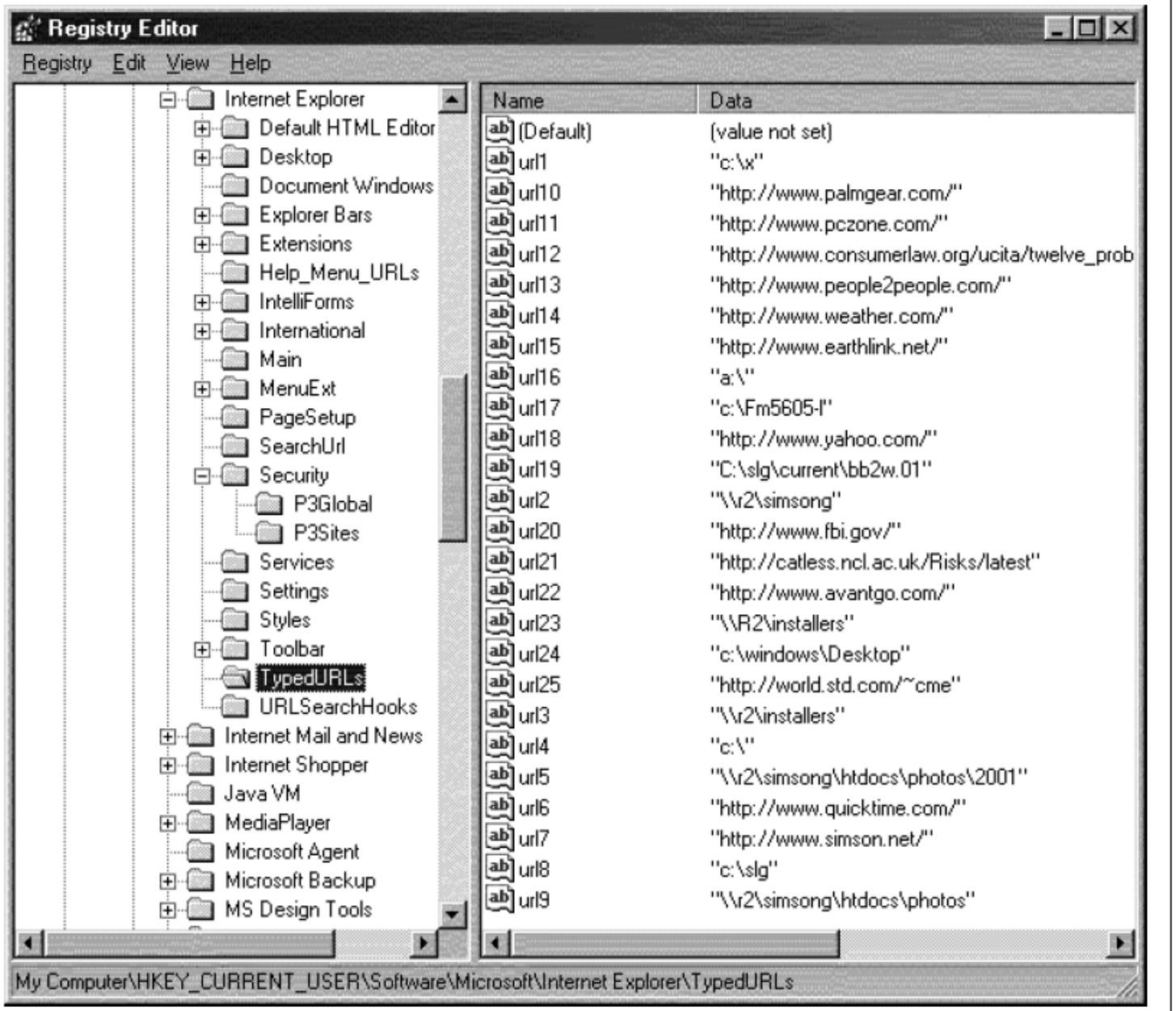


*Figure 9-9. Internet Explorer stores the last typed URLs at the Registry Key HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs.*

# Passwords, Form-Filling, and AutoComplete Settings

- Browsers store:
  - Form data
  - Usernames
  - Passwords
- Convenient but risky.
- Figure 9-10: AutoComplete prompt

**Clearing AutoComplete with Internet Explorer**

- Content tab → AutoComplete
- Clear forms and passwords
- Figure 9-11: AutoComplete settings

**Clearing Sensitive Information with Netscape Navigator**

- Password Manager
- Figure 9-12: Clear sensitive information

# Passwords, Form-Filling, and AutoComplete Settings


*Figure 9-10. Internet Explorer's AutoComplete system will remember fields that you recently entered into web forms. This feature can be very handy, but it can also reveal information to other people who have access to your computer.*

# Passwords, Form-Filling, and AutoComplete Settings

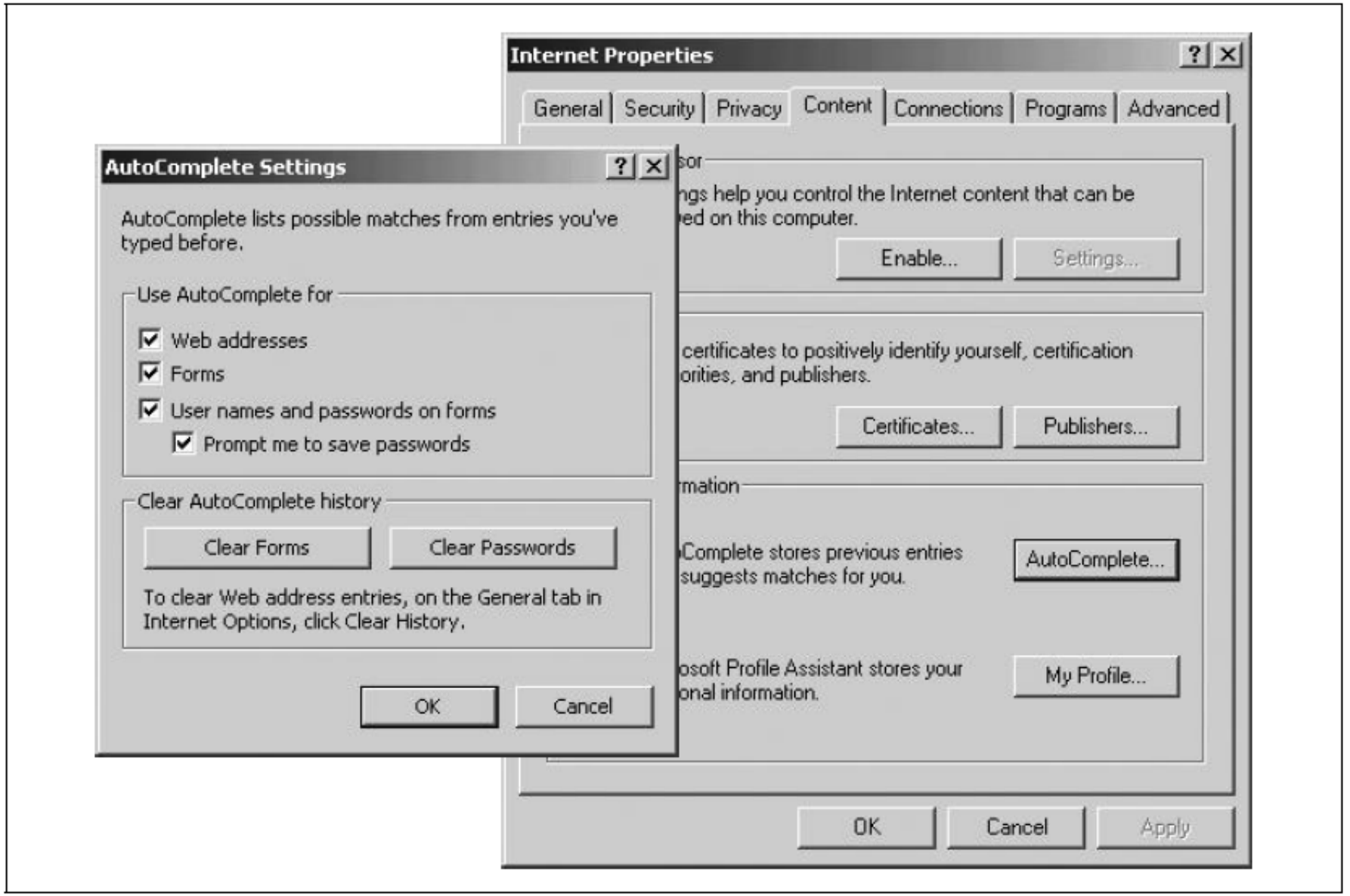


*Figure 9-11. Internet Explorer's AutoComplete Settings panel allows you to control where AutoComplete is used. You can also clear AutoComplete information for forms and/or passwords.*

# Passwords, Form-Filling, and AutoComplete Settings

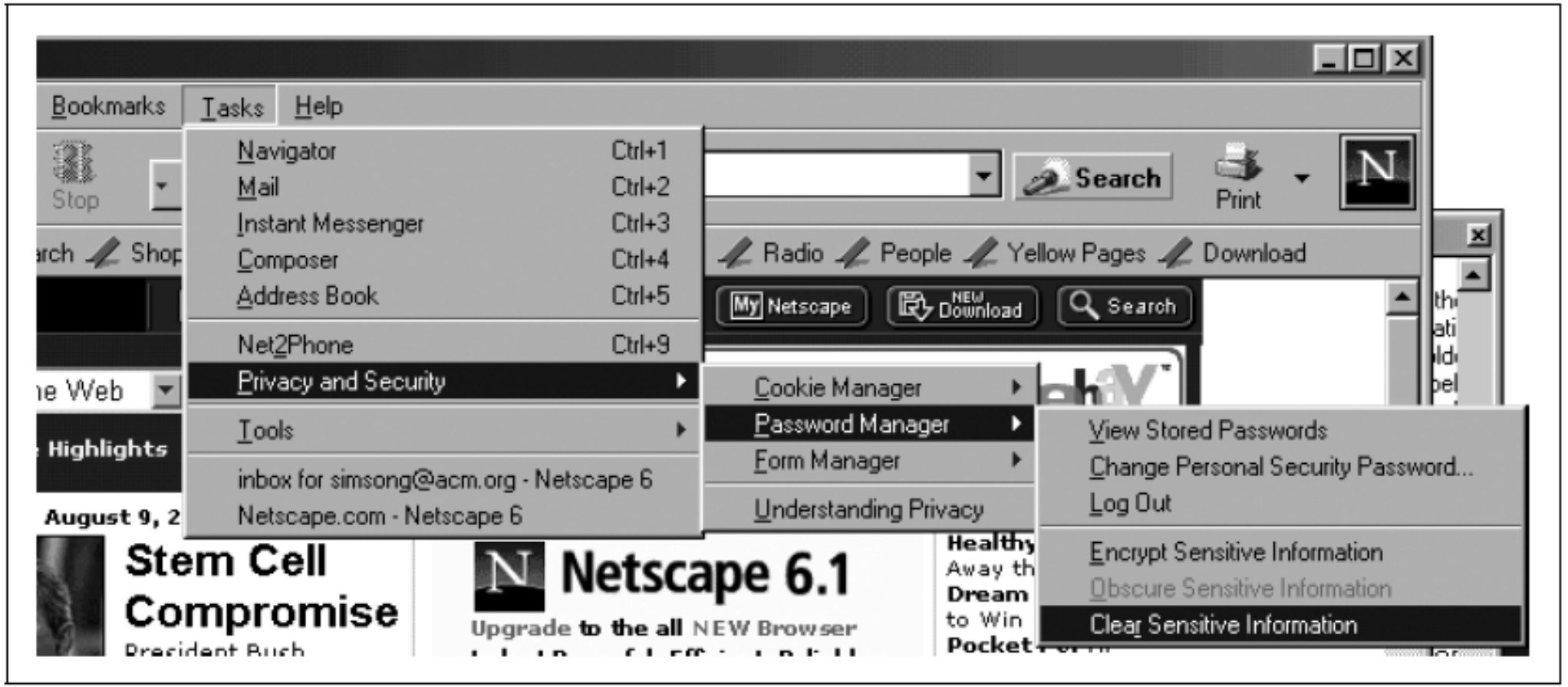


*Figure 9-12. Netscape's Password Manager has an option that allows you to clear sensitive information that is stored on your computer.*

# Avoiding Spam and Junk Email

- Spam is a major privacy concern.
- Causes:
  - Time loss
  - Privacy invasion
  - ISP customer loss

# Protect Your Email Address

- Avoid publishing email addresses.
- Remove listings from online directories.
- Avoid posting to:
  - Mailing lists
  - Usenet
- Choose uncommon usernames.

## Use Address Munging

- Modify email addresses to confuse spam bots.
- Prefer mangling domain names.

# Use an Antispam Service or Software

- **Antispam services:**
  - Filter messages externally
  - Use whitelists
- **Examples**:
  - BrightMail
  - SpamCop
- **Antispam software:**
  - Runs locally
  - Requires maintenance
- **Examples**:
  - SpammerSlammer
  - Spam Exterminator

# Identity Theft

- Identity theft involves misuse of personal data.
- Example: Stephen Shaw case
- Consequences:
  - Financial loss
  - Credit damage
  - Emotional distress
  - Employment difficulties
- Often takes years to resolve.
- Common methods:
  - Stolen credit reports
  - Trash rummaging
- Phishing scams

# Protecting Yourself From Identity Theft

- Identity theft thrives due to weak identity verification.
- Consumers can take preventive steps.

**Shred Your Trash**

- Use strip or cross-cut shredders.
- Shred documents with personal data.

**Monitor Your Credit Report**

- Regularly check reports from:
  - Equifax
  - Experian
  - TransUnion
- Consider monitoring services.

# Protecting Yourself From Identity Theft (cont..)

**Be Careful of Wallet Contents**

- Do not carry:
  - Social Security card
  - Birth certificate
- Photocopy cards for records.

**Cancel Unnecessary Credit Cards**

- Reduce exposure.

**Avoid Using SSNs as Account Numbers**

- Request alternate identifiers.

# Protecting Yourself From Identity Theft (cont..)

**Separate Online and Offline Credit Cards**

- Use virtual card numbers when possible.

**Don’t Give Personal Information to Callers**

- Verify identity of callers.

**Use Passwords on Accounts**

- Replace “mother’s maiden name” with passwords.

# If You Are the Victim of Identity Theft

- Report to:
  - Police
  - Secret Service
  - Postal Inspector
- Contact:
  - FTC Identity Theft Hotline
  - Banks and credit card companies
- Obtain and dispute all credit reports.
- Consider legal assistance.

# 3. Privacy-Protecting Technologies

- Technologies used to safeguard privacy while using the Web
- Commonly referred to as privacy-protecting technologies
- Focus on tools rather than a buyer's guide

**Scope of the Chapter**

- Introduces major program categories:
  - Blocking ads
  - Crushing cookies
  - Anonymous browsing
  - Secure email
- Examples of tools in each category
- Demonstration of selected programs
- Internet tools evolve rapidly → chapter is a survey, not a permanent guide

# Blocking Ads and Crushing Cookies

- Web browsers are increasingly designed to **deliver advertisements**.
- Major browser companies (Microsoft, Netscape, Opera) profit from advertising.
- Figure 10-1: Shows browsers functioning as ad-delivery platforms.
- Unlike traditional advertising:
  - Internet ads can track users
  - Personal data can be collected and correlated
- Advertisers can:
  - Track browsing behavior
  - Build detailed user profiles
- The Internet's design also allows users to:
  - Defend against cookies
  - Block advertisements

# Blocking Ads and Crushing Cookies


*Figure 10-1. On today's Internet, companies that develop web browsers have also created large web sites that are funded by advertising dollars. Browsers have become, in effect, programs for delivering advertisements to consumers.*

## Local HTTP Proxies

- Proxy servers relay requests between browsers and web servers.
- Commonly used in corporate firewalls.
- A local HTTP proxy:
  - Runs on the user's own computer
  - Proxies HTTP (web) traffic
- Figure 10-2: Shows a local HTTP proxy between the user and the Web.
- Because of its position, a local proxy can:
  - Monitor browsing activity
  - Preview web pages
  - Modify web content

# Local HTTP Proxies

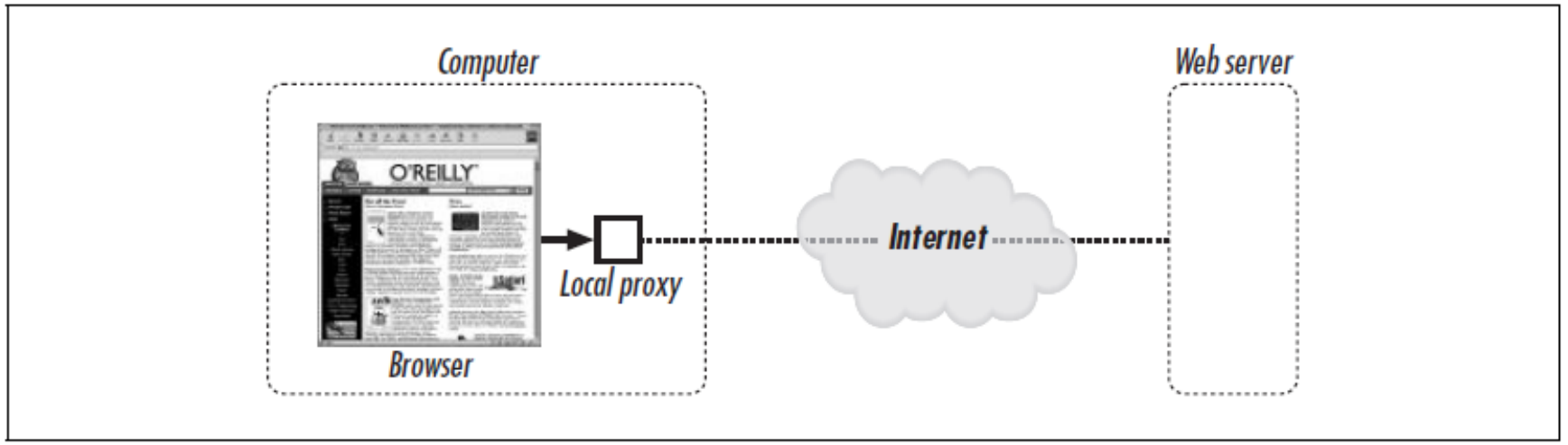


*Figure 10-2. A local HTTP proxy sits between the browser on your computer and the rest of the Internet. Because of its position, a local proxy can change the way that you view the Web.*

# Capabilities of a Local HTTP Proxy

- Record all visited web pages
- Block or allow access to specific sites
- Insert or remove cookies
- Edit HTML content
- Modify downloaded images
- If controlled by the user:
  - Becomes a powerful privacy tool
- If controlled by others:
  - Can be invasive and dangerous

## Using Ad Blockers

- Ad blockers often use local HTTP proxies.
- Two main ad-blocking methods:
  - Blocking ad-related URLs
  - Editing HTML to remove ads
- Figures 10-3, 10-4, 10-5: Demonstrate ad blocking and HTML modification.

**Reasons to Block Advertisements**

- Ads are distracting
- Ads waste screen space
- Ads slow down page loading
- Ads often contain tracking technologies (cookies)

# Using Ad Blockers

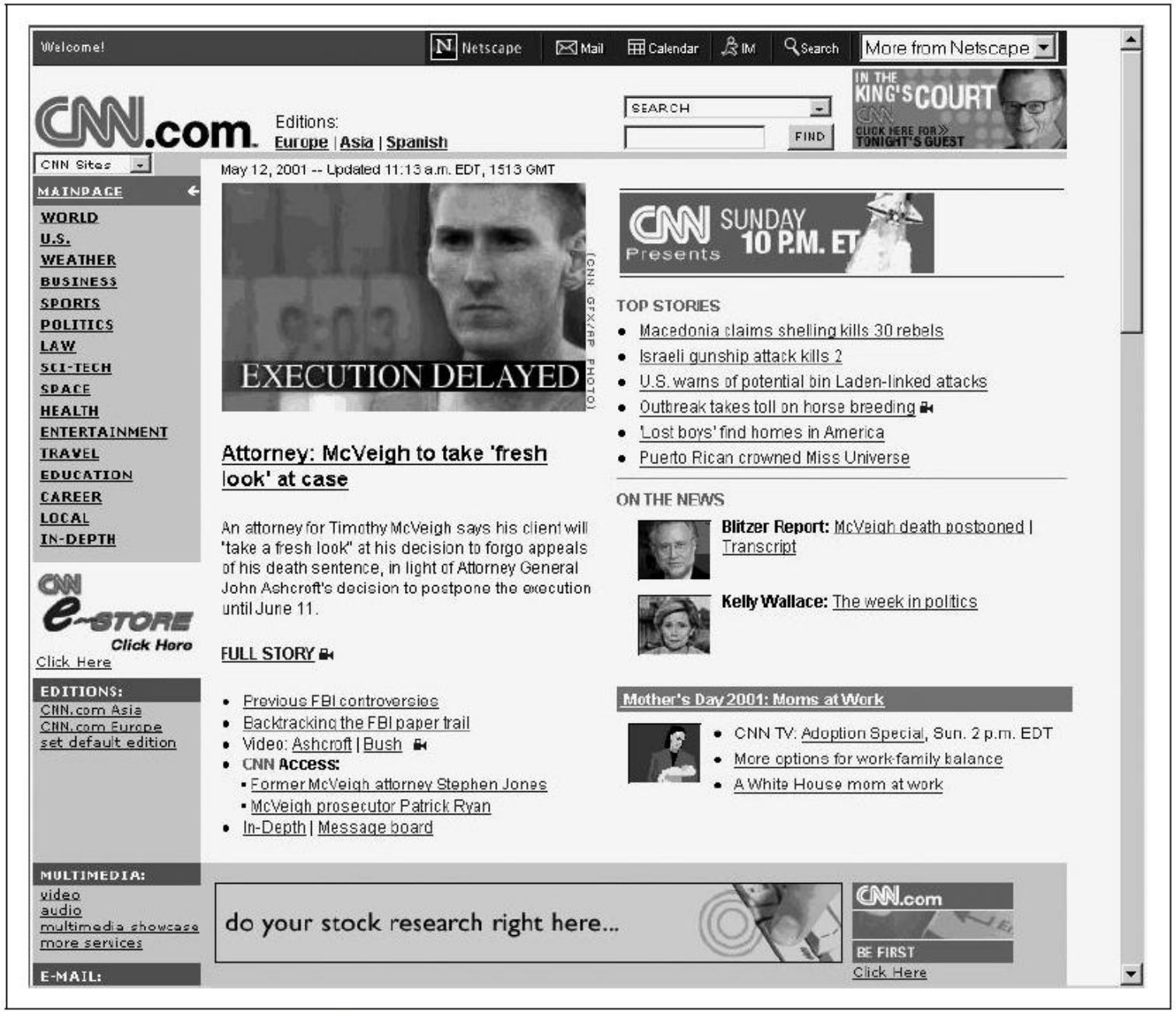


*Figure 10-3. The CCN.com home page on May 12, 2001. This page contains four advertisements.*

# Using Ad Blockers


*Figure 10-4. The CNN.com home page, as viewed through the Junkbuster HTTP proxy. Junkbuster recognizes the URLs of many advertisements and blocks them from being downloaded. The web browser displays these blocked images as boxes with an "X."*

# Using Ad Blockers


*Figure 10-5. The CNN.com home page, as viewed through the AdSubtract HTTP proxy. AdSubtract edits the HTML as it travels from the web site to the browser and automatically removes the tags that cause some advertisements to be displayed. Notice how the page is automatically reformatted so that more content appears on the screen.*

**Disadvantages of Blocking Ads**

- Some ads contain useful information
- Many websites rely on ad revenue
- Blocking ads may harm free content availability

# Crushing Cookies

- Many ad blockers also crush cookies.
- Selective cookie blocking allows:
  - Blocking cookies from advertisers
  - Allowing cookies from trusted sites (banks, brokers)
- This balances privacy and functionality.

# Additional Features of Ad Blockers

- Remove background music and images
- Disable JavaScript, Java, and ActiveX
- Stop animated GIFs
- Block pop-ups
- Prevent browser history manipulation
- Disable auto-refresh pages
- Block refer links
- Ad blockers can block **dozens of ads** after only a few pages.
- Table 10-1: Lists available ad-blocking programs.
- Most ad blockers:
  - Run on Windows
  - Some can protect entire local networks

# Additional Features of Ad Blockers

*Table 10-1. A survey of ad blocking programs*

| Program | Features | Comments |
|---|---|---|
| AdSubtract[a]<br>*http://www.adsubtract.com* | Ad blocking<br>Cookie management<br>Sophisticated filtering | Windows only. Several different versions (some free) with different features available. |
| Internet Junkbuster Proxy<br>*http://www.junkbuster.com* | Ad blocking<br>Cookie management | Free. Windows and a variety of Unix systems. |
| Freedom Internet Privacy Suite<br>*http://www.freedom.net* | Ad blocking<br>Cookie management<br>Form-filling<br>Many other privacy features | Free. Windows and Linux. Optional subscription service provides for anonymous web browsing and email. |
| Norton Internet Security<br>*http://www.symantec.com/sabu/nis/nis_pe/* | Ad blocking<br>Cookie management<br>Personal firewall<br>Many other security features | Windows only. |
| WebWasher<br>*http://www.webwasher.com* | Ad blocking<br>Cookie management<br>Sophisticated filtering | Windows only. |

[a] Simson Garfinkel is on the advisory board of AdSubtract's publisher, InterMute.

# Anonymous Browsing

- HTTP proxies cannot hide IP addresses.
- IP addresses:
  - Contain personal information
  - Allow tracking across websites
- IPs can be used to identify users via logs and legal orders.

**Examples of IP Address Tracking**

- **MIT Media Lab hostname:**
  - Linked directly to a single user
- **Media One cable modem hostname:**
  - Linked via ISP records
- **WebTV proxy server:**
  - Shared among many users
  - Logs still exist
- **Dial-up server hostnames:**
  - Reassigned over time
  - Usage records retained

## IP Addresses in Email

- Web-based email often includes IP addresses in headers
- Example shown using Hotmail headers
- IP leakage may reveal location and identity

# Simple Approaches to Protecting Your IP Address

**Browse from a Public Terminal**

- Public libraries and universities offer anonymity
- Institutions are often committed to user privacy

**Use America Online**

- AOL uses caching proxy servers
- User IP is hidden behind proxy names
- Example proxy hostnames listed
- Privacy depends on AOL policies and legal pressure

**Use Your ISP's Web Cache or Proxy Server**

- ISP proxies mask end-user IPs
- Remote servers see the proxy IP instead of the user's

# Anonymous Web Browsing Services

- Provide stronger anonymity than simple methods
- Operate as proxy services
- Figure 10-6: Shows anonymous proxy architecture
- Key feature:
  - No log files kept
- Cannot comply with court orders for user activity

# Anonymous Web Browsing Services

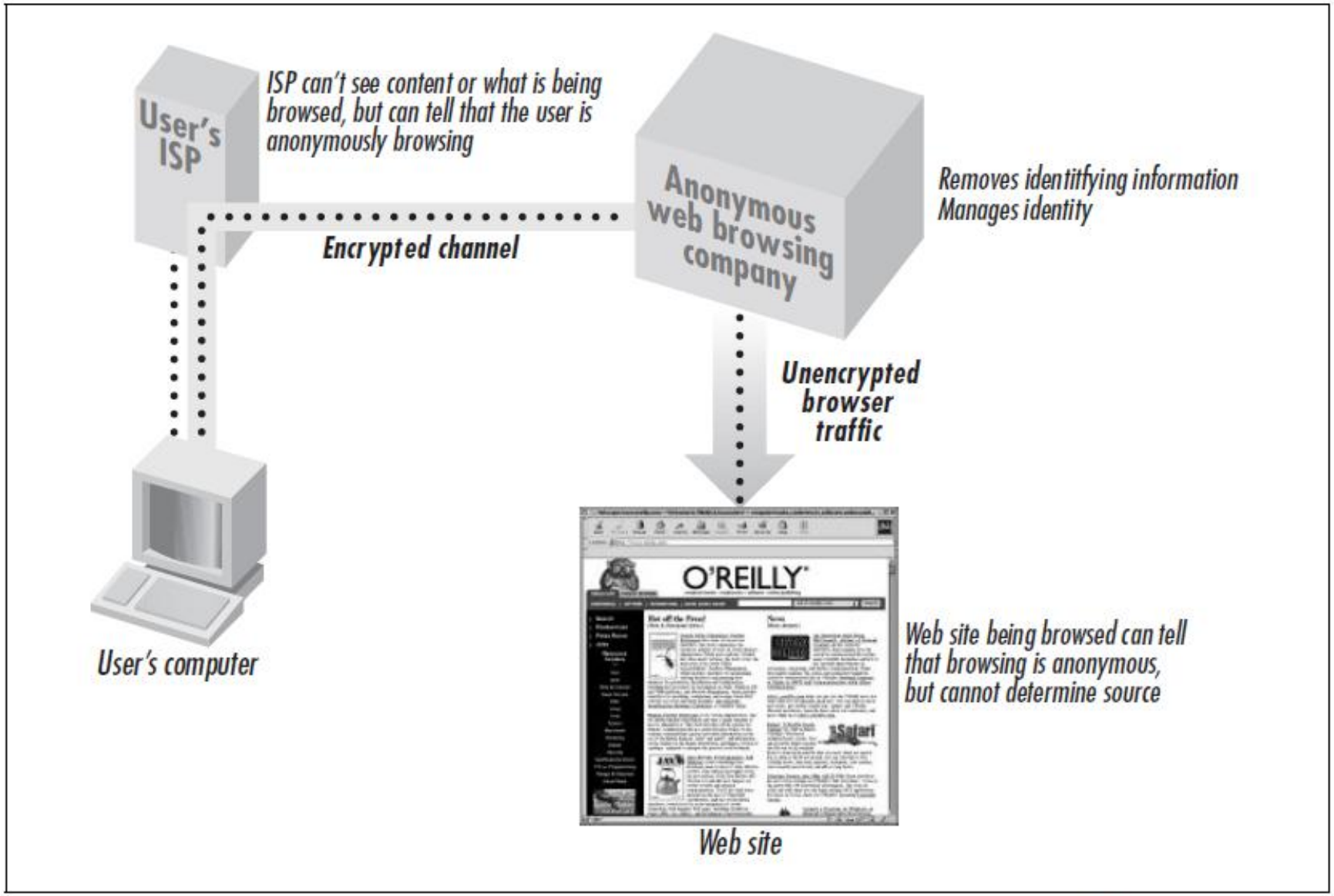


*Figure 10-6. An anonymous web browsing service acts like a proxy server or a cache, except that no records are kept by the operator*

# Anonymizer.com

- One of the first anonymous browsing services
- Requires:
  - No software installation
  - No browser reconfiguration
- Users enter URLs on the Anonymizer website
- URLs are rewritten to maintain anonymity
- Example HTML rewriting shown
- Figure 10-7: Web page viewed through Anonymizer
- Offers:
  - Free ad-supported service
  - Paid service (~$5/month in 2001)
  - Secure encrypted tunnel option

# Anonymizer.com

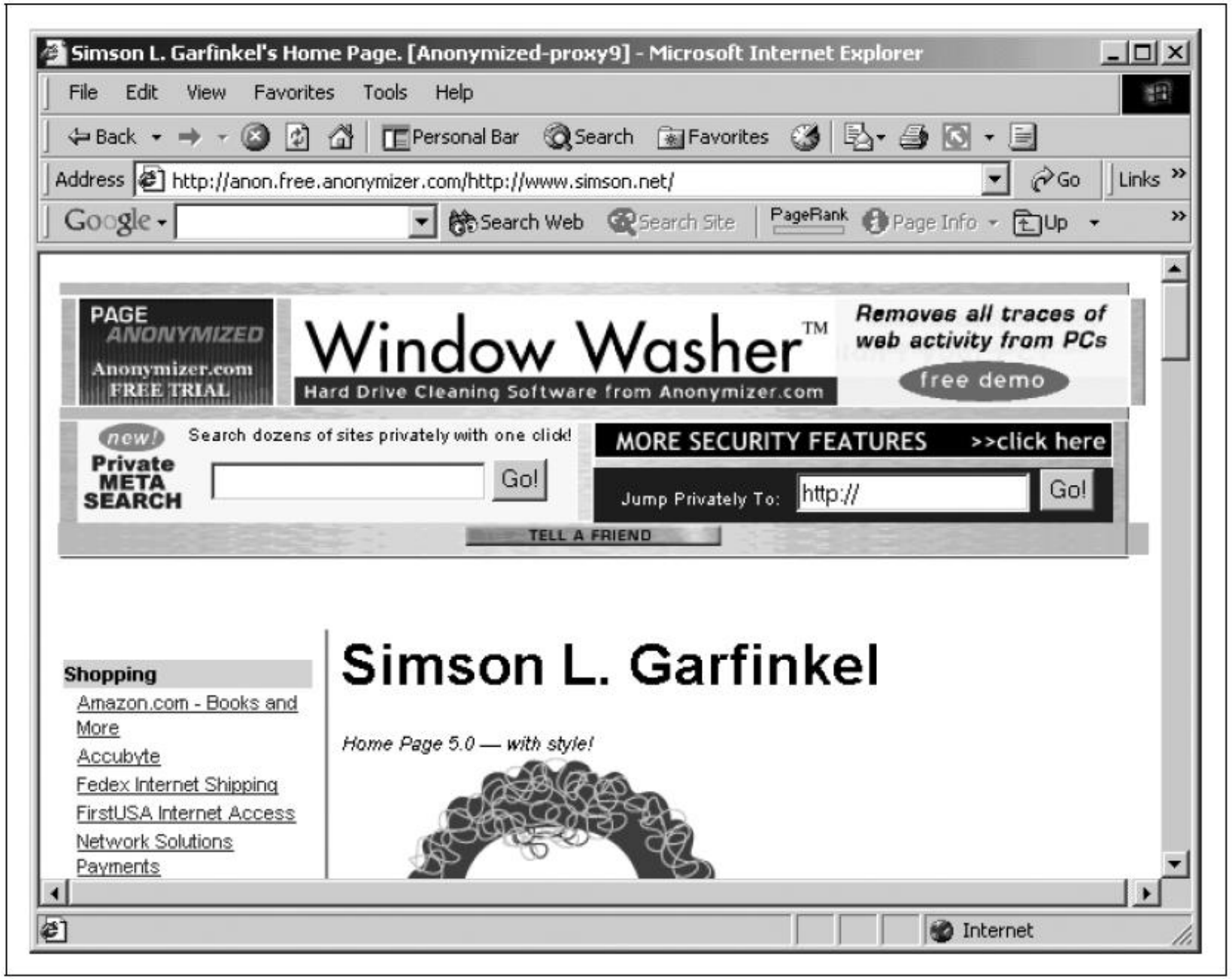


*Figure 10-7. The Anonymizer web privacy service uses URL rewriting to provide anonymous web browsing*

## Freedom, by Zero Knowledge Systems

- Uses **multiple proxy servers** across countries
- Figure 10-8: Shows multi-hop encrypted routing
- Each packet:
  - Encrypted in multiple layers
  - Decrypted step-by-step by different servers
- Offers:
  - Anonymous browsing
  - Anonymous chat
  - Untraceable encrypted email
- Supports multiple identities (**nyms**)
- Each nym can:
  - Use separate cookies
  - Block cookies
- Cost: $49.95/year (includes 5 nyms)

# Freedom, by Zero Knowledge Systems

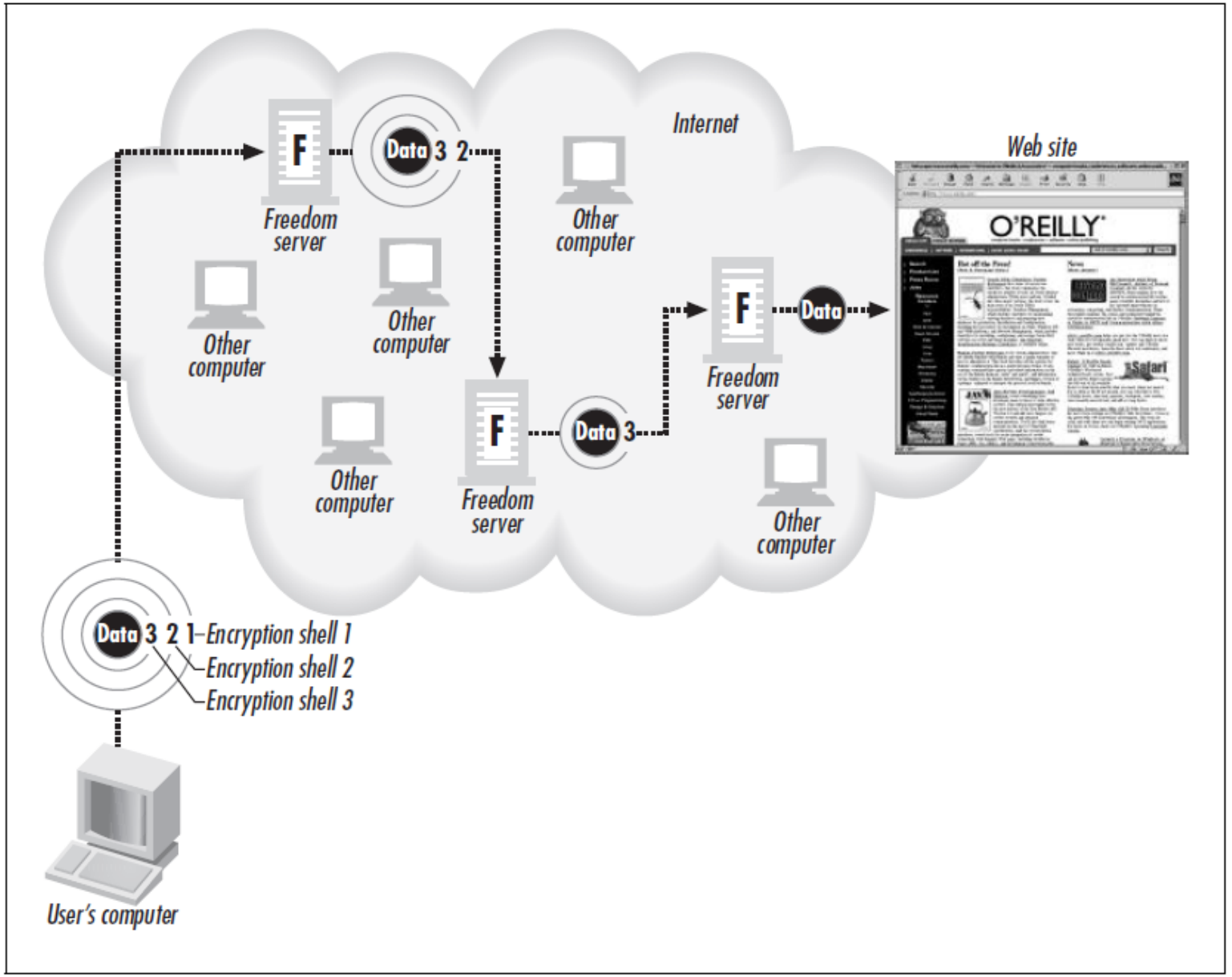


*Figure 10-8. Each packet of data sent through the Freedom Network is encrypted with three distinct layers of encryption*

## safeWeb

- Similar to Anonymizer
- Key features:
  - Free service
  - SSL encryption
  - Customization options
- Supported by non-tracking ads
- Figure 10-9: safeWeb interface

# safeWeb

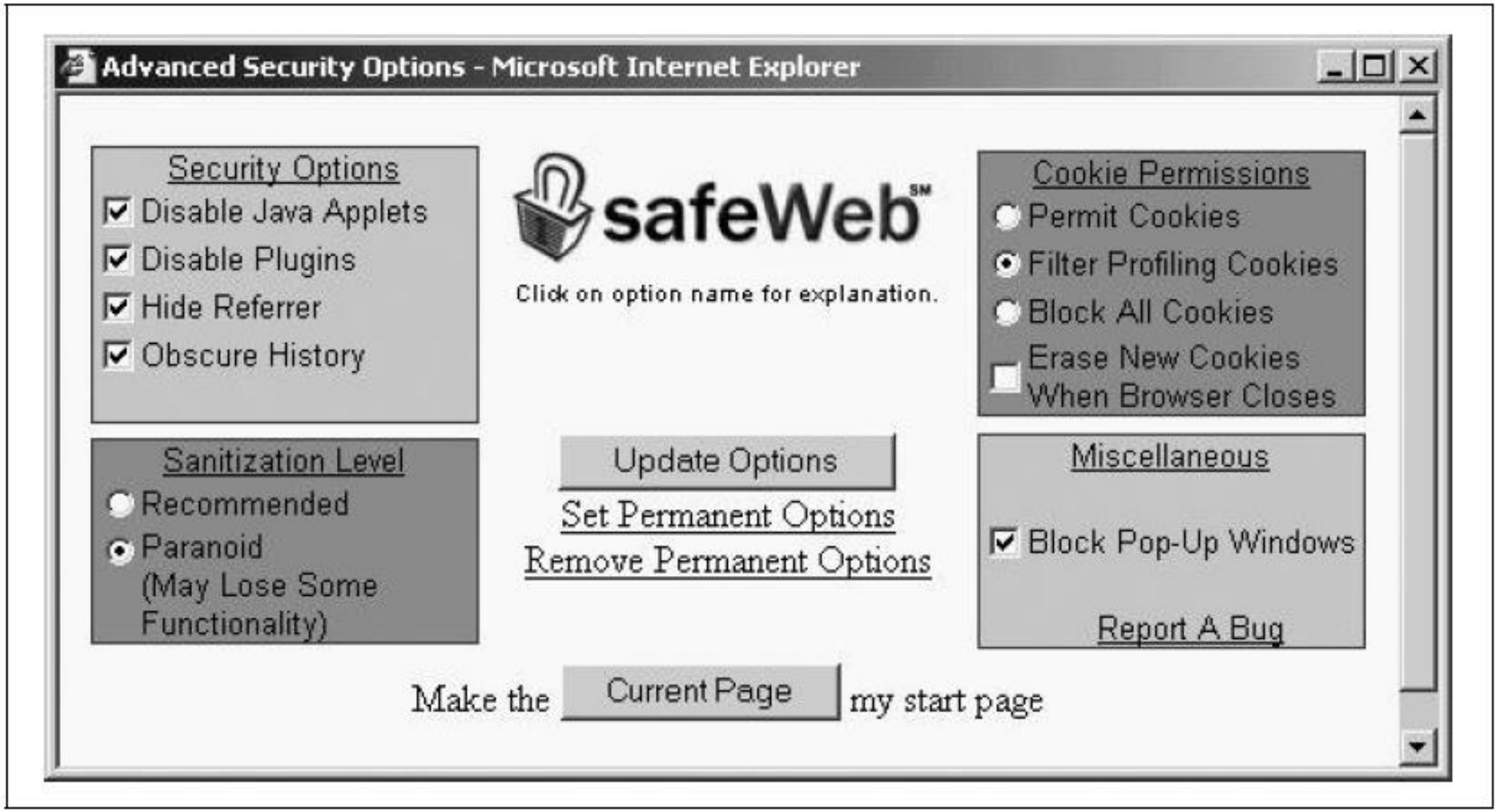


*Figure 10-9. safeWeb's customization panel allows you to control how much information about your computer is revealed when you browse "anonymously"*

## Secure Email

- Email often carries highly sensitive information
- Standard email lacks security
- Threats include:
  - Identity leakage
  - ISP or employer monitoring
  - Misdelivery
  - Unauthorized access
  - Forwarding without consent
  - Message tampering
- These are real, experienced risks
- Can be mitigated using proper technologies

# Hotmail, Yahoo Mail, and Other Web-Based Email Services

- Provide:
  - Free or low-cost email
  - Access from anywhere
- Useful for:
  - Semi-permanent addresses
  - Anonymous use with anonymous browsing
- Risks include:
  - Provider access to all emails
  - No end-to-end encryption
  - Exposure to subpoenas
  - Interception without SSL
  - Advertisements added to messages
- Useful for disposable or single-purpose email accounts

# Hushmail

- Secure web-based email service
- Figure 10-10: Hushmail interface
- Encrypts messages so:
  - Even Hushmail staff cannot read them
- Encryption occurs on the user's computer
- Figure 10-11: Client-side encryption process
- Uses public-key cryptography
- Private key protected by user passphrase
- If passphrase is forgotten:
  - Account is unrecoverable
- Messages:
  - Automatically encrypted and decrypted
  - Not stored unencrypted on servers or disks
- Offers:
  - Free ad-supported version
  - Premium paid version

# Hushmail

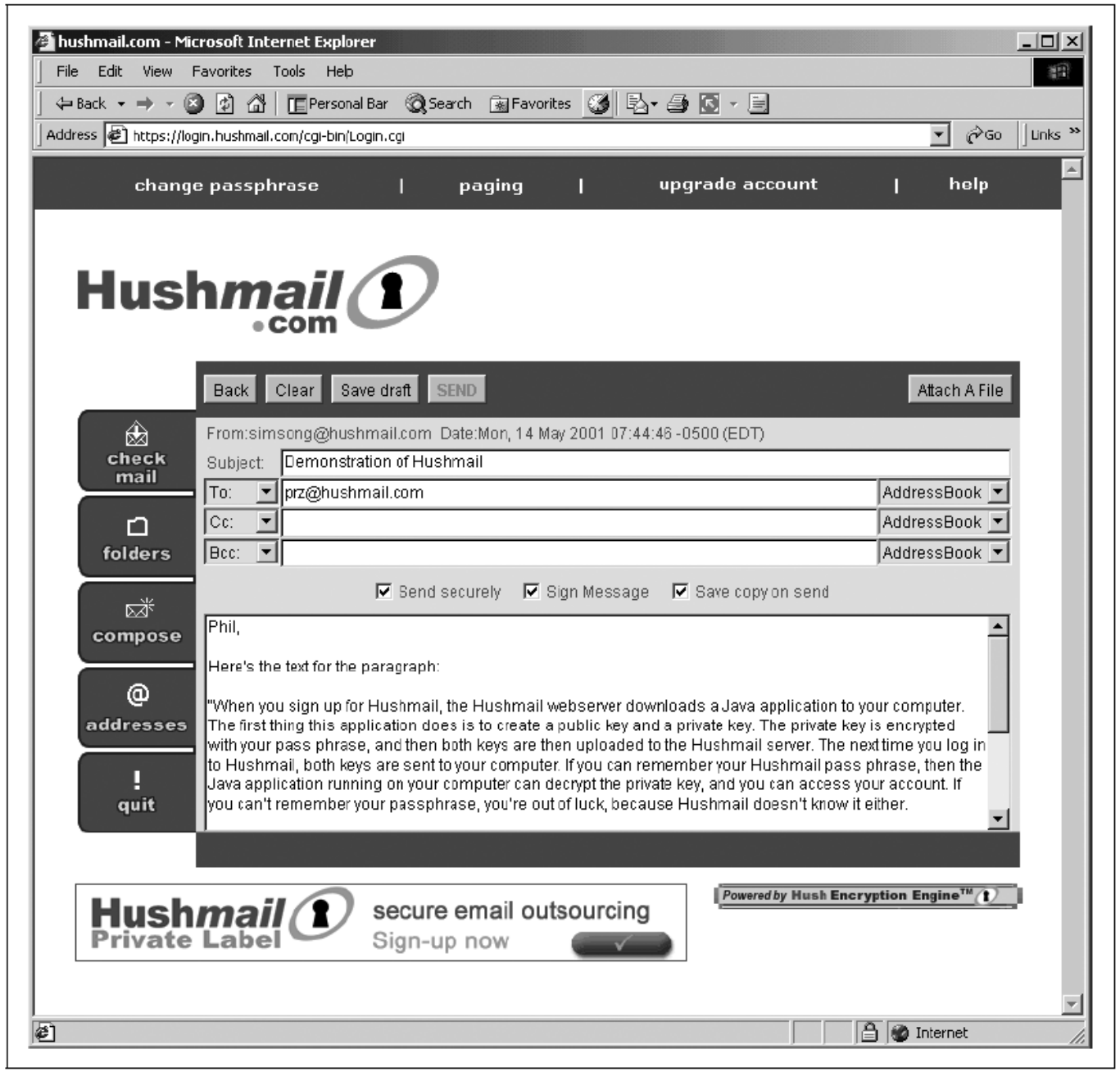


*Figure 10-10. Hushmail looks like other web-based mail systems, but it is much more secure because all messages are encrypted and decrypted on the end user machines, rather than the server*

# Hushmail

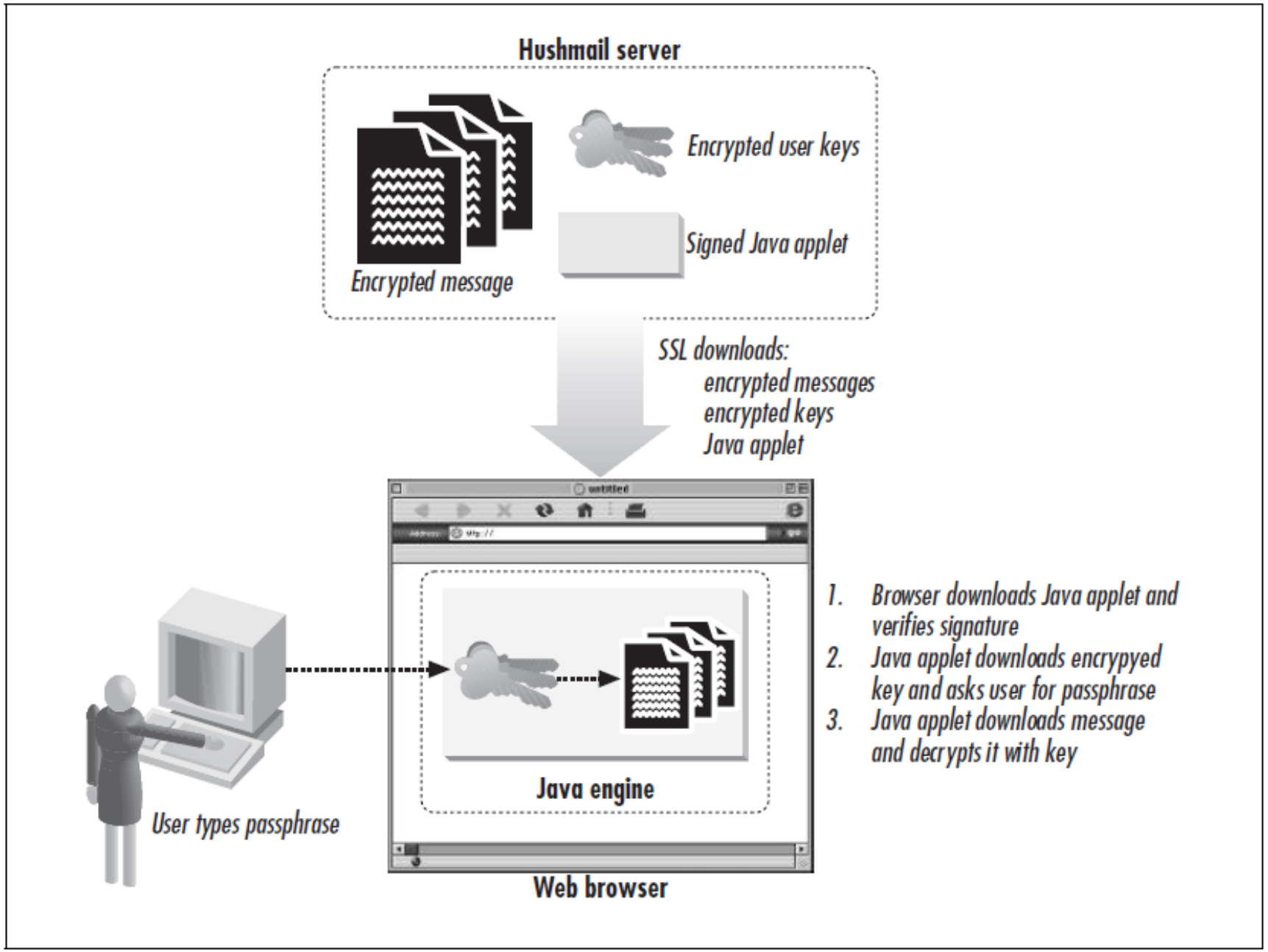


*Figure 10-11. Encryption in the Hushmail system happens inside a browser on the end user's computer*

# Omniva's Self-Destructing Email

- Email copies exist in many locations
- Figure 10-12: Shows multiple email copies
- Email archives are valuable in:
  - Investigations
  - Litigation
- Omniva uses time-limited cryptographic access
- Sender chooses message expiration date
- Figure 10-13: Encryption and key distribution
- Encrypted messages are unreadable without keys
- Figure 10-14 & 10-15: Key-based access and expiration
- After expiration:
  - Key is deleted
  - Message becomes unreadable
- Does not prevent:
  - Printing
  - Manual copying
- Improves privacy and reduces long-term exposure

# Omniva's Self-Destructing Email (cont..)

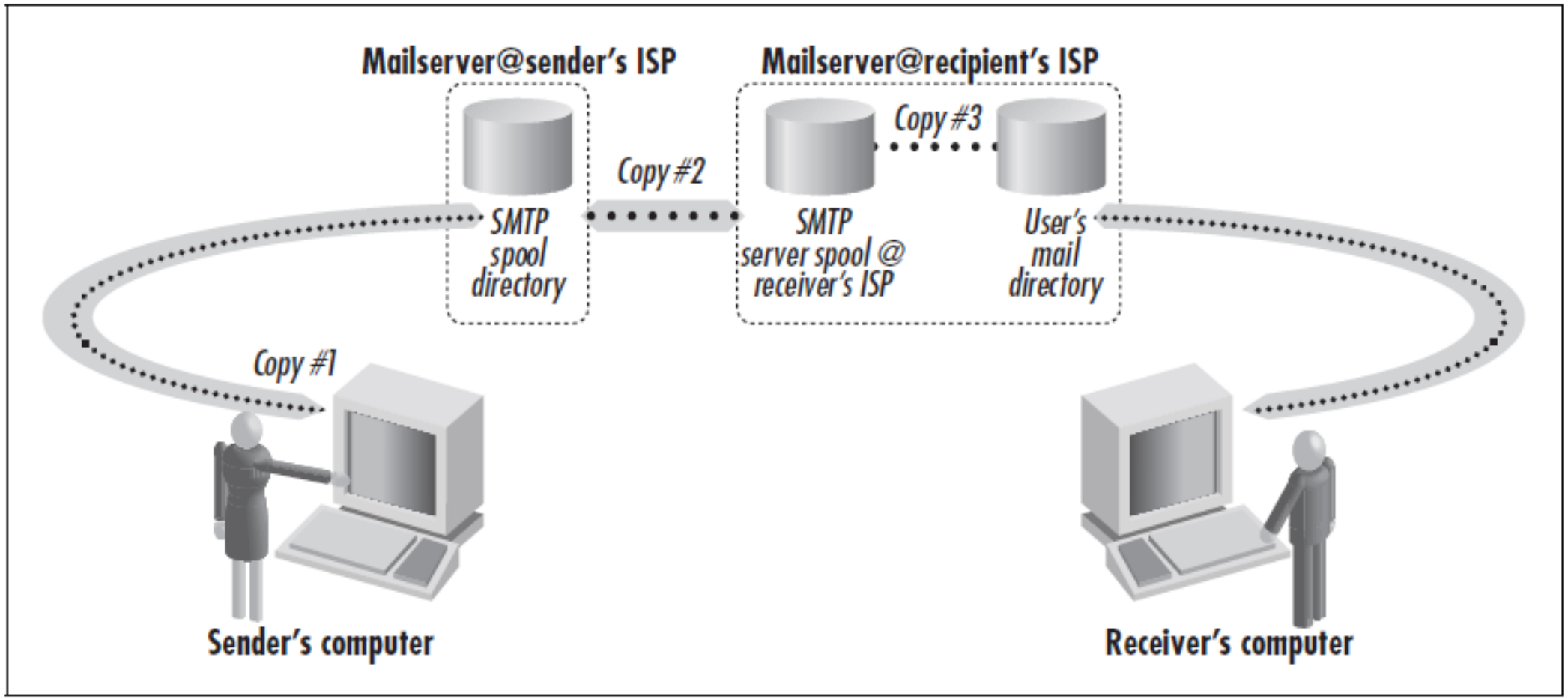


*Figure 10-12. The typical email message is copied at least four times—and sometimes many more*

# Omniva's Self-Destructing Email (cont..)

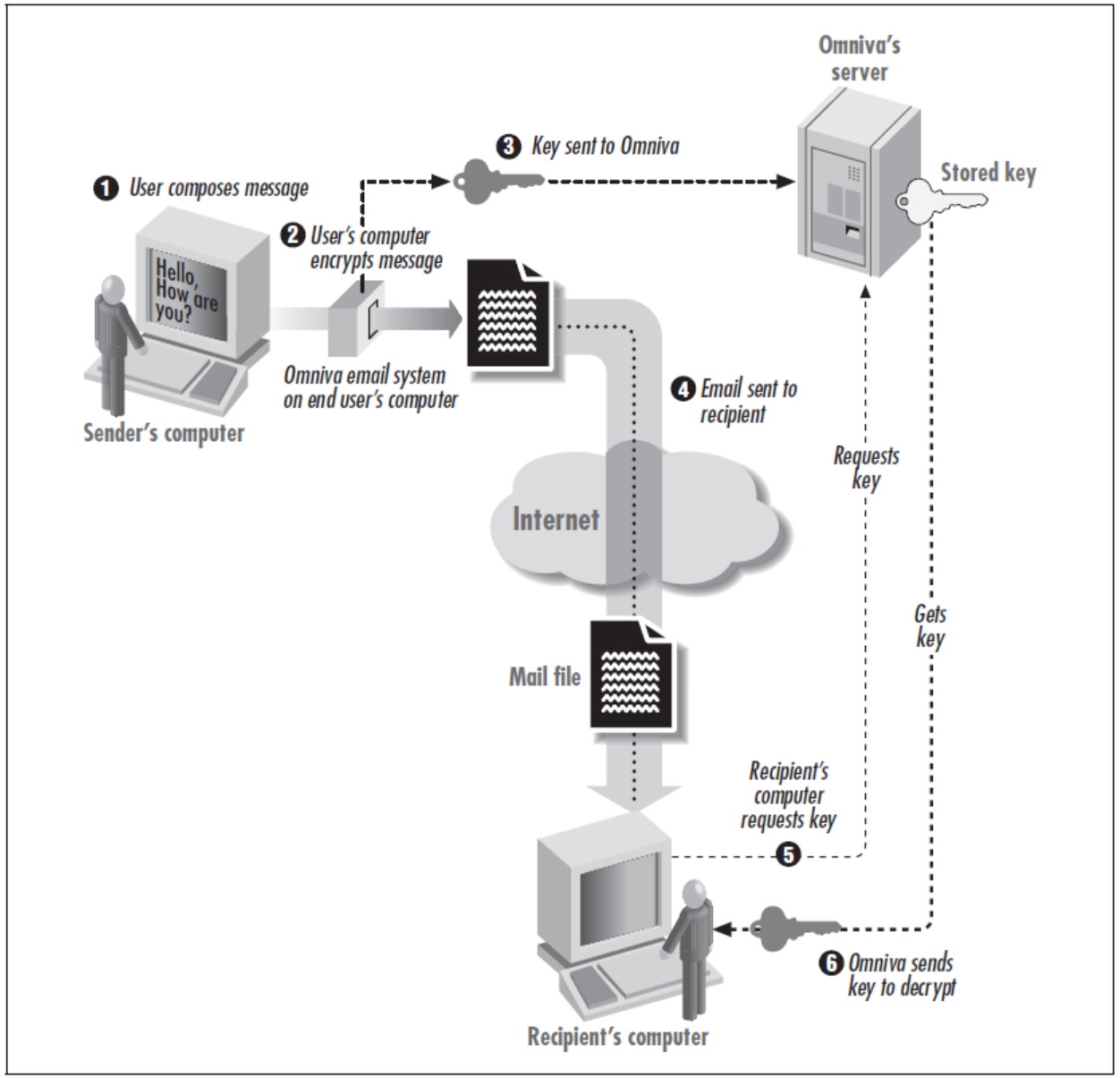


*Figure 10-13. The Omniva email system relies on encryption and a central key server to assure that email messages will be unintelligible after their expiration date.*

# Omniva's Self-Destructing Email (cont..)

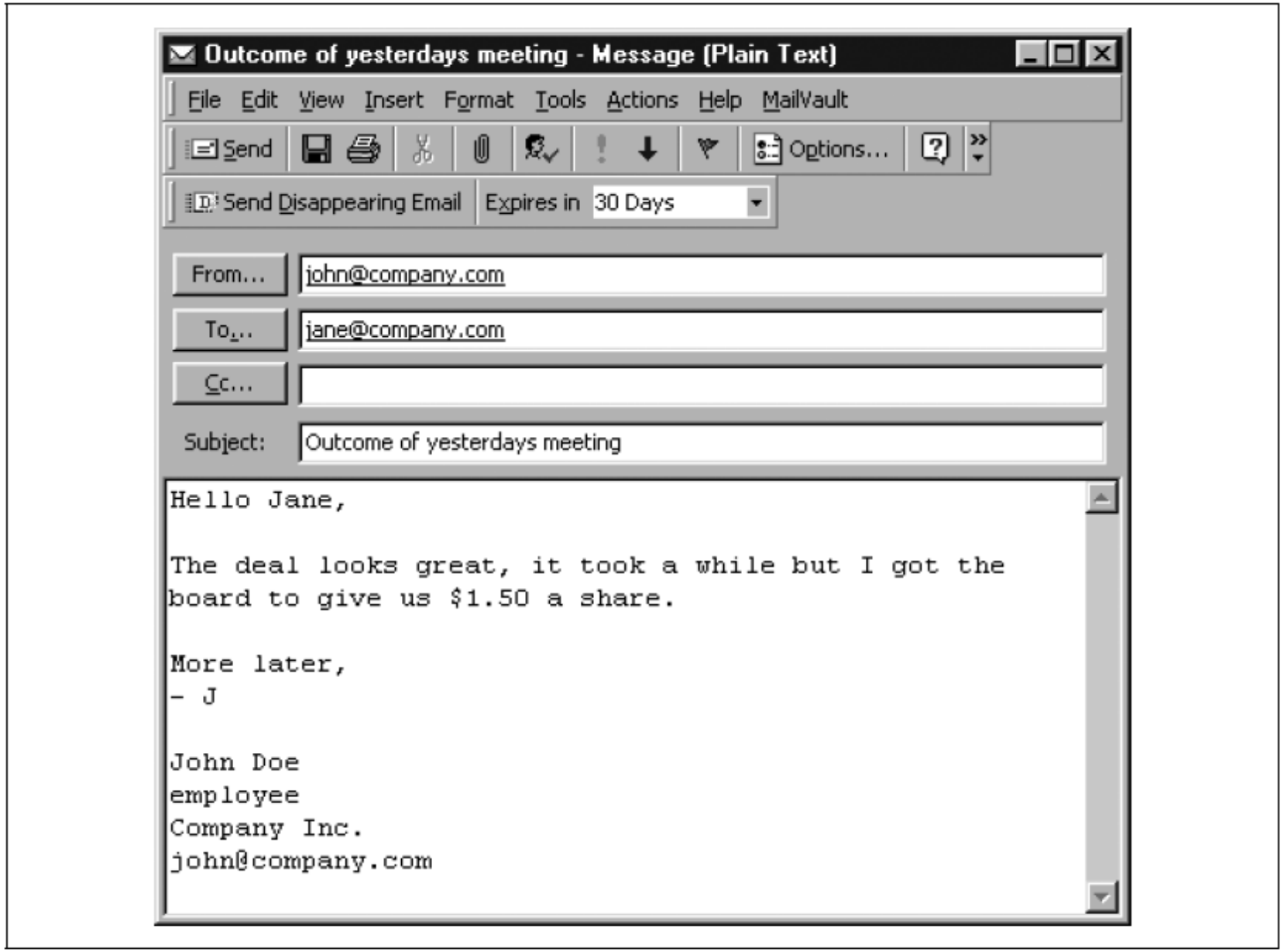


*Figure 10-14. A message composed with the Omniva system message is given an expiration date*

# Omniva's Self-Destructing Email (cont..)

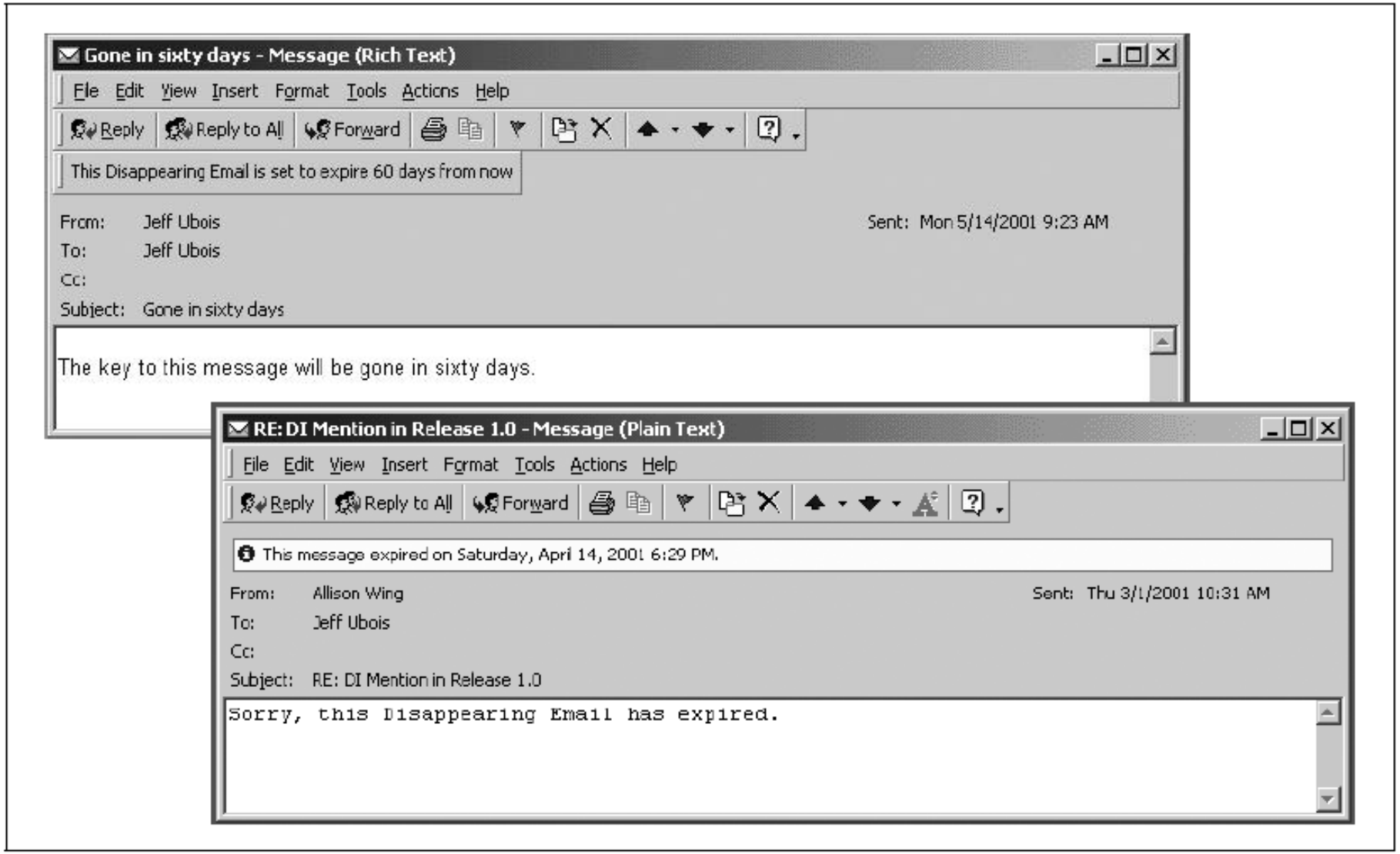


*Figure 10-15. Viewing a message on Omniva Email depends on whether the message has expired. This example shows a message that hasn't expired (left) and another message that has (right).*

# 4. Backups and Antitheft

- Focuses on:
  - Data loss
  - Theft
  - System recovery
- Threats include:
  - Hardware failure
  - Theft
  - Disasters
  - Human error

# Using Backups to Protect Your Data

- Backups are copies of important data
- Can be:
  - Simple (Zip disk)
  - Complex (tape + restore floppy)
- Allow system restoration after loss

# Make Backups!

- Failures are unpredictable
- Backups prevent permanent data loss
- Insurance replaces hardware, not data
- Essential for recovery after disasters

# Why Make Backups?

**Reasons**

- Archival records
- User error
- System-staff error
- Hardware failure
- Software corruption
- Electronic break-ins
- Theft
- Natural and human-made disasters

# What Should You Back Up?

- Two strategies:
  1. Back up only unique data
  2. Back up everything
- Recommended: Back up everything
- Simplifies restoration
- Protects against missing installation media

# Types of Backups

**Level-Zero Backup**

- Initial full system backup

**Full Backup**

- Copies all files regularly

**Incremental Backup**

- Copies only changed files
- Common strategy:
  - Full backup biweekly
  - Incremental backup nightly
- Figure 11-1: Rotating backup tapes

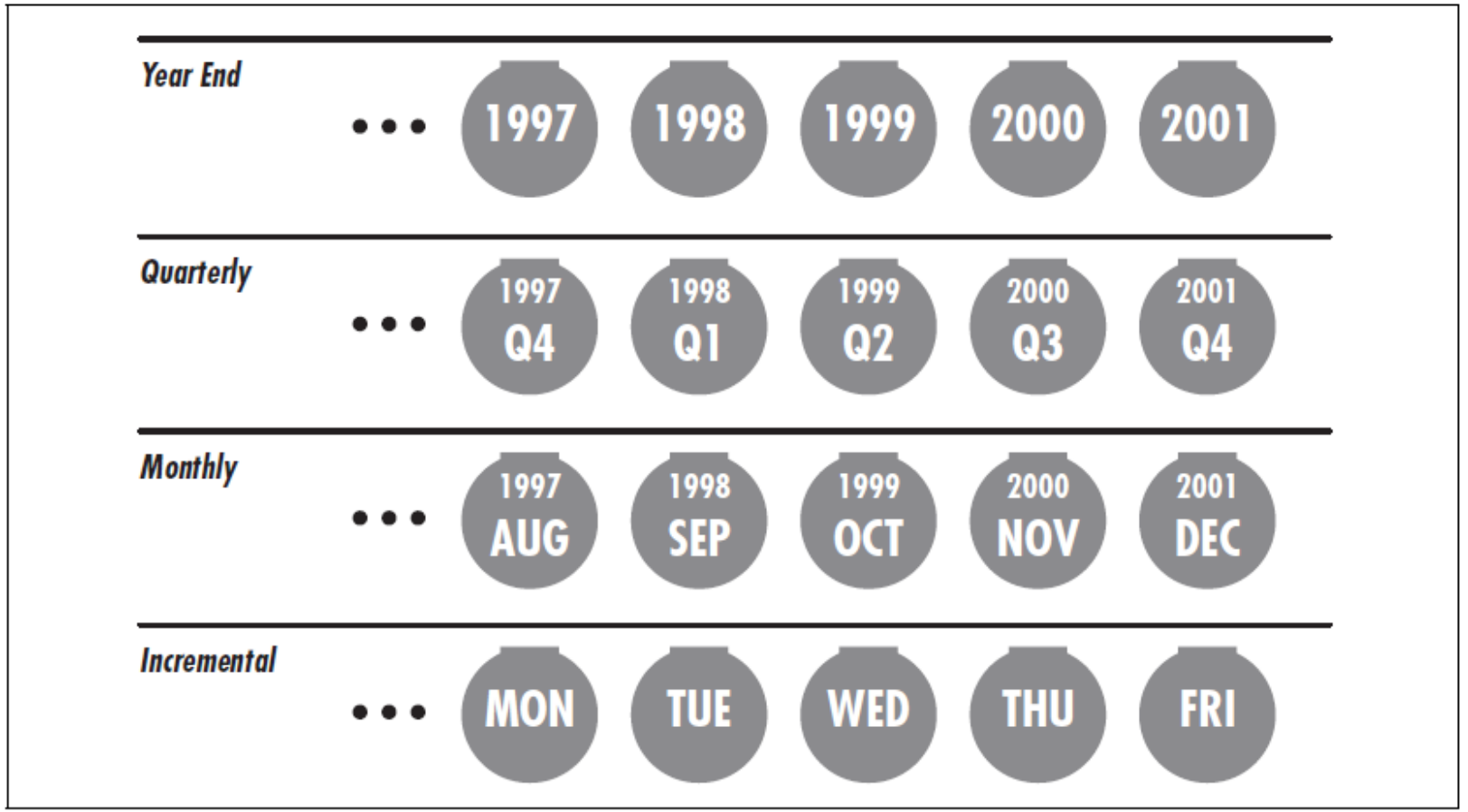


*Figure 11-1. An incremental backup*

# Guarding Against Media Failure

- Use tandem backup sets (A and B)
- Protects against tape failure
- Periodically test restores
- Annual full restoration recommended

# Security for Backups

**Physical Security**

- Remove media from drives
- Store backups off-site
- Use media-safe fireproof storage

**Data Security**

- Backups contain all data
- Encrypt backups
- Secure encryption keys
- Use escrow or shared key systems

# Legal Issues

- Backup tapes may be subpoenaed
- Retention policies should apply to backups
- Segregate sensitive data
- Back up carefully

# Preventing Theft

- Theft often occurs due to opportunity
- Prevention reduces risk significantly

# Locks

- Laptops include security slots
- Figure 11-2: Laptop lock slot
- Cable locks prevent grab-and-run theft
- Vendors: Kensington, Kryptonite

*Figure 11-2. Most laptops today are sold with a security slot (reprinted with permission of Kensington)*

# Tagging

- Equipment tags deter resale
- Figure 11-3: STOP theft tag
- Tags:
  - Are serial-numbered
  - Leave permanent marks if removed
- Used by governments and universities


*Figure 11-3. The Security Tracking of Office Property (STOP) tag is a simple and effective way to label your laptop (reprinted with permission)*

# Laptop Recovery Software and Services

- Tracing software reports location
- Example: Computrace
- Cost-effective
- Works unless disk is reformatted

# Awareness

- Simple habits reduce theft:
  - Never leave laptops unattended
  - Secure laptops in hotels
  - Carry laptops personally
  - Avoid window-side placement