Inexplicable Indicators and Puzzling Pop-ups

Security Software from an End User Perspective

Lorrie Faith Cranor

December 2006
http://lorrie.cranor.org/

CMU Usable Privacy and Security Laboratory

Carnegie Mellon

The user experience

How do users stay safe online?

PAL Spyware
webroot
Spy Sweeper
2004
Spyware Eliminator
Anonymous Surfing
Privacy Protection That Defends Your Confidential Information
COOKIES
POP!
SPAM
Hormel
Norton
AntiVirus
2004
symantec.
OEM VERSION
Net Nanny
Encryption for Everyone
PGP
Pretty Good Privacy
HARDENED
Simson Garfinkel
O'Reilly & Associates, Inc.

After installing all that security and privacy software

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

Secondary tasks

“Users do not want to be responsible for, nor concern themselves with, their own security.”

- Blake Ross

Concerns may not be aligned

- Security experts are concerned about the bad guys getting in
- Users may be more concerned about locking themselves out

Grey: Smartphone based access-control system

- Deployed in CMU building with computer security faculty and students
- Nobody questions that the security works
- But lots of concerns about getting locked out

L. Bauer, L. F. Cranor, M. K. Reiter, and K. Vaniea. **Lessons Learned from the Deployment of a Smartphone-Based Access-Control System.** Technical Report CMU-CyLab-06-016, CyLab, Carnegie Mellon University, October 2006. http://www.cylab.cmu.edu/default.aspx?id=2244

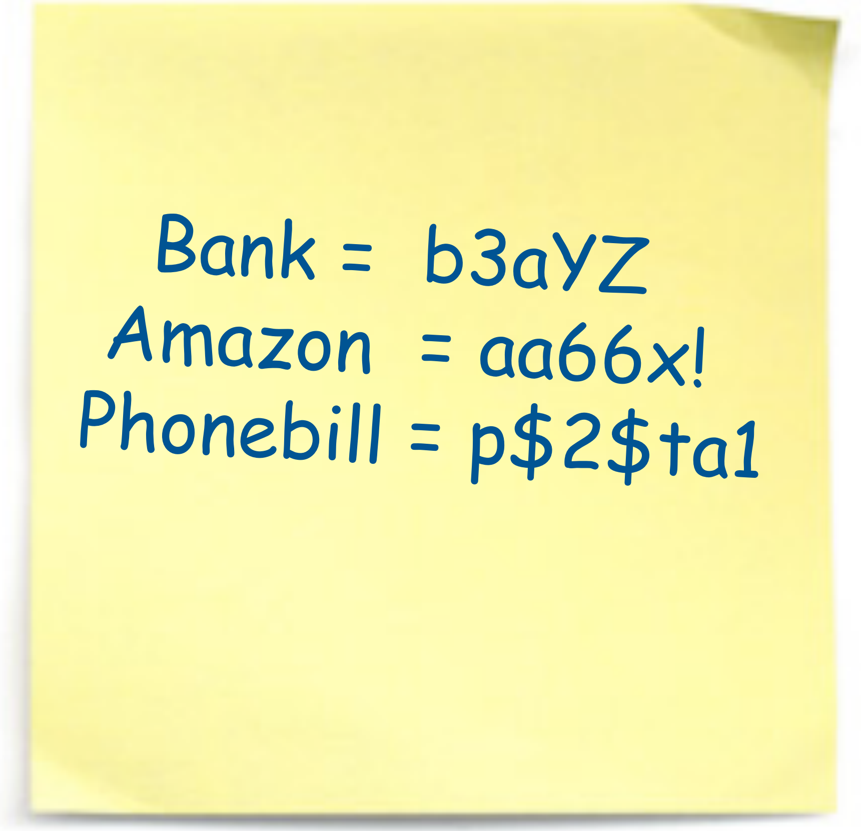
Secure, but usable?

Unusable security frustrates users

Typical password 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

Approaches to usable security

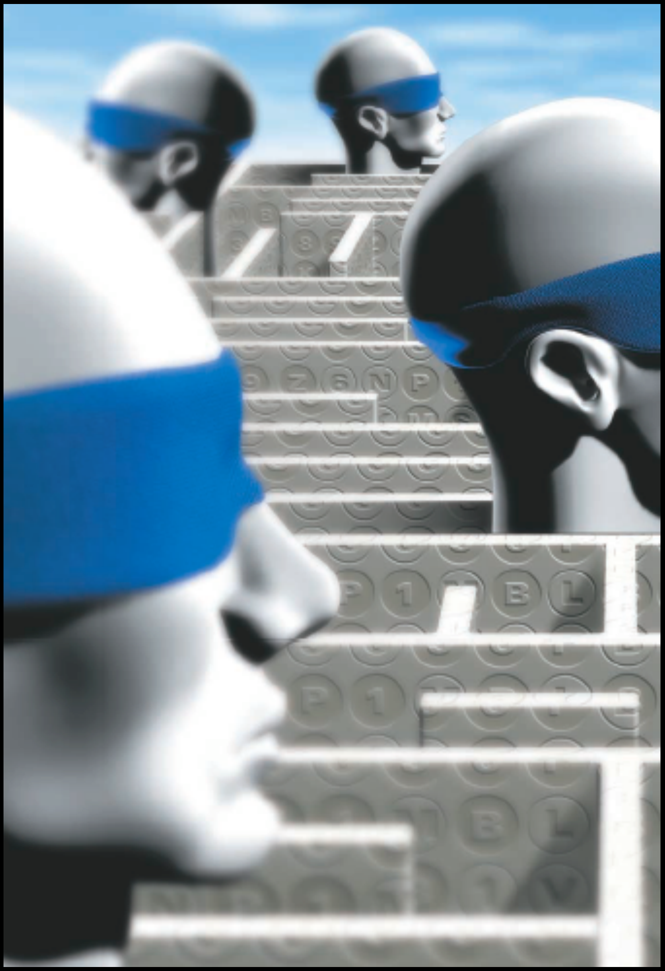
- Make it "just work"
  - Invisible security
- Make security/privacy understandable
  - Make it visible
  - Make it intuitive
  - Use metaphors that users can relate to
- Train the user

Make it “just work”

This makes users very happy

(but it’s not that easy)

Make decisions

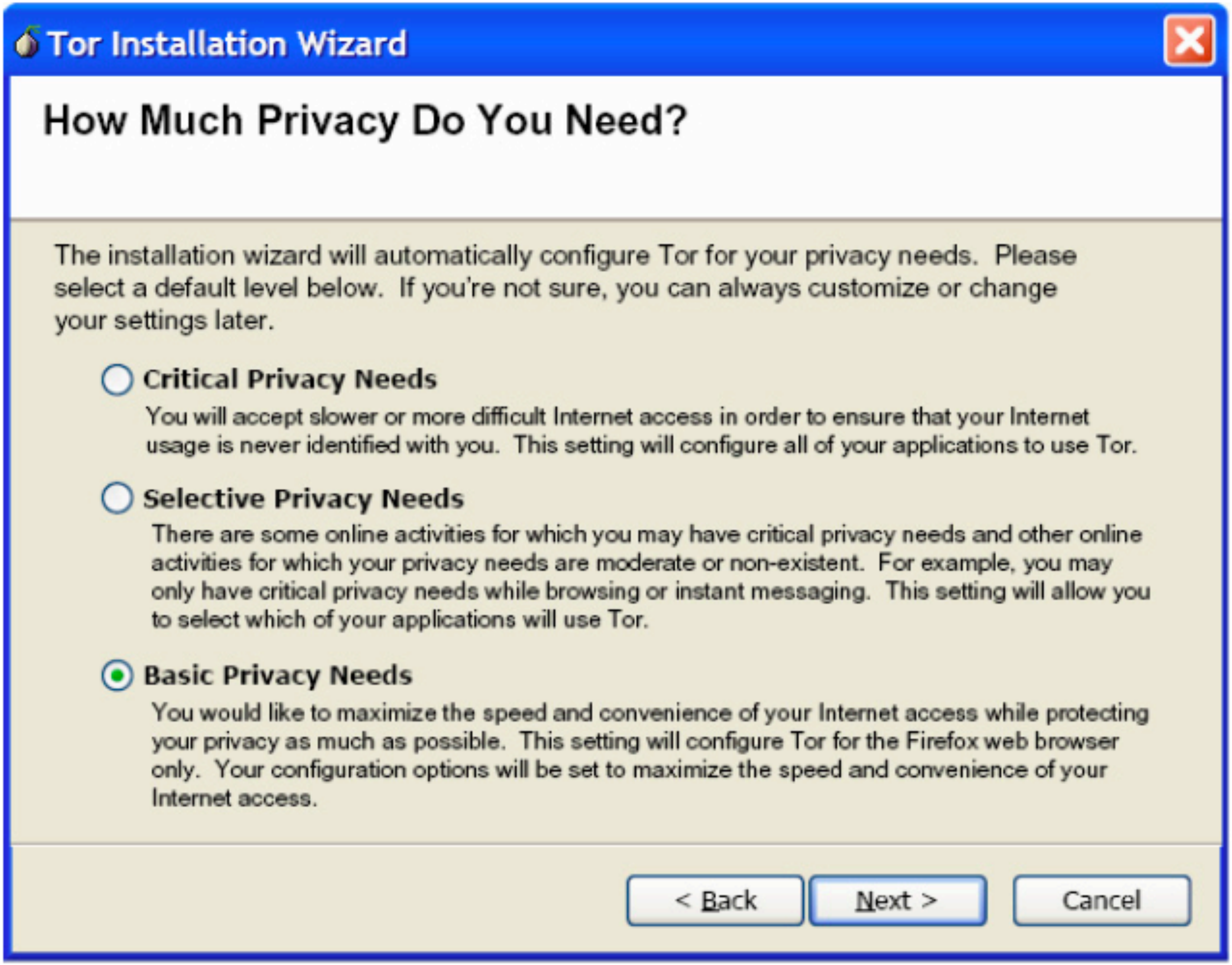


- Developers should not expect users to make decisions they themselves can’t make

Make security understandable

“Present choices, not dilemmas”

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



How Much Privacy Do You Need?

The installation wizard will automatically configure Tor for your privacy needs. Please select a default level below. If you're not sure, you can always customize or change your settings later.

○ **Critical Privacy Needs**

You will accept slower or more difficult Internet access in order to ensure that your Internet usage is never identified with you. This setting will configure all of your applications to use Tor.

○ **Selective Privacy Needs**

There are some online activities for which you may have critical privacy needs and other online activities for which your privacy needs are moderate or non-existent. For example, you may only have critical privacy needs while browsing or instant messaging. This setting will allow you to select which of your applications will use Tor.

● **Basic Privacy Needs**

You would like to maximize the speed and convenience of your Internet access while protecting your privacy as much as possible. This setting will configure Tor for the Firefox web browser only. Your configuration options will be set to maximize the speed and convenience of your Internet access.

Train the user

Training people not to fall for phish

- Laboratory study of 28 non-expert computer users
- Asked to evaluate 10 web sites, take 15 minute break, evaluate 10 more web sites
- Experimental group read web-based training materials during break, control group played solitaire
- Experimental group performed significantly better identifying phish after training
- People can learn from web-based training materials, if only we could get them to read them!

How do we get people trained?

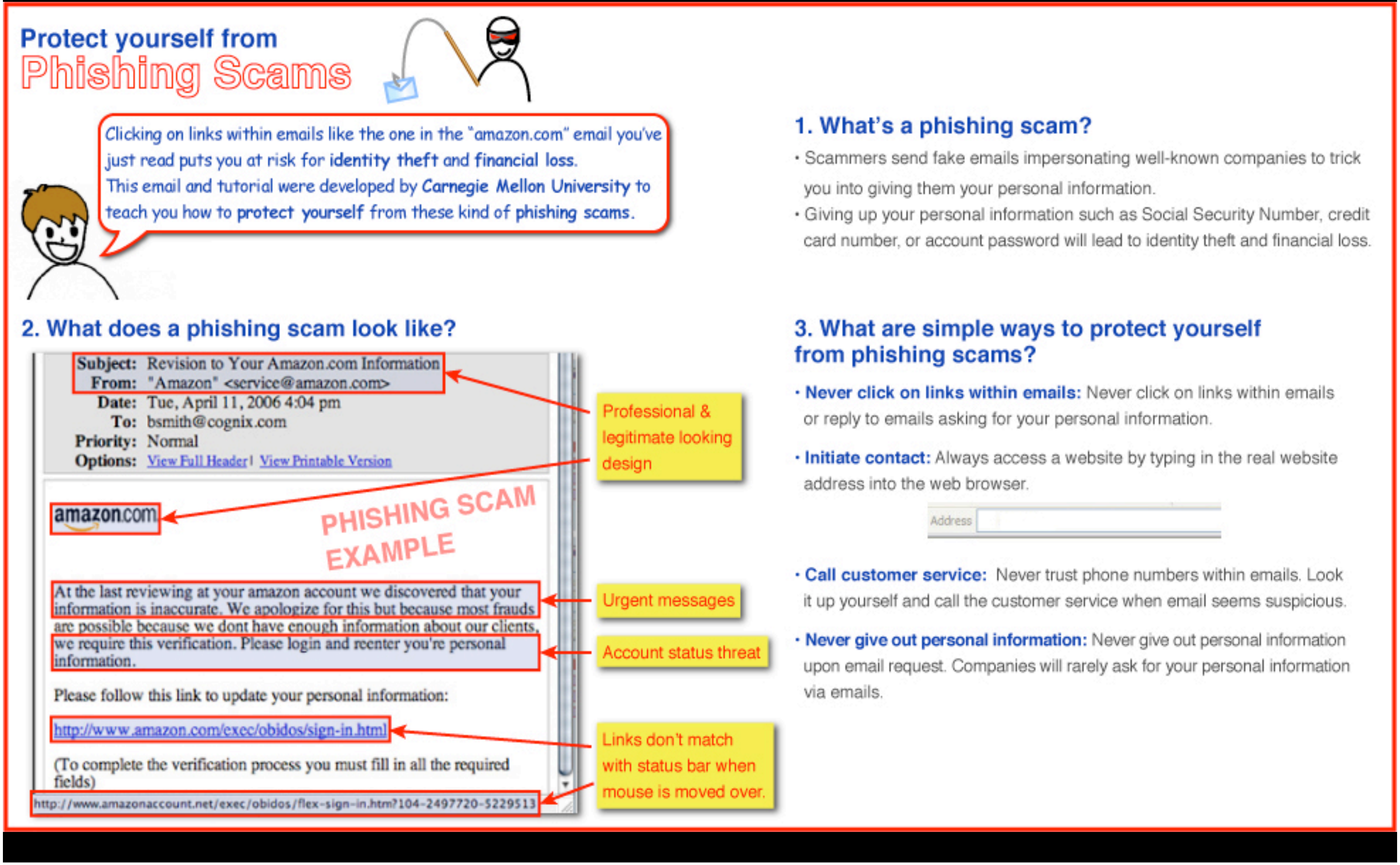
- Most people don't proactively look for training materials on the web
- Many companies send "security notice" emails to their employees and/or customers
- But these tend to be ignored
  - Too much to read
  - People don't consider them relevant

Embedded training

- Can we "train" people during their normal use of email to avoid phishing attacks?
  - Periodically, people get sent a training email
  - Training email looks like a phishing attack
  - If person falls for it, intervention warns and highlights what cues to look for in succinct and engaging format

P. Kumaraguru, Y. Rhee, A. Acquisti, L. Cranor, J. Hong, and E. Nunge. **Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System.** CyLab Technical Report. CMU-CyLab-06-017, 2006. http://www.cylab.cmu.edu/default.aspx?id=2253

Diagram intervention



Protect yourself from
Phishing Scams

Clicking on links within emails like the one in the "amazon.com" email you've just read puts you at risk for **identity theft** and **financial loss**.
This email and tutorial were developed by **Carnegie Mellon University** to teach you how to **protect yourself** from these kind of **phishing scams**.

1. What's a phishing scam?

- Scammers send fake emails impersonating well-known companies to trick you into giving them your personal information.
- Giving up your personal information such as Social Security Number, credit card number, or account password will lead to identity theft and financial loss.

2. What does a phishing scam look like?

Subject: Revision to Your Amazon.com Information
From: "Amazon" <service@amazon.com>
Date: Tue, April 11, 2006 4:04 pm
To: bsmith@cognix.com
Priority: Normal
Options: View Full Header | View Printable Version

amazon.com

PHISHING SCAM EXAMPLE

At the last reviewing at your amazon account we discovered that your information is inaccurate. We apologize for this but because most frauds are possible because we dont have enough information about our clients, we require this verification. Please login and reenter you're personal information.

Please follow this link to update your personal information:

http://www.amazon.com/exec/obidos/sign-in.html

(To complete the verification process you must fill in all the required fields)

http://www.amazonaccount.net/exec/obidos/flex-sign-in.htm?104-2497720-5229513

Professional & legitimate looking design

Urgent messages

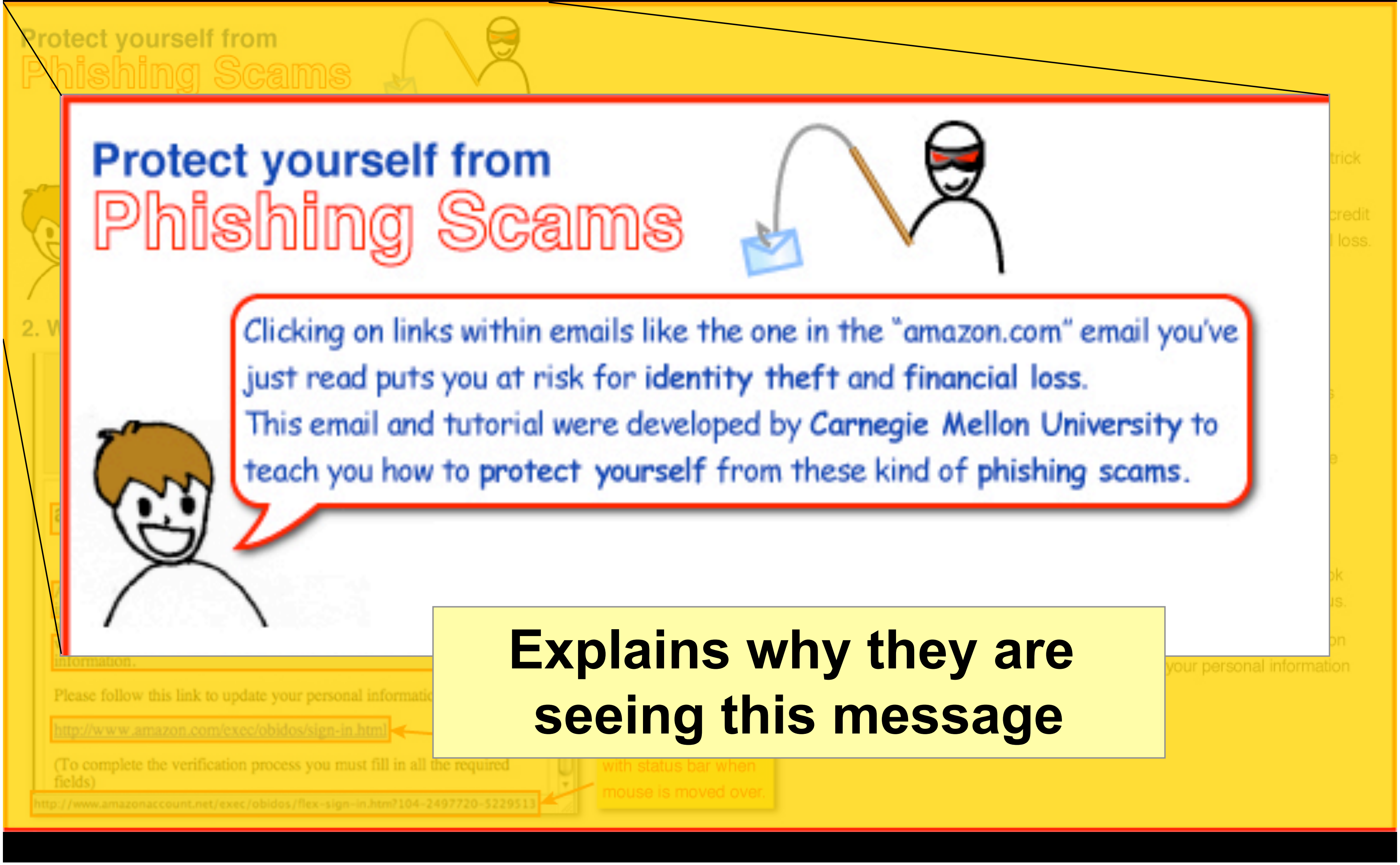
Account status threat

Links don't match with status bar when mouse is moved over.

3. What are simple ways to protect yourself from phishing scams?

- **Never click on links within emails:** Never click on links within emails or reply to emails asking for your personal information.
- **Initiate contact:** Always access a website by typing in the real website address into the web browser.

- **Call customer service:** Never trust phone numbers within emails. Look it up yourself and call the customer service when email seems suspicious.
- **Never give out personal information:** Never give out personal information upon email request. Companies will rarely ask for your personal information via emails.



Protect yourself from
Phishing Scams

Clicking on links within emails like the one in the "amazon.com" email you've just read puts you at risk for identity theft and financial loss.
This email and tutorial were developed by Carnegie Mellon University to teach you how to protect yourself from these kind of phishing scams.

Please follow this link to update your personal informatio

http://www.amazon.com/exec/obidos/sign-in.html

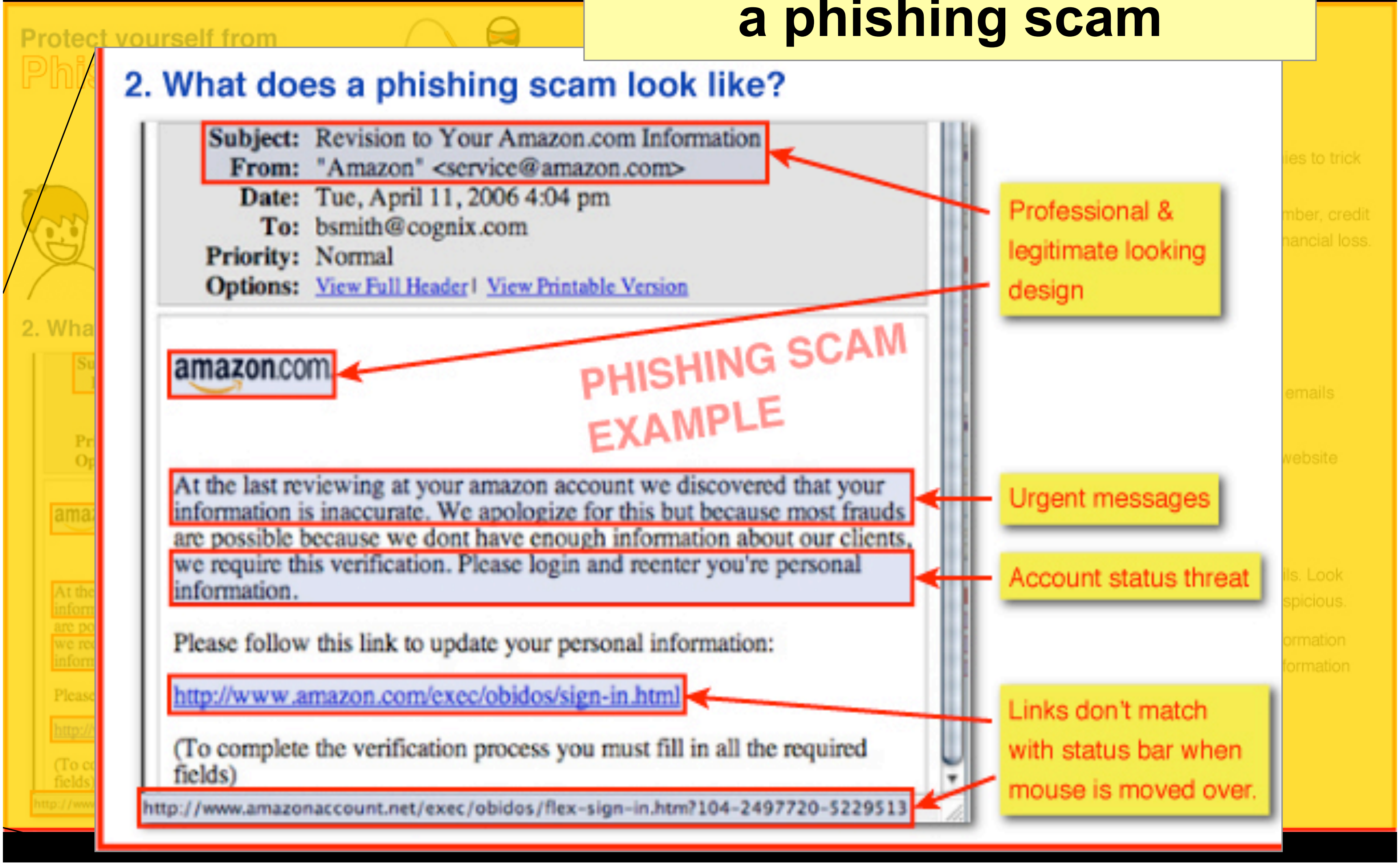
(To complete the verification process you must fill in all the required fields)

http://www.amazonaccount.net/exec/obidos/flex-sign-in.htm?104-2497720-5229513

with status bar when mouse is moved over.

Explains why they are seeing this message

Explains how to identify a phishing scam



2. What does a phishing scam look like?

Subject: Revision to Your Amazon.com Information
From: "Amazon" <service@amazon.com>
Date: Tue, April 11, 2006 4:04 pm
To: bsmith@cognix.com
Priority: Normal
Options: View Full Header | View Printable Version

amazon.com

PHISHING SCAM EXAMPLE

At the last reviewing at your amazon account we discovered that your information is inaccurate. We apologize for this but because most frauds are possible because we dont have enough information about our clients, we require this verification. Please login and reenter you're personal information.

Please follow this link to update your personal information:

http://www.amazon.com/exec/obidos/sign-in.html

(To complete the verification process you must fill in all the required fields)

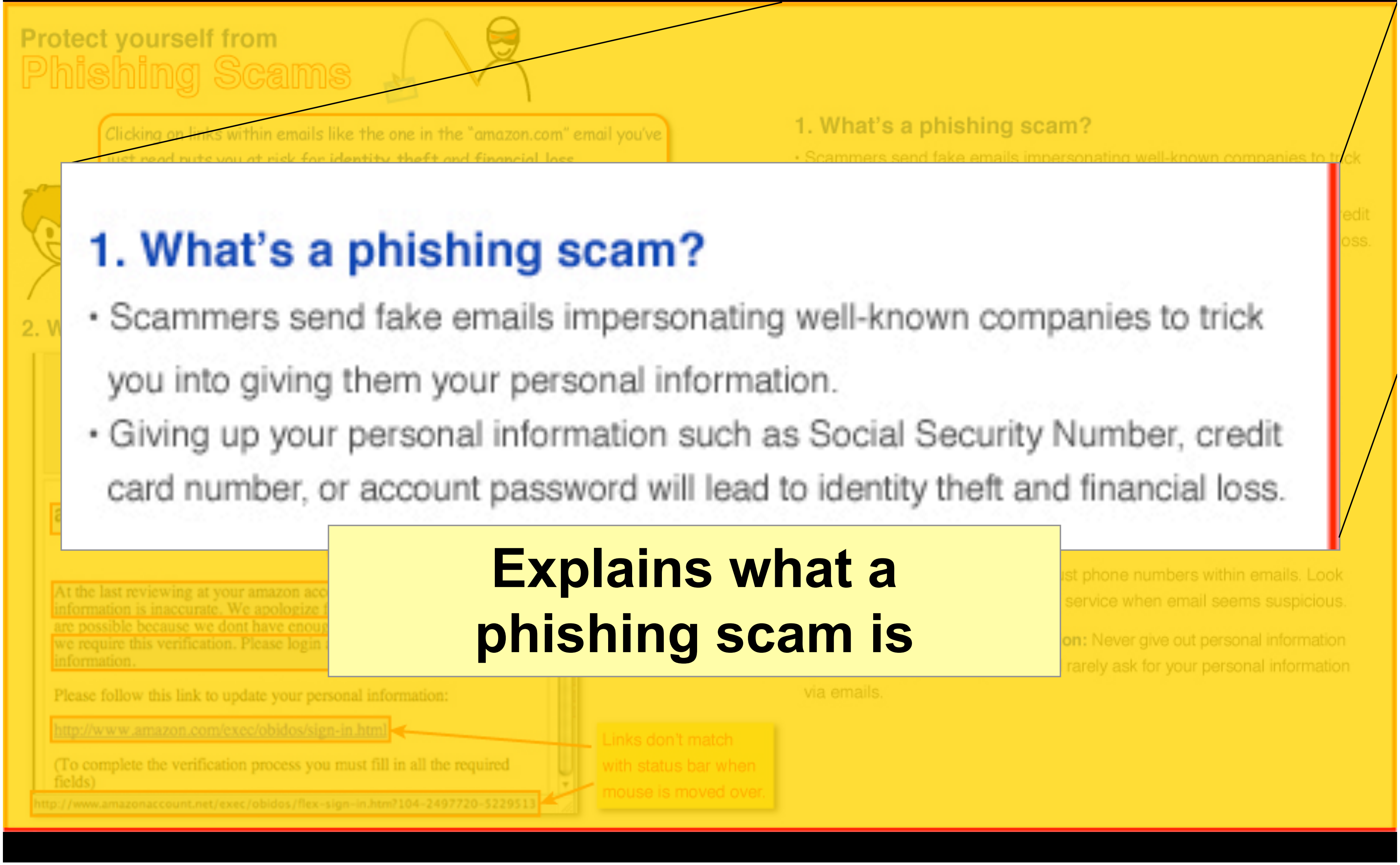
http://www.amazonaccount.net/exec/obidos/flex-sign-in.htm?104-2497720-5229513

Professional & legitimate looking design

Urgent messages

Account status threat

Links don't match with status bar when mouse is moved over.



Protect yourself from

Phishing Scams

Clicking on links within emails like the one in the "amazon.com" email you've just read puts you at risk for identity theft and financial loss.

1. What's a phishing scam?

- Scammers send fake emails impersonating well-known companies to trick you into giving them your personal information.
- Giving up your personal information such as Social Security Number, credit card number, or account password will lead to identity theft and financial loss.

2. W

At the last reviewing at your amazon acc information is inaccurate. We apologize f are possible because we dont have enoug we require this verification. Please login information.

Please follow this link to update your personal information:

http://www.amazon.com/exec/obidos/sign-in.html

(To complete the verification process you must fill in all the required fields)

http://www.amazonaccount.net/exec/obidos/flex-sign-in.htm?104-2497720-5229513

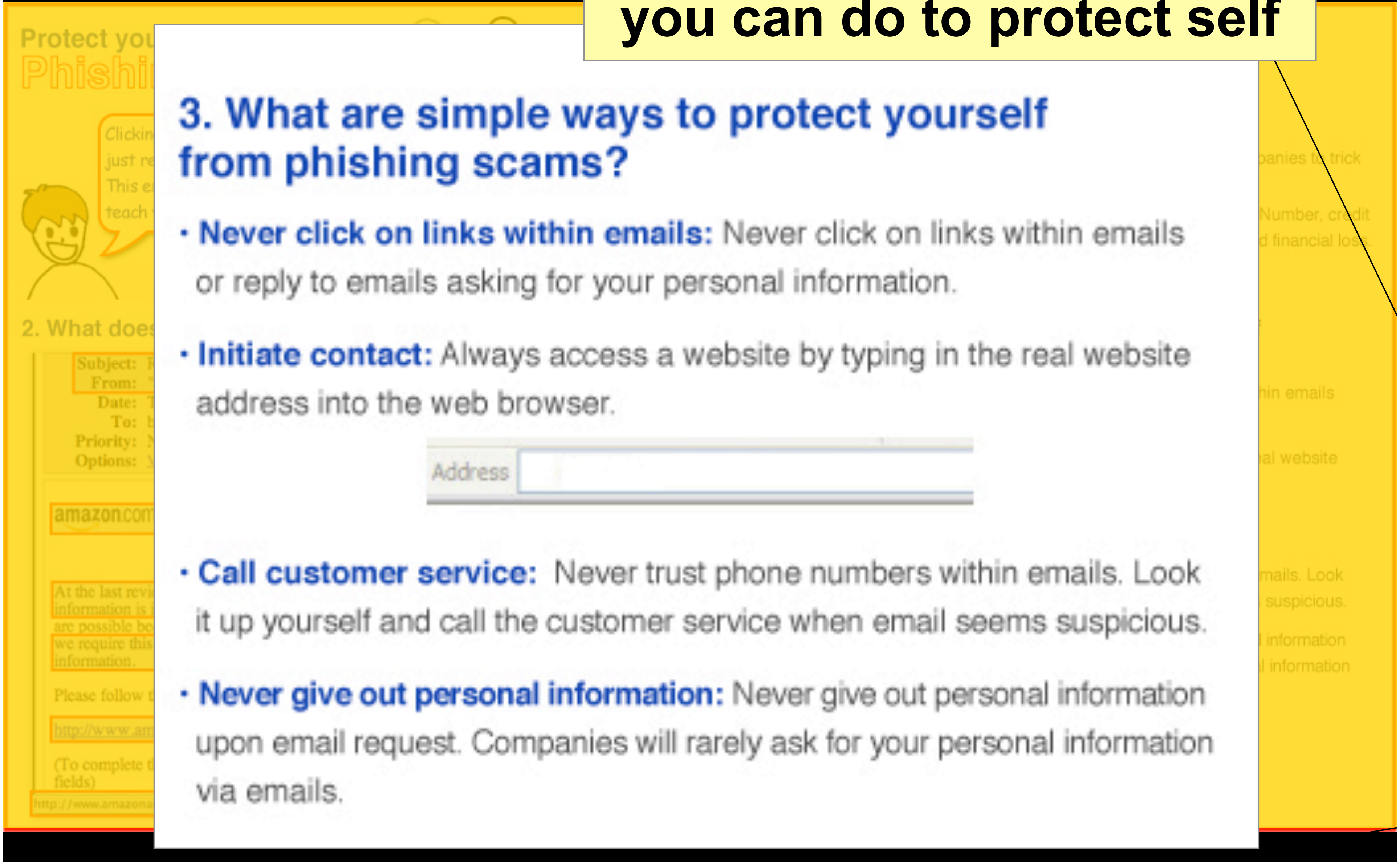
Links don't match with status bar when mouse is moved over.

st phone numbers within emails. Look service when email seems suspicious.

on: Never give out personal information rarely ask for your personal information via emails.

Explains what a phishing scam is

Explains simple things you can do to protect self

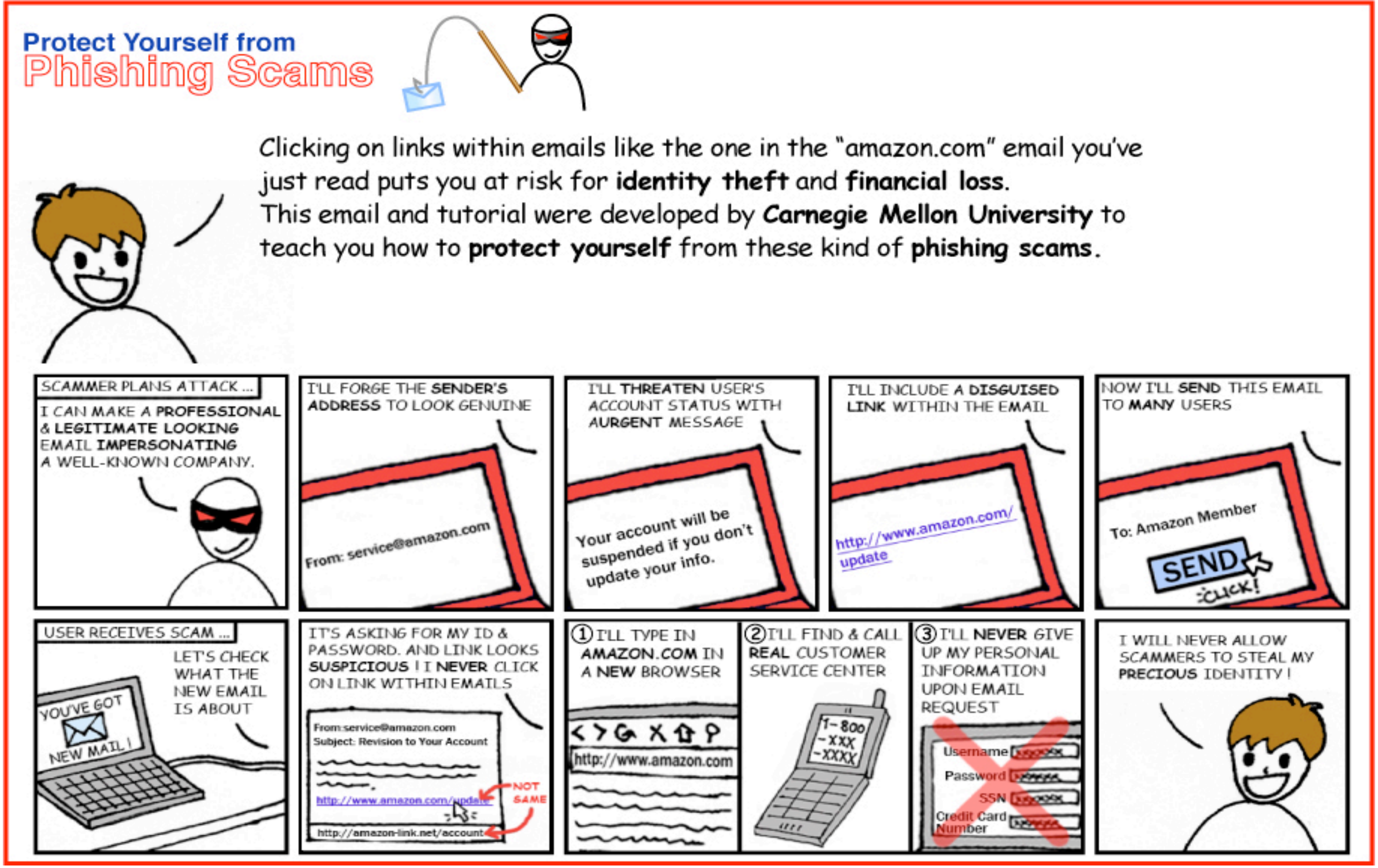


3. What are simple ways to protect yourself from phishing scams?

- **Never click on links within emails:** Never click on links within emails or reply to emails asking for your personal information.
- **Initiate contact:** Always access a website by typing in the real website address into the web browser.

- **Call customer service:** Never trust phone numbers within emails. Look it up yourself and call the customer service when email seems suspicious.
- **Never give out personal information:** Never give out personal information upon email request. Companies will rarely ask for your personal information via emails.

Comic strip intervention



Clicking on links within emails like the one in the "amazon.com" email you've just read puts you at risk for **identity theft** and **financial loss**.
This email and tutorial were developed by **Carnegie Mellon University** to teach you how to **protect yourself** from these kind of **phishing scams**.

Protect Yourself from
Phishing Scams
SCAMMER PLANS ATTACK ...
I CAN MAKE A PROFESSIONAL & LEGITIMATE LOOKING EMAIL IMPERSONATING A WELL-KNOWN COMPANY.
I'LL FORGE THE SENDER'S ADDRESS TO LOOK GENUINE
From: service@amazon.com
I'LL THREATEN USER'S ACCOUNT STATUS WITH AURGENT MESSAGE
Your account will be suspended if you don't update your info.
I'LL INCLUDE A DISGUISED LINK WITHIN THE EMAIL
http://www.amazon.com/update
NOW I'LL SEND THIS EMAIL TO MANY USERS
To: Amazon Member
SEND
CLICK!
USER RECEIVES SCAM ...
YOU'VE GOT NEW MAIL!
LET'S CHECK WHAT THE NEW EMAIL IS ABOUT
IT'S ASKING FOR MY ID & PASSWORD. AND LINK LOOKS SUSPICIOUS ! I NEVER CLICK ON LINK WITHIN EMAILS
From:service@amazon.com
Subject: Revision to Your Account
http://www.amazon.com/update
NOT SAME
http://amazon-link.net/account
① I'LL TYPE IN AMAZON.COM IN A NEW BROWSER
http://www.amazon.com
② I'LL FIND & CALL REAL CUSTOMER SERVICE CENTER
1-800-XXX-XXXX
③ I'LL NEVER GIVE UP MY PERSONAL INFORMATION UPON EMAIL REQUEST
Username
Password
SSN
Credit Card Number
I WILL NEVER ALLOW SCAMMERS TO STEAL MY PRECIOUS IDENTITY!

Embedded training evaluation

- **Lab study compared two prototype interventions to standard security notice emails from Ebay and PayPal**
  - Existing practice of security notices is ineffective
  - Diagram intervention somewhat better
  - Comic strip intervention worked best
  - Interventions most effective when based on real brands

How do we know whether security is usable?

Need to observe users

- We are not our users!

(you may be surprised by what users really do)

Wireless privacy study

- Many users unaware that communications over wireless computer networks are not private
- How can we raise awareness?

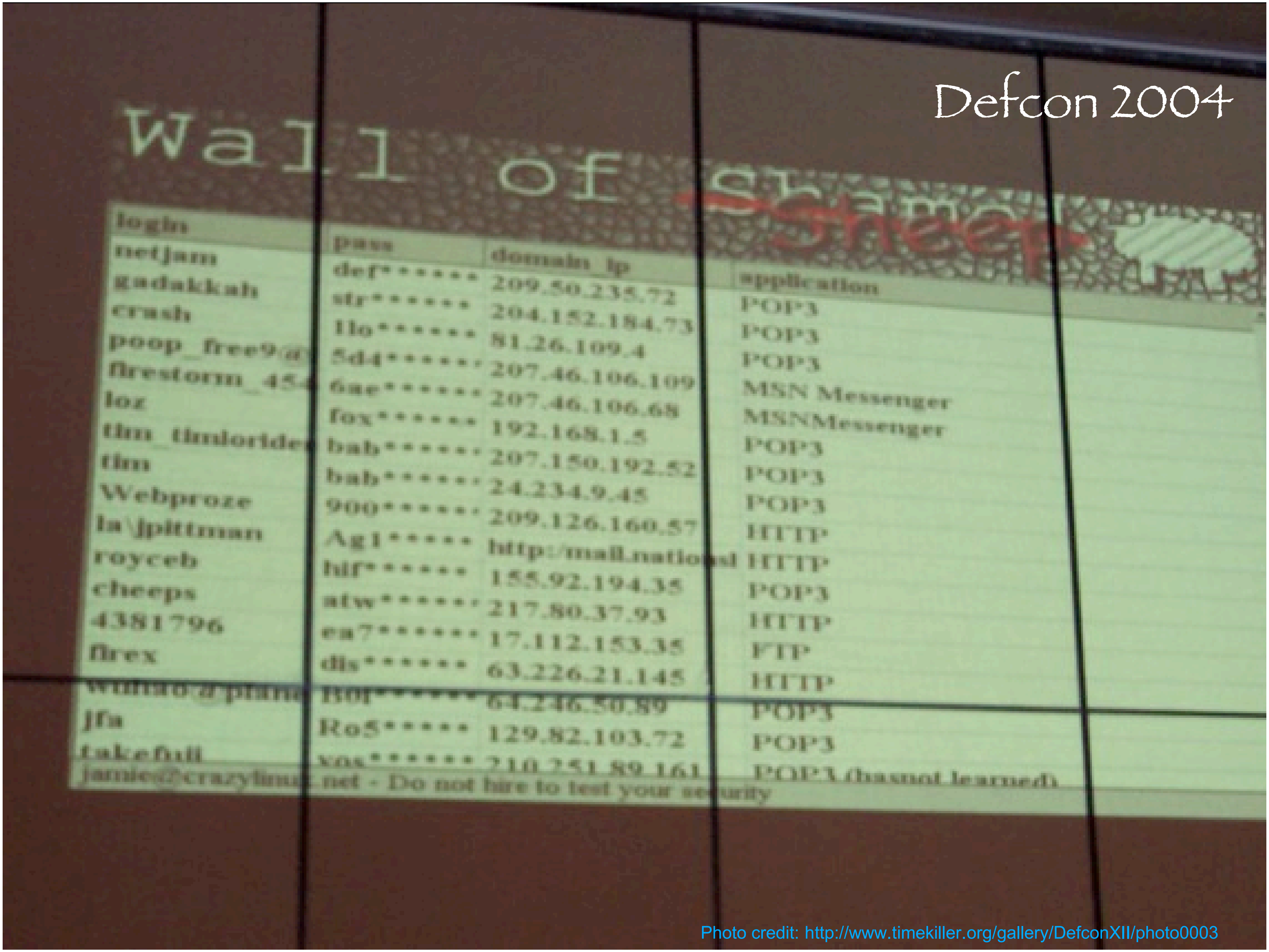
B. Kowitz and L. Cranor. **Peripheral Privacy Notifications for Wireless Networks.** In *Proceedings of the 2005 Workshop on Privacy in the Electronic Society*, 7 November 2005, Alexandria, VA.

Wall of sheep

Defcon 2001

Photo credit: Kyoorius @ techfreakz.org http://www.techfreakz.org/defcon10/?slide=38

Defcon 2004



login	pass	domain_ip	application
netjam	def*******	209.50.235.72	POP3
gadakkah	stf*******	204.152.184.73	POP3
crash	1lo*******	81.26.109.4	POP3
poop_free9@	5d4*******	207.46.106.109	MSN Messenger
firestorm_454	6ae*******	207.46.106.68	MSNMessenger
loz	fox*******	192.168.1.5	POP3
tim_timloride	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	hif*******	155.92.194.35	POP3
cheeps	atw*******	217.80.37.93	HTTP
4381796	ea7*******	17.112.153.35	FTP
firex	dis*******	63.226.21.145	HTTP
wuhao@plane	Boj*******	64.246.50.89	POP3
jfa	Ro5******	129.82.103.72	POP3
takefull	xos*******	210.251.89.161	POP3 (hasnot learned)

jamie@crazylinux.net - Do not hire to test your security

Photo credit: http://www.timekiller.org/gallery/DefconXII/photo0003

Peripheral display

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

network
privacy
wireless

Experimental trial

- Eleven 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

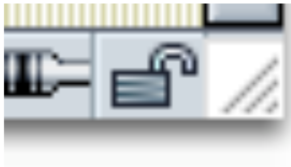
Privacy awareness increased

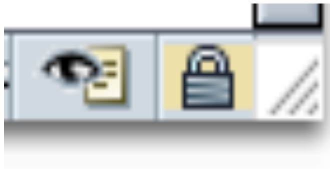
“I feel like my information /activity / privacy are not being protected …. seems like someone can monitor or get my information from my computer, or even publish them.”

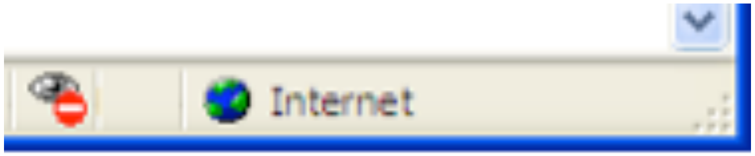
But only while the display was on

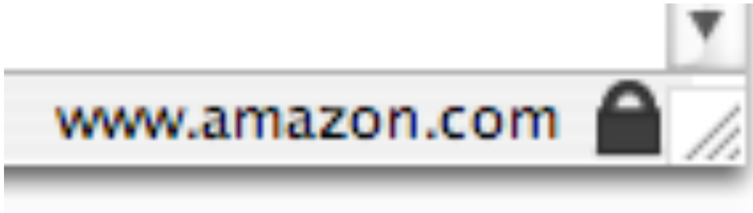
“Now that words [projected on the wall] are gone, I'll go back to the same.”

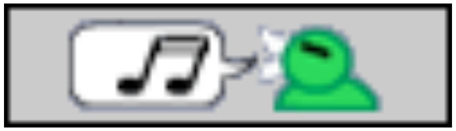
Security and privacy indicators

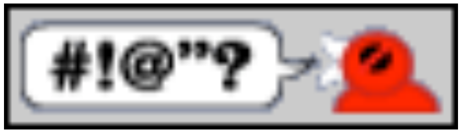


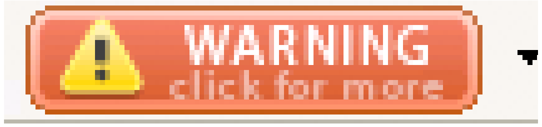










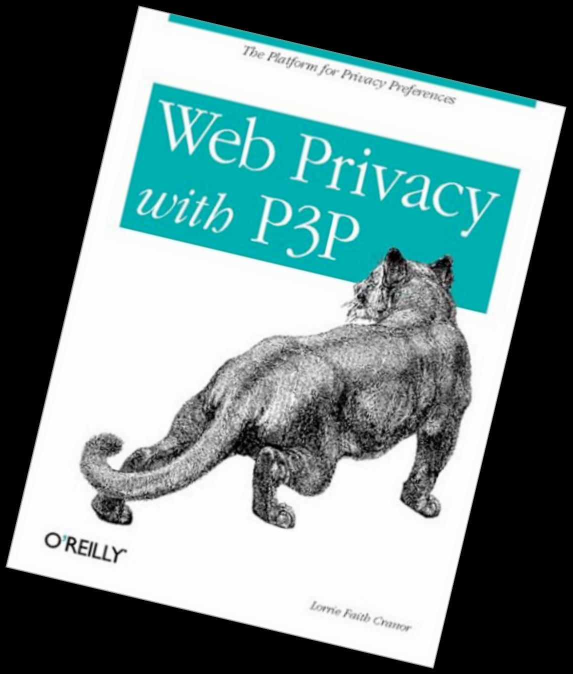


Evaluating indicators

- Case study: Privacy Bird

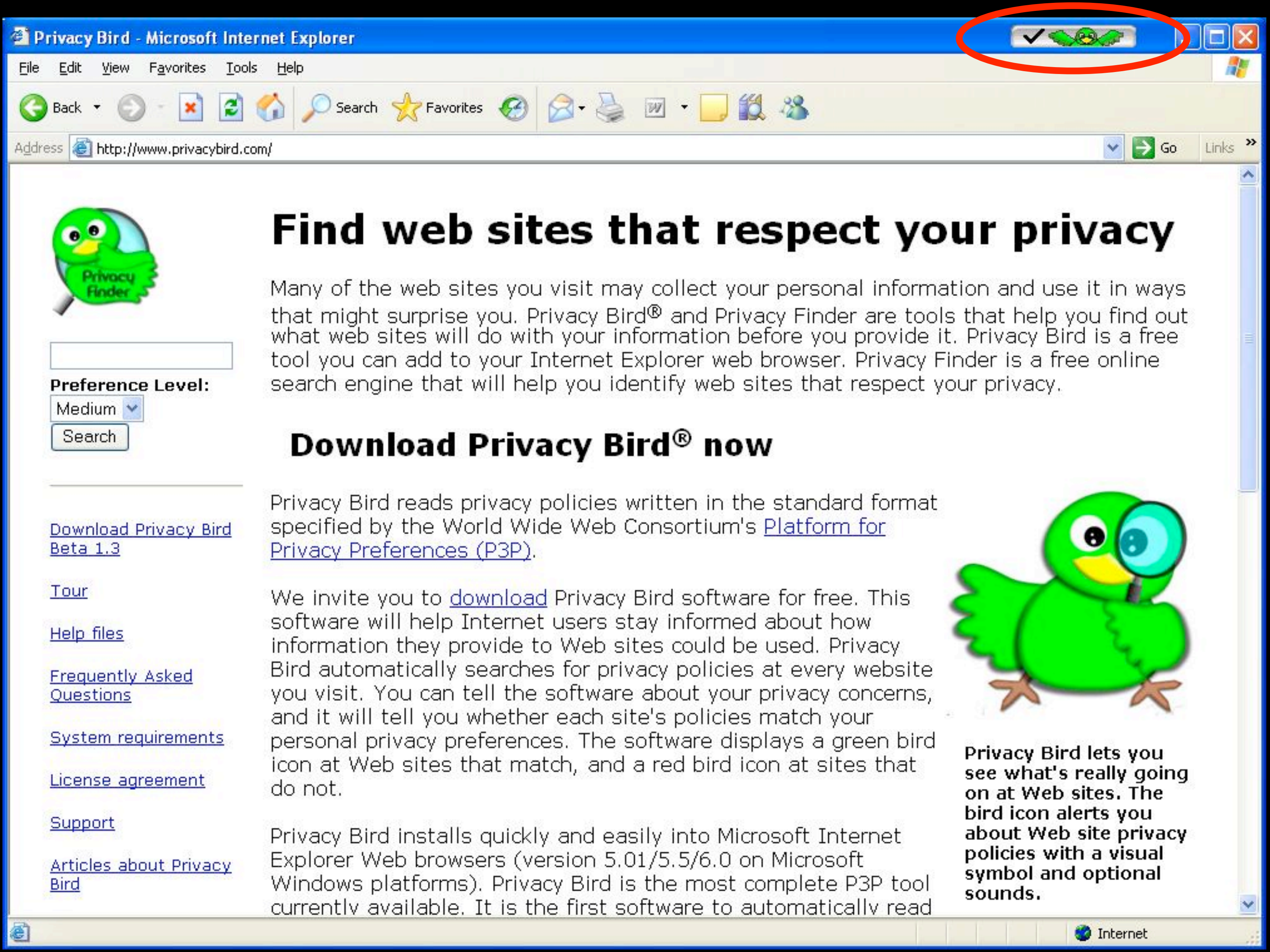
Platform for Privacy Preferences (P3P)

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



Privacy Bird

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



Find web sites that respect your privacy

Many of the web sites you visit may collect your personal information and use it in ways that might surprise you. Privacy Bird® and Privacy Finder are tools that help you find out what web sites will do with your information before you provide it. Privacy Bird is a free tool you can add to your Internet Explorer web browser. Privacy Finder is a free online search engine that will help you identify web sites that respect your privacy.

Preference Level: Medium

Search

- Download Privacy Bird Beta 1.3
- Tour
- Help files
- Frequently Asked Questions
- System requirements
- License agreement
- Support
- Articles about Privacy Bird

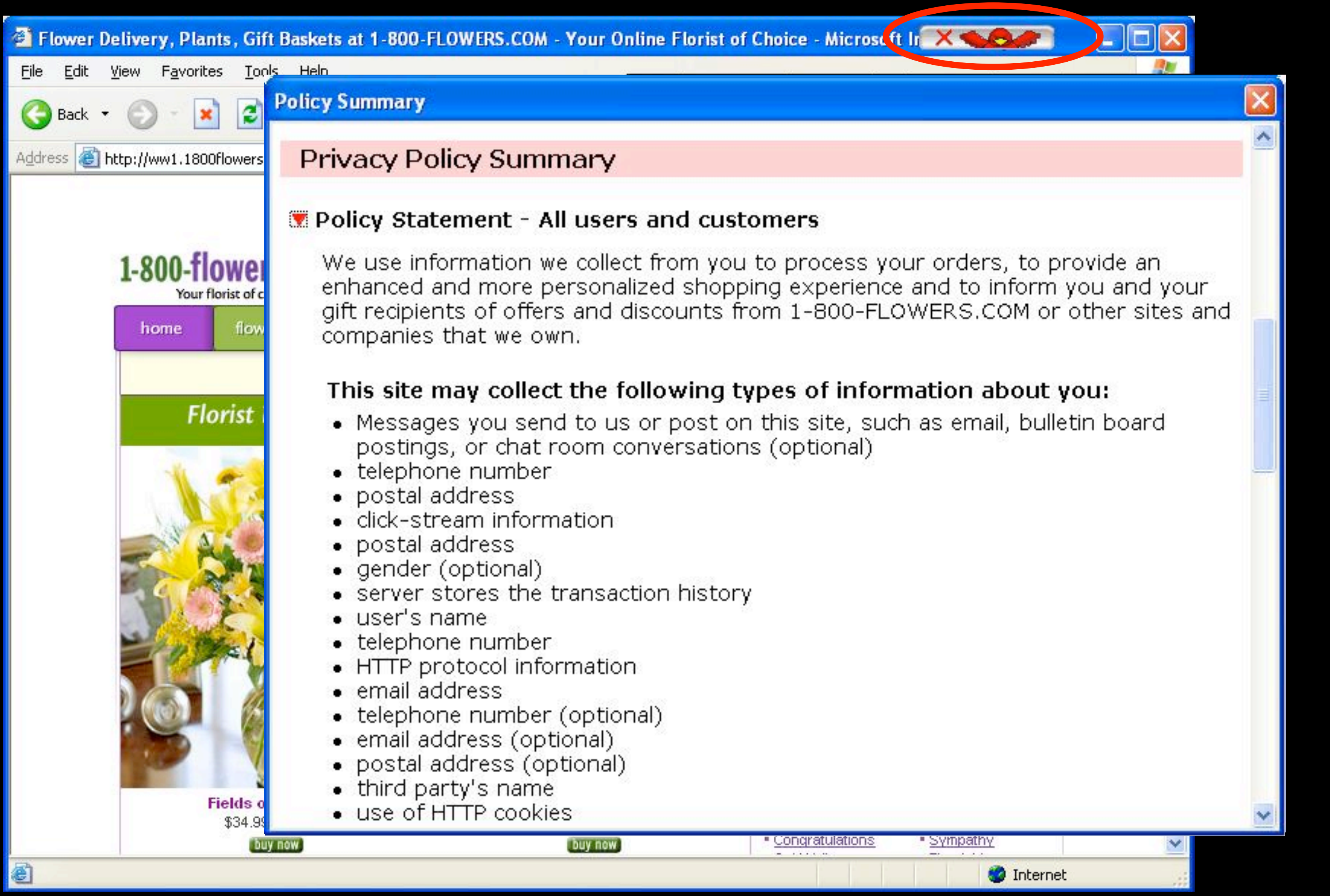
Download Privacy Bird® now

Privacy Bird reads privacy policies written in the standard format specified by the World Wide Web Consortium's Platform for Privacy Preferences (P3P).

We invite you to download Privacy Bird software for free. This software will help Internet users stay informed about how information they provide to Web sites could be used. Privacy Bird automatically searches for privacy policies at every website you visit. You can tell the software about your privacy concerns, and it will tell you whether each site's policies match your personal privacy preferences. The software displays a green bird icon at Web sites that match, and a red bird icon at sites that do not.

Privacy Bird installs quickly and easily into Microsoft Internet Explorer Web browsers (version 5.01/5.5/6.0 on Microsoft Windows platforms). Privacy Bird is the most complete P3P tool currently available. It is the first software to automatically read

Privacy Bird lets you see what's really going on at Web sites. The bird icon alerts you about Web site privacy policies with a visual symbol and optional sounds.


Flower Delivery, Plants, Gift Baskets at 1-800-FLOWERS.COM - Your Online Florist of Choice - Microsoft In
File Edit View Favorites Tools Help
Back
Address http://ww1.1800flowers
1-800-flowe
Your florist of c
home
flow
Florist
Fields o
$34.9
buy now
buy now
Congratulations
Sympathy
Internet
Policy Summary

Privacy Policy Summary

Policy Statement - All users and customers

We use information we collect from you to process your orders, to provide an enhanced and more personalized shopping experience and to inform you and your gift recipients of offers and discounts from 1-800-FLOWERS.COM or other sites and companies that we own.

This site may collect the following types of information about you:

- Messages you send to us or post on this site, such as email, bulletin board postings, or chat room conversations (optional)
- telephone number
- postal address
- click-stream information
- postal address
- gender (optional)
- server stores the transaction history
- user's name
- telephone number
- HTTP protocol information
- email address
- telephone number (optional)
- email address (optional)
- postal address (optional)
- third party's name
- use of HTTP cookies

Critique Privacy Bird

- Security people
  - Can attackers spoof it?
  - What if P3P policy contains lies?
  - Can P3P policies be digitally signed?
  - What about main-in-the-middle attacks?

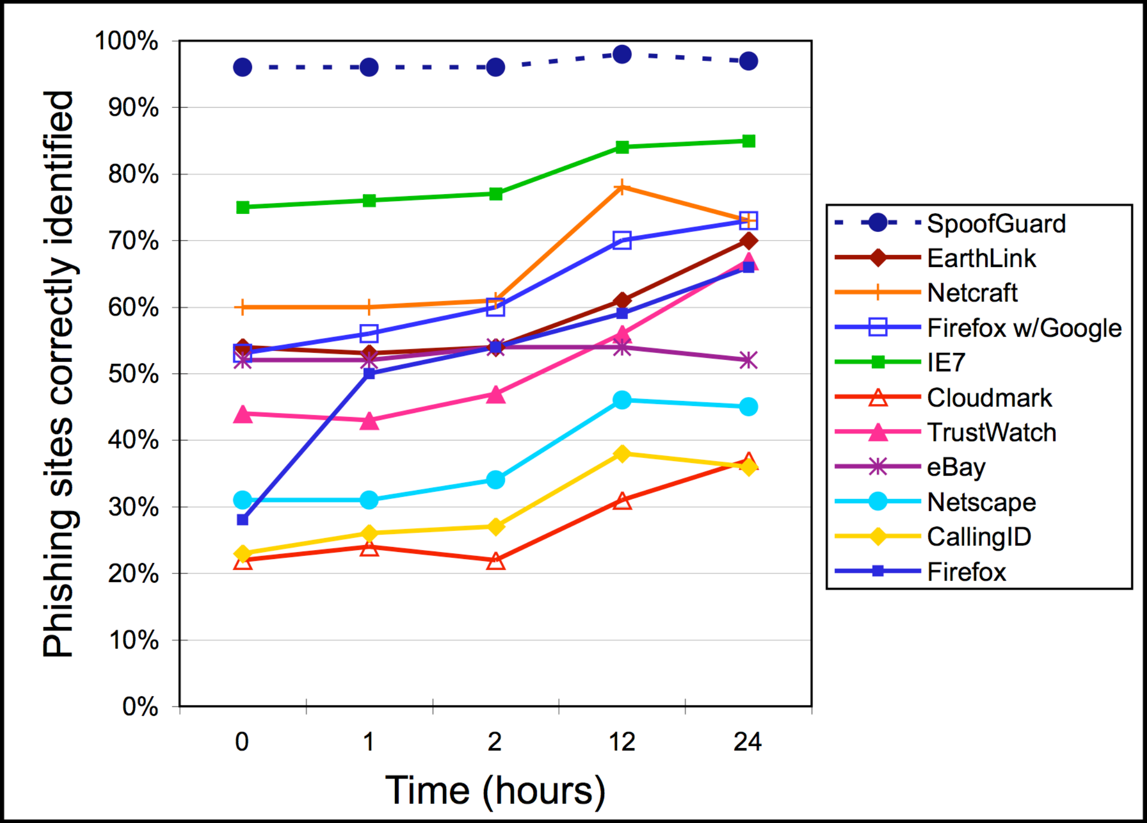
- Usability people
  - Green/red color blind problem
  - Do people notice it in corner of browser?
  - Do people understand privacy implications?
  - Why a bird?

Typical security evaluation

Does it behave correctly when *not* under attack?

- No false positives or false negatives

Anti-phishing tools

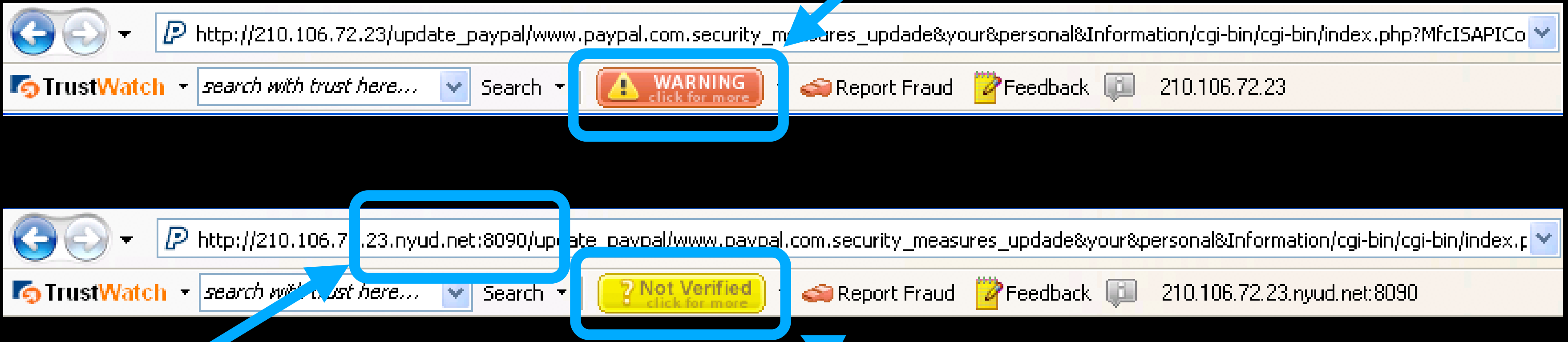


Y. Zhange, S. Egelman, L. Cranor, and J. Hong. **Phinding Phish: Evaluating Anti-Phishing Tools.** In *Proceedings of NSSS 2006*, forthcoming.

Does it behave correctly when under attack?

- Can attackers cause wrong indicator to appear?

Correct indicator


http://210.106.72.23/update_paypal/www.paypal.com.security_m ures_updade&your&personal&Information/cgi-bin/cgi-bin/index.php?MfcISAPICo

search with trust here...

210.106.72.23

http://210.106.7 .23.nyud.net:8090/up ate_paypal/www.paypal.com.security_measures_updade&your&personal&Information/cgi-bin/cgi-bin/index.p

search wi ust here...

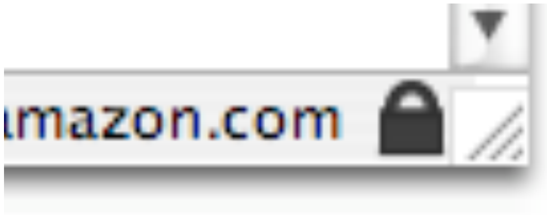
210.106.72.23.nyud.net:8090

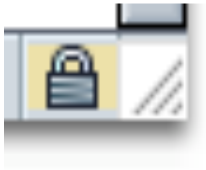
Wrong indicator

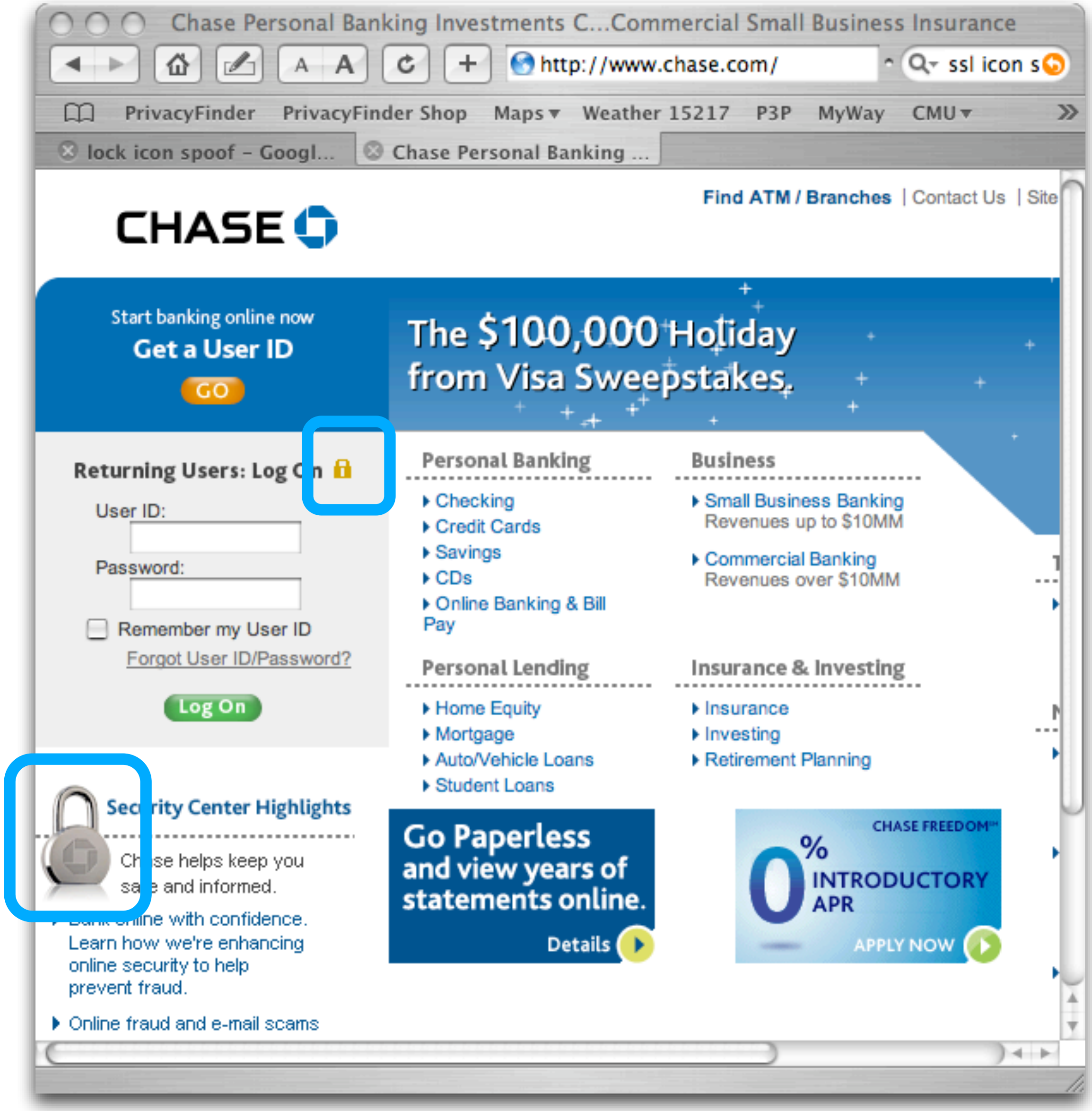
Attacker redirects through CDN

Can it be spoofed or obscured?

- Can attacker provide indicator users will rely on instead of real indicator?







Start banking online now

Get a User ID

The $100,000 Holiday from Visa Sweepstakes.

Returning Users: Log On

User ID:

Password:

□ Remember my User ID

Forgot User ID/Password?

Security Center Highlights

Chase helps keep you safe and informed.

- Bank online with confidence. Learn how we're enhancing online security to help prevent fraud.
- Online fraud and e-mail scams

Personal Banking

- Checking
- Credit Cards
- Savings
- CDs
- Online Banking & Bill Pay

Business

- Small Business Banking
Revenues up to $10MM
- Commercial Banking
Revenues over $10MM

Personal Lending

- Home Equity
- Mortgage
- Auto/Vehicle Loans
- Student Loans

Insurance & Investing

- Insurance
- Investing
- Retirement Planning

Go Paperless and view years of statements online.

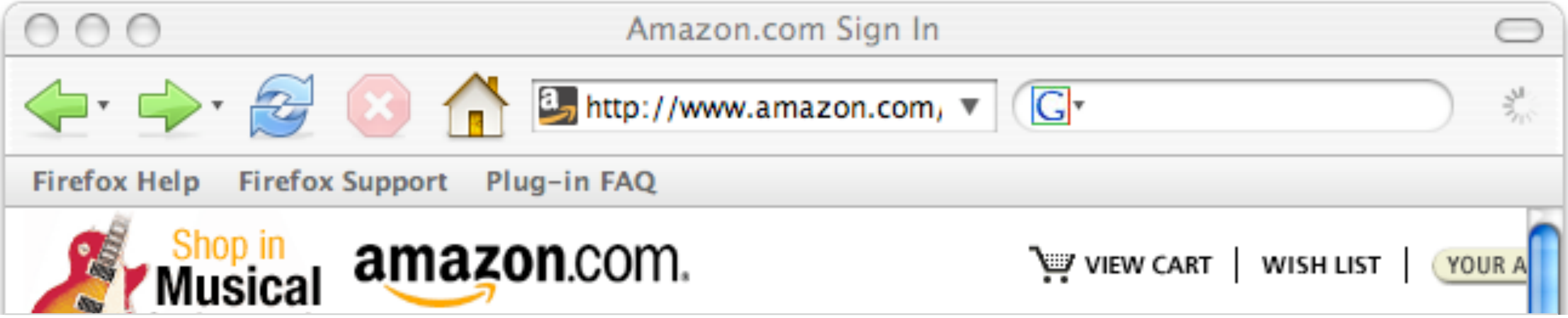
CHASE FREEDOM℠

0% INTRODUCTORY APR

Usability evaluation

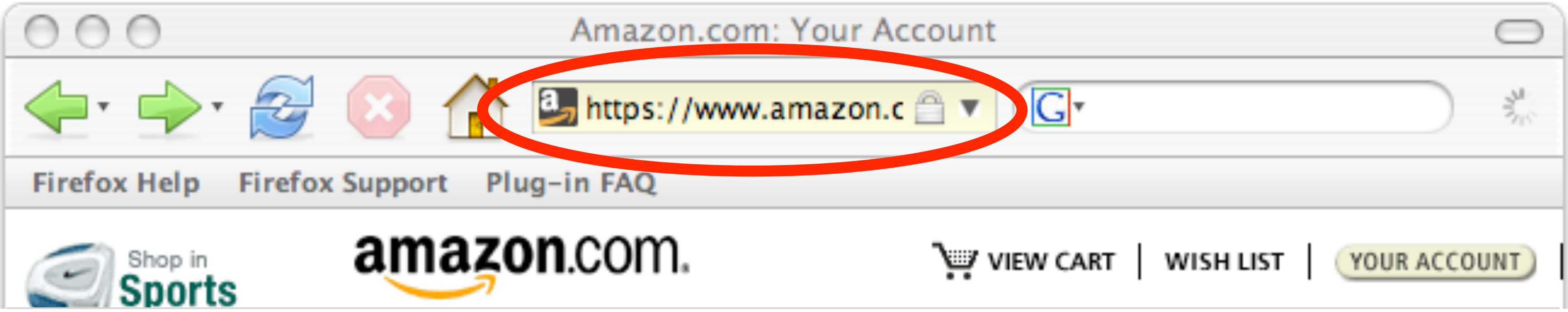
Do users notice it?

- If users don’t notice indicator all bets are off
- “What lock icon?”
    - Few users notice lock icon in browser chrome, https, etc.



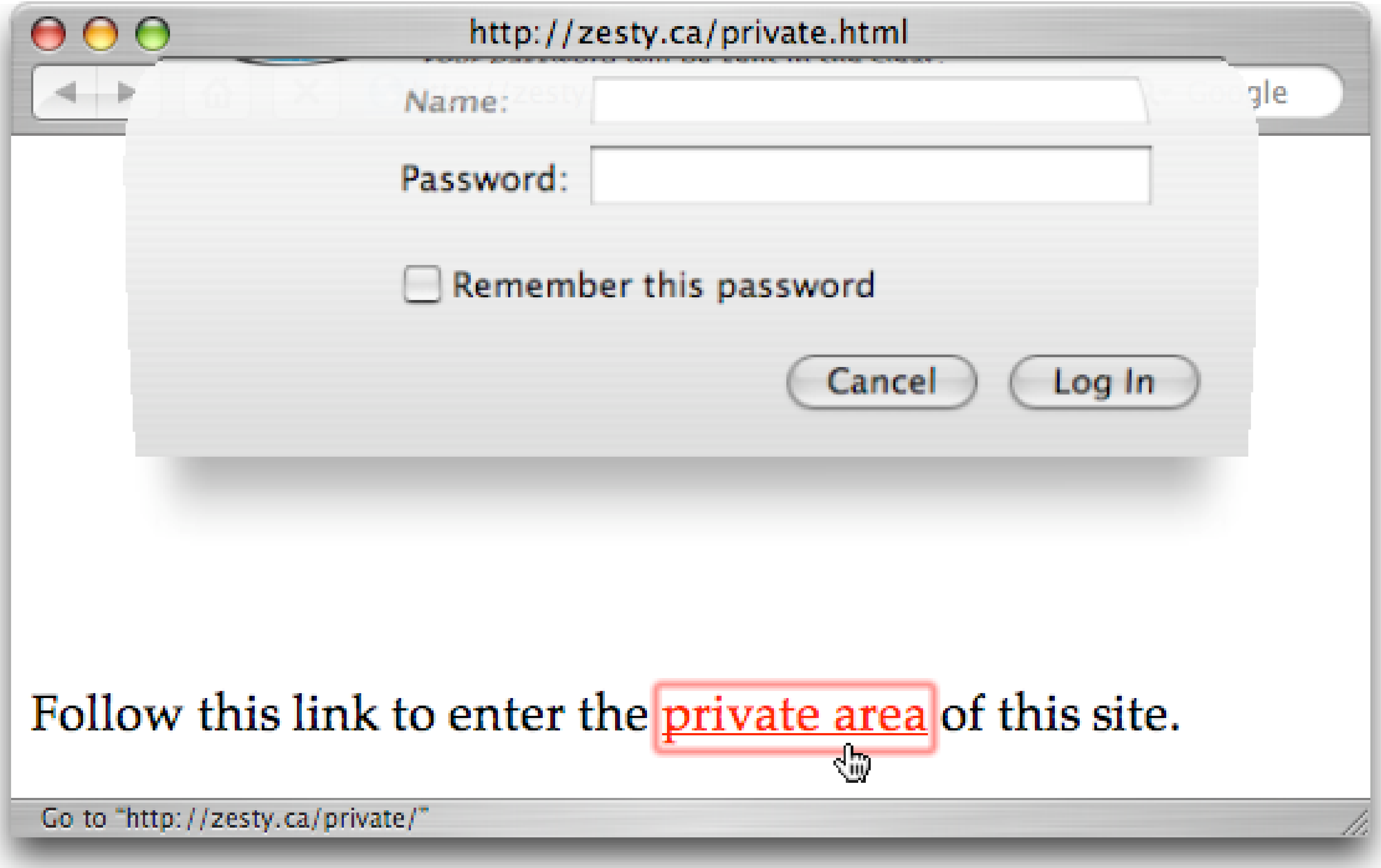
Amazon.com Sign In

http://www.amazon.com,



Amazon.com: Your Account

https://www.amazon.c



http://zesty.ca/private.html

Follow this link to enter the private area of this site.

Go to "http://zesty.ca/private/"

Do users know what it means?

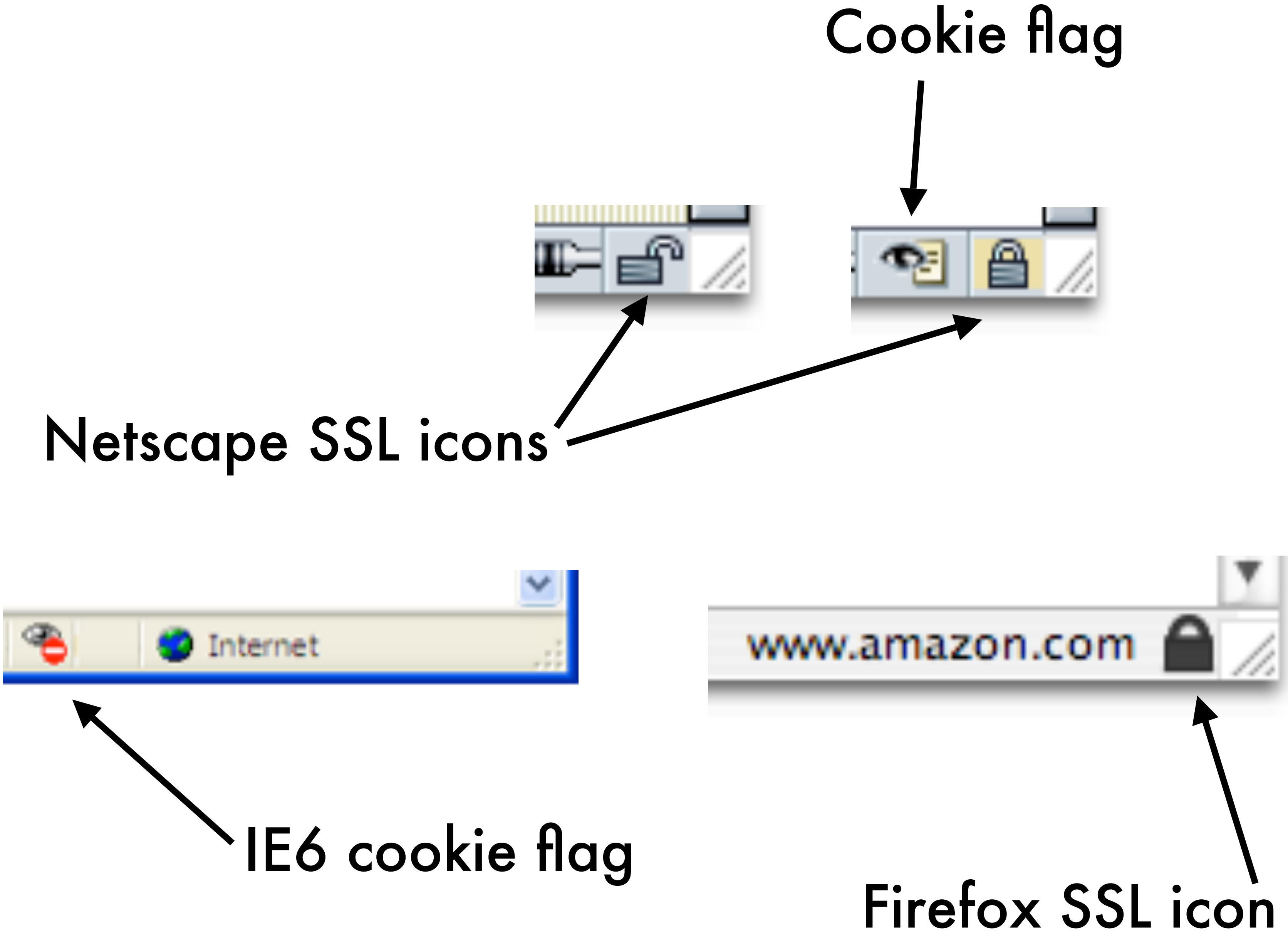
Web browser lock icon:

> "I think that it means secured, it symbolizes some kind of security, somehow."

Web browser security pop-up:

> "Yeah, like the certificate has expired. I don't actually know what that means."

J. Downs, M. Holbrook, and L. Cranor. **Decision Strategies and Susceptibility to Phishing.** In *Proceedings of the 2006 Symposium On Usable Privacy and Security*, 12-14 July 2006, Pittsburgh, PA.



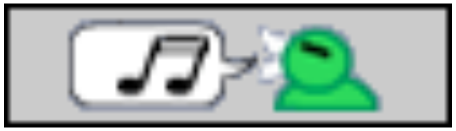
Cookie flag

Netscape SSL icons

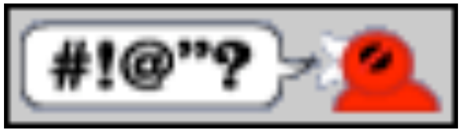
IE6 cookie flag

Firefox SSL icon

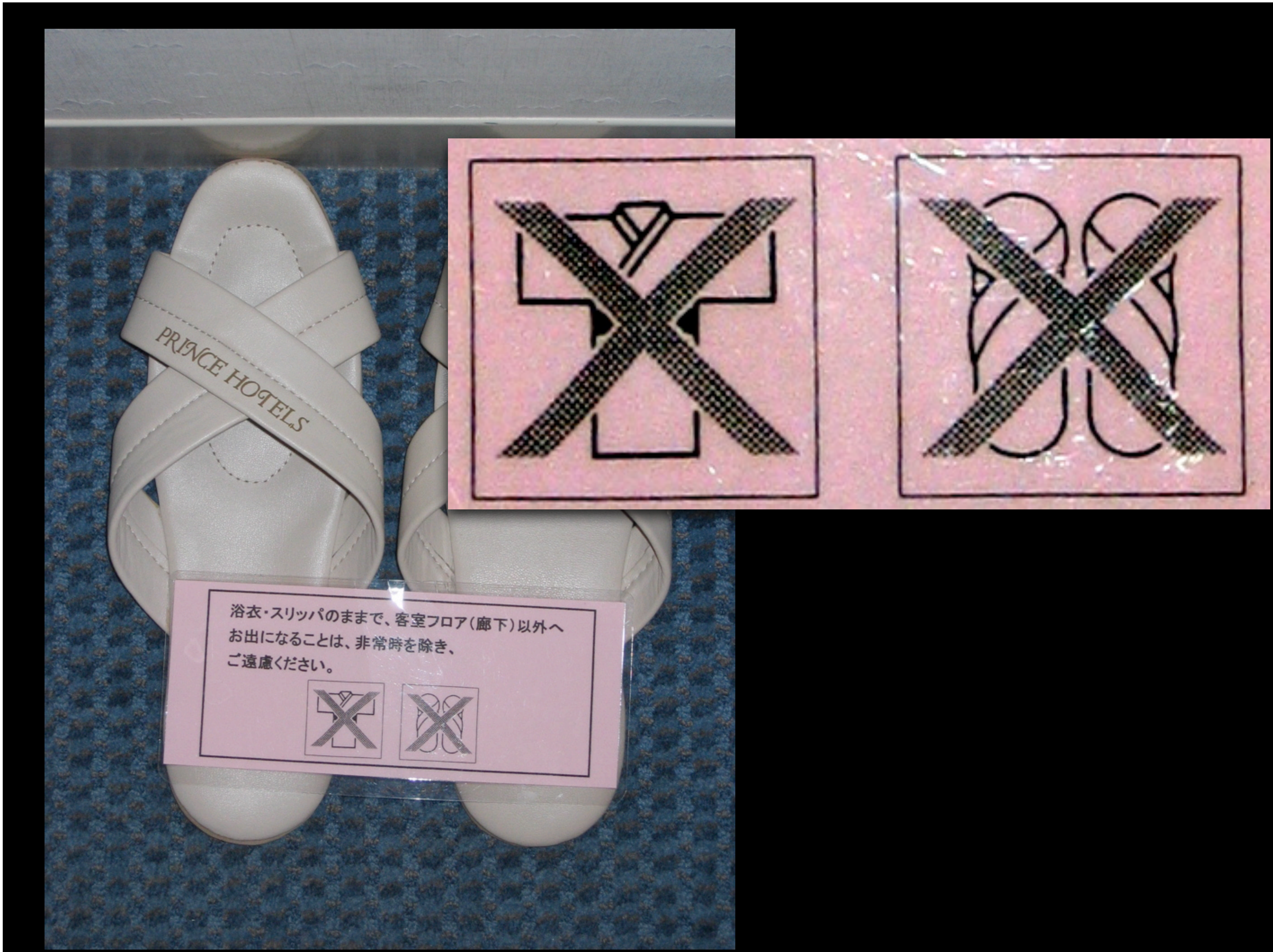
Privacy Bird icons



Privacy policy ***__matches__*** user's privacy preferences

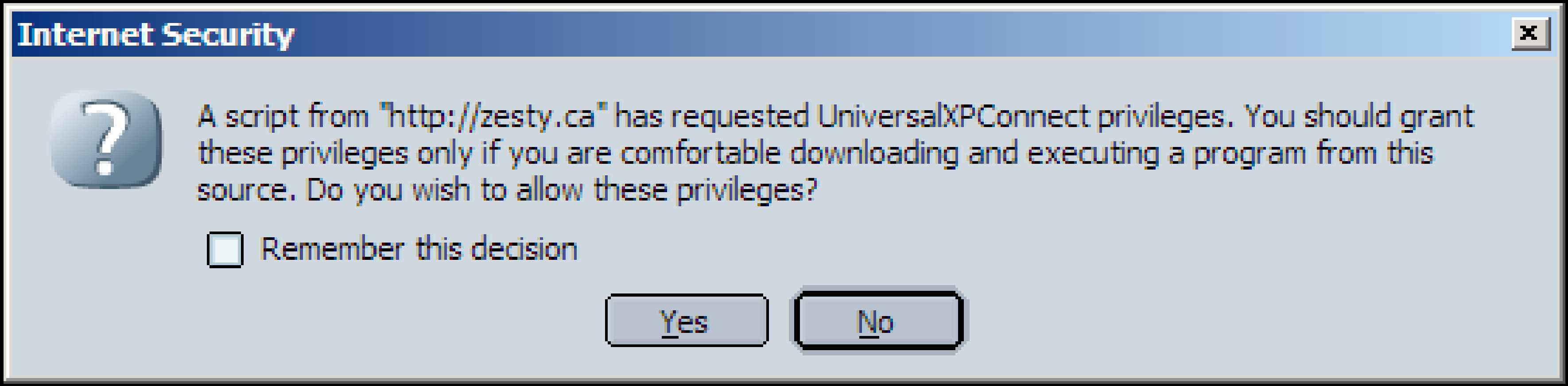


Privacy policy ***__does not match__*** user's privacy preferences



浴衣・スリッパのままで、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。

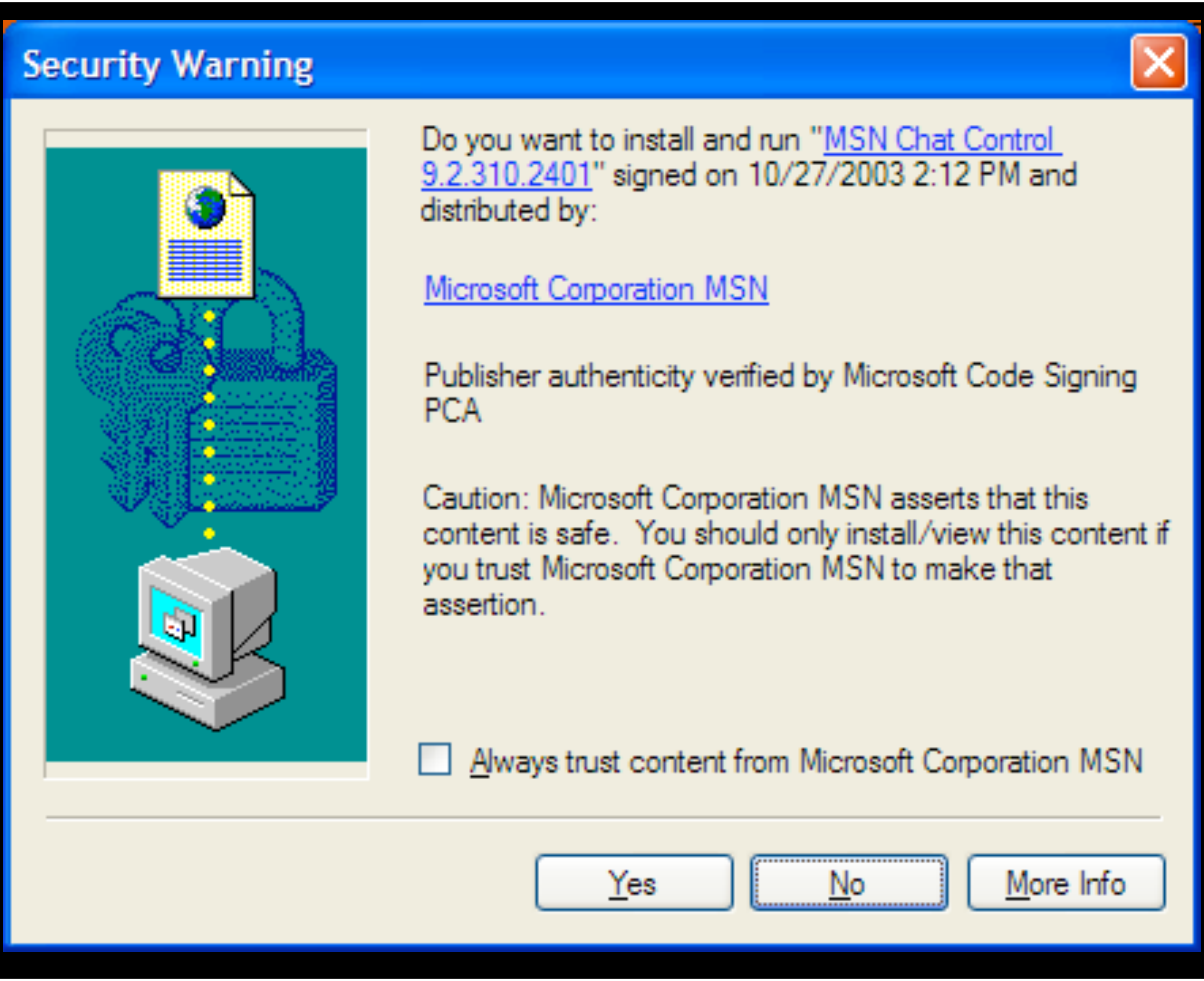
Do users know what to do when they see it?



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



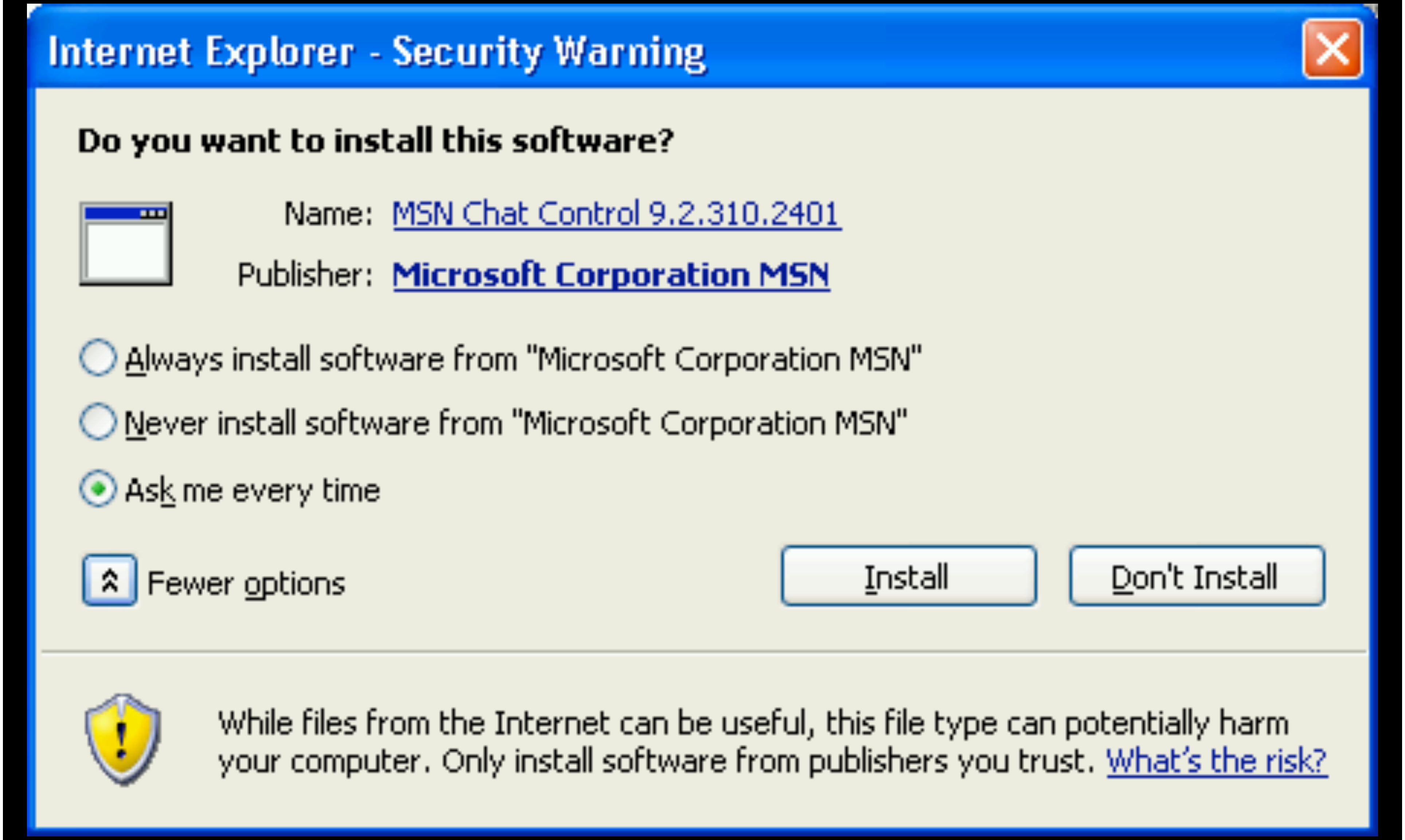
Do you want to install and run "MSN Chat Control 9.2.310.2401" signed on 10/27/2003 2:12 PM and distributed by:

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



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

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?

Do they actually do it?

“I would probably experience some brief, vague sense of unease and close the box and go about my business.”

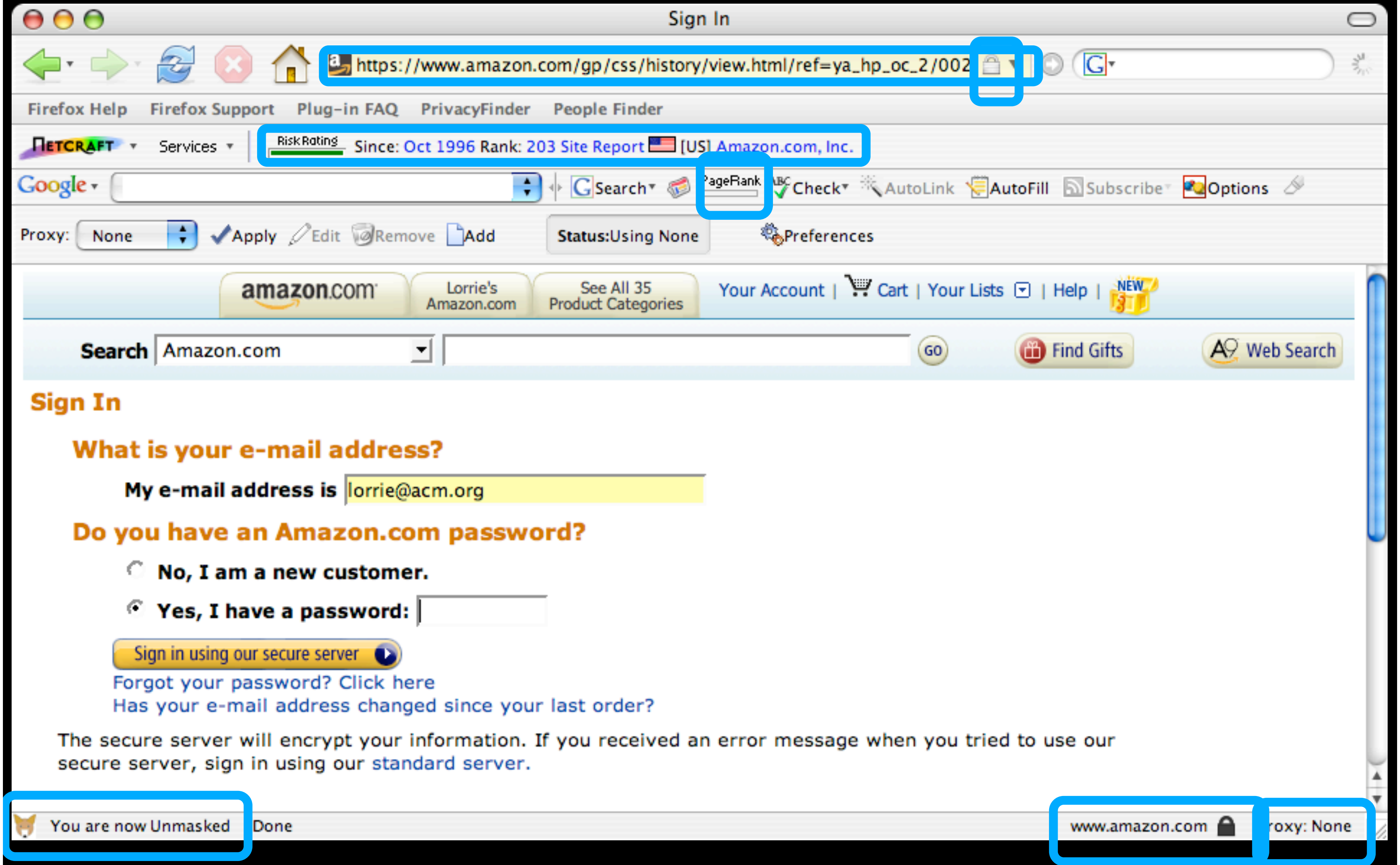
DO NOT
PICK
UP
VIRUSES

Do they keep doing it?

- Difficult to measure in laboratory setting
- Need to collect data on users in natural environment over extended period of time

How does it interact with other indicators?

- Indicator overload?



Sign In

What is your e-mail address?

My e-mail address is lorrie@acm.org

Do you have an Amazon.com password?

○ **No, I am a new customer.**

● **Yes, I have a password:**

Sign in using our secure server

Forgot your password? Click here

Has your e-mail address changed since your last order?

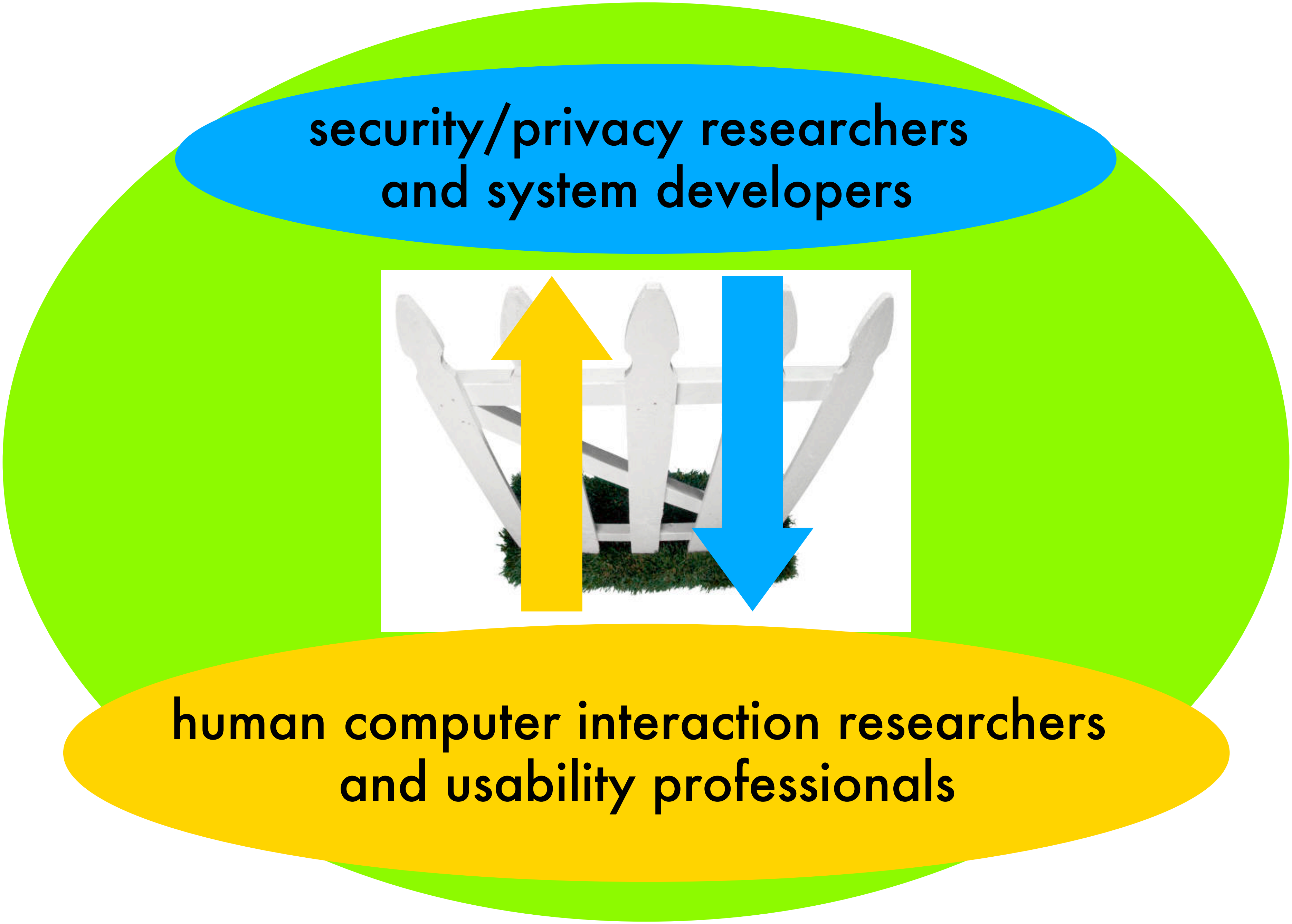
The secure server will encrypt your information. If you received an error message when you tried to use our secure server, sign in using our standard server.

Security evaluation

- Does indicator behave correctly when not under attack?
  - No false positives or false negatives
- Does indicator behave correctly when under attack?
  - Can attackers cause wrong indicator to appear?
- Can indicator be spoofed or obscured?
  - Can attacker provide indicator users will rely on instead of real indicator?

Questions to ask

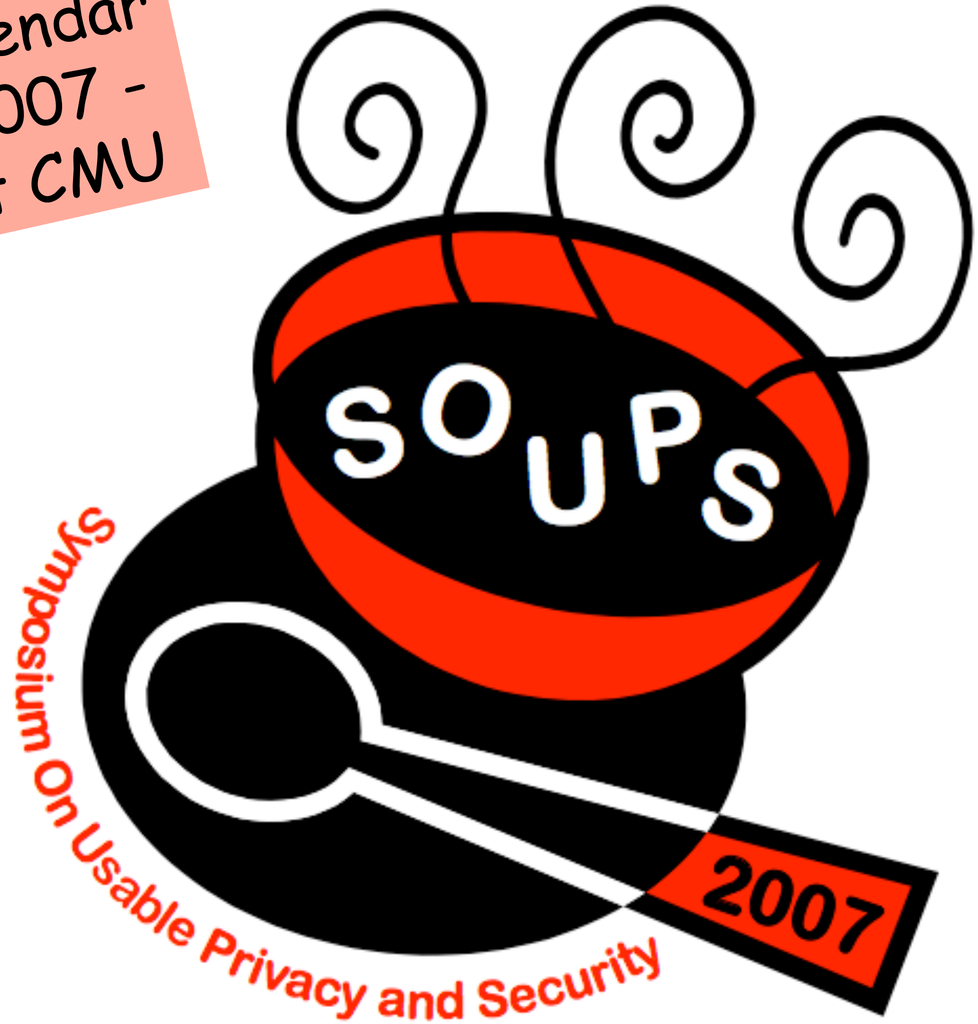
- Do users notice it?
- Do they know what it means?
- Do they know what they are supposed to do when they see it?
- Will they actually do it?
- Will they keep doing it?
- How does it interact with other indicators?



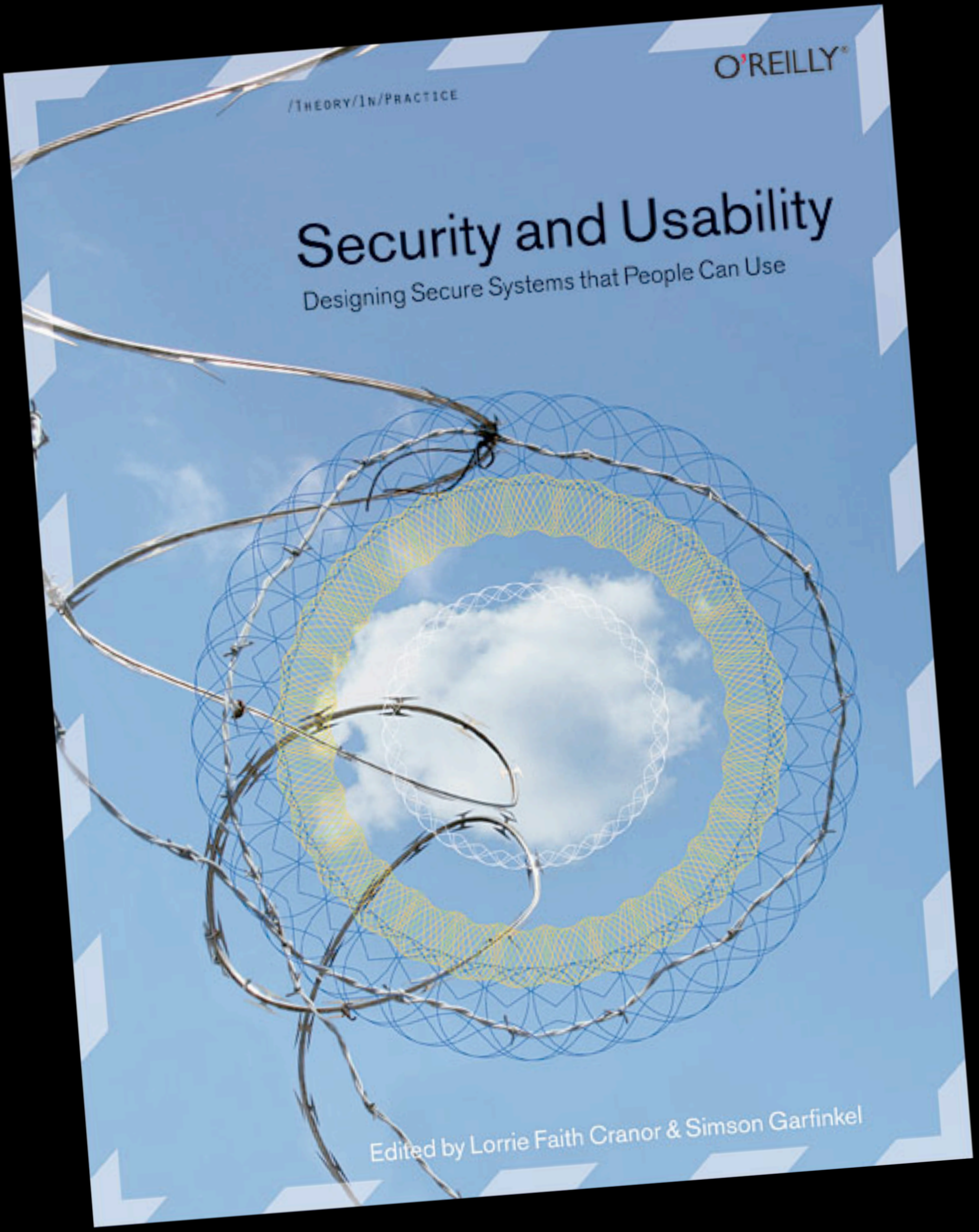
security/privacy researchers and system developers

human computer interaction researchers and usability professionals

Mark your calendar for SOUPS 2007 - July 18-20 at CMU



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



O'REILLY®

/THEORY/IN/PRACTICE

Security and Usability

Designing Secure Systems that People Can Use

Edited by Lorrie Faith Cranor & Simson Garfinkel

CMU Usable Privacy and Security Laboratory

http://cups.cs.cmu.edu/

Carnegie Mellon