7 Flaws of Identity Management: Usability and Security Challenges

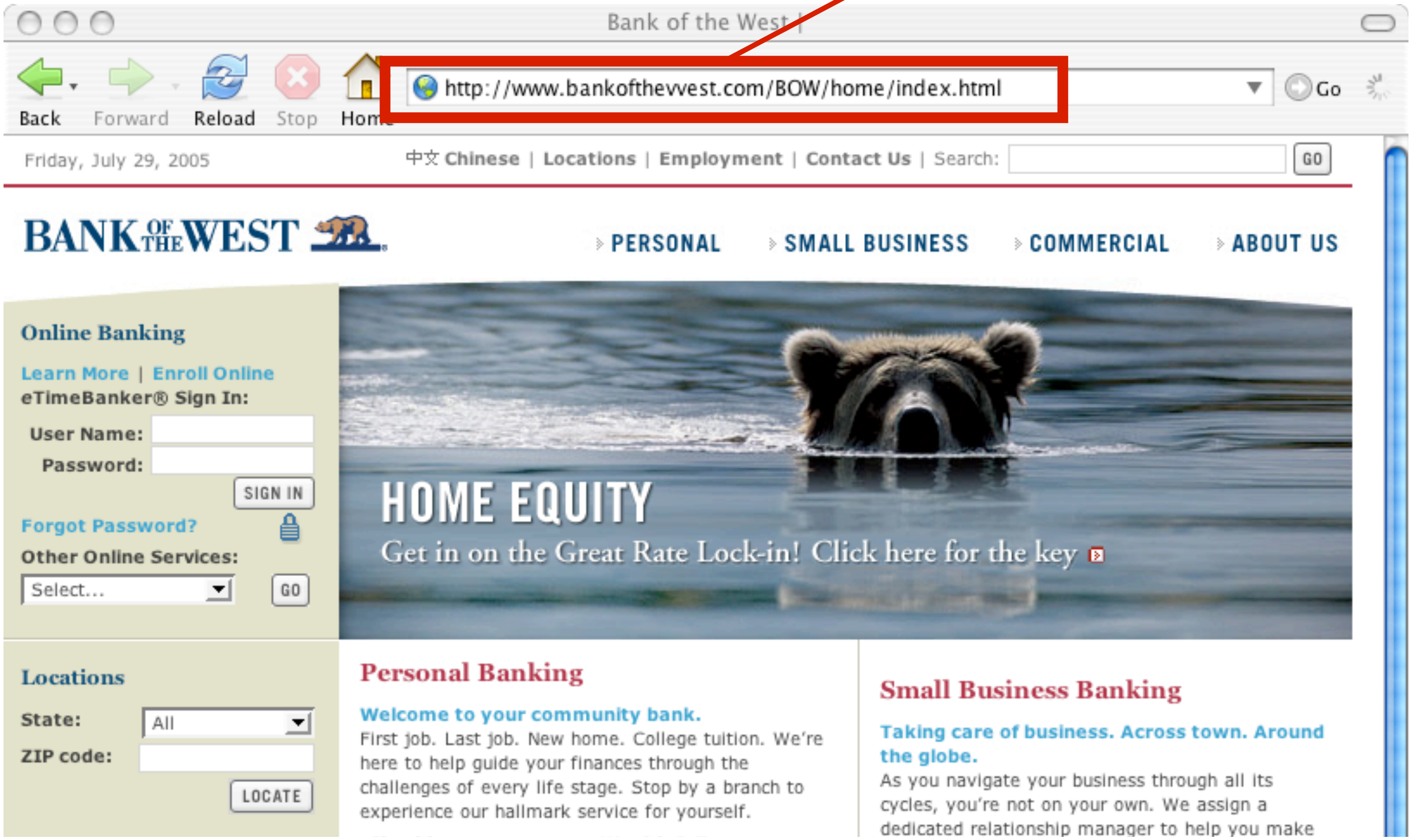
Rachna Dhamija
Harvard University
and CommerceNet

joint work with
Lisa Dusseault, CommerceNet

Outline

- Why Phishing Works study
- Bank of America SiteKey study
- Usability Challenges for Identity Management

www.bankofthevvest.com



http://www.bankofthevvest.com/BOW/home/index.html

Friday, July 29, 2005

中文 Chinese | Locations | Employment | Contact Us | Search: GO

BANK OF THE WEST

PERSONAL SMALL BUSINESS COMMERCIAL ABOUT US

Online Banking

Learn More | Enroll Online

eTimeBanker® Sign In:

User Name:

Password:

SIGN IN

Forgot Password?

Other Online Services:

Select... GO

Locations

State: All

ZIP code:

LOCATE

HOME EQUITY

Get in on the Great Rate Lock-in! Click here for the key

Personal Banking

Welcome to your community bank.

First job. Last job. New home. College tuition. We're here to help guide your finances through the challenges of every life stage. Stop by a branch to experience our hallmark service for yourself.

Small Business Banking

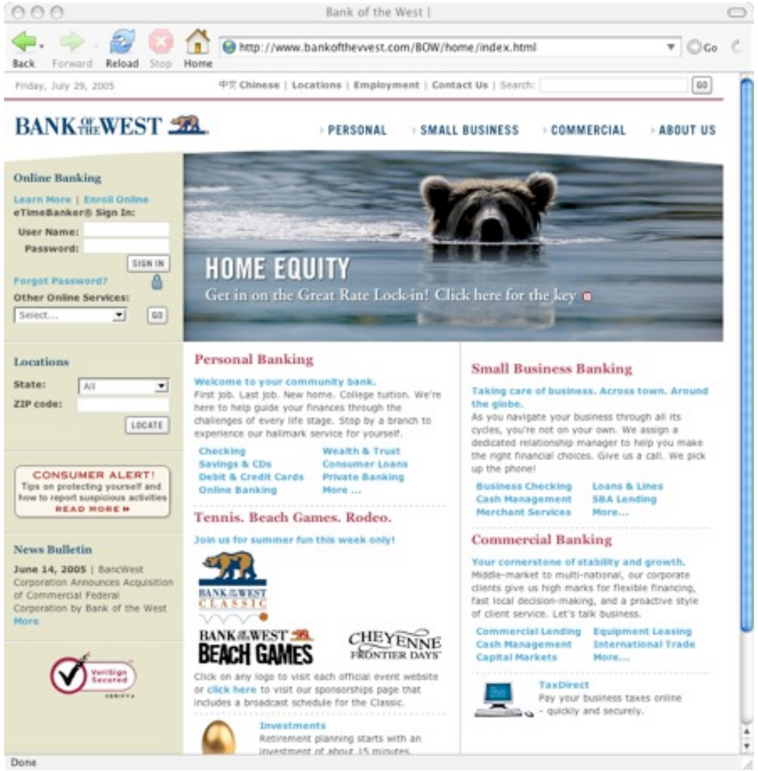
Taking care of business. Across town. Around the globe.

As you navigate your business through all its cycles, you're not on your own. We assign a dedicated relationship manager to help you make

Why Phishing Works
(Dhamija, Tygar CHI 2006)

- *Why* do users fall for phishing attacks?

- 22 users viewed 20 websites
  - Phishing & legitimate websites
  - Asked to think aloud
  - Is this a real or phishing website? Why or why not? How confident are you?



http://www.bankofthevvest.com/BOW/home/index.html

Friday, July 29, 2005

HOME EQUITY

Get in on the Great Rate Lock-in! Click here for the key

Online Banking

Learn More | Enroll Online

eTimeBanker® Sign In:

User Name:

Password:

Forgot Password?

Other Online Services:

Locations

State: All

ZIP code:

CONSUMER ALERT! Tips on protecting yourself and how to report suspicious activities READ MORE »

News Bulletin

June 14, 2005 | BancWest Corporation Announces Acquisition of Commercial Federal Corporation by Bank of the West More

Personal Banking

Welcome to your community bank.

First job. Last job. New home. College tuition. We're here to help guide your finances through the challenges of every life stage. Stop by a branch to experience our hallmark service for yourself.

Checking | Wealth & Trust
Savings & CDs | Consumer Loans
Debit & Credit Cards | Private Banking
Online Banking | More ...

Tennis. Beach Games. Rodeo.

Join us for summer fun this week only!

Click on any logo to visit each official event website or click here to visit our sponsorships page that includes a broadcast schedule for the Classic.

Investments

Retirement planning starts with an investment of about 15 minutes.

Small Business Banking

Taking care of business. Across town. Around the globe.

As you navigate your business through all its cycles, you're not on your own. We assign a dedicated relationship manager to help you make the right financial choices. Give us a call. We pick up the phone!

Business Checking | Loans & Lines
Cash Management | SBA Lending
Merchant Services | More...

Commercial Banking

Your cornerstone of stability and growth.

Middle-market to multi-national, our corporate clients give us high marks for flexible financing, fast local decision-making, and a proactive style of client service. Let's talk business.

Commercial Lending | Equipment Leasing
Cash Management | International Trade
Capital Markets | More...

TaxDirect

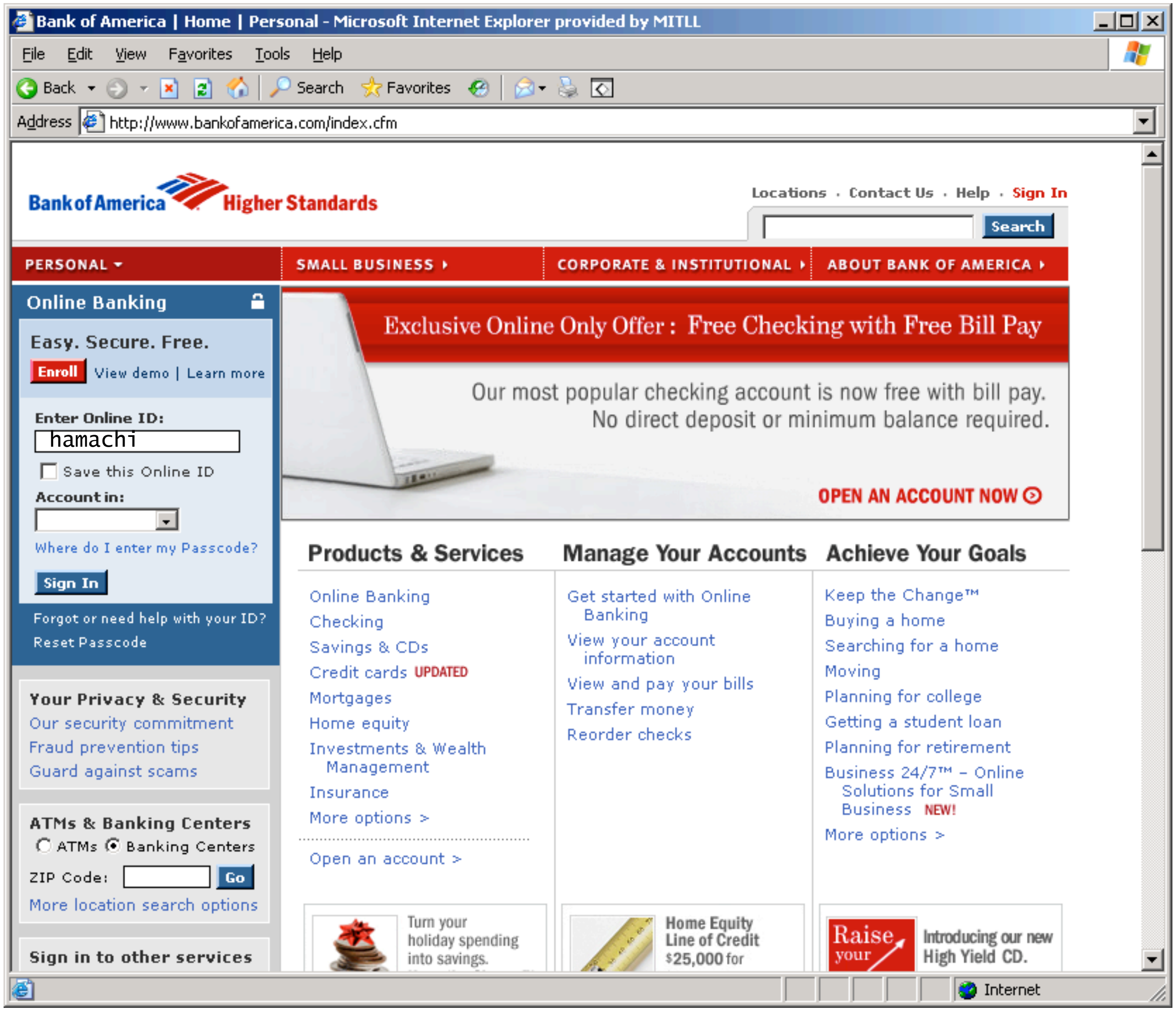
Pay your business taxes online - quickly and securely.

➜ Some good phishing sites fooled more than 90%

➜ 23% use only content of the page to make a determination
36% use content and URL

➜ Users ignore SSL, rely on the wrong indicators

Emperors New Security Indicators (IEEE Security & Privacy 2007)


Bank of America | Home | Personal - Microsoft Internet Explorer provided by MITLL
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Internet

http://www.bankofamerica.com/index.cfm

Bank of America Higher Standards

Locations · Contact Us · Help · Sign In

Search

PERSONAL | SMALL BUSINESS | CORPORATE & INSTITUTIONAL | ABOUT BANK OF AMERICA

Online Banking

Easy. Secure. Free.

Enroll | View demo | Learn more

1

Enter Online ID: hamachi

□ Save this Online ID

Account in:

Where do I enter my Passcode?

Sign In

Forgot or need help with your ID?

Reset Passcode

Your Privacy & Security

Our security commitment

Fraud prevention tips

Guard against scams

ATMs & Banking Centers

○ ATMs ● Banking Centers

ZIP Code: Go

More location search options

Sign in to other services

Exclusive Online Only Offer : Free Checking with Free Bill Pay

Our most popular checking account is now free with bill pay.
No direct deposit or minimum balance required.

OPEN AN ACCOUNT NOW

Products & Services

- Online Banking
- Checking
- Savings & CDs
- Credit cards UPDATED
- Mortgages
- Home equity
- Investments & Wealth Management
- Insurance
- More options >
- Open an account >

Manage Your Accounts

- Get started with Online Banking
- View your account information
- View and pay your bills
- Transfer money
- Reorder checks

Achieve Your Goals

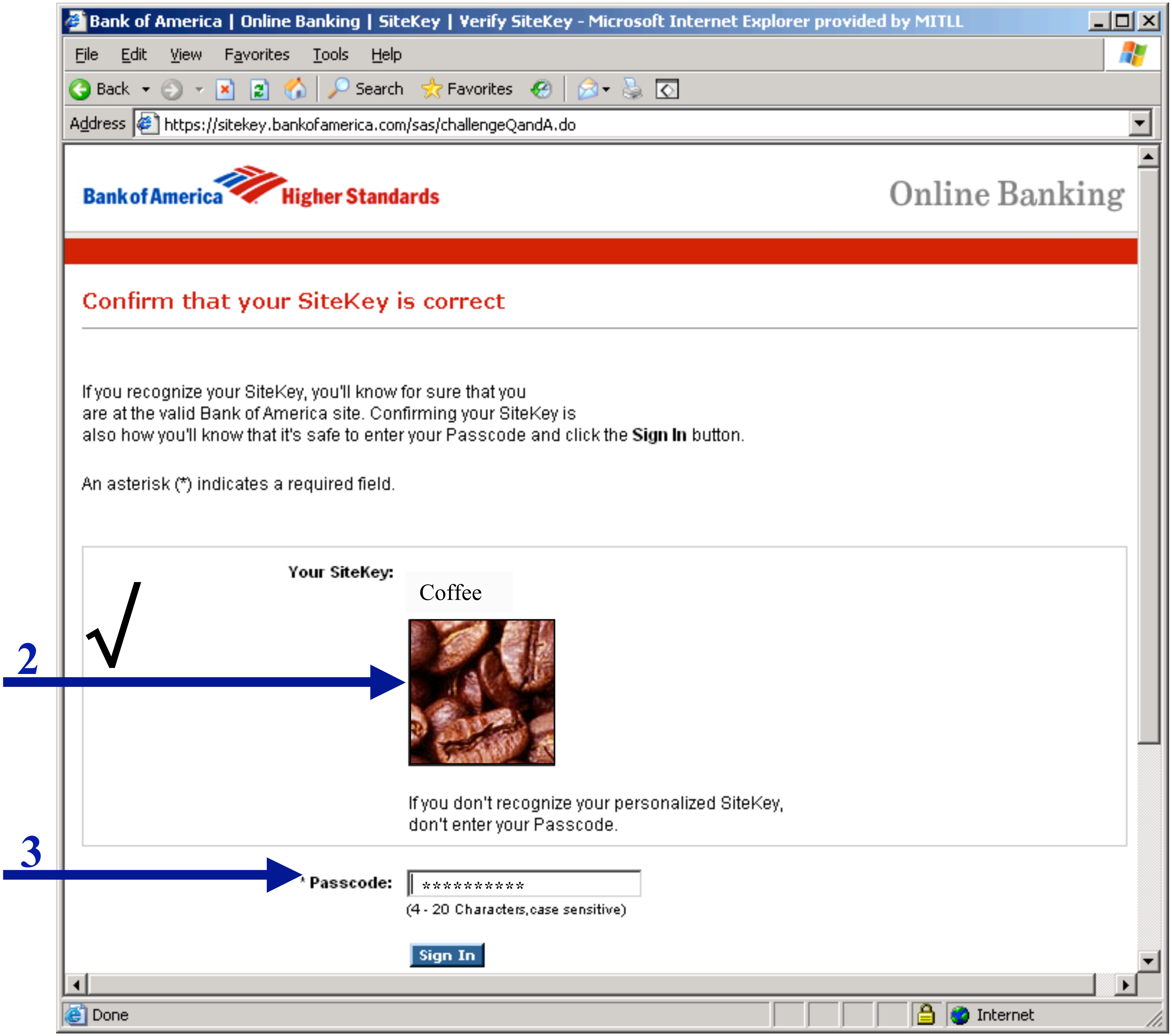
- Keep the Change™
- Buying a home
- Searching for a home
- Moving
- Planning for college
- Getting a student loan
- Planning for retirement
- Business 24/7™ – Online Solutions for Small Business NEW!
- More options >

Turn your holiday spending into savings.

Home Equity Line of Credit $25,000 for

Raise your

Introducing our new High Yield CD.



https://sitekey.bankofamerica.com/sas/challengeQandA.do

Confirm that your SiteKey is correct

If you recognize your SiteKey, you'll know for sure that you
are at the valid Bank of America site. Confirming your SiteKey is
also how you'll know that it's safe to enter your Passcode and click the **Sign In** button.

An asterisk (*) indicates a required field.

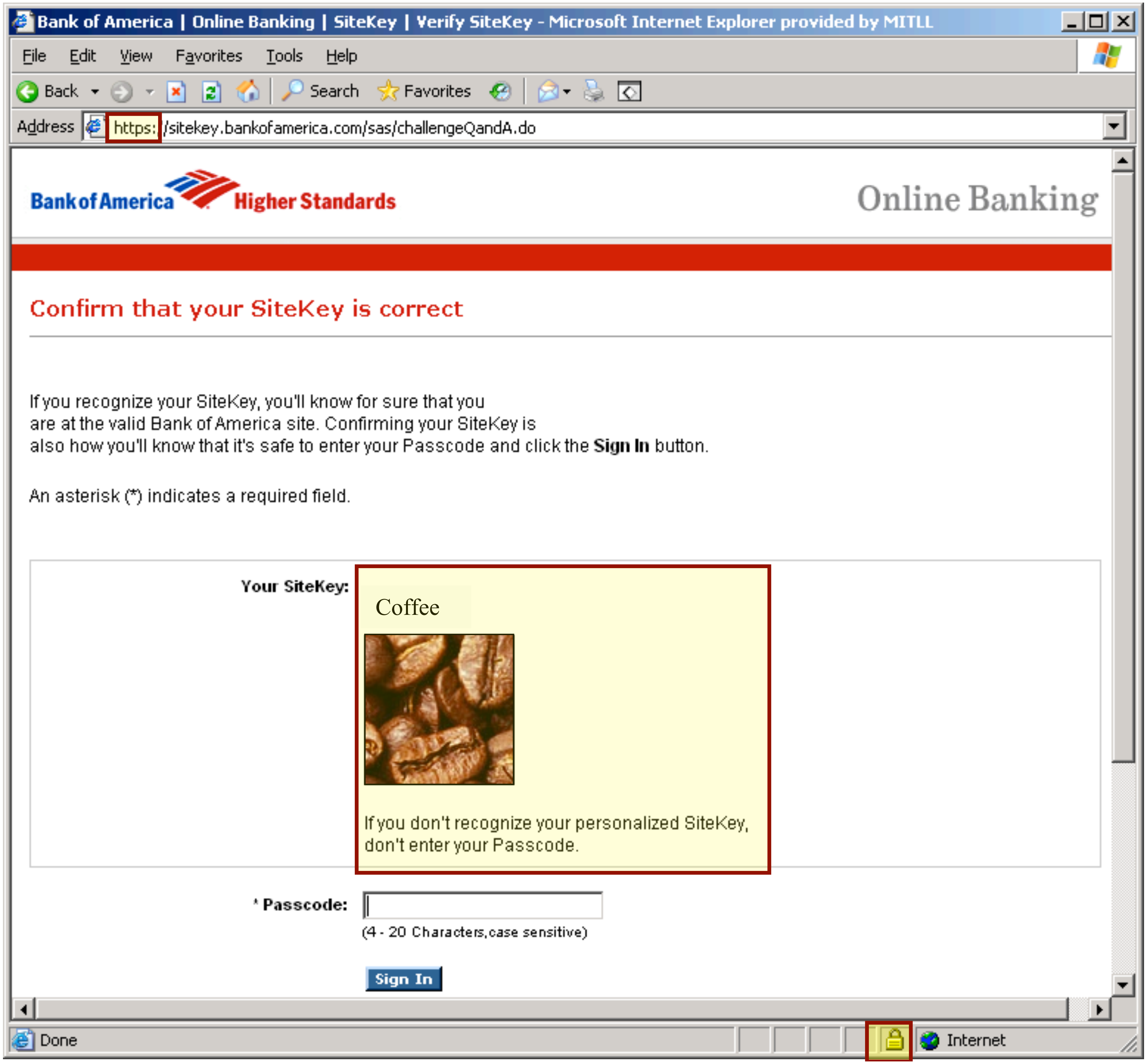
Your SiteKey: Coffee

If you don't recognize your personalized SiteKey,
don't enter your Passcode.

* **Passcode:** **********
(4 - 20 Characters,case sensitive)

Will users check indicators before entering passwords?

We asked Bank of America users to conduct common online banking tasks….



Bank of America | Online Banking | SiteKey | Verify SiteKey - Microsoft Internet Explorer provided by MITLL

https://sitekey.bankofamerica.com/sas/challengeQandA.do

Bank of America Higher Standards

Online Banking

Confirm that your SiteKey is correct

If you recognize your SiteKey, you'll know for sure that you are at the valid Bank of America site. Confirming your SiteKey is also how you'll know that it's safe to enter your Passcode and click the **Sign In** button.

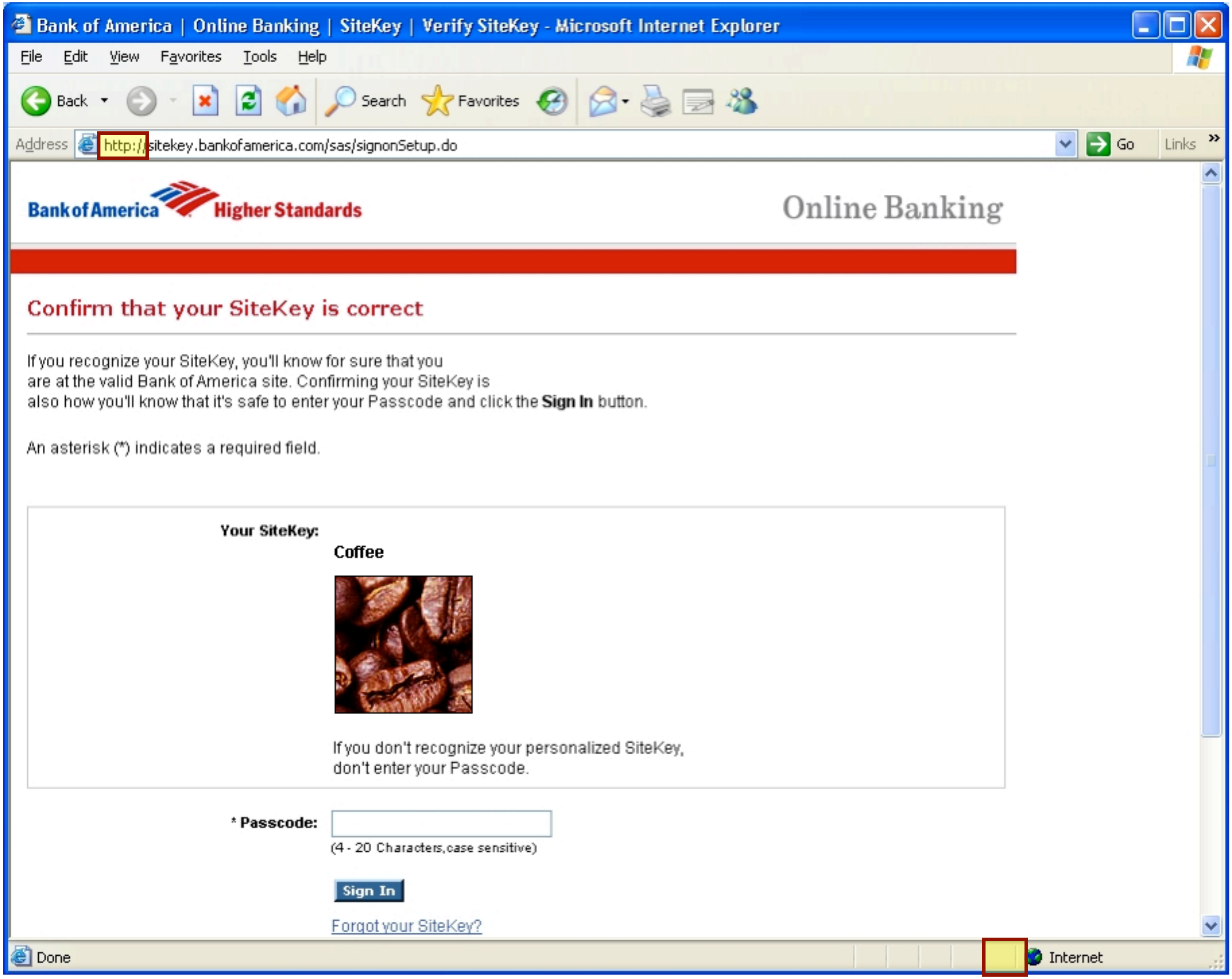
An asterisk (*) indicates a required field.

Your SiteKey: Coffee

If you don't recognize your personalized SiteKey, don't enter your Passcode.

* Passcode:

(4 - 20 Characters,case sensitive)


Bank of America | Online Banking | SiteKey | Verify SiteKey - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://sitekey.bankofamerica.com/sas/signonSetup.do
Go
Links
Bank of America Higher Standards
Online Banking
Done
Internet

Confirm that your SiteKey is correct

If you recognize your SiteKey, you'll know for sure that you are at the valid Bank of America site. Confirming your SiteKey is also how you'll know that it's safe to enter your Passcode and click the **Sign In** button.

An asterisk (*) indicates a required field.

Your SiteKey:

Coffee

If you don't recognize your personalized SiteKey, don't enter your Passcode.

*** Passcode:** ____

(4 - 20 Characters, case sensitive)

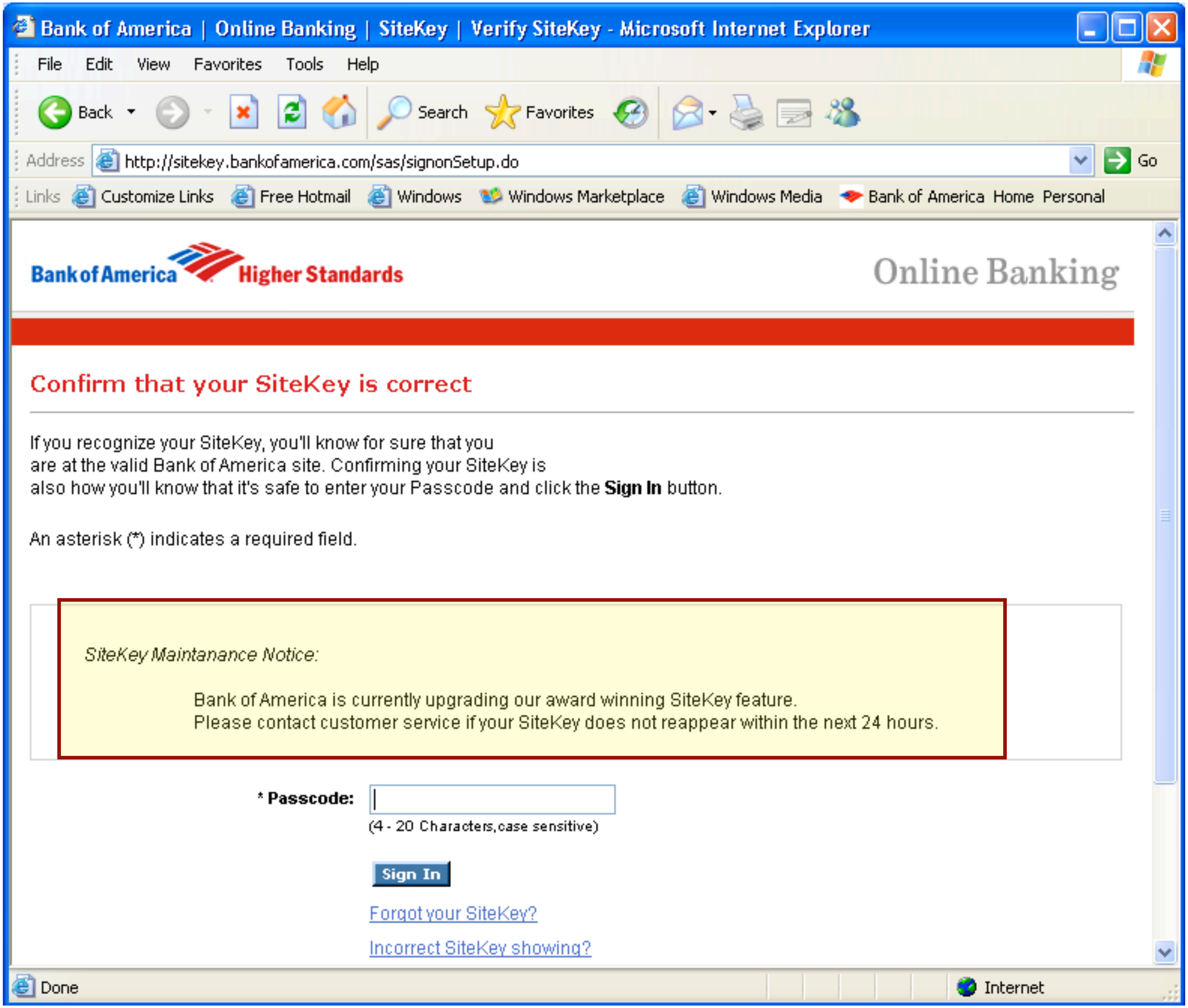
Sign In

Forgot your SiteKey?

Results: HTTPS indicators removed

Group	**Sent password**	**Withheld**
Role playing	18 (100%)	
Security primed	18 (100%)	
Personal Account	27 (100%)	

All 63 participants entered their password!



http://sitekey.bankofamerica.com/sas/signonSetup.do

Confirm that your SiteKey is correct

If you recognize your SiteKey, you'll know for sure that you
are at the valid Bank of America site. Confirming your SiteKey is
also how you'll know that it's safe to enter your Passcode and click the **Sign In** button.

An asterisk (*) indicates a required field.

SiteKey Maintanance Notice:

Bank of America is currently upgrading our award winning SiteKey feature.
Please contact customer service if your SiteKey does not reappear within the next 24 hours.

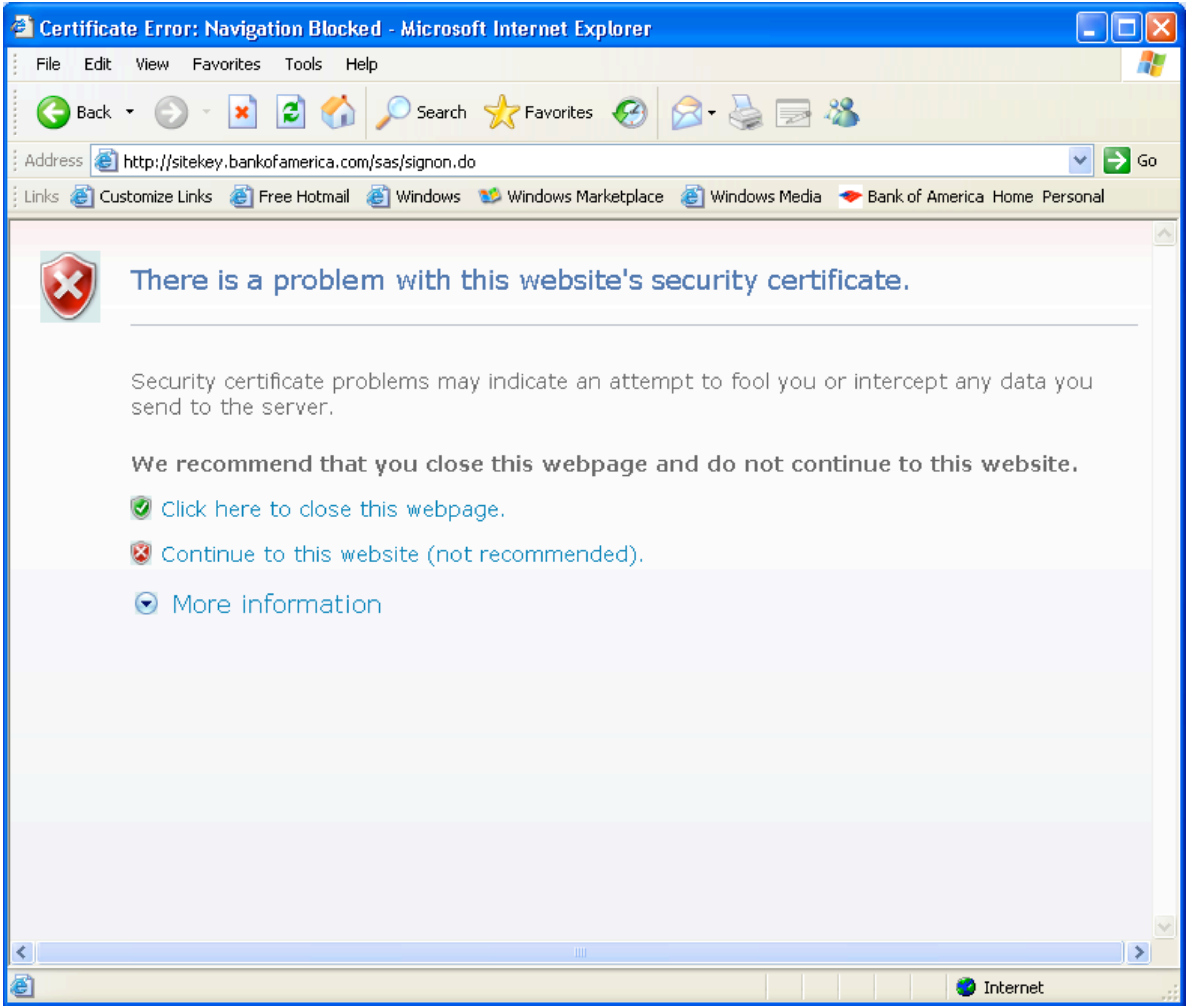
* **Passcode:**
(4 - 20 Characters,case sensitive)

Forgot your SiteKey?

Incorrect SiteKey showing?

Results: Sitekey removed

Group	**Sent password**	**Withheld**
Role playing	18 (100%)	
Security primed	17 (100%)	
Personal Account	23 (92%)	2 (8%)



Certificate Error: Navigation Blocked - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://sitekey.bankofamerica.com/sas/signon.do
Go
Links
Customize Links
Free Hotmail
Windows
Windows Marketplace
Windows Media
Bank of America Home Personal
Internet

There is a problem with this website's security certificate.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

Results: Warning page inserted

Group	**Sent password**	**Withheld**
Role playing	10 (56%)	8 (44%)
Security primed	12 (71%)	5 (29%)
Personal Account	8 (36%)	14 (64%)

7 Laws of Identity

7 Flaws of Identity

Challenge 1

Users don’t want to “manage” their identity

Users don’t think…

“I want to be secure”

“I want to go to my bank securely”

“I want to login to my bank”

Users are task focused

“I want to pay my bills”

Attackers add urgency

URGENT

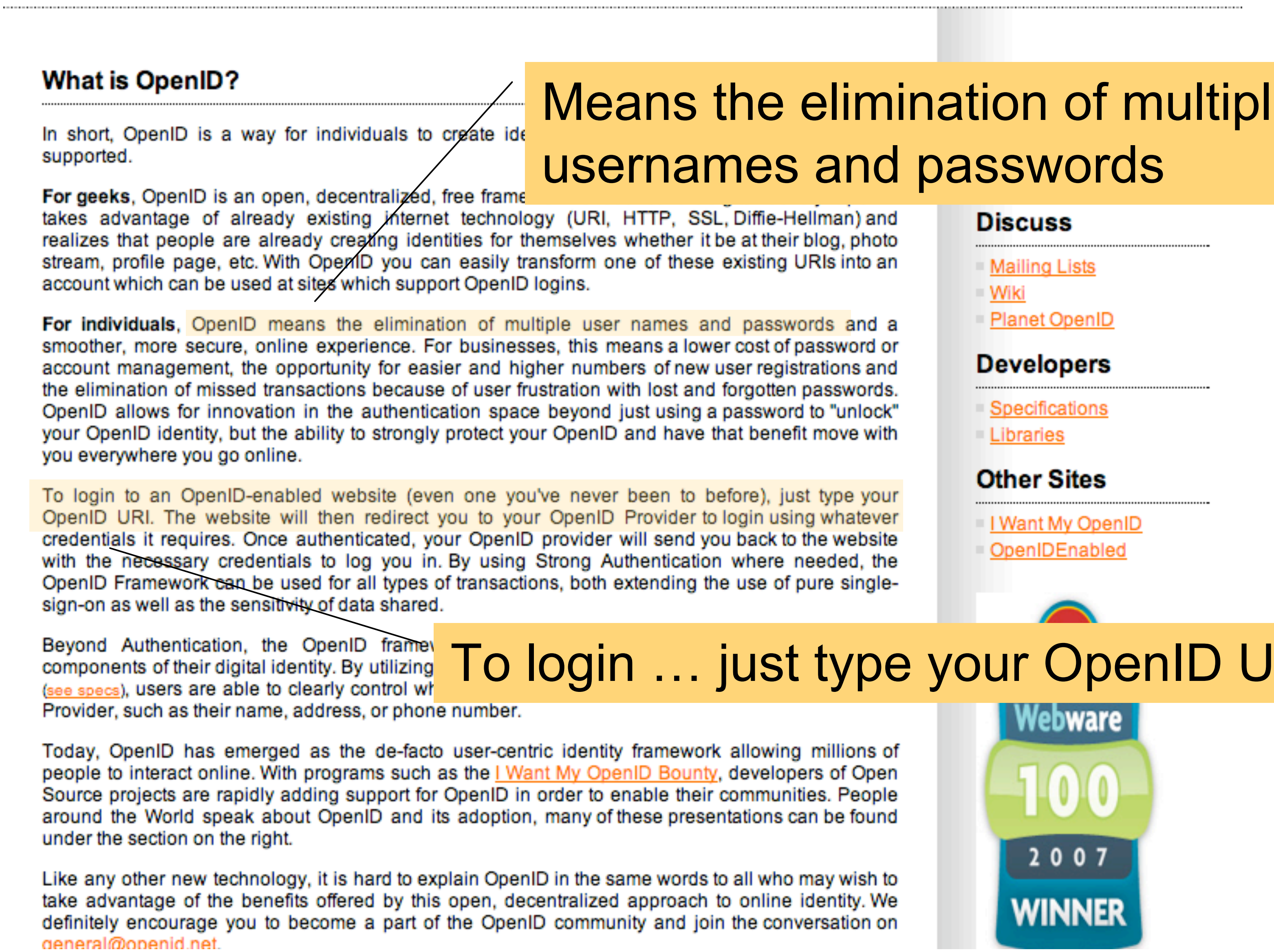
“I have to update my account NOW, or my account will be closed ”

Challenge 2

Identity management can increase cognitive burden

OpenID

Means the elimination of multiple usernames and passwords



What is OpenID?

In short, OpenID is a way for individuals to create ide
supported.

For geeks, OpenID is an open, decentralized, free frame
takes advantage of already existing internet technology (URI, HTTP, SSL, Diffie-Hellman) and realizes that people are already creating identities for themselves whether it be at their blog, photo stream, profile page, etc. With OpenID you can easily transform one of these existing URIs into an account which can be used at sites which support OpenID logins.

For individuals, OpenID means the elimination of multiple user names and passwords and a smoother, more secure, online experience. For businesses, this means a lower cost of password or account management, the opportunity for easier and higher numbers of new user registrations and the elimination of missed transactions because of user frustration with lost and forgotten passwords. OpenID allows for innovation in the authentication space beyond just using a password to "unlock" your OpenID identity, but the ability to strongly protect your OpenID and have that benefit move with you everywhere you go online.

To login to an OpenID-enabled website (even one you've never been to before), just type your OpenID URI. The website will then redirect you to your OpenID Provider to login using whatever credentials it requires. Once authenticated, your OpenID provider will send you back to the website with the necessary credentials to log you in. By using Strong Authentication where needed, the OpenID Framework can be used for all types of transactions, both extending the use of pure single-sign-on as well as the sensitivity of data shared.

Beyond Authentication, the OpenID framev
components of their digital identity. By utilizing
(see specs), users are able to clearly control wh
Provider, such as their name, address, or phone number.

Today, OpenID has emerged as the de-facto user-centric identity framework allowing millions of people to interact online. With programs such as the I Want My OpenID Bounty, developers of Open Source projects are rapidly adding support for OpenID in order to enable their communities. People around the World speak about OpenID and its adoption, many of these presentations can be found under the section on the right.

Like any other new technology, it is hard to explain OpenID in the same words to all who may wish to take advantage of the benefits offered by this open, decentralized approach to online identity. We definitely encourage you to become a part of the OpenID community and join the conversation on general@openid.net.

Discuss

- Mailing Lists
- Wiki
- Planet OpenID

Developers

- Specifications
- Libraries

Other Sites

- I Want My OpenID
- OpenIDEnabled

To login … just type your OpenID URI

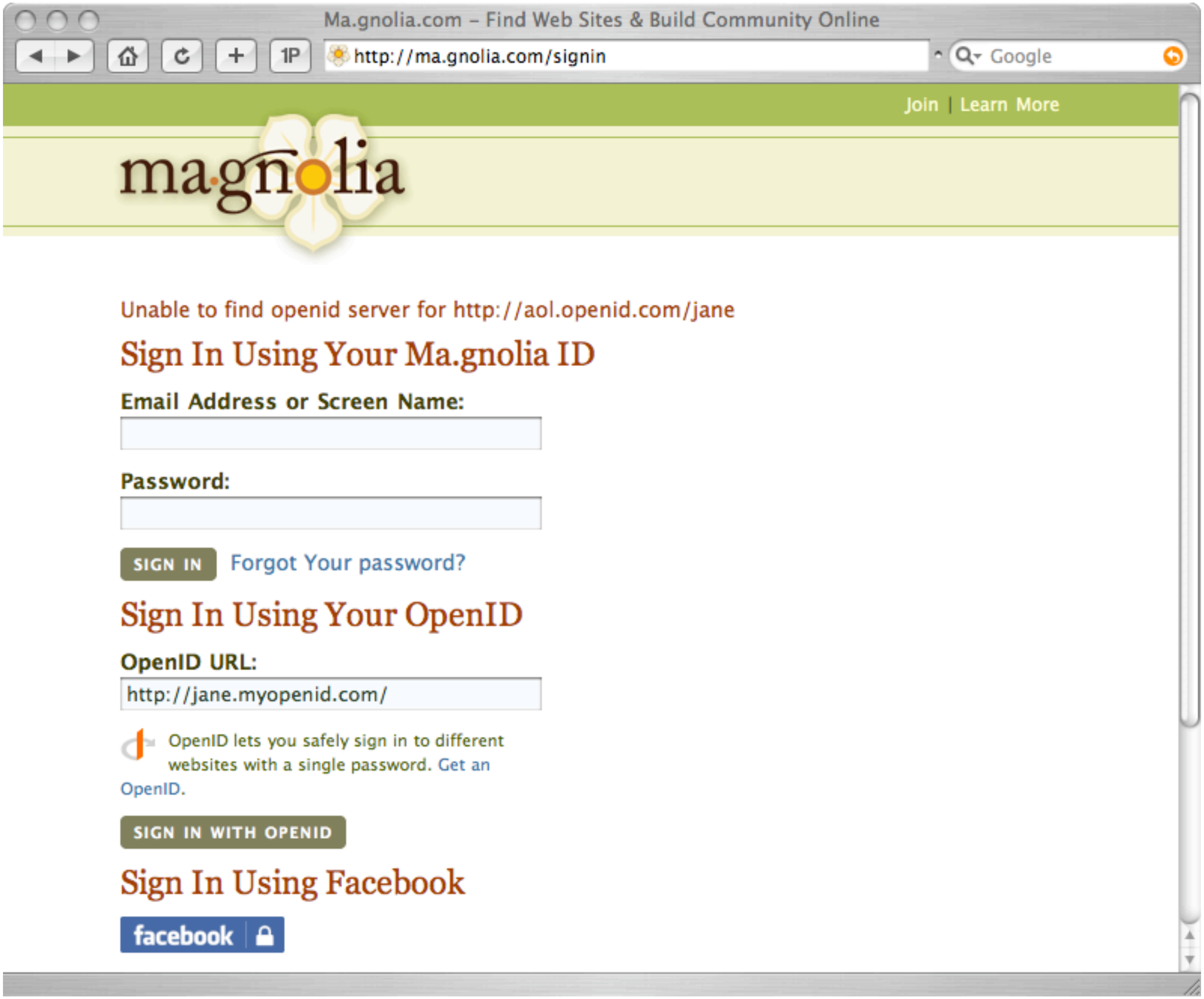
Users don’t understand URIs

`http://jane.livejournal.com/`

`http://openid.aol.com/jane/`

`http://jane.myopenid.com/`

`http://jane.pip.verisignlabs.com/`


Ma.gnolia.com – Find Web Sites & Build Community Online
http://ma.gnolia.com/signin
Google
Join | Learn More
magnolia

Unable to find openid server for http://aol.openid.com/jane

Sign In Using Your Ma.gnolia ID

Email Address or Screen Name:

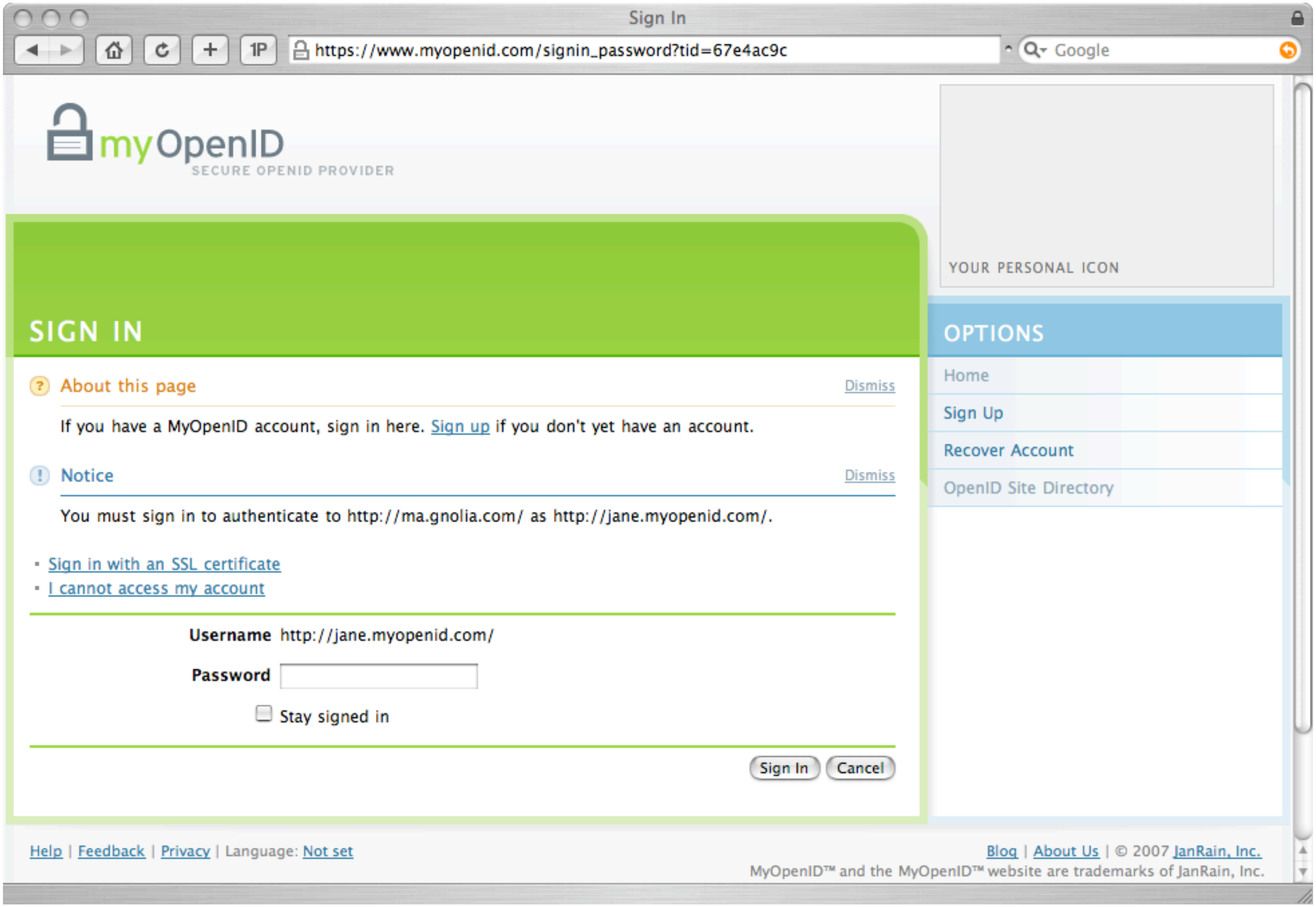
Password:

Sign In Using Your OpenID

OpenID URL: http://jane.myopenid.com/

OpenID lets you safely sign in to different websites with a single password. Get an OpenID.

Sign In Using Facebook


Sign In
https://www.myopenid.com/signin_password?tid=67e4ac9c
Google
myOpenID
SECURE OPENID PROVIDER
YOUR PERSONAL ICON
OPTIONS
Home
Sign Up
Recover Account
OpenID Site Directory
Dismiss
Dismiss
Sign In
Cancel
Help | Feedback | Privacy | Language: Not set
Blog | About Us | © 2007 JanRain, Inc.
MyOpenID™ and the MyOpenID™ website are trademarks of JanRain, Inc.

SIGN IN

About this page

If you have a MyOpenID account, sign in here. Sign up if you don't yet have an account.

Notice

You must sign in to authenticate to http://ma.gnolia.com/ as http://jane.myopenid.com/.

- Sign in with an SSL certificate
- I cannot access my account

Username http://jane.myopenid.com/

Password

□ Stay signed in

➜ OpenID doubles user trust decisions

Challenge 3

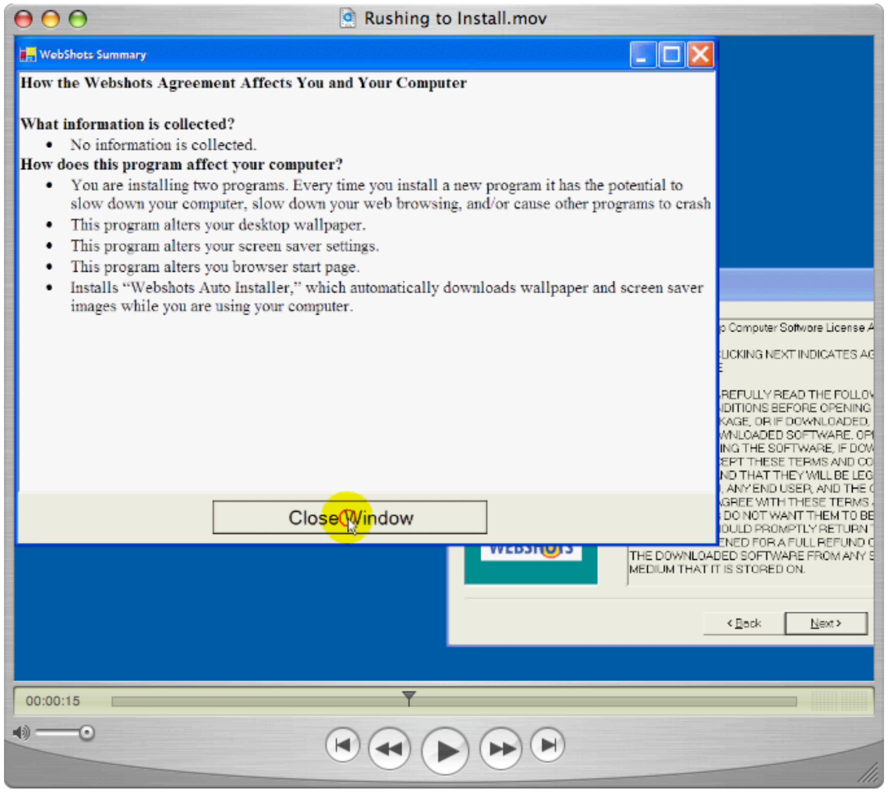
Identity management can maximize information disclosure

User-centric identity:

- “Technical identity systems must only reveal information identifying a user with the user’s consent.” - Kim Cameron
- “… the technical protocol lets the user control the flow *absolutely*, by making them an intermediary at run time.” - Eve Maler
- “The user is in the middle of a data transaction. This does not mean the user has to approve every transaction...” - Dick Hardt

Achieving Informed Consent is Hard

Video: an experiment in simplifying EULAs



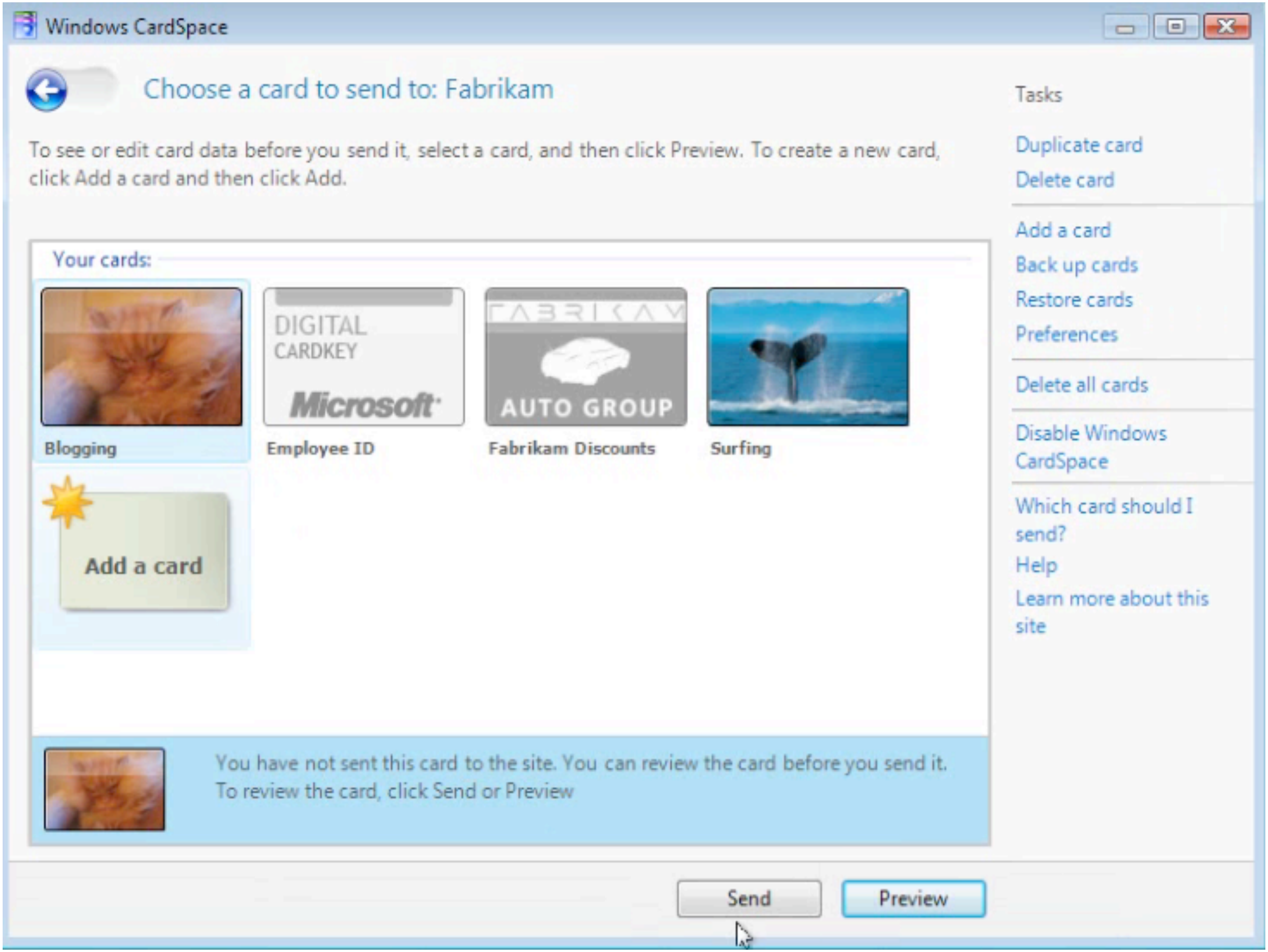
How the Webshots Agreement Affects You and Your Computer

What information is collected?

- No information is collected.

How does this program affect your computer?

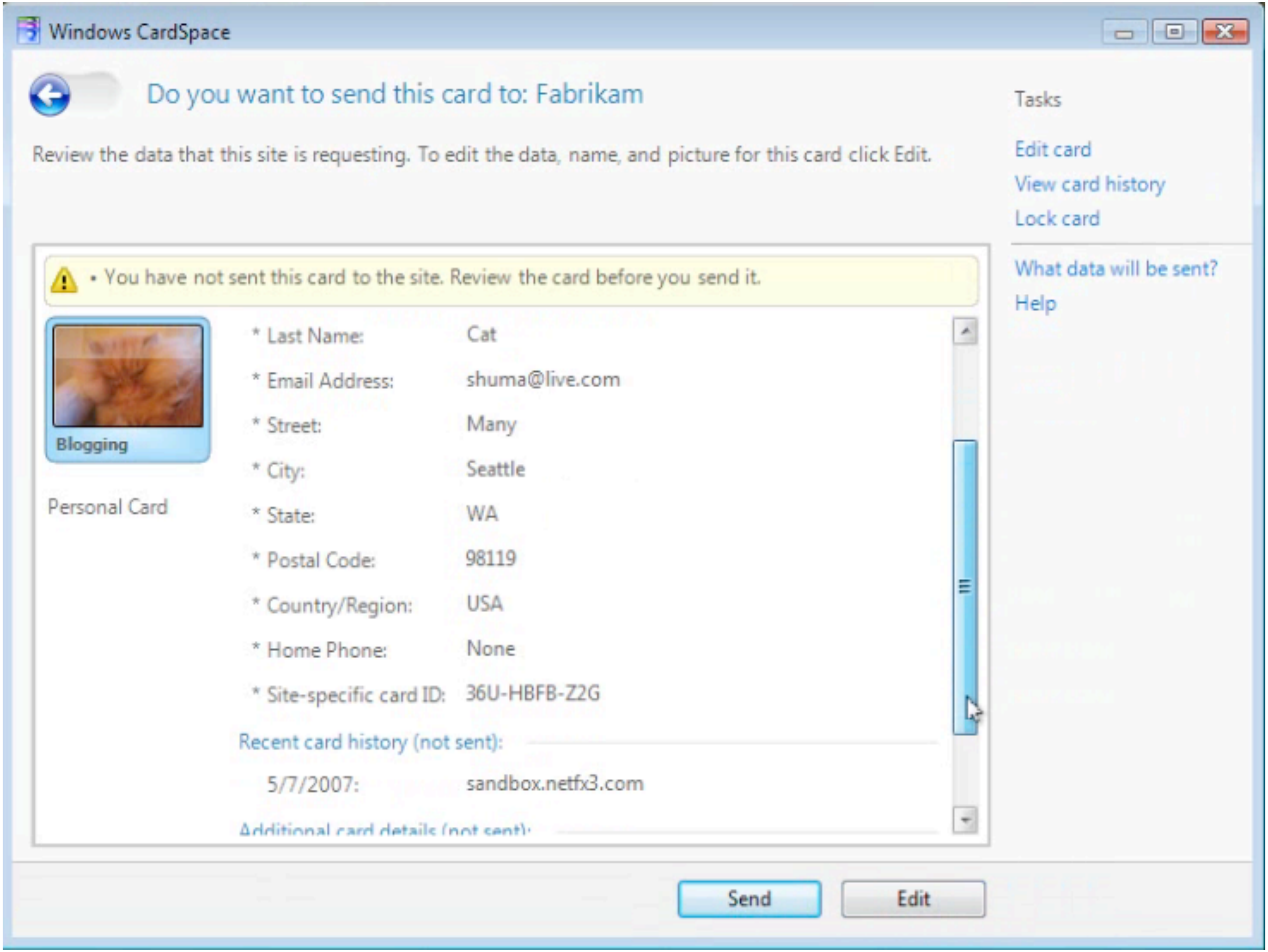
- You are installing two programs. Every time you install a new program it has the potential to slow down your computer, slow down your web browsing, and/or cause other programs to crash
- This program alters your desktop wallpaper.
- This program alters your screen saver settings.
- This program alters you browser start page.
- Installs "Webshots Auto Installer," which automatically downloads wallpaper and screen saver images while you are using your computer.



Choose a card to send to: Fabrikam

To see or edit card data before you send it, select a card, and then click Preview. To create a new card, click Add a card and then click Add.

You have not sent this card to the site. You can review the card before you send it. To review the card, click Send or Preview



Do you want to send this card to: Fabrikam

Review the data that this site is requesting. To edit the data, name, and picture for this card click Edit.

• You have not sent this card to the site. Review the card before you send it.

Personal Card

* Last Name:	Cat
* Email Address:	shuma@live.com
* Street:	Many
* City:	Seattle
* State:	WA
* Postal Code:	98119
* Country/Region:	USA
* Home Phone:	None
* Site-specific card ID:	36U-HBFB-Z2G

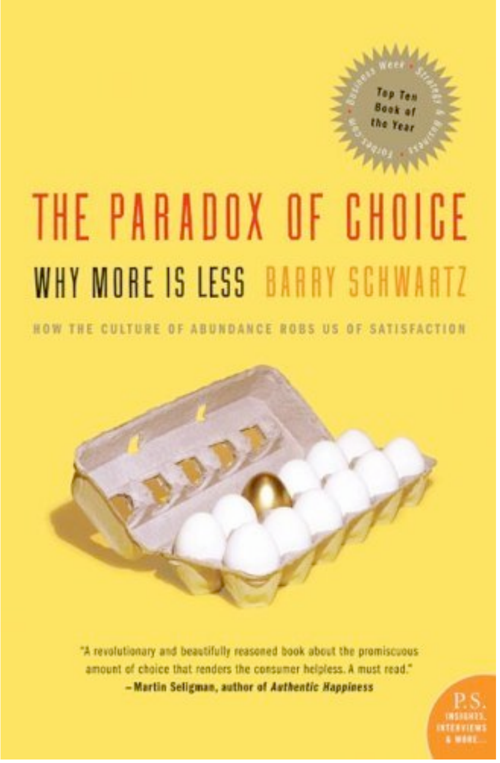
Recent card history (not sent):

5/7/2007:	sandbox.netfx3.com

Additional card details (not sent):

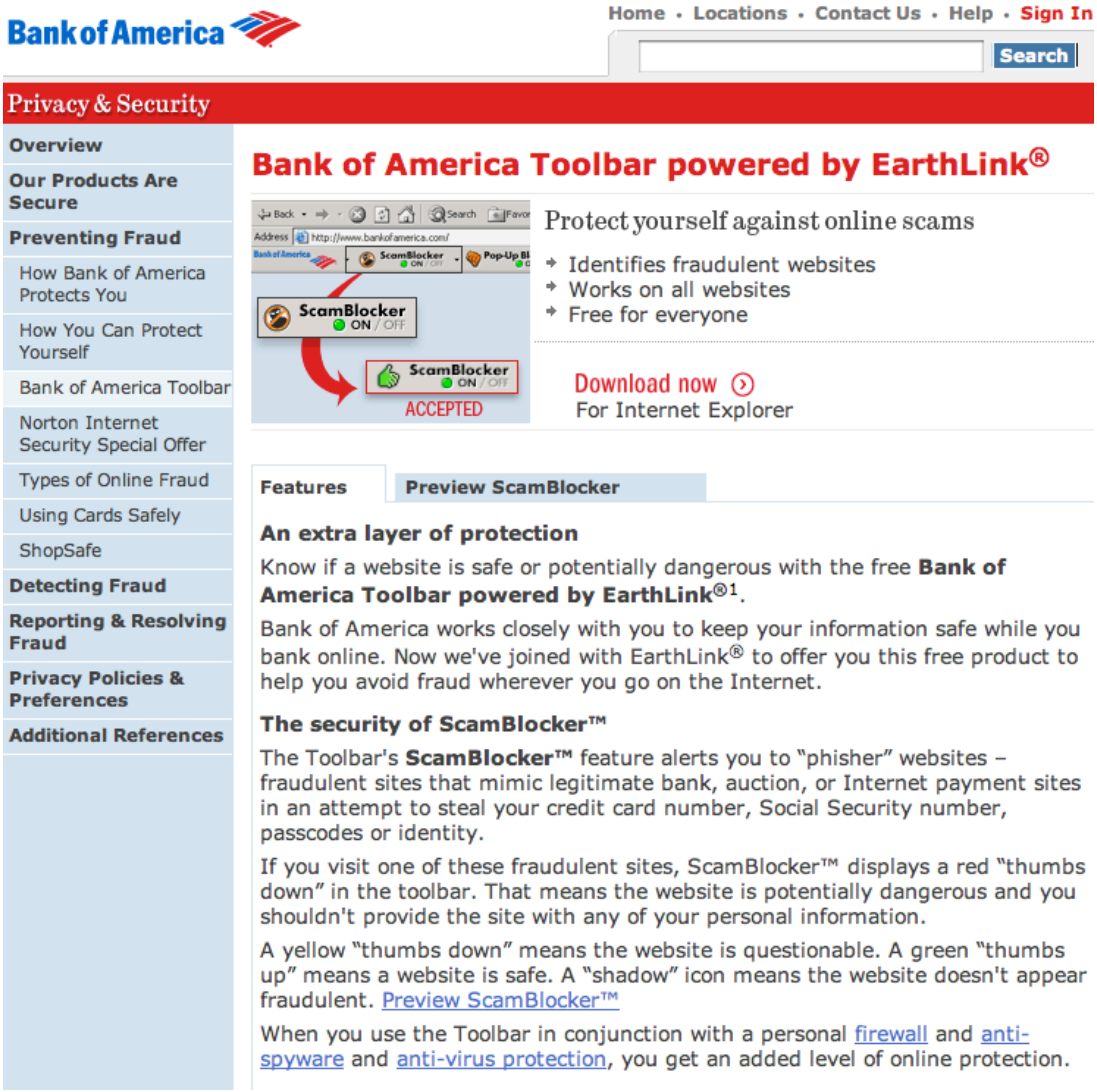
More dialog boxes ≠ Consent

More trust decisions ≠ Control


Business Week • Strategy & Business • Forbes.com
Top Ten Book of the Year
THE PARADOX OF CHOICE
WHY MORE IS LESS
BARRY SCHWARTZ
HOW THE CULTURE OF ABUNDANCE ROBS US OF SATISFACTION
"A revolutionary and beautifully reasoned book about the promiscuous amount of choice that renders the consumer helpless. A must read."
–Martin Seligman, author of Authentic Happiness
P.S.
INSIGHTS, INTERVIEWS & MORE...

Challenge 4

Attacks are too easy with existing software



Overview

Our Products Are Secure

Preventing Fraud

How Bank of America Protects You

How You Can Protect Yourself

Bank of America Toolbar

Norton Internet Security Special Offer

Types of Online Fraud

Using Cards Safely

ShopSafe

Detecting Fraud

Reporting & Resolving Fraud

Privacy Policies & Preferences

Additional References

Bank of America Toolbar powered by EarthLink®

Protect yourself against online scams

- Identifies fraudulent websites
- Works on all websites
- Free for everyone

Download now ›

For Internet Explorer

Features | Preview ScamBlocker

An extra layer of protection

Know if a website is safe or potentially dangerous with the free **Bank of America Toolbar powered by EarthLink®**[1].

Bank of America works closely with you to keep your information safe while you bank online. Now we've joined with EarthLink® to offer you this free product to help you avoid fraud wherever you go on the Internet.

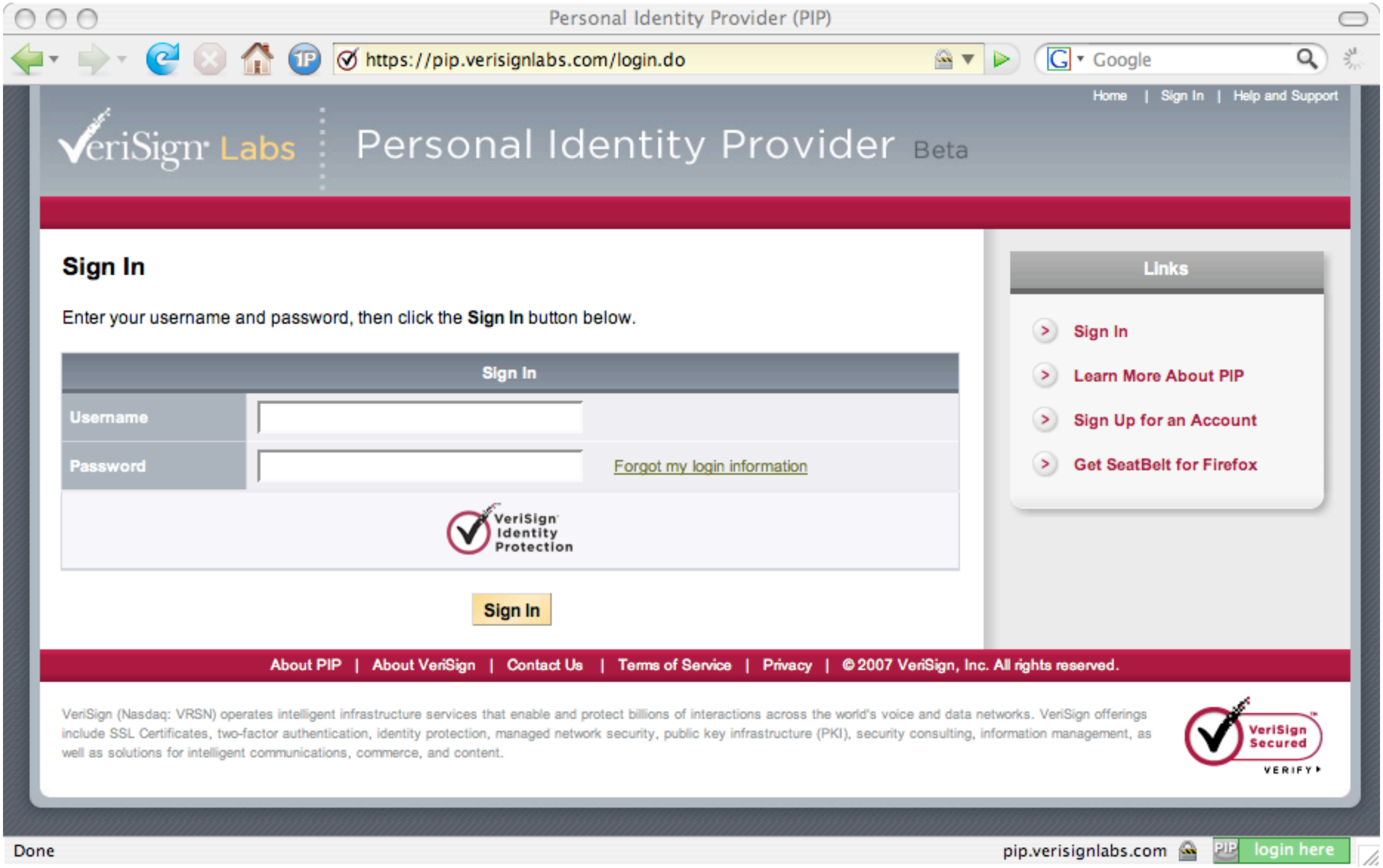
The security of ScamBlocker™

The Toolbar's **ScamBlocker™** feature alerts you to "phisher" websites – fraudulent sites that mimic legitimate bank, auction, or Internet payment sites in an attempt to steal your credit card number, Social Security number, passcodes or identity.

If you visit one of these fraudulent sites, ScamBlocker™ displays a red "thumbs down" in the toolbar. That means the website is potentially dangerous and you shouldn't provide the site with any of your personal information.

A yellow "thumbs down" means the website is questionable. A green "thumbs up" means a website is safe. A "shadow" icon means the website doesn't appear fraudulent. Preview ScamBlocker™

When you use the Toolbar in conjunction with a personal firewall and anti-spyware and anti-virus protection, you get an added level of online protection.



Personal Identity Provider (PIP)
https://pip.verisignlabs.com/login.do
Google
Home | Sign In | Help and Support
VeriSign Labs
Personal Identity Provider Beta
Links
Sign In
Learn More About PIP
Sign Up for an Account
Get SeatBelt for Firefox
Sign In
Username
Password
Forgot my login information
VeriSign Identity Protection
Sign In
About PIP | About VeriSign | Contact Us | Terms of Service | Privacy | © 2007 VeriSign, Inc. All rights reserved.
VeriSign Secured
VERIFY
Done
pip.verisignlabs.com
PIP login here

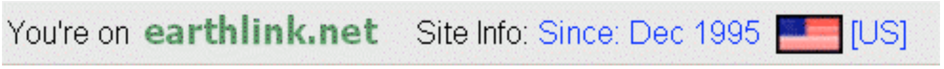
Sign In

Enter your username and password, then click the **Sign In** button below.

VeriSign (Nasdaq: VRSN) operates intelligent infrastructure services that enable and protect billions of interactions across the world's voice and data networks. VeriSign offerings include SSL Certificates, two-factor authentication, identity protection, managed network security, public key infrastructure (PKI), security consulting, information management, as well as solutions for intelligent communications, commerce, and content.

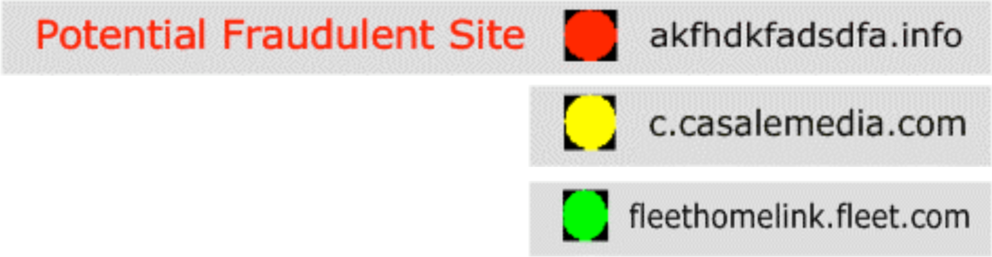
Do toolbars prevent phishing attacks?
(Wu, Miller & Garfinkel, 2006)

Neutral-information Toolbar (Netcraft, Spoofstick)


You're on earthlink.net Site Info: Since: Dec 1995 [US]

45% spoof rate

System-decision Toolbar (Spoofguard, eBay)

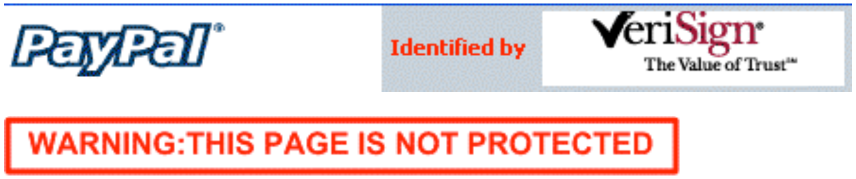

Potential Fraudulent Site ● akfhdkfadsdfa.info

● c.casalemedia.com

● fleethomelink.fleet.com

38% spoof rate

SSL-verification Toolbar (Trustbar)


PayPal® Identified by VeriSign® The Value of Trust℠

WARNING:THIS PAGE IS NOT PROTECTED

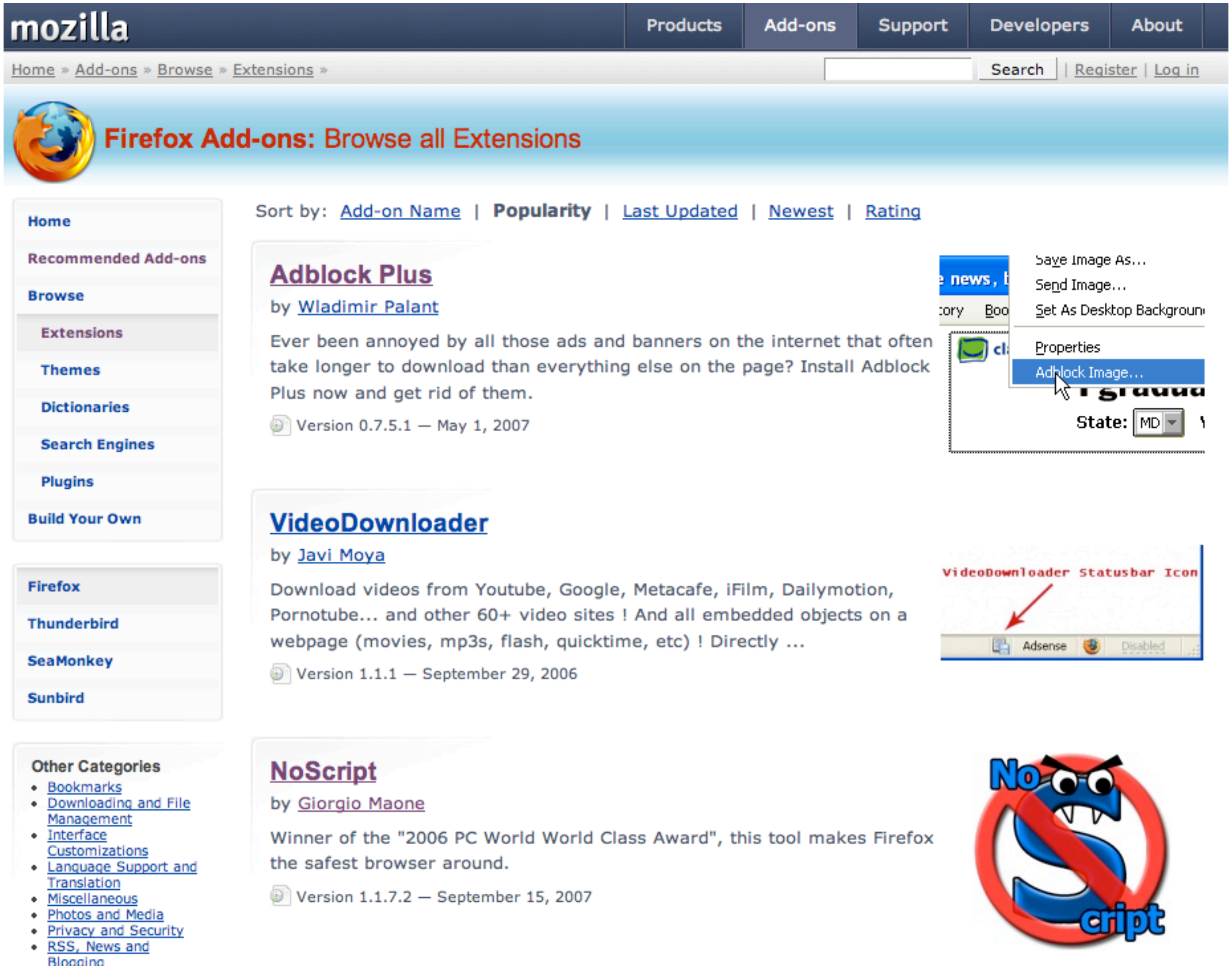
33% spoof rate

Security indicators are a symptom of flawed design

Challenge 5

We need better software

But users aren’t motivated to get it



Firefox Add-ons: Browse all Extensions

- Home
- Recommended Add-ons
- Browse
  - Extensions
  - Themes
  - Dictionaries
  - Search Engines
  - Plugins
- Build Your Own

- Firefox
- Thunderbird
- SeaMonkey
- Sunbird

Other Categories

- Bookmarks
- Downloading and File Management
- Interface Customizations
- Language Support and Translation
- Miscellaneous
- Photos and Media
- Privacy and Security
- RSS, News and Blogging

Sort by: Add-on Name | **Popularity** | Last Updated | Newest | Rating

Adblock Plus
by Wladimir Palant

Ever been annoyed by all those ads and banners on the internet that often take longer to download than everything else on the page? Install Adblock Plus now and get rid of them.

Version 0.7.5.1 — May 1, 2007

VideoDownloader
by Javi Moya

Download videos from Youtube, Google, Metacafe, iFilm, Dailymotion, Pornotube... and other 60+ video sites ! And all embedded objects on a webpage (movies, mp3s, flash, quicktime, etc) ! Directly ...

Version 1.1.1 — September 29, 2006

NoScript
by Giorgio Maone

Winner of the "2006 PC World World Class Award", this tool makes Firefox the safest browser around.

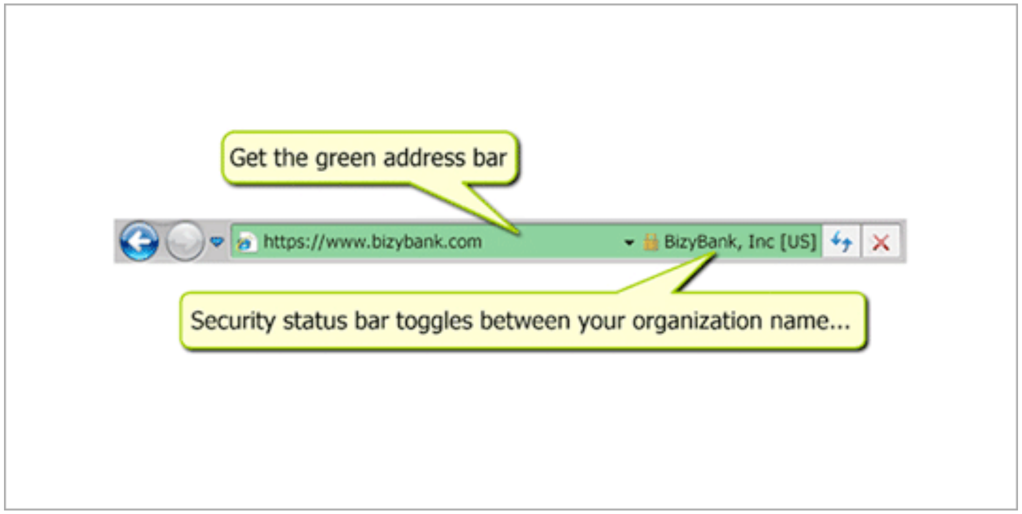
Version 1.1.7.2 — September 15, 2007

Integration with OS or browsers

Problem:

- Change is hard
- Interfaces conflict

Benefits attackers!

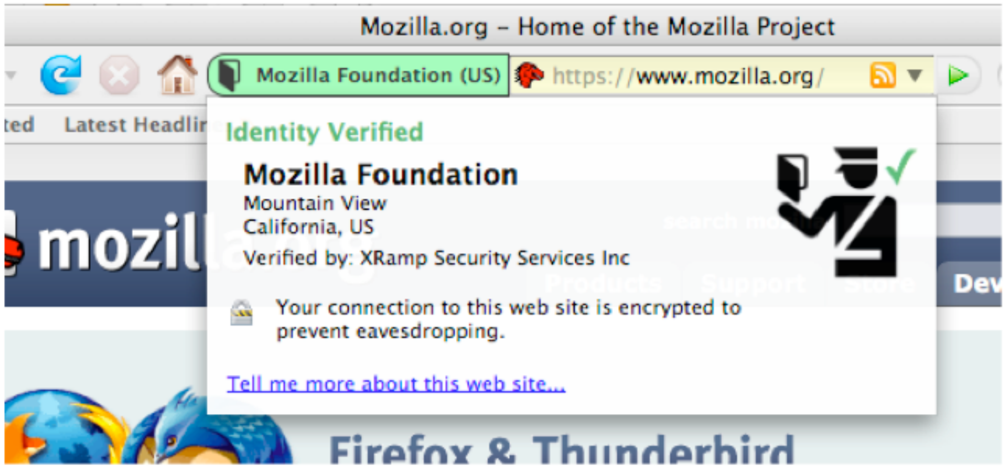


Get the green address bar

https://www.bizybank.com

BizyBank, Inc [US]

Security status bar toggles between your organization name...



Mozilla.org – Home of the Mozilla Project

Mozilla Foundation (US)

https://www.mozilla.org/

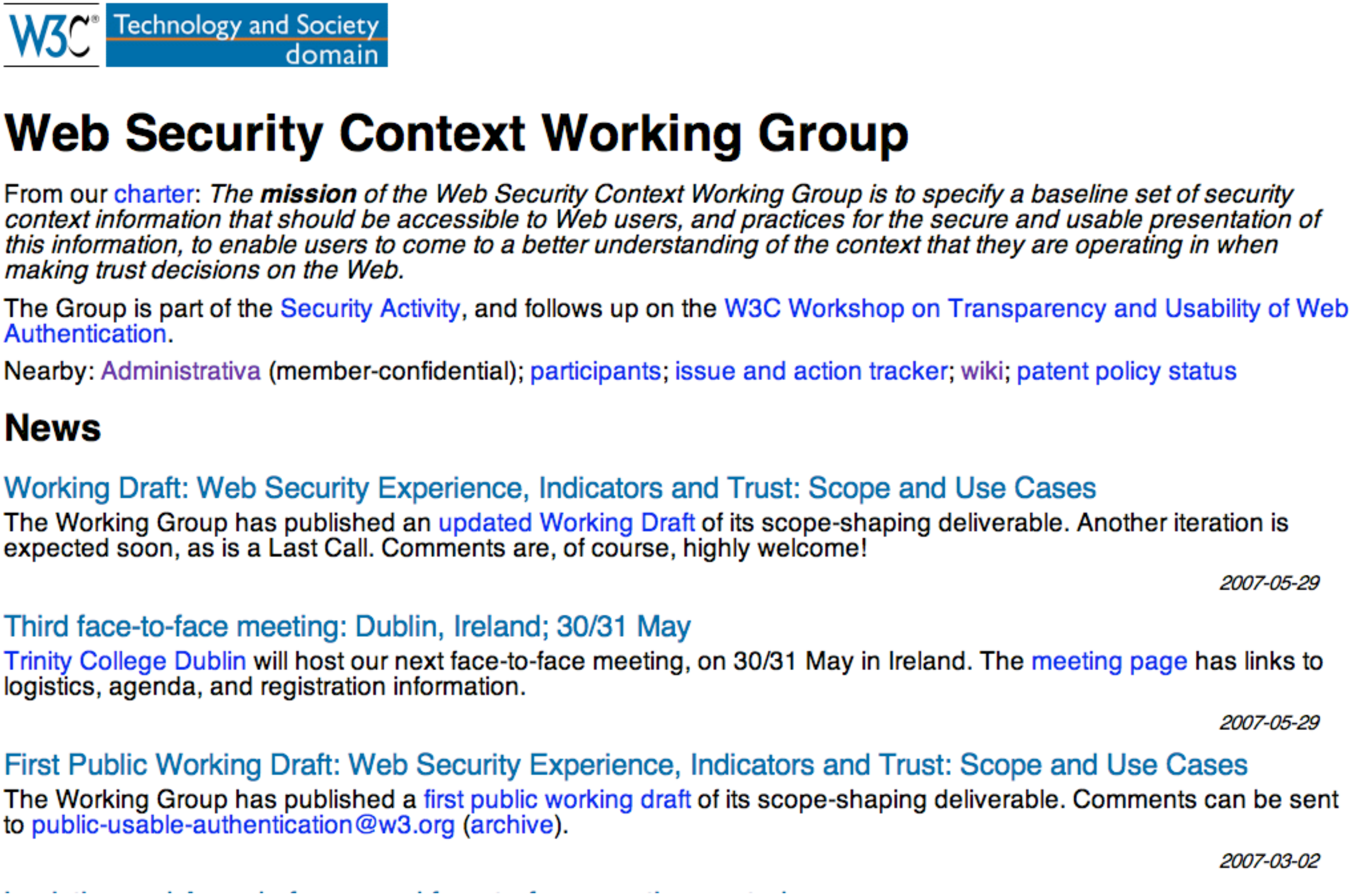
Identity Verified

Mozilla Foundation
Mountain View
California, US
Verified by: XRamp Security Services Inc

Your connection to this web site is encrypted to prevent eavesdropping.

Tell me more about this web site...

Can standards help?



Web Security Context Working Group

From our charter: *The **mission** of the Web Security Context Working Group is to specify a baseline set of security context information that should be accessible to Web users, and practices for the secure and usable presentation of this information, to enable users to come to a better understanding of the context that they are operating in when making trust decisions on the Web.*

The Group is part of the Security Activity, and follows up on the W3C Workshop on Transparency and Usability of Web Authentication.

Nearby: Administrativa (member-confidential); participants; issue and action tracker; wiki; patent policy status

News

Working Draft: Web Security Experience, Indicators and Trust: Scope and Use Cases

The Working Group has published an updated Working Draft of its scope-shaping deliverable. Another iteration is expected soon, as is a Last Call. Comments are, of course, highly welcome!

2007-05-29

Third face-to-face meeting: Dublin, Ireland; 30/31 May

Trinity College Dublin will host our next face-to-face meeting, on 30/31 May in Ireland. The meeting page has links to logistics, agenda, and registration information.

2007-05-29

First Public Working Draft: Web Security Experience, Indicators and Trust: Scope and Use Cases

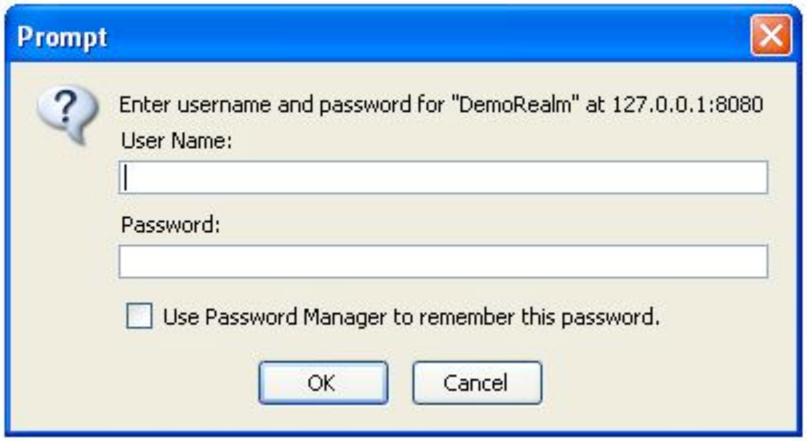
The Working Group has published a first public working draft of its scope-shaping deliverable. Comments can be sent to public-usable-authentication@w3.org (archive).

2007-03-02

Challenge 6

Relying parties want to control user relationship & experience

Compare digest authentication…



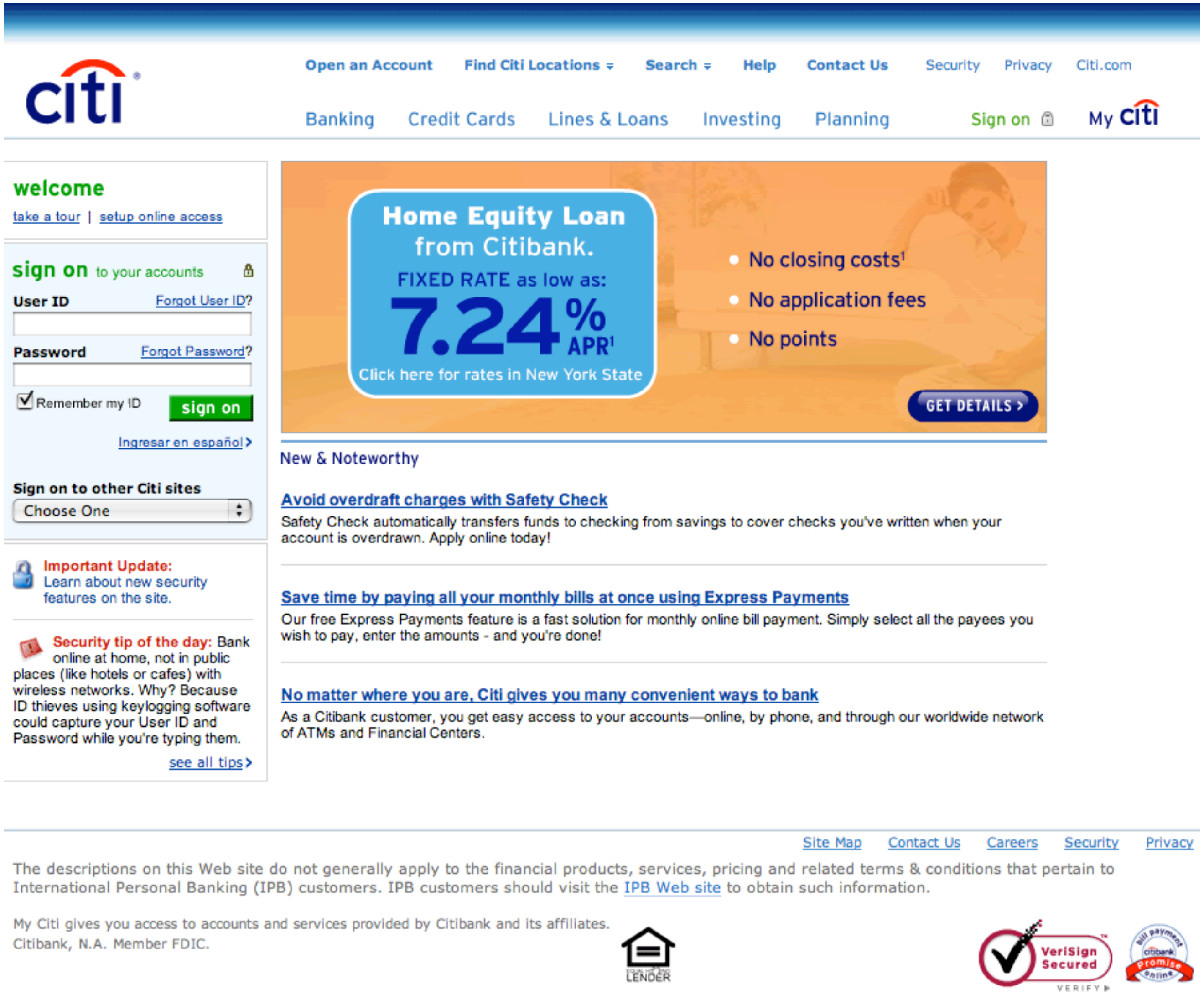
Enter username and password for "DemoRealm" at 127.0.0.1:8080

User Name:

Password:

□ Use Password Manager to remember this password.

… to password forms.



welcome

take a tour | setup online access

sign on to your accounts

User ID Forgot User ID?

Password Forgot Password?

☑ Remember my ID

Ingresar en español ›

Sign on to other Citi sites

Important Update: Learn about new security features on the site.

Security tip of the day: Bank online at home, not in public places (like hotels or cafes) with wireless networks. Why? Because ID thieves using keylogging software could capture your User ID and Password while you're typing them.

see all tips ›

Home Equity Loan from Citibank.

FIXED RATE as low as:

7.24% APR[1]

Click here for rates in New York State

- No closing costs[1]
- No application fees
- No points

New & Noteworthy

Avoid overdraft charges with Safety Check

Safety Check automatically transfers funds to checking from savings to cover checks you've written when your account is overdrawn. Apply online today!

Save time by paying all your monthly bills at once using Express Payments

Our free Express Payments feature is a fast solution for monthly online bill payment. Simply select all the payees you wish to pay, enter the amounts - and you're done!

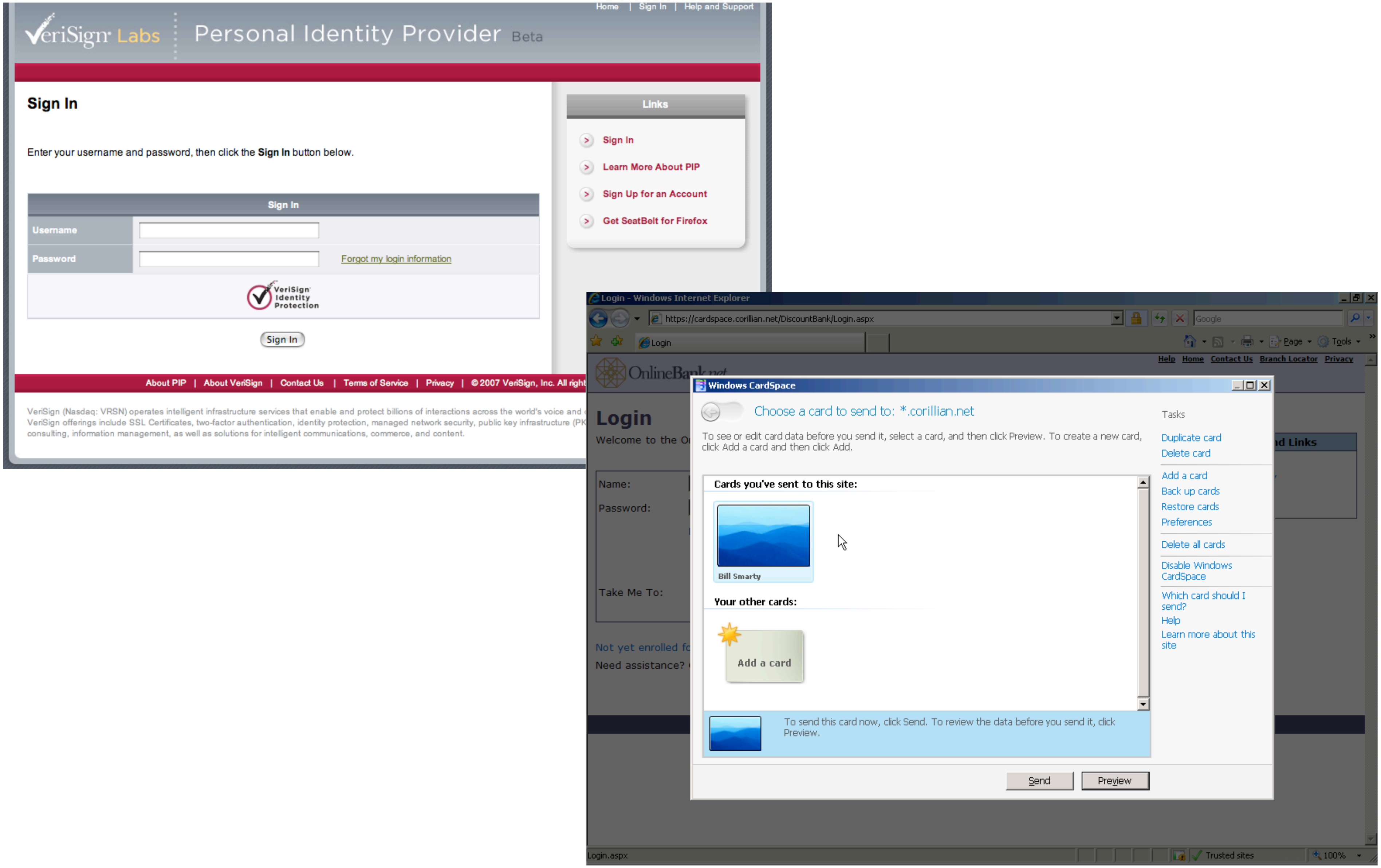
No matter where you are, Citi gives you many convenient ways to bank

As a Citibank customer, you get easy access to your accounts—online, by phone, and through our worldwide network of ATMs and Financial Centers.

The descriptions on this Web site do not generally apply to the financial products, services, pricing and related terms & conditions that pertain to International Personal Banking (IPB) customers. IPB customers should visit the IPB Web site to obtain such information.

My Citi gives you access to accounts and services provided by Citibank and its affiliates.
Citibank, N.A. Member FDIC.

RPs don’t want to send the user “away”



Home | Sign In | Help and Support
VeriSign Labs
Personal Identity Provider Beta
Links
Sign In
Learn More About PIP
Sign Up for an Account
Get SeatBelt for Firefox
Sign In
Username
Password
Forgot my login information
VeriSign Identity Protection
Sign In
About PIP | About VeriSign | Contact Us | Terms of Service | Privacy | © 2007 VeriSign, Inc. All right

Sign In

Enter your username and password, then click the **Sign In** button below.

VeriSign (Nasdaq: VRSN) operates intelligent infrastructure services that enable and protect billions of interactions across the world's voice and
VeriSign offerings include SSL Certificates, two-factor authentication, identity protection, managed network security, public key infrastructure (PK
consulting, information management, as well as solutions for intelligent communications, commerce, and content.

Choose a card to send to: *.corillian.net

To see or edit card data before you send it, select a card, and then click Preview. To create a new card, click Add a card and then click Add.

To send this card now, click Send. To review the data before you send it, click Preview.

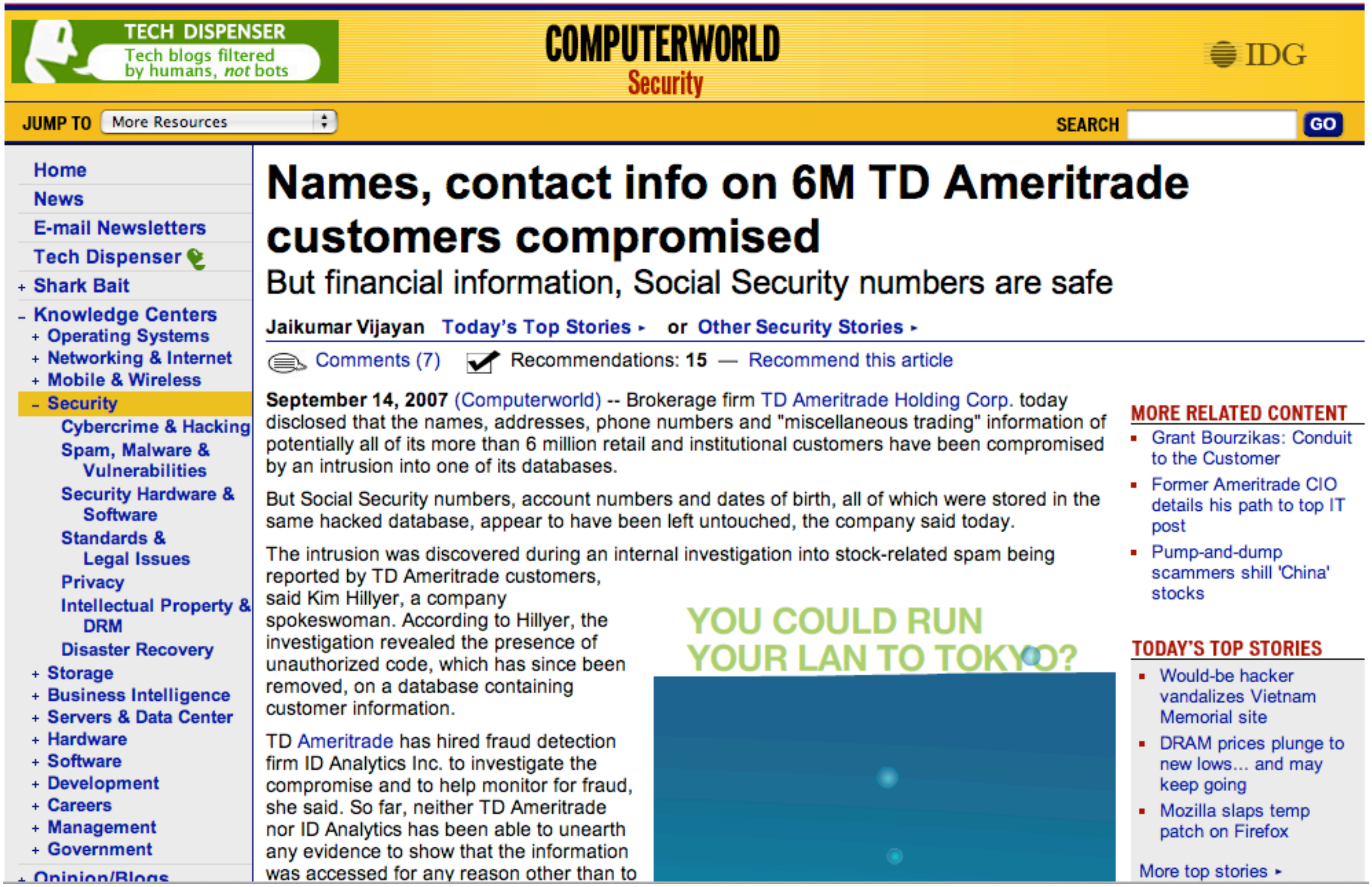
Challenge 7

Trust.

Some users are too trusting

- “People make fake websites to get passwords??”
- “Why would a phishing site display a phishing warning? It must be real.”
- “Sometimes I type in my password to see if I have an account there.”

Other users don’t trust anyone



Names, contact info on 6M TD Ameritrade customers compromised

But financial information, Social Security numbers are safe

Jaikumar Vijayan   Today’s Top Stories ▸   or Other Security Stories ▸

Comments (7)   ✓ Recommendations: 15 — Recommend this article

September 14, 2007 (Computerworld) -- Brokerage firm TD Ameritrade Holding Corp. today disclosed that the names, addresses, phone numbers and "miscellaneous trading" information of potentially all of its more than 6 million retail and institutional customers have been compromised by an intrusion into one of its databases.

But Social Security numbers, account numbers and dates of birth, all of which were stored in the same hacked database, appear to have been left untouched, the company said today.

The intrusion was discovered during an internal investigation into stock-related spam being reported by TD Ameritrade customers, said Kim Hillyer, a company spokeswoman. According to Hillyer, the investigation revealed the presence of unauthorized code, which has since been removed, on a database containing customer information.

TD Ameritrade has hired fraud detection firm ID Analytics Inc. to investigate the compromise and to help monitor for fraud, she said. So far, neither TD Ameritrade nor ID Analytics has been able to unearth any evidence to show that the information was accessed for any reason other than to

MORE RELATED CONTENT

- Grant Bourzikas: Conduit to the Customer
- Former Ameritrade CIO details his path to top IT post
- Pump-and-dump scammers shill 'China' stocks

TODAY'S TOP STORIES

- Would-be hacker vandalizes Vietnam Memorial site
- DRAM prices plunge to new lows... and may keep going
- Mozilla slaps temp patch on Firefox

More top stories ▸

Implications for Design

- Give users something they want
  - Security and identity management are secondary goals
- Reduce cognitive burden
  - Don’t replace one burden with others
  - Don’t overwhelm users with more warnings, dialogs, and indicators - leads to habituation
  - Reduce trust decisions
- Help users to detect spoofing attacks
  - Users misplace trust in logos and indicators
  - Assume that uniform graphic designs will be copied!

Implications for Design (cont.)

- If you want trust, be trustworthy
  - Need early reviews from security community
  - Spoof your own designs in user testing
  - Publish security and usability results

Questions?

Rachna Dhamija
Center for Research on Computation and Society
Harvard University
rachna@deas.harvard.edu

References

- Why Phishing Works, Dhamija, Hearst and Tygar, CHI 2006

  http://www.deas.harvard.edu/~rachna/
- Emperor's New Security Indicators, Schechter, Dhamija, Ozment and Fischer, IEEE Security and Privacy 2007

  http://www.deas.harvard.edu/~rachna/
- 7 Laws of Identity, Kim Cameron

  http://www.identityblog.com/stories/2004/12/09/thelaws.html
- User Centric Identity Quotes
  - Kim Cameron: http://www.identityblog.com/stories/2004/12/09/thelaws.html
  - Eve Maler: http://www.xmlgrrl.com/blog/archives/2006/06/19/r-e-sp-e-c-t/
  - Dick Hardt: http://identity20.com/?p=61
- Photo credits
  - Horse blinders: http://flickr.com/photos/ritechus/24107637/
  - Traffic tree: http://www.flickr.com/photos/oobrien/7597395/