

Towards Usable Web Privacy and Security



Lorrie Faith Cranor

November 2005

<http://lorrie.cranor.org/>

CMU Usable Privacy and Security Laboratory

Carnegie Mellon

Unusable security & privacy

- Unpatched Windows machines compromised in minutes
- Phishing web sites increasing by 28% each month
- Most PCs infected with spyware (avg. = 25)
- Users have more passwords than they can remember and practice poor password security
- Enterprises store confidential information on laptops and mobile devices that are frequently lost or stolen

Grand Challenge

“Give end-users security controls they can understand and privacy they can control for the dynamic, pervasive computing environments of the future.”

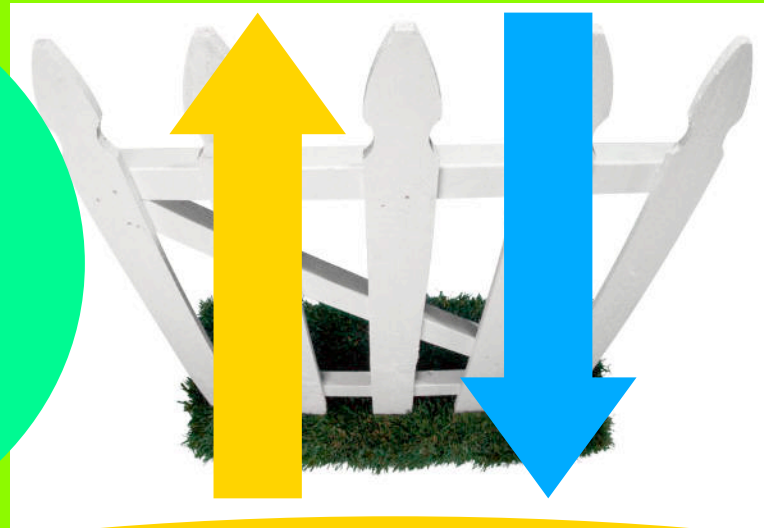
- Computing Research Association 2003

security controls they can understand
privacy they can control

Just work

**security/privacy researchers
and system developers**

**Web
standards
authors and
user agent
developers**



**human computer interaction researchers
and usability professionals**

Mark your calendar
for SOUPS 2006 -
July 14-16 at CMU



Symposium On Usable Privacy and Security (SOUPS)

July 6-8, 2005

Pittsburgh, PA USA

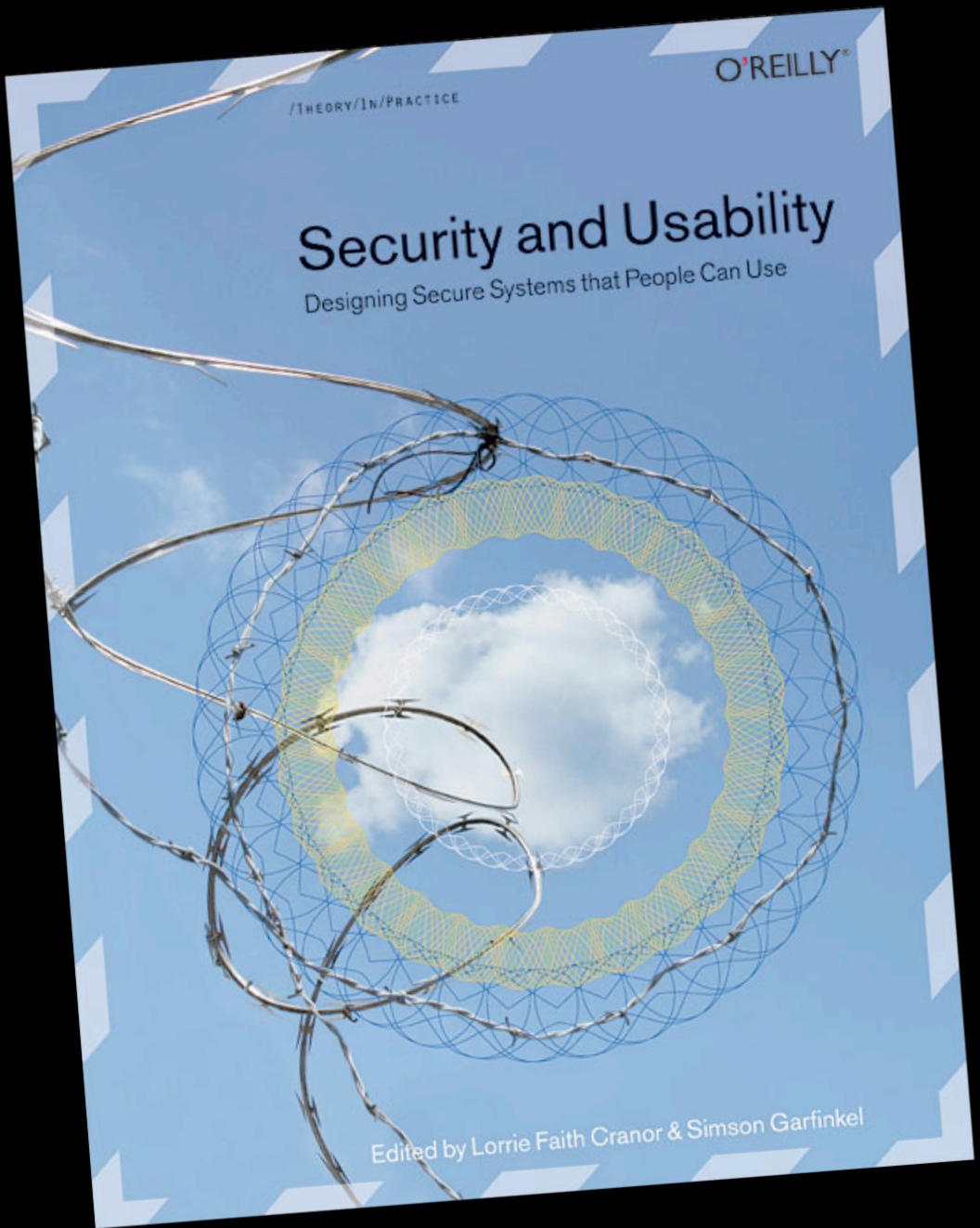
<http://cups.cs.cmu.edu/soups/>

/THEORY/IN/PRACTICE

O'REILLY®

Security and Usability

Designing Secure Systems that People Can Use



Edited by Lorrie Faith Cranor & Simson Garfinkel

Agenda

1. Problems and approaches
2. Passwords
3. Symbols & metaphors
4. Rethinking cookies
5. Making Web privacy visible

Problems and approaches



1.

How do you stay safe
online?

Advice

US-CERT Cyber Security Tip ST04-003 -- Good Security Habits

http://www.us-cert.gov/cas/tips/ST04-003.html

Home | FAQ | Contact

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Search US-CERT

> Advanced Search

National Cyber Alert System

Cyber Security Tip ST04-003

GetNetWise | You're one click away

http://www.getnetwise.org/

Home

Online Safety | Privacy | Online Security | Spam | Search | Glossary | Questions | Join Us

GetNetWise about ...

- Spotlight on Spyware**
If your computer has become increasingly annoying pop-up ads, you may have downloaded spyware. Find ways to prevent, locate or uninstall spyware on your computer.
- Keeping Children Safe Online**
Learn about the risks kids face online. Search or browse for Internet safety products, browse great sites families can visit together, and learn how to identify online trouble and get law enforcement contact information.
- Stopping Unwanted E-mail and Spam**
Learn how to prevent unwanted email from flooding your inbox and how to report the spammers.
- Protecting Your Computer From Hackers and Viruses**
Learn about the risks that hackers and viruses pose to your computer files and software. Take steps to prevent viruses from infecting your software and to keep hackers from compromising your computer.
- Keeping Your Personal Info Private**
Learn about tools and techniques to better control how much personal information you share with online stores, Web sites, e-mailers and other people who may use your computer.

Kids' Safety | Spam | Security

Go to "http://privacy.getnetwise.org/"

... adopt that, if performed
... chances that the information
... have to your information?
... and, legitimately or not, gain physical
... mates, co-workers, members of a cleaning
... who could gain remote access to your
... as you have a computer and connect it to a
... something else accessing or corrupting your
... that make it more difficult.
... away from it. Even if you only step away from
... enough time for someone else to destroy or

TOP TEN CYBER SECURITY TIPS FOR TEENS, THEIR TEACHERS AND FAMILIES

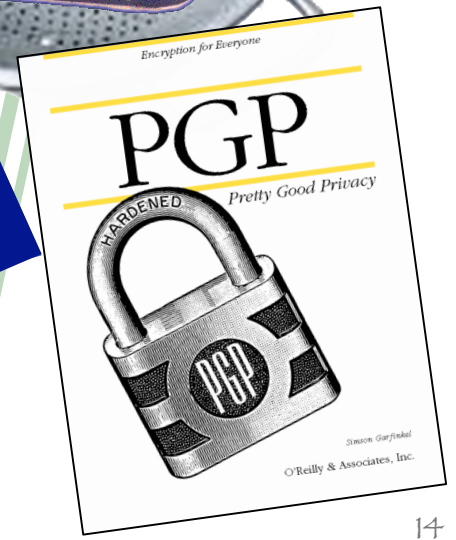
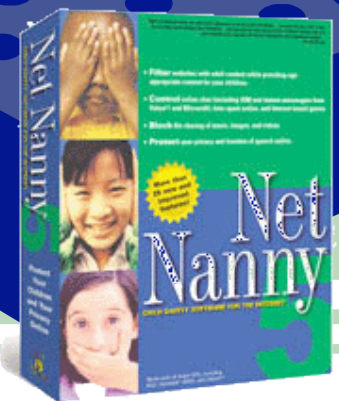
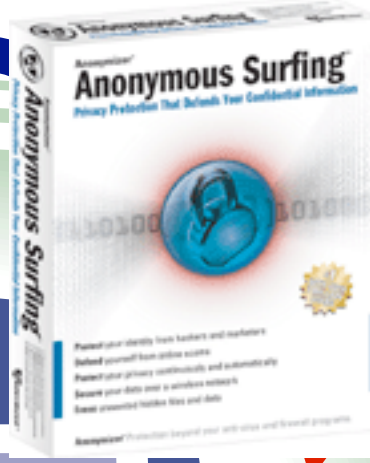
- Be a responsible cyber citizen.**
If you use the Internet, you're a citizen of a global community—a cyber citizen. Just like being a citizen of your local community, being a cyber citizen has responsibilities. Use the Internet to share knowledge that makes people's lives better. Keep safe, use good manners and respect the laws.
- Use anti-virus software.**
A computer virus is a program that can invade your computer and damage or destroy information. Anti-virus software is designed to protect you and your computer against known viruses. But with new viruses emerging daily, anti-virus programs need to be updated regularly. Check with the web site of your anti-virus software company to see some sample descriptions of viruses and to get regular updates for your software. Stop viruses in their tracks!
- Do not open email from unknown sources.**
Delete email from unknown sources. Watch out for files attached to e-mails, particularly those with an "exe" extension—even if people you know sent them to you. Some files transport and distribute viruses and other programs that can permanently destroy files and damage computers and Web sites. Do not forward e-mail if you are not completely sure that any attached files are safe.
- Use hard-to-guess passwords and keep them private.**
Do not write passwords down on small pieces of paper taped to your computer. You would be surprised how many people are sloppy about keeping their passwords private. Passwords that are easy to guess are a bad choice. In other words, if your name is "Dan," do not make your password "Dan." Change your passwords regularly and don't give your passwords to anyone! Tell your family that combinations of letters, numbers and symbols are harder to crack than just words.
- Protect computers with firewalls.**
Install firewalls for your family—it is not difficult. A firewall helps prevent hackers from breaking into your computer or the computers that belong to your family. Firewalls help prevent thieves from stealing and using private information including your phone number and credit card numbers, which may be stored on a family computer.
- Do not share access to your computers with strangers. Learn about file sharing risks.**
Your computer operating system may allow other computers on a network, including the Internet, to access the hard-drive of your computer in order to "share files." This ability to share files can be used to infect your computer with a virus or look at the files on your computer if you do not pay close attention. Check your operating system and other program help files to learn how to disable file sharing. Do not share access to your computer with strangers!
- Disconnect from the Internet when not in use.**
The Internet is a two-way road. You get information and also send information. Turning off the Internet makes sure that someone else on the Internet can't enter your computer and cause harm. Disconnecting your computer from the Internet when you are not online lessens the chance that someone will be able to access your computer.
- Back-up your computer regularly.**
If your family back up all household computers onto external media such as CD's or diskettes.
- Regularly download security protection update "patches".**
Many files are regularly found in operating systems and application software. Companies that make software release these files called "patches" that you should install to correct the latest software flaw. It is a good idea to check for security updates on the publisher's Web site for all the software you own.
- Tip your family to check computer security on a regular basis.**
Check your computer security at least twice a year. To help remember, do it when you change the clocks for daylight-savings time. Check for all of the items listed previously.

For more information on cyber security, visit www.getnetwise.org for free curriculum consultants with McGraw-Hill Education that teaches the skills necessary for safe, responsible and effective computer and Internet use.

10 Tips: Online Dating Safety

OnlineDatingService.net

Experts recommend...



After installing all that
security and privacy
software

Do you have any time left to
get any work done?

Secondary tasks

Approaches to usable security

- Make it “just work”
 - Invisible security
- Make security/privacy understandable
 - Make it visible
 - Make it intuitive
 - Use metaphors that users can relate to
- Train the user



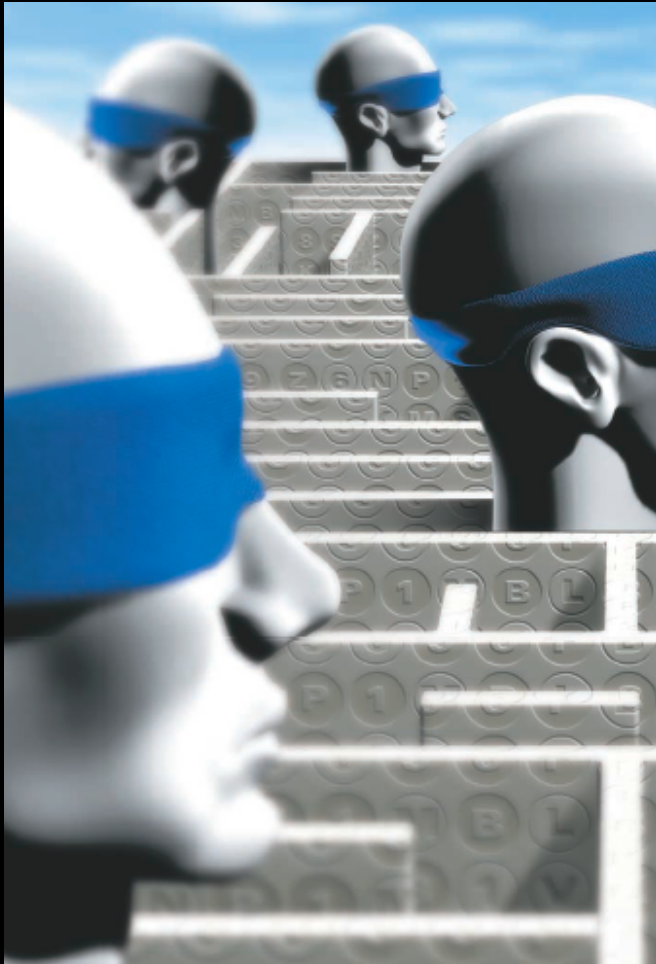
DO NOT
PICK
UP
VIRUSES

Firefox security assumptions

1. Users want to believe that their products are keeping them secure.
2. Users do not want to be responsible for, nor concern themselves with, their own security.
3. We know more about security than our users do.

- Blake Ross 

Make decisions



- Developers should not expect users to make decisions they themselves can't make

Present choices, not dilemmas

- Chris Nodder
(in charge of user
experience for XP SP2)

Internet Security



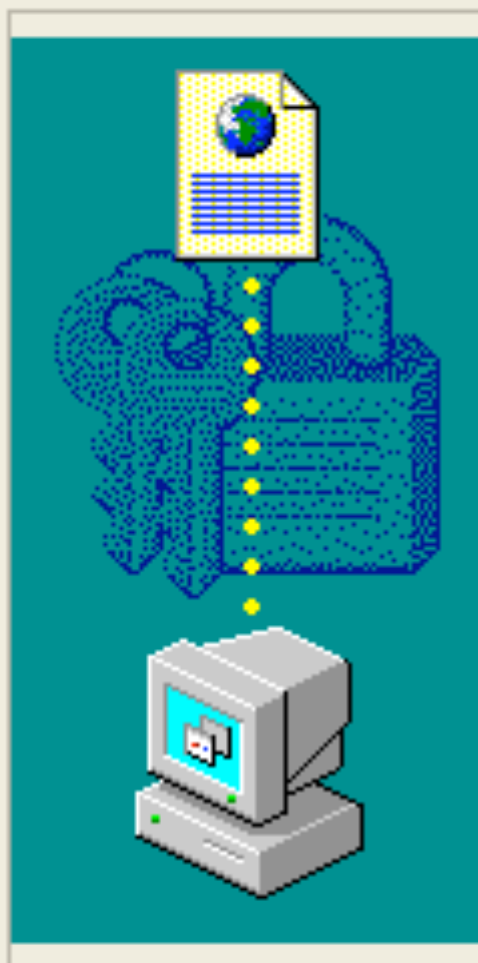
A script from "http://zesty.ca" has requested UniversalXPConnect privileges. You should grant these privileges only if you are comfortable downloading and executing a program from this source. Do you wish to allow these privileges?

Remember this decision

Yes

No

Security Warning



Do you want to install and run "[MSN Chat Control 9.2.310.2401](#)" signed on 10/27/2003 2:12 PM and distributed by:

[Microsoft Corporation MSN](#)

Publisher authenticity verified by Microsoft Code Signing PCA

Caution: Microsoft Corporation MSN asserts that this content is safe. You should only install/view this content if you trust Microsoft Corporation MSN to make that assertion.

[Always trust content from Microsoft Corporation MSN](#)

[Yes](#)

[No](#)

[More Info](#)

Internet Explorer - Security Warning



Do you want to install this software?



Name: [MSN Chat Control 9.2.310.2401](#)

Publisher: [Microsoft Corporation MSN](#)

- Always install software from "Microsoft Corporation MSN"
- Never install software from "Microsoft Corporation MSN"
- Ask me every time



Fewer options

Install

Don't Install



While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. [What's the risk?](#)

Passwords



2.

Typical advice

- Pick a hard to guess password
- Don't use it anywhere else
- Change it often
- Don't write it down

What do users do when every
web site wants a password?

Bank = b3aYZ
Amazon = aa66x!
Phonebill = p\$2\$ta1



Password keeper software

- Run on PC or handheld
- Only remember one password

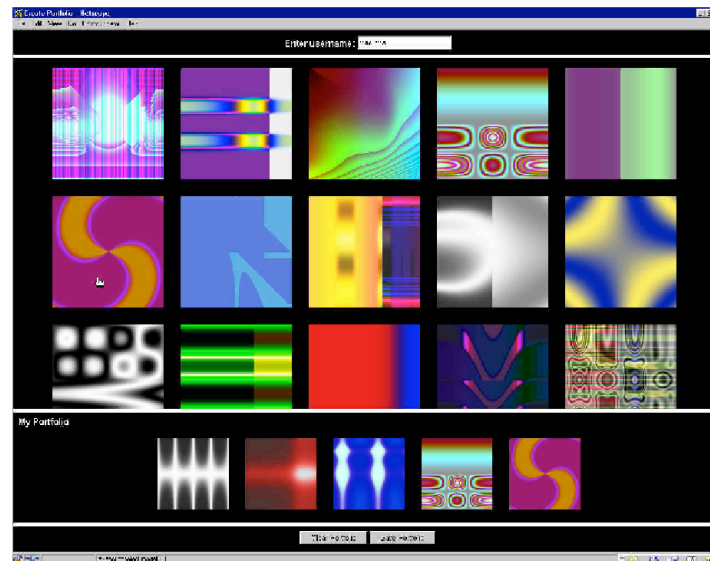
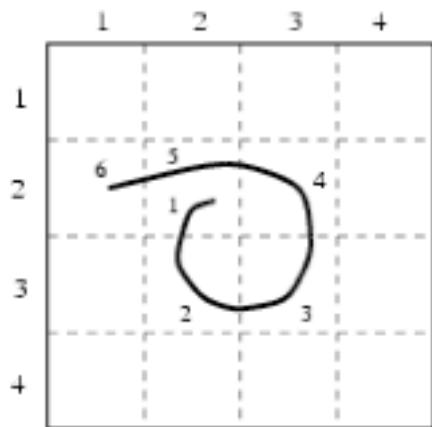
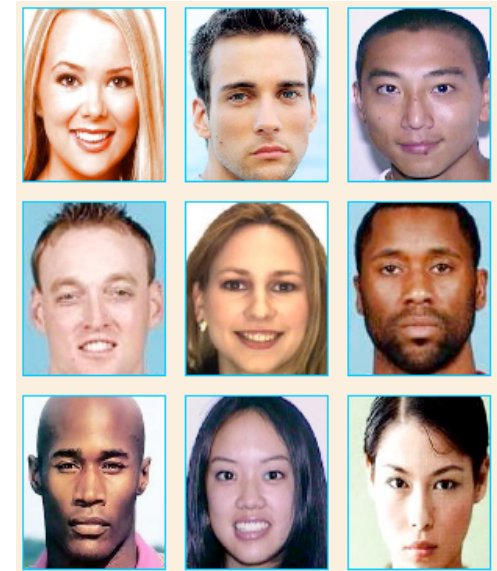
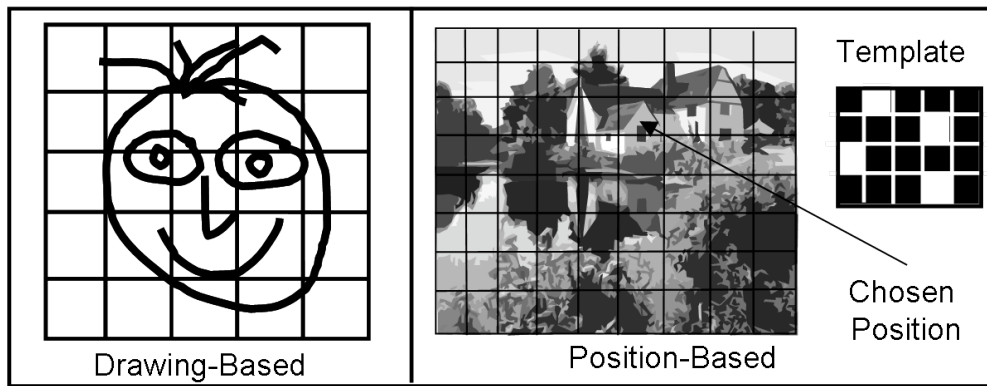
Single sign-on

- Login once to get access to all your passwords

Biometrics

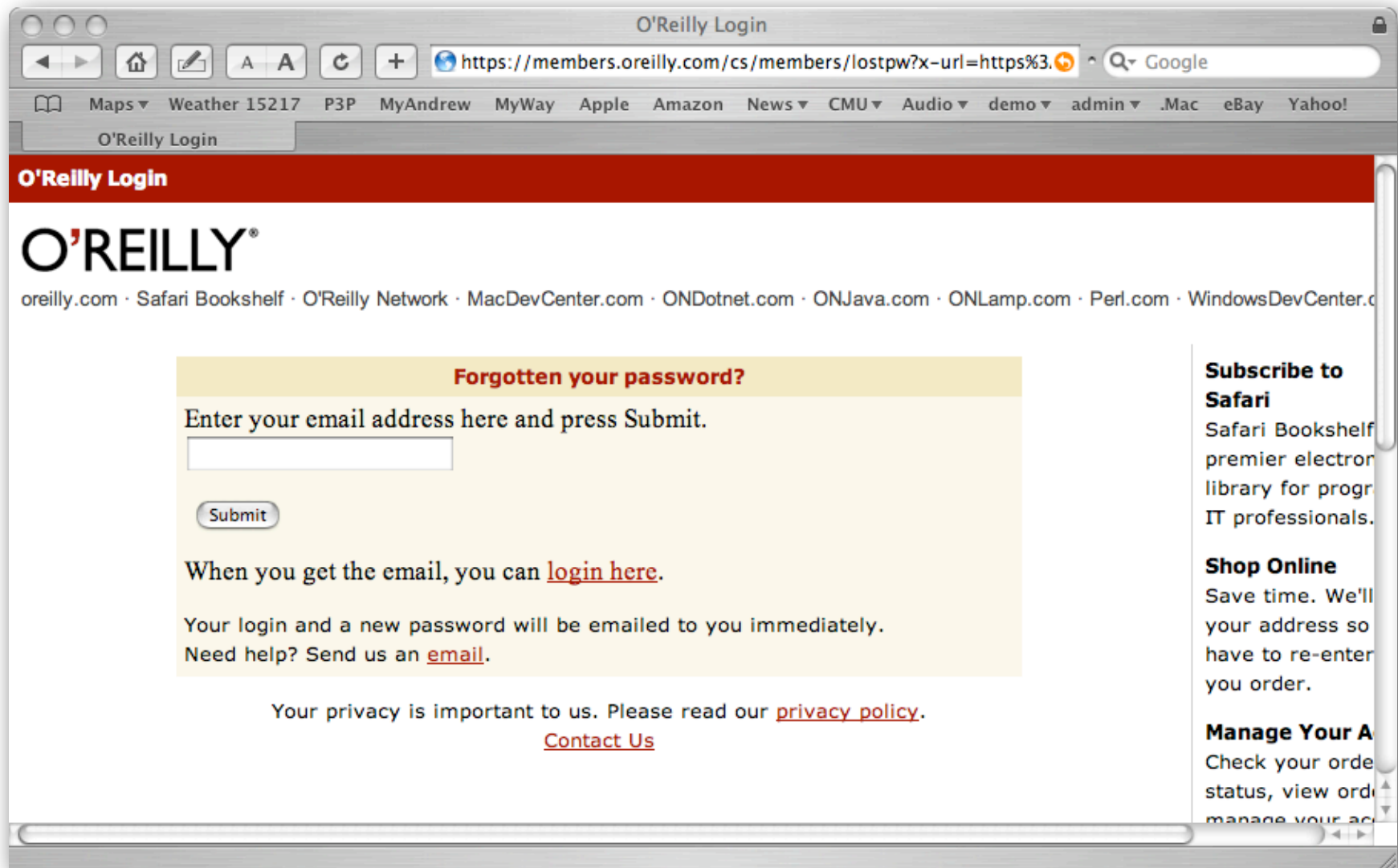


Graphical passwords



Rely on “forgotten password” mechanism

- Email password or magic URL to address on file
- Challenge questions



Proposal

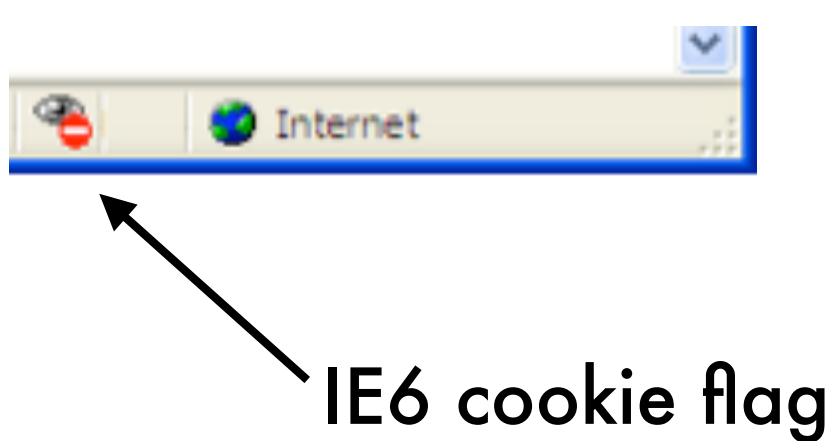
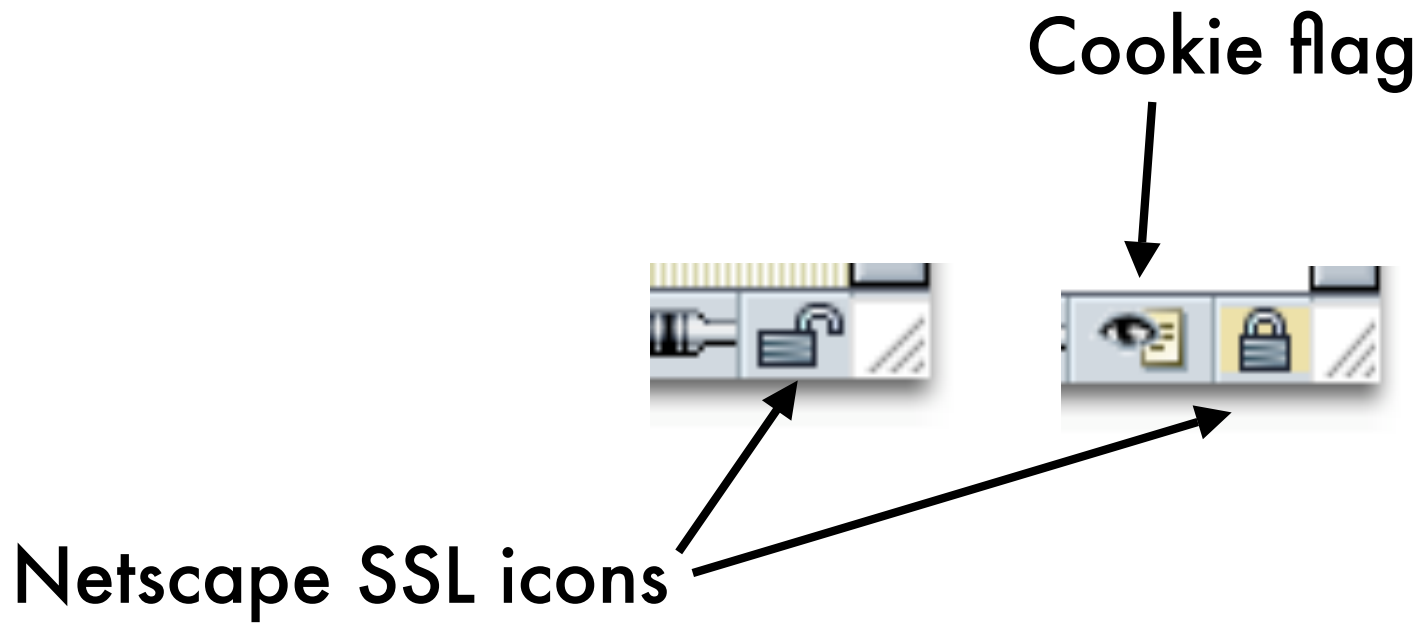
- Why not make this the normal way to access infrequently used sites?

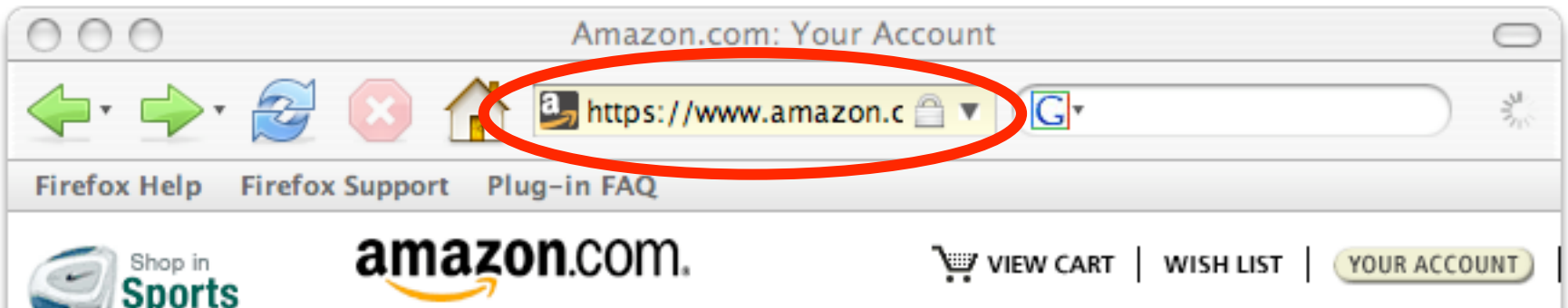
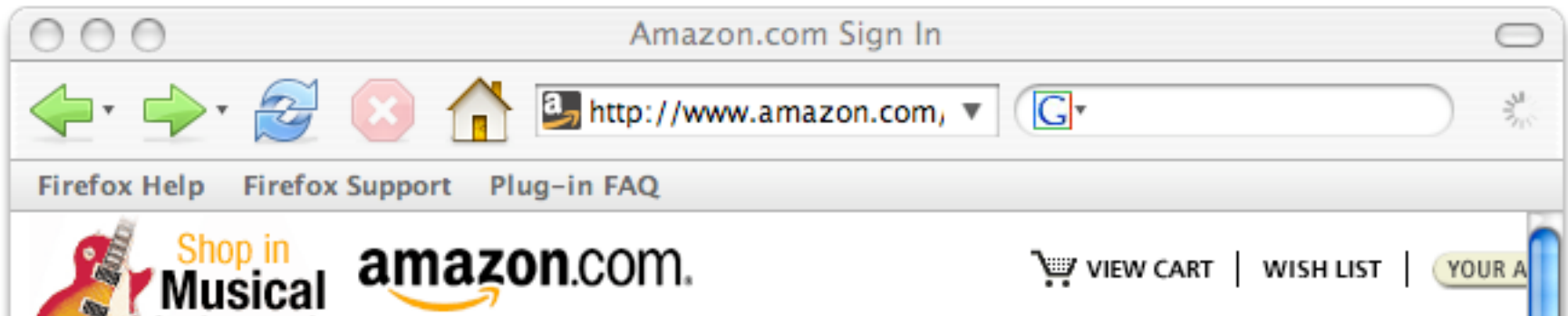
Symbols & Metaphors

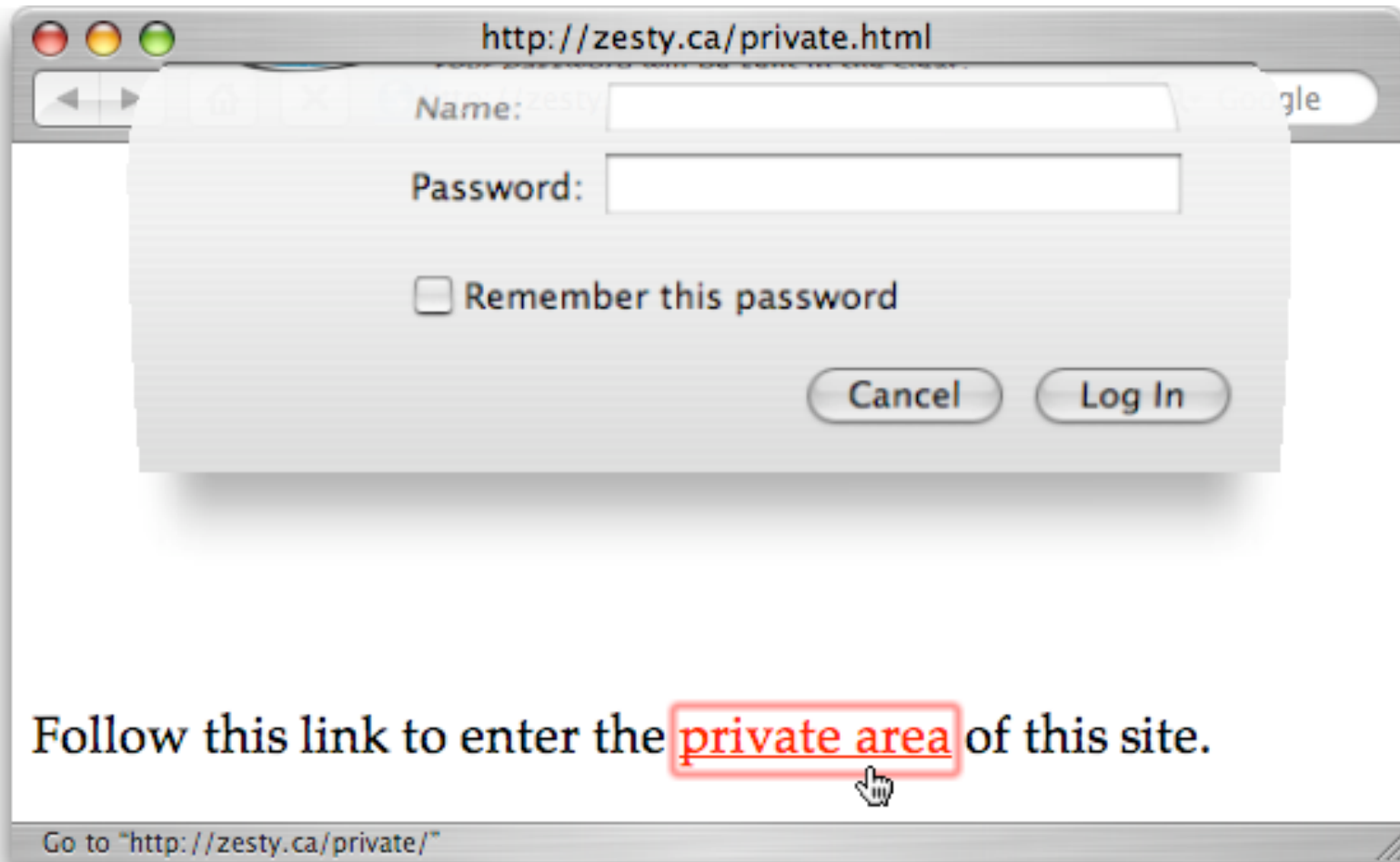


3.









Why do I use a key
rather than a pen to
make a digital signature?



Privacy Bird icons

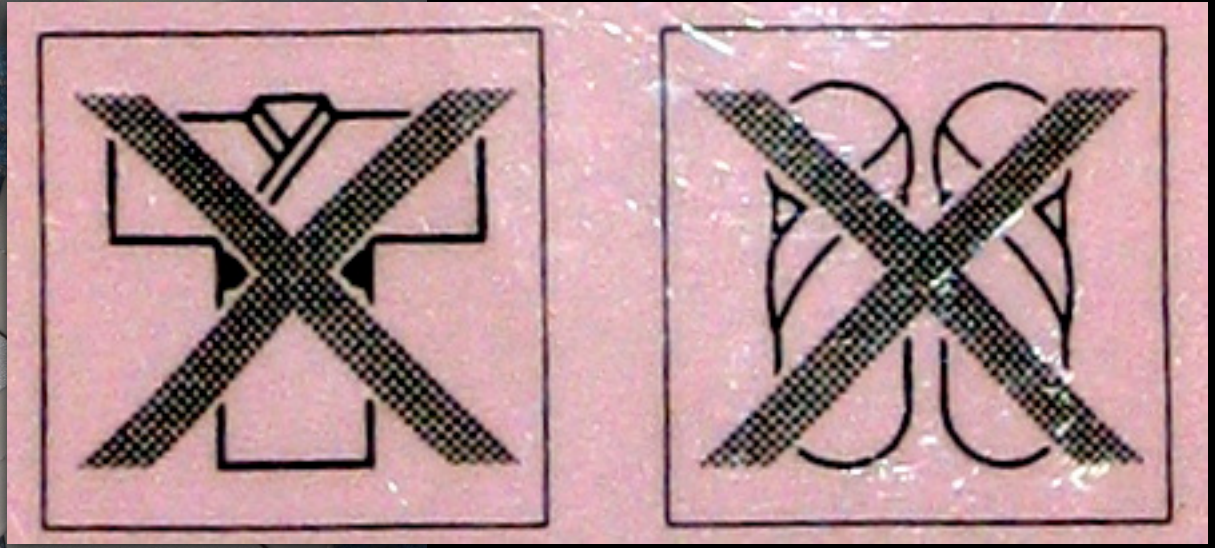
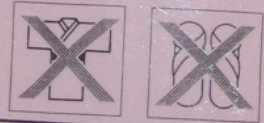


Privacy policy
matches user's
privacy preferences

Privacy policy
does not
match user's
privacy
preferences



浴衣・スリッパのまま、客室フロア(廊下)以外へ
お出になることは、非常時を除き、
ご遠慮ください。



Rethinking cookies



4.

Privacy Alert



The Web site "doubleclick.net" has requested to save a file on your computer called a "cookie." This file may be used to track usage information. Do you want to allow this?

Apply my decision to all cookies from this Web site

Allow Cookie

Block Cookie

More Info

Help

Google Planning to Roll Out E-Mail Service - Microsoft IE

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media Print

Address <http://www.nytimes.com/2004/03/31/technology/31CND-GOOGLE.html?hp>

Acumen user menu sites using cookies: X m3.doubleclick.net www.nytimes.com

The New York Times

NYTimes: [Home](#) - [Site Index](#) - [Archive](#) - [Help](#)

Go to a Section Quotes:

Get the answers with Re CBSMarketWatch MarketWatch.com

[NYTimes.com](#) > [Technology](#)

Google Planning to Roll Out E-M

By JOHN MARKOFF
Published: March 31, 2004

SAN FRANCISCO, March 31 — Google Inc., the c
planning to up the ante in its competition with Y
a new consumer-oriented electronic mail service.

Website: m3.doubleclick.net

Basics

- X site cookies blocked by [rule](#)
[allow site cookies](#)
- 5/5 users who have visited site block
- site's cookies (1 explicitly, 4 by rule)
-mavens: 2/2 (0,2)

More detail

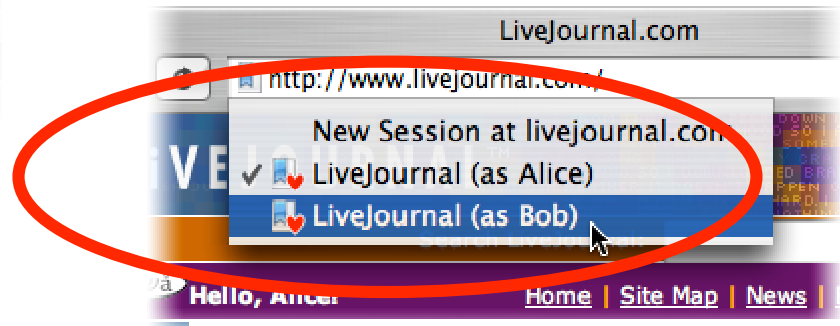
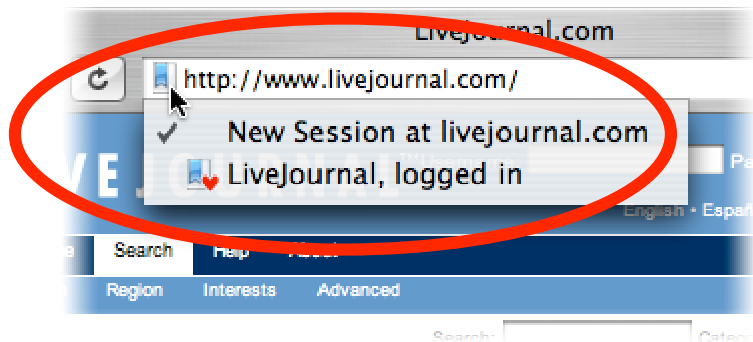
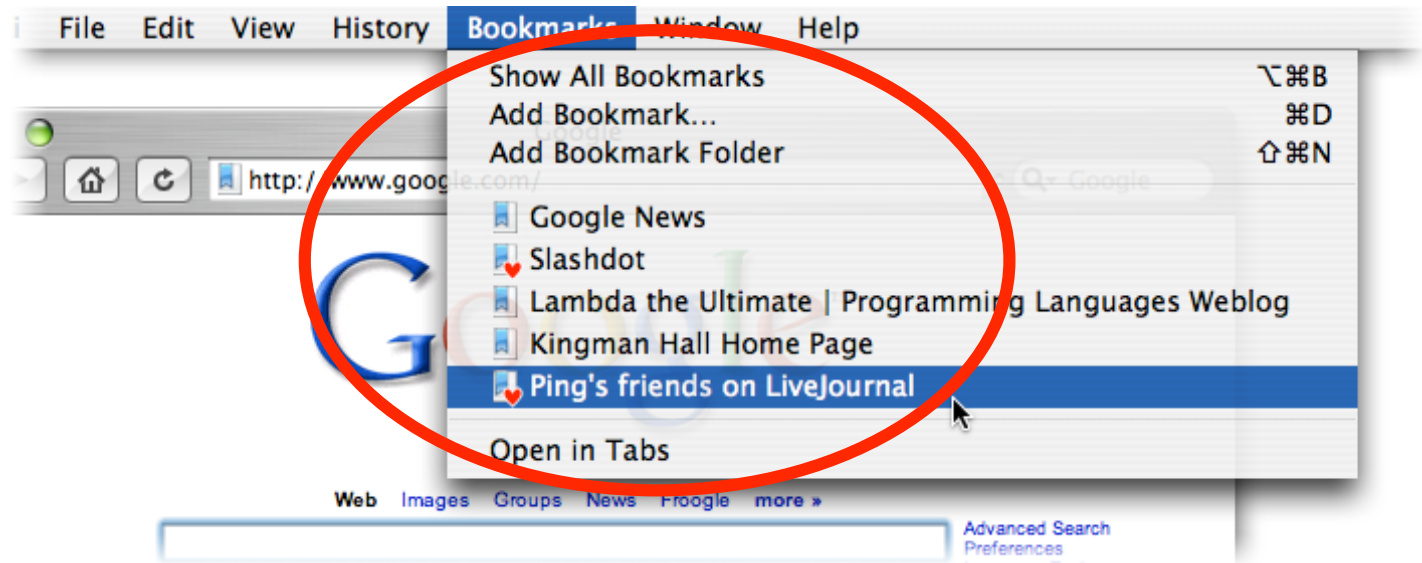
[m3.doubleclick.net's cookies](#)

child sites: none

parent sites: ● [doubleclick.net](#)

System data

number of users: 9
number of websites: 2590
number of webpages: 30215



Making Web privacy visible



5.

Privacy

“the claim of individuals... to determine for themselves when, how, and to what extent information about them is communicated to others.”

- Alan Westin, 1967

Process

“Each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication....”

- Alan Westin, 1967

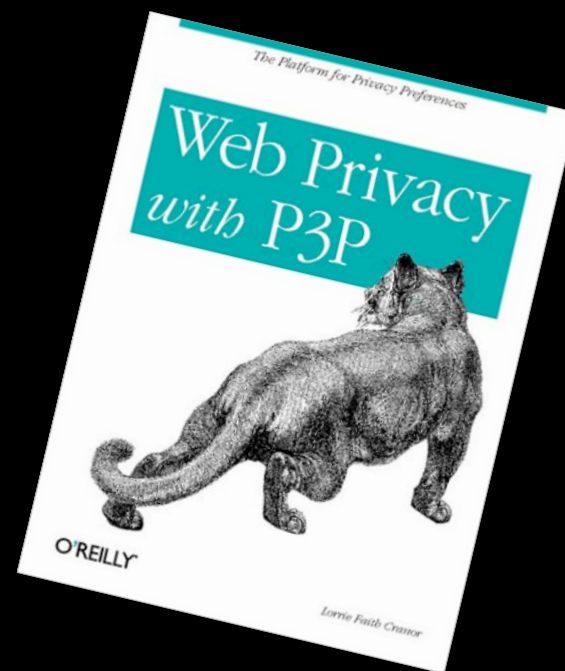
Web site privacy policies

- Many posted
- Few read

What if your browser
could read privacy
policies for you?

Platform for Privacy Preferences (P3P)

- 2002 W3C Recommendation
- XML format for Web privacy policies
- Protocol enables clients to locate and fetch policies from servers



P3P/XML encoding

```
<POLICIES xmlns="http://www.w3.org/2002/01/P3Pv1">
  <POLICY discuri="http://p3pbook.com/privacy.html"
    name="policy">
    <ENTITY>
      <DATA-GROUP>
        <DATA
          ref="#business.contact-info.online.email">privacy@p3pbook.com
        </DATA>
        <DATA
          ref="#business.contact-info.online.uri">http://p3pbook.com/
        </DATA>
        <DATA ref="#business.name">Web Privacy With P3P</DATA>
      </DATA-GROUP>
    </ENTITY>
    <ACCESS><nonident/></ACCESS>
    <STATEMENT>
      <CONSEQUENCE>We keep standard web server logs.</CONSEQUENCE>
      <PURPOSE><admin/><current/><develop/></PURPOSE>
      <RECIPIENT><ours/></RECIPIENT>
      <RETENTION><indefinitely/></RETENTION>
      <DATA-GROUP>
        <DATA ref="#dynamic.clickstream"/>
        <DATA ref="#dynamic.http"/>
      </DATA-GROUP>
    </STATEMENT>
  </POLICY>
</POLICIES>
```

P3P version (points to xmlns attribute)

Location of human-readable privacy policy (points to discuri attribute)

P3P policy name (points to name attribute)

Site's name and contact info (bracketed on the left, points to the ENTITY section)

Access disclosure (points to ACCESS element)

Human-readable explanation (points to CONSEQUENCE element)

How data may be used (points to PURPOSE element)

Data recipients (points to RECIPIENT element)

Data retention policy (points to RETENTION element)

Types of data collected (points to DATA-GROUP element)

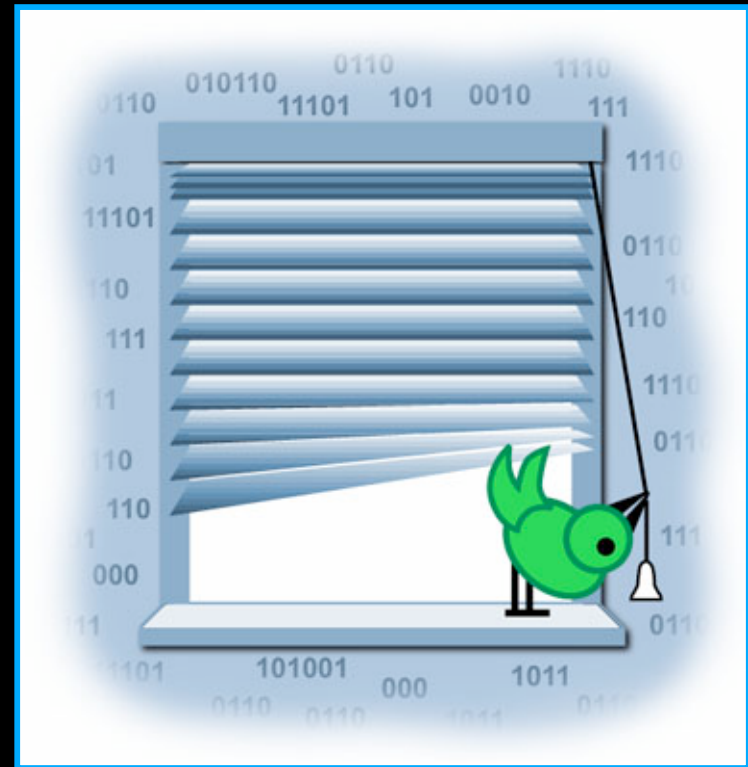
Statement (bracketed on the left, points to the STATEMENT section)

P3P adoption

- Web site adoption as of May 2005
 - 15% of top 2000 domains
 - 21% of top 500 domains
 - 29% of top 100 domains
- User agents
 - Limited P3P functionality in IE6 and Navigator 7
 - Other P3P user agents available

AT&T Privacy Bird

- P3P user agent
- Free download
<http://privacybird.com/>
- Compares user preferences with P3P policies




Shane Zachary Cranor's Home Page - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media

Address <http://shane.cranor.org/> Go Links >>

Shane Zachary Cranor




[Photo Album](#) | [Latest Photos](#) | [2001 Favorite Photos](#) | [2002 Favorite Photos](#) | [2003 Favorite Photos](#)

[Watch a movie of Shane at 2 1/4 putting on his sandals and talking about mowing the lawn.](#) "What am I doing?" he asks. "I'm putting them on slowly," he says (he really means "loosely"). If you are not sure what he's saying, [read the transcript](#).

Shane's Photo Album

- [Shane's First Year](#)
- [Shane's Second Year](#)
- [Shane at 24-25 Months](#)
- [Shane at 26-27 Months](#)



Done Internet



Shane Zachary Cranor's Home Page - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print

Address <http://shane.cranor.org/> Go Links >>

Shane Zachary



Shane's Photo Album

- [Shane's First Year](#)
- [Shane's Second Year](#)
- [Shane at 24-25 Months](#)
- [Shane at 26-27 Months](#)

Done

Policy Summary

Shane Cranor's Home Page Privacy Practices

Privacy Policy Check

Shane Cranor's Home Page's privacy policy *matches your preferences.*

Privacy Policy Summary

This site has the following statements in its policy:

- [Site Statement 1](#)

Site Statement 1

Types of Information Collected:

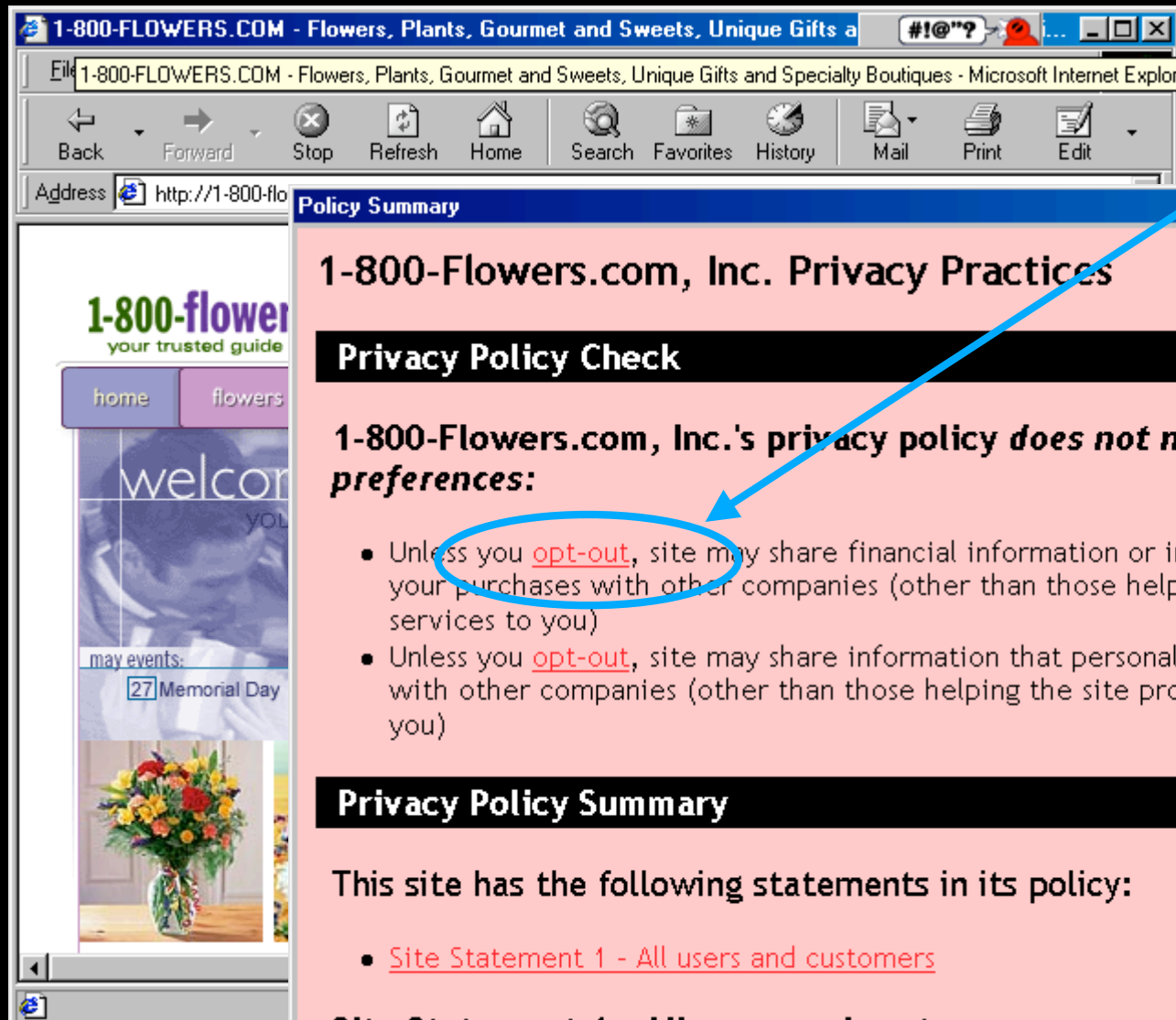
- HTTP protocol information
- Click-stream information

How your information will be used:

- Research and development
- To complete the activity for which the data was provided
- Web site and system administration

Who will use your information:

- This web site and its agents



Link to
opt-out page

1-800-Flowers.com, Inc. Privacy Practices

Privacy Policy Check

1-800-Flowers.com, Inc.'s privacy policy does not match your preferences:

- Unless you [opt-out](#), site may share financial information or information about your purchases with other companies (other than those helping the site provide services to you)
- Unless you [opt-out](#), site may share information that personally identifies you with other companies (other than those helping the site provide services to you)

Privacy Policy Summary

This site has the following statements in its policy:

- [Site Statement 1 - All users and customers](#)

Site Statement 1 - All users and customers

Types of Information Collected:

How can I find a site that
will protect my privacy?

PrivacyFinder Search for: books

http://search.privacybird.com/?q=books&changekey=0& Google


PrivacyFinder Maps Weather 15217 P3P MyWay CMU Audio demo admin News (1165) MyAndrew .Mac


PrivacyFinder Search for: b...

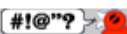
PrivacyFinder books

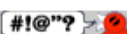
Preference Level: Low Medium High Custom




Search API: Google Yahoo

 [BookFinder.com](#)
online bookstore comparison shopping agent that searches the inventory of individual new, used, and out-of-print vendors and reports on pricing and availability.
[www.bookfinder.com/](#) - [Cached](#) - [Privacy Policy](#) - [Similar Pages](#)

 [Powell's Books - Used Books, Rare Books, New Books, and Out of Print Books](#)
Powell's Books - Used Books, Rare Books, New Books, and Out of Print Books Powell's Books - Used Books, Rare Books, New Books, and Out of Print Books Powell's Books is the largest independent used and new ...
[www.powells.com/](#) - [No Cache](#) - [Privacy Policy](#) - [Similar Pages](#)

 [Barnes & Noble.com - Home](#)
BarnesandNoble.com - The World's Largest Bookseller Online ... 0 Items. BROWSE BOOKS. WHAT'S NEW ... Then see more Books That Breathe Fire in a new collection that's hot on dragons. ...
[www.barnesandnoble.com/](#) - [No Cache](#) - [Privacy Policy](#) - [Similar Pages](#)

 [BookBrowser](#)
collection of reading lists from Barnes & Noble with excerpts for each book. Learn more about your favorite authors, discover what America's reading, or see what titles are coming soon.
[www.barnesandnoble.com/bookbrowser/](#) - [Cached](#) - [Privacy Policy](#) - [Similar Pages](#)

[Amazon.com: Online Shopping for Electronics, Apparel, Computers, Books, DVDs & more](#)
Online shopping from the earth's biggest selection of books, magazines, music, DVDs, videos, electronics, computers, software, apparel & accessories, shoes, jewelry, tools & hardware, housewares, furniture, sporting goods, beauty & personal care...  Books, Music, DVD.  Books.  DVD ...
[www.amazon.com/](#) - [No Cache](#) - [Similar Pages](#)

[Borders.com](#)
online retail site for music, video, and books including computer and children's books.
[www.borders.com/](#) - [Cached](#) - [Similar Pages](#)

[abebooks](#)
specializes in connecting buyers and sellers of used, rare, and out-of-print books. Includes a database of booksellers' inventory lists searchable by author, title, publisher, and keyword.
[www.abebooks.com/](#) - [Cached](#) - [Similar Pages](#)

Wireless privacy

- Many users unaware that communications over wireless computer networks are not private

Wall of sheep

Defcon 2001



Defcon 2004

Wall of Shame

login	pass	domain ip	application
netjam	def*****	209.50.235.72	POP3
gadakkah	str*****	204.152.184.73	POP3
crash	llo*****	81.26.109.4	POP3
poop_free9@	5d4*****	207.46.106.109	MSN Messenger
frestorm_454	6ae*****	207.46.106.68	MSN Messenger
loz	fox*****	192.168.1.5	POP3
tim_tindorides	bab*****	207.150.192.52	POP3
tim	bab*****	24.234.9.45	POP3
Webproze	900*****	209.126.160.57	HTTP
la\jpittman	Ag1*****	http://mail.national	HTTP
royceb	hlF*****	155.92.194.35	POP3
cheeps	atw*****	217.80.37.93	HTTP
4381796	ea7*****	17.112.153.35	FTP
frex	dis*****	63.226.21.145	HTTP
wuhao@ptan	B0f*****	64.246.50.89	POP3
jfa	Ro5*****	129.82.103.72	POP3
takefull	vae*****	210.251.89.161	POP3 (has not learned)
jamie@crazylinux	net - Do not hire to test your security		

Peripheral display

- Help users form more accurate expectations of privacy
- Without making the problem worse



Experimental trial

- 11 subjects in student workspace
- Data collected by survey and traffic analysis
- Did they refine their expectations of privacy?

Results

- No change in behavior
- Peripheral display raised privacy awareness in student workspace
- But they didn't really get it

Privacy awareness increased

“I feel like my information /activity /
privacy are not being protected
seems like someone can monitor or
get my information from my
computer, or even publish them.”

But only while the display
was on

“Now that words [projected on
the wall] are gone, I'll go back to
the same.”

Questions to ask about a security or privacy cue

- Do users notice it?
- Do they know what it means?
- Do they know what they are supposed to do when they see it?
- Will they actually do it?
- Will they keep doing it?

*security controls they can understand
privacy they can control*



CMU Usable Privacy and Security Laboratory
<http://cups.cs.cmu.edu/>

CarnegieMellon