Multi-Factor Authentication: Security or Snake Oil?

Steven Myers
Rachna Dhamija
Jeffrey Friedberg

Phishing & Identity Theft

- Historically most online banking done with passwords (single-factor authentication)
- Password communicated over SSL/TLS secured channel.
- Very susceptible to phishing/pharming/ malware.

FDIC & FFIEC Recommendations

- Federal Deposit Insurance Corporation & Federal Financial Institutions Examination Council:

  all banks to have *enhanced* authentication by end of 2006.

- Note: enhanced is not the same as multi-factor

Problems with Previous Server Authentication

- SSL is simply not understood by users
  - SSL Lock Icons & https indicators
  - Certificates, Root Certificates & Verification
  - Secure sessions, newly spawned windows
  - See yesterday's tutorial for more info
- Users cannot authenticate websites, and so give out credentials improperly.

Welcome to Gmail

https://www.google.com/accour

sitekeyacm_pr

Getting Started | Latest Headlines | Apple | Amazon | eBay | Yahoo! | News | Threat Chaos

Disable | Cookies | CSS | Forms | Images | Information | Miscellaneous | Out

Gmail by Google BETA

Welcome to Gmail

A Google approach to email.

Gmail is a new kind of webmail, built on the idea that email can be more intuitive, efficient, and useful. And maybe even fun. After all, Gmail has:

Fast search
Use Google search to **find the exact message** you want, no matter when it was sent or received.

Lots of space
Over 2877.908276 megabytes (and counting) of free storage so you'll never need to delete another message.

Sign in to Gmail with your Google **Account**

Username:

Password:

Remember me on this computer.

Sign in

I cannot access my account

Done

www.google.com

Chase Personal Banking Investments Credit Cards Home Auto Commercial ...

http://www.chase.com/

Google

Getting Started | Latest Headlines | Apple | Amazon | eBay | Yahoo! | News | Threat Chaos

Disable | Cookies | CSS | Forms | Images | Information | Miscellaneous

CHASE

Find ATM / Branches | Contact Us |

Start banking online now
Get a User ID
GO

Your account's calling.
Keep in touch with your money.

Get

Returning Users: Log On

User ID:

Password:

Remember my User ID

Forgot User ID/Password?

Log On

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

Business
- Business Banking Revenues up to $10MM
- Commercial Banking Revenues over $10MM
- Business Credit Cards

Personal Lending
- Home Equity Loans & Lines of Credit

Insurance & Investing
- Insurance
- Investing

Done

Welcome to Gmail

https://www.google.com/accounts/ServiceLogin?se

Google

Apple (36) | Amazon | eBay | Yahoo! | News (91)

Welcome to Gmail

Gmail by Google BETA

Welcome to Gmail

A Google approach to email.

Gmail is a new kind of webmail, built on the idea that email can be more intuitive, efficient, and useful. And maybe even fun. After all, Gmail has:

Fast search
Use Google search to **find the exact message** you want, no matter when it was sent or received.

Lots of space
Over 2878.102404 megabytes (and counting) of free storage so you'll never need to delete another

Sign in to Gmail with your Google **Account**

Username:

Password:

Remember me on this computer.

Sign in

L Jean Camp

http://www.ljean.com/

Google

Getting Started | Latest Headlines | Apple | Amazon | eBay | Yahoo! | News | Threat Chaos

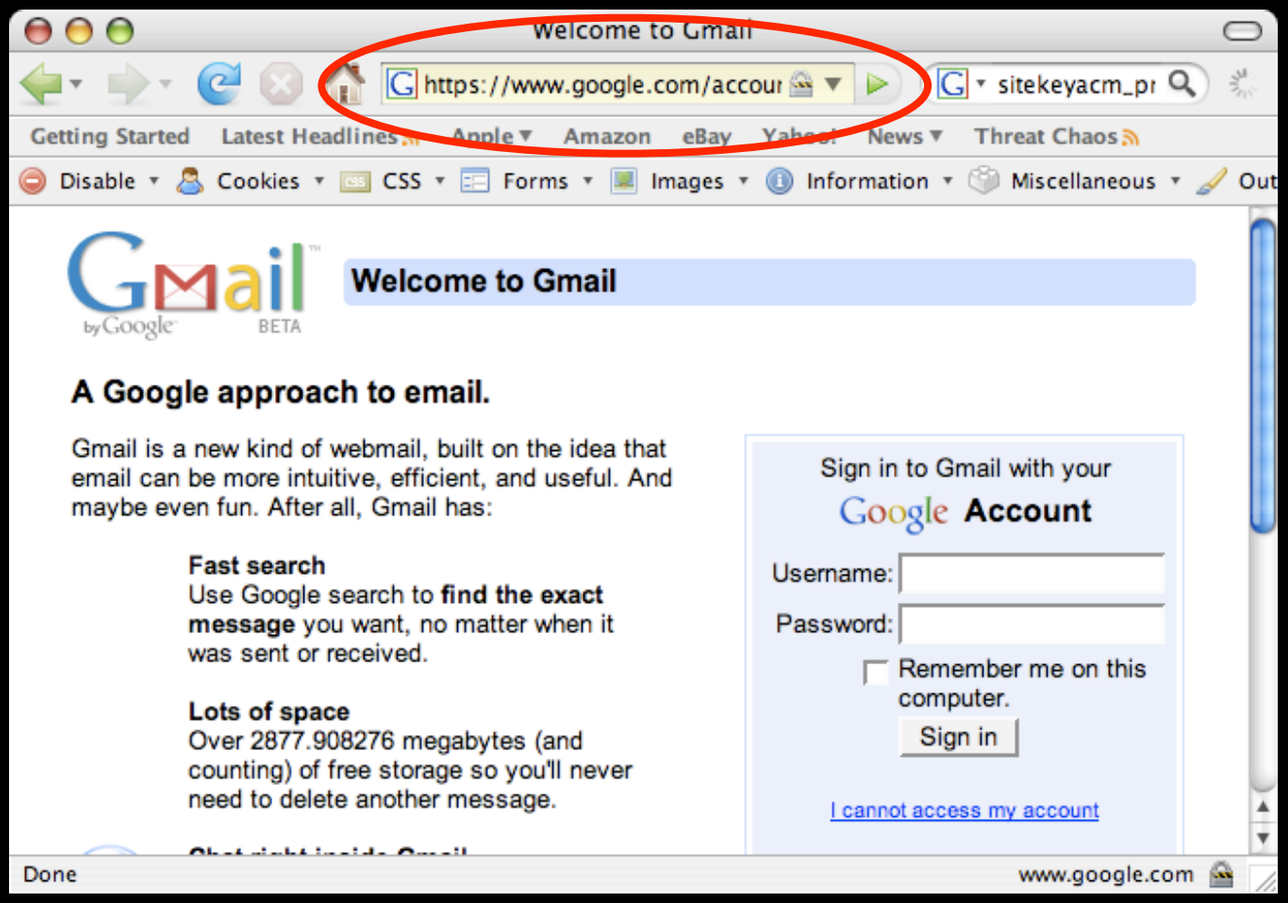
Disable | Cookies | CSS | Forms | Images | Information | Miscellaneous

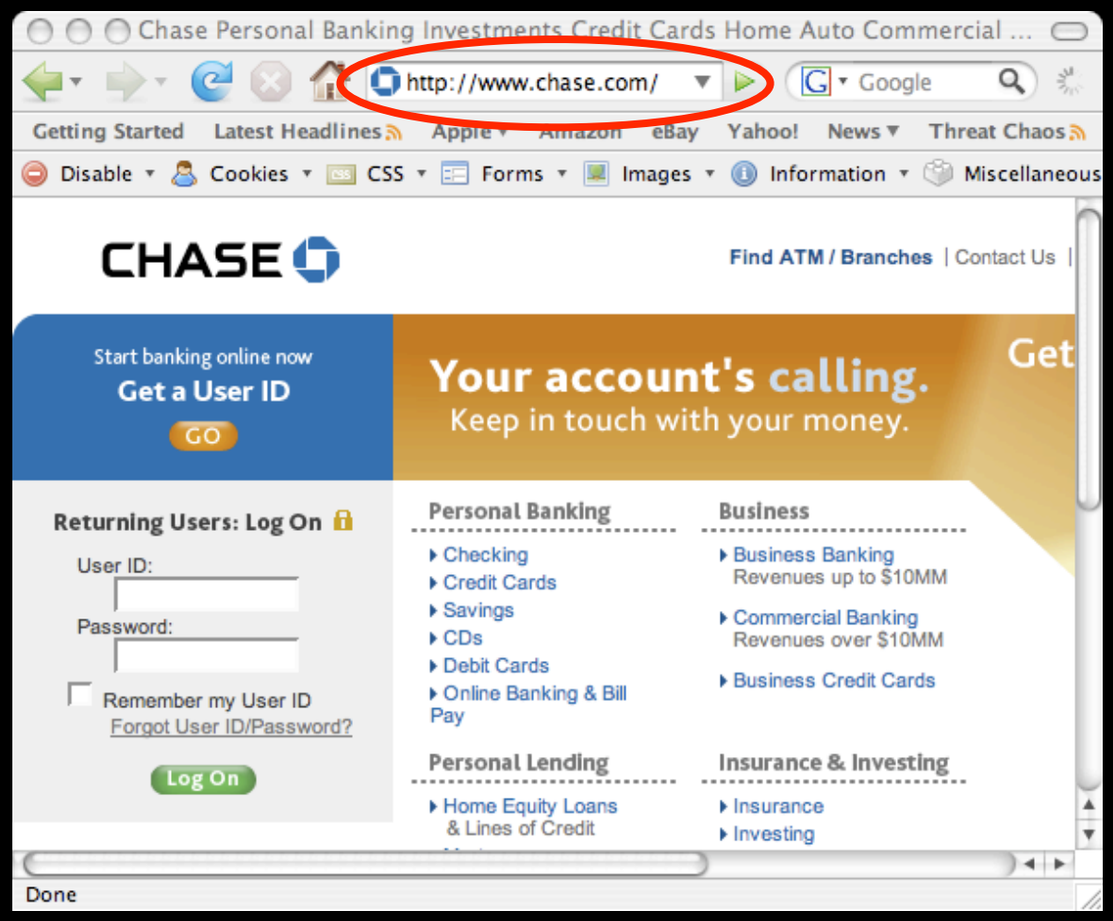
L Jean Camp

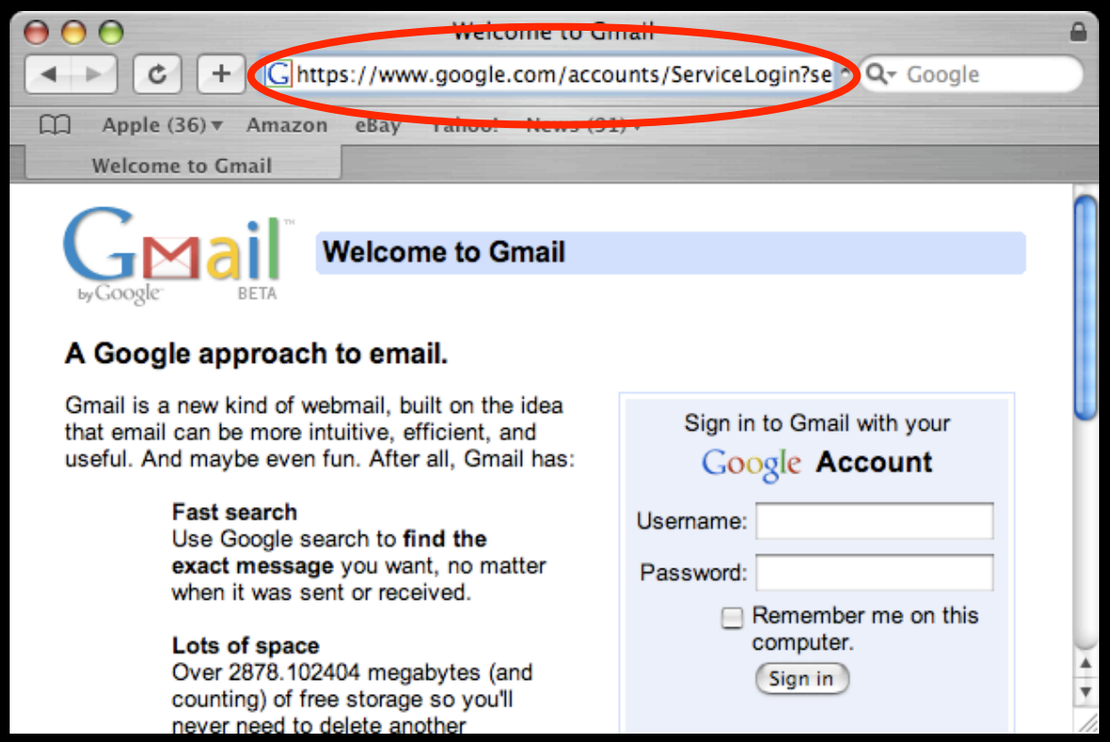
Contact | Resume | CV | Research | Teaching | Students | Design for Values | Security

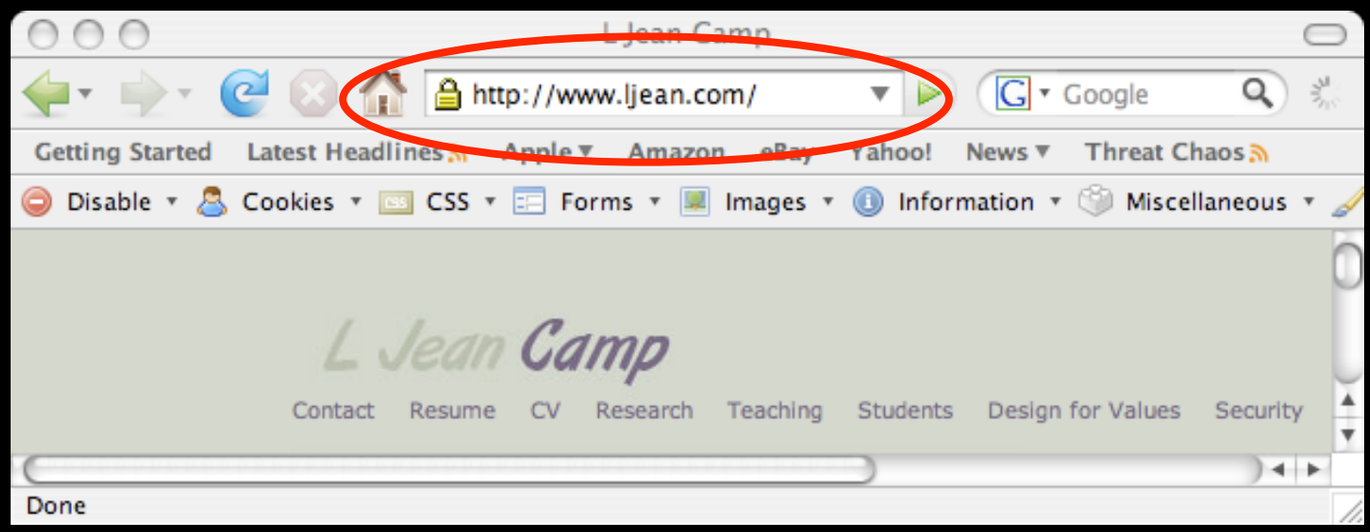
Done

Address Bars

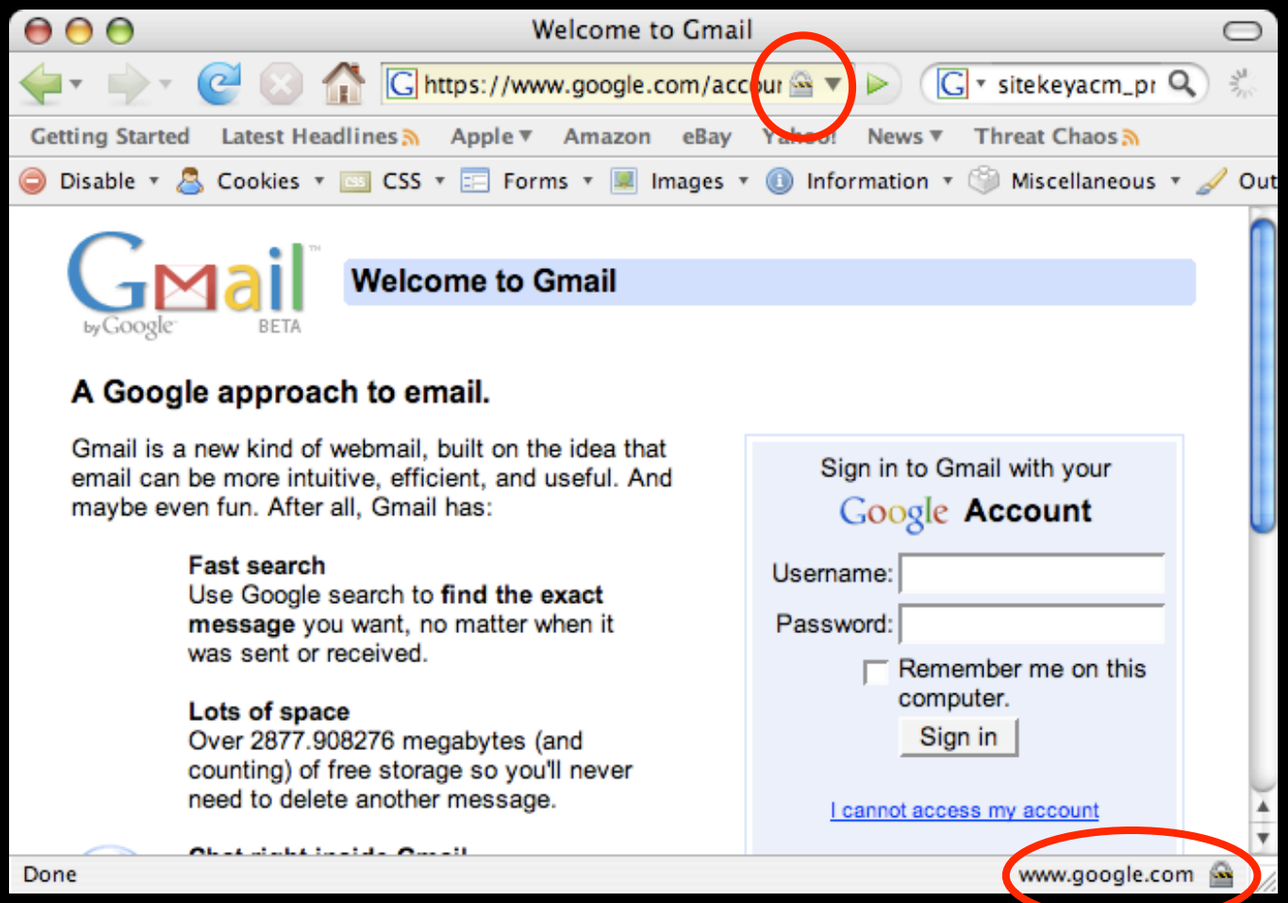


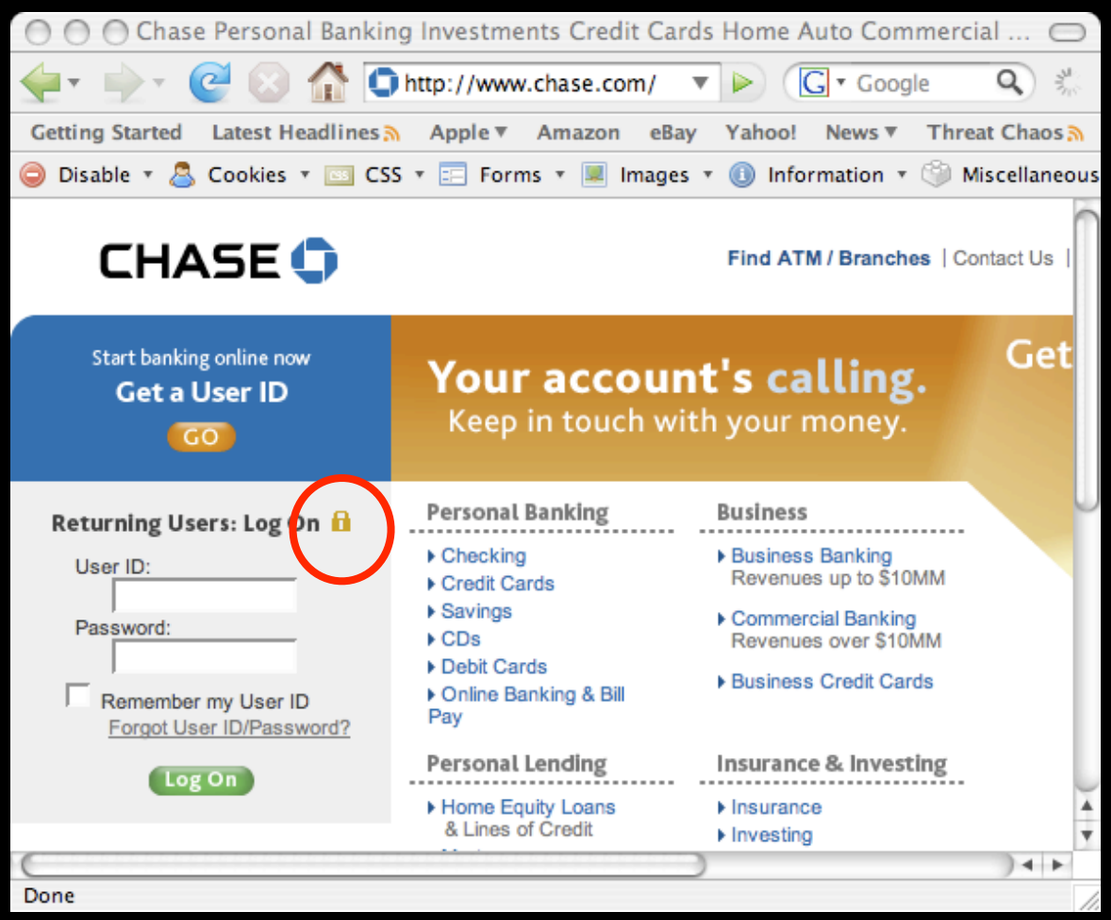


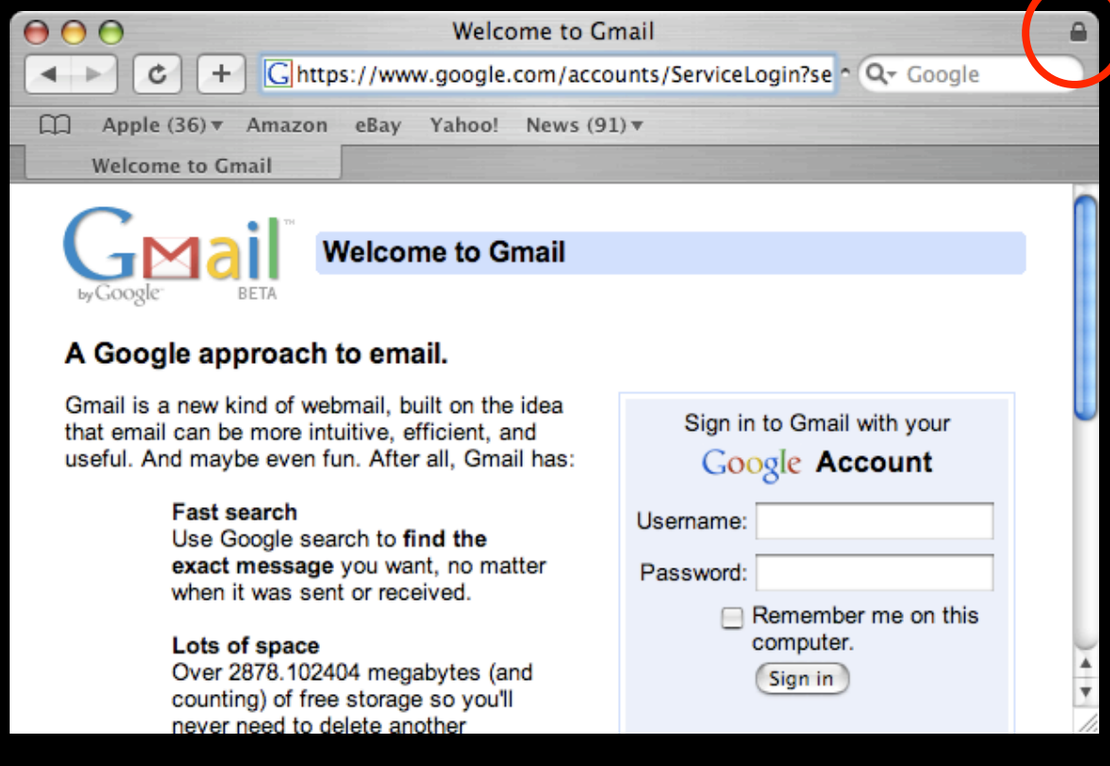


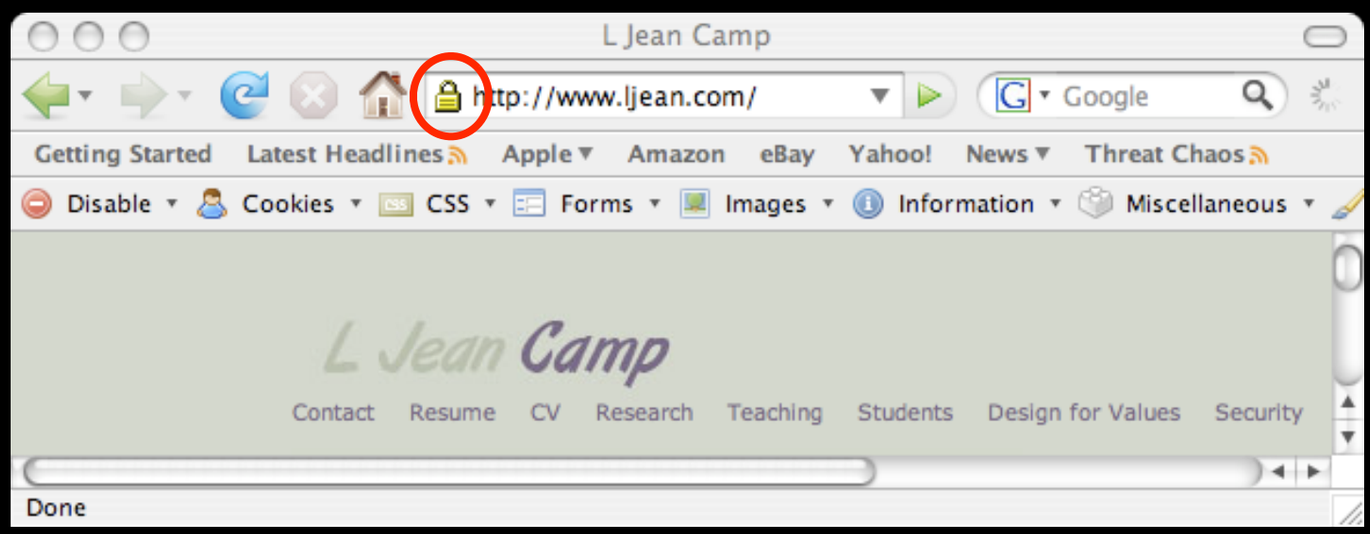


Lock Icons

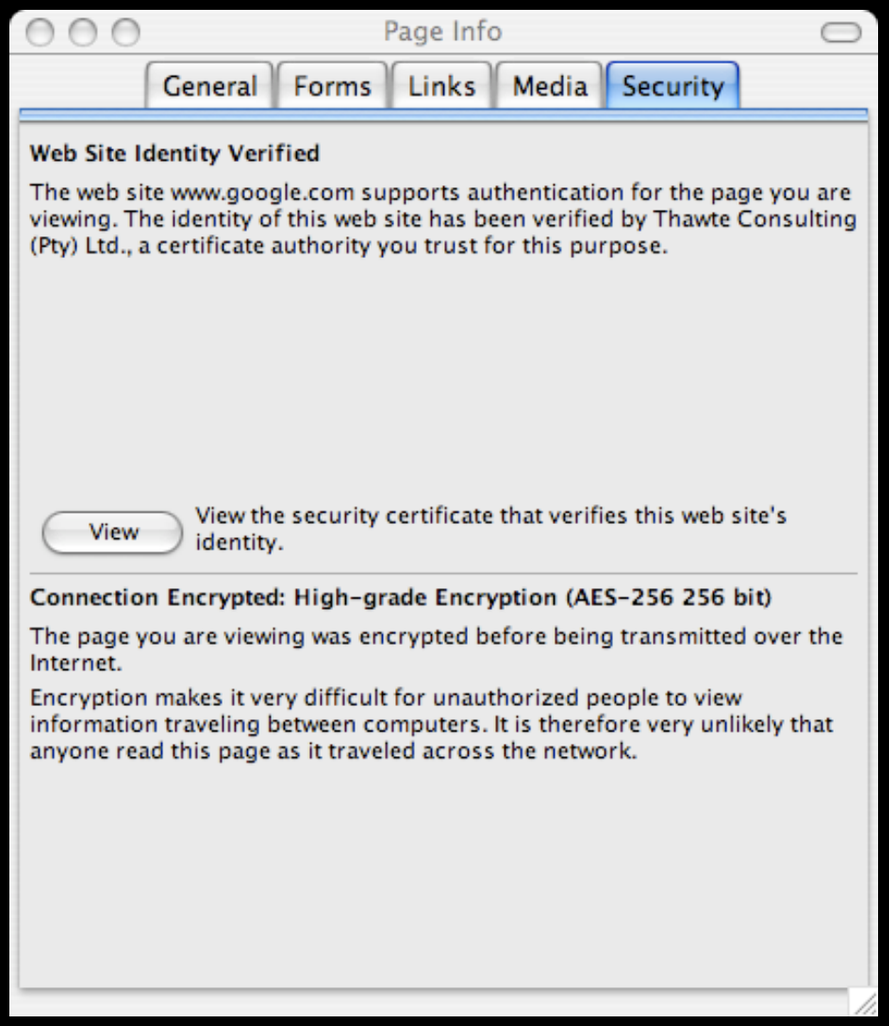

Welcome to Gmail
https://www.google.com/accour
sitekeyacm_pr
Getting Started
Latest Headlines
Apple
Amazon
eBay
News
Threat Chaos
Disable
Cookies
CSS
Forms
Images
Information
Miscellaneous
Gmail by Google BETA
Welcome to Gmail
A Google approach to email.
Gmail is a new kind of webmail, built on the idea that email can be more intuitive, efficient, and useful. And maybe even fun. After all, Gmail has:
Fast search
Use Google search to find the exact message you want, no matter when it was sent or received.
Lots of space
Over 2877.908276 megabytes (and counting) of free storage so you'll never need to delete another message.
Sign in to Gmail with your Google Account
Username:
Password:
Remember me on this computer.
Sign in
I cannot access my account
Done
www.google.com

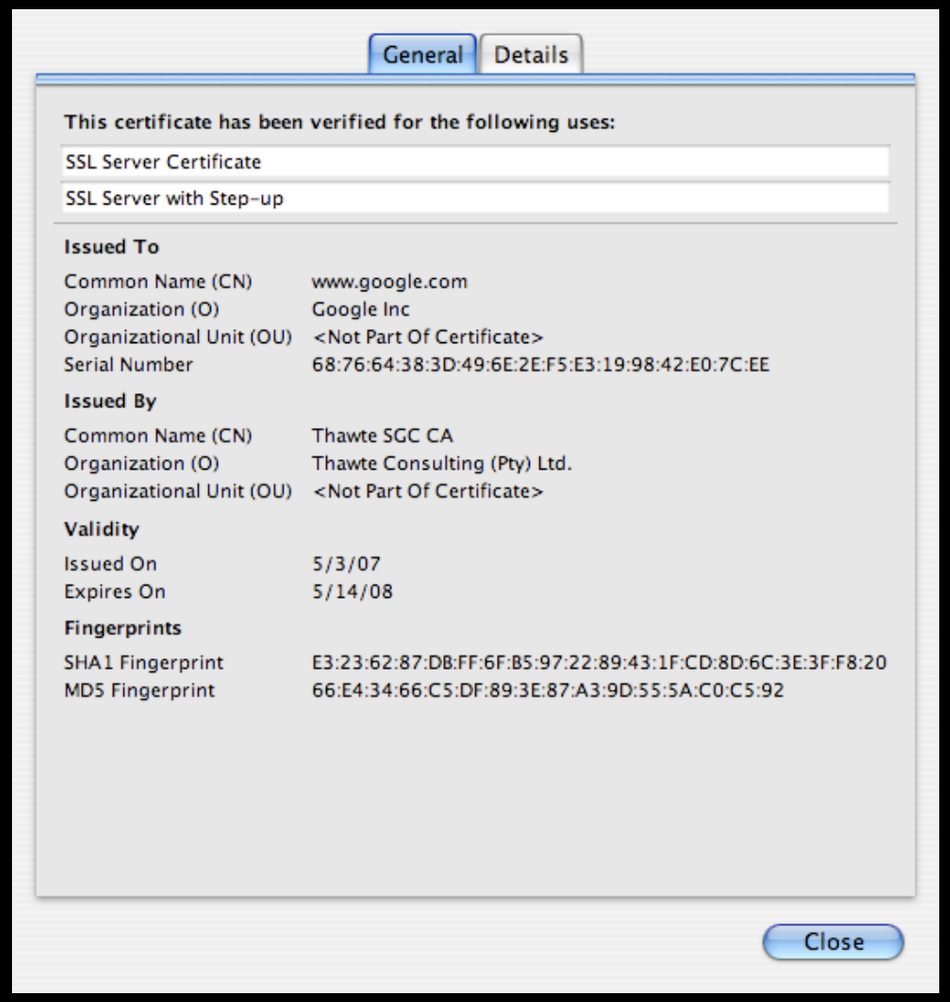

Chase Personal Banking Investments Credit Cards Home Auto Commercial ...
http://www.chase.com/
Google
Getting Started
Latest Headlines
Apple
Amazon
eBay
Yahoo!
News
Threat Chaos
Disable
Cookies
CSS
Forms
Images
Information
Miscellaneous
CHASE
Find ATM / Branches | Contact Us |
Start banking online now
Get a User ID
GO
Your account's calling.
Keep in touch with your money.
Get
Returning Users: Log On
User ID:
Password:
Remember my User ID
Forgot User ID/Password?
Log On
Personal Banking
Checking
Credit Cards
Savings
CDs
Debit Cards
Online Banking & Bill Pay
Business
Business Banking
Revenues up to $10MM
Commercial Banking
Revenues over $10MM
Business Credit Cards
Personal Lending
Home Equity Loans & Lines of Credit
Insurance & Investing
Insurance
Investing
Done

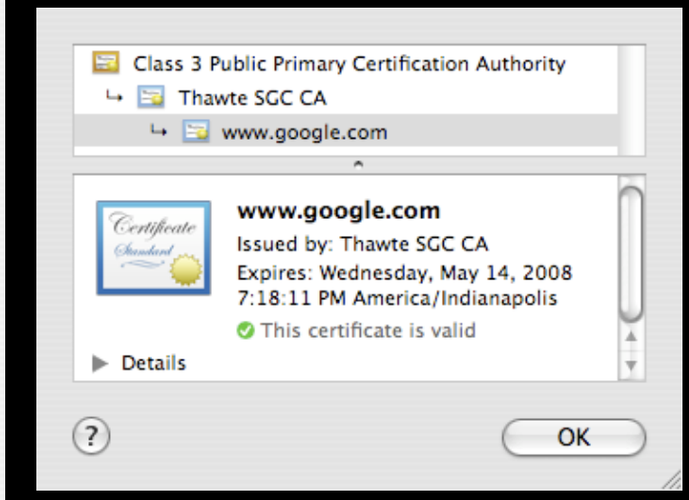

Welcome to Gmail
https://www.google.com/accounts/ServiceLogin?se
Google
Apple (36)
Amazon
eBay
Yahoo!
News (91)
Welcome to Gmail
Gmail by Google BETA
Welcome to Gmail
A Google approach to email.
Gmail is a new kind of webmail, built on the idea that email can be more intuitive, efficient, and useful. And maybe even fun. After all, Gmail has:
Fast search
Use Google search to find the exact message you want, no matter when it was sent or received.
Lots of space
Over 2878.102404 megabytes (and counting) of free storage so you'll never need to delete another
Sign in to Gmail with your Google Account
Username:
Password:
Remember me on this computer.
Sign in


L Jean Camp
http://www.ljean.com/
Google
Getting Started
Latest Headlines
Apple
Amazon
eBay
Yahoo!
News
Threat Chaos
Disable
Cookies
CSS
Forms
Images
Information
Miscellaneous
L Jean Camp
Contact
Resume
CV
Research
Teaching
Students
Design for Values
Security
Done

Certificate Dialogs







- No consistency
- Can average user make heads or tails of info provided?

What Security Problem is Being Solved?

- Do we want to prevent credential loss?
- Credit fraud or other monetary loss?
- Money laundering?
- Data loss (leading to secondary loss, privacy or full fledged ID theft)?

How Expensive are Solutions?

- Initial Enrollment Costs
- Deployment Costs
- Support Costs
- Financial industry is phobic of any client side solutions
- If cost per transaction is not lower than teller, ignore it.

Who are the Adversaries?

- Phishers
- Pharmers
- Crimeware
- Traditional Fraud (Family members, co-workers, etc.....)

Mutual Authentication?

- People are tricked in phishing because the website doesn't authenticate itself
  - SSL doesn't count
- Mutual Authentication may solve phishing/ pharming, but what about malware?
- Session Hijacking malware exists: eGold, ABN Ambro, other unreported cases...

Initial & Revalidation Enrollment Problems

- Strong authentication does not help if the right person isn't enrolled in the first place.
- Proper and secure initial enrollment can be expensive.
- Ditto for Revalidation
- These problems won't be addressed today, but are just as, if not more, important.

Single Sign-on vs. Transaction Based Authentication

- Most US banks use single-sign on
  - Artifact of current authentication techniques?
- Many European banks use authentication at the transaction level.
- Transaction based authentication is the only defense against session hijacking

3 Keys to Authentication

- Something you .....

1. Know
   - Passwords, challenge answers, etc..
2. Are
   - Biometrics (all types)
3. Have
   - Tokens, SecureID, Scratch-Pads, Cookies

Prevention vs. Detection

- Prevention: Focus on preventing credential/ information loss.
- Detection: Assume credentials will be lost, prevent stolen credentials from being misused.

Some Solutions?

Back-end Fraud Detection System

- Risk measurement programs measure:
  - IP addresses
  - geo-graphic locations
  - packet/person travel times
  - transfers to suspect companies/countries
- Strange behavior puts stop on account
- Doesn’t prevent credential loss or private data breach.

Digital One-Time Passwords 1

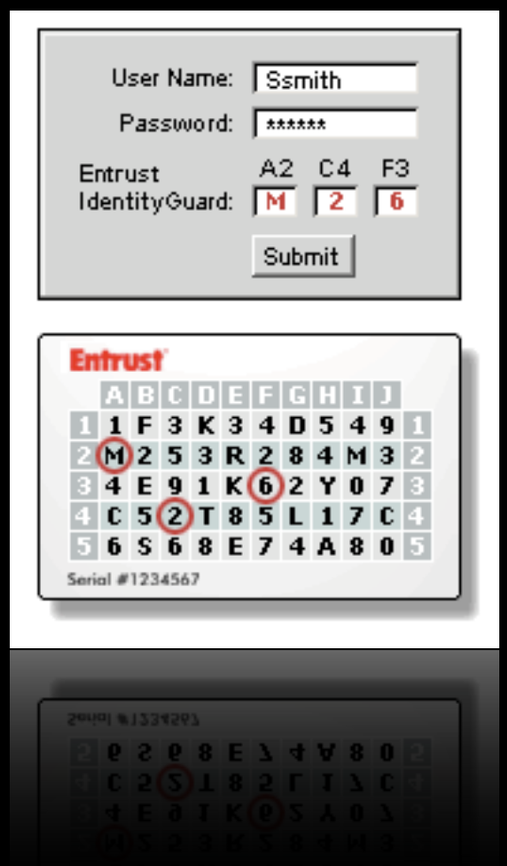
- RSA SecurID
- Server synched random number generator
- Numbers generated every 30-60 sec.
- Numbers effectively unpredictable
- Lost tokens use serial numbers or other challenge questions.
- Timing features makes it unlikely solution for MA or Transactions

Digital One-Time Passwords II

- InCard Token
- Same form-factor as credit-card
- People are familiar with these
- Random number generated with button push.
- Better for MA and Transaction usability

Grid Based One-Time Passwords I

- Grid Cards (Entrust GridAuth)
- User is issued grid of random alpha-numeric characters.
- Can be used for MA and TFA.
- User requests characters at specific grid locations for MA.
- Server requests characters for TFA



Paper Based One-Time Passwords II

- Scratch Cards (Entrust GridAuth)
- Issued card is covered list of OTPs
- User reveals one password per use.
- Can be used for MA and TFA
- New cards must be reissued in timely fashion.

Crypto Tokens

- Contains secret-keys, certificates and the ability to sign, verify, decrypt and/or encrypt.
- Can be used to sign username, nonce and password.
- Needs OS specific drivers
- Interface Trusted Path Issues make malware worrisome.

Server Authentication Via Images

- A Shared Secret-Image is shown to user before password is released.
  - Bank of America Site-Key
  - Yahoo! Site-Seal

Here's How SiteKey Works

By passing back and forth secret information that only you and Bank of America know, you can feel even more secure with your Online Banking experience. We recognize you and you recognize us. Learn more or sign up now.

Online Banking Sign In

View demo | Learn more | Enroll

Use Saved Online ID

**********12345

Use or add another Online ID

Sign in using my SiteKey

1 Enter your Online ID.

2 Click **Sign In using my SiteKey.**

Your SiteKey Image and Message:

cute dog

3 If we recognize your computer: We will display your SiteKey.

What was your high school mascot?

*** Answer:**

4 If we don't recognize your computer: We will ask you one of your SiteKey Challenge Questions.
After you answer your SiteKey Challenge question correctly, your SiteKey will display.

Passcode: ********

5 Once you recognize your SiteKey, you know you are at the valid Bank of America site. You can then feel safe to enter your passcode and continue to Online Banking.

To take advantage of this new security feature now, click the **Sign Up** button below. Then, just follow the simple on-screen instructions to set up your SiteKey and SiteKey Challenge Questions.

Sign Up | Return to Customer Service

Secure Area

Passmark Overview

- Cookie & Flash Objects installed on computer to identify it later

Bank of America Higher Standards

Online Banking

If your SiteKey is correct, you know you are at the valid Bank of America site.

If you recognize your SiteKey, please enter your passcode and click the **Sign In** button.

An asterisk (*) indicates a required field.

Your SiteKey:

my private message

*** Passcode:** ••••••

(4-12 numbers and/or letters, case sensitive)

Sign In

Forgot your SiteKey?

Incorrect SiteKey showing?

Reset passcode

Secure Area

- Identified computers are presented with identifying image after username is supplied.

Bank of America Higher Standards

Online Banking

We do not recognize your computer

We do not recognize the computer you are signing in from.

To ensure your online security, please answer your SiteKey Challenge Question. If you want us to remember this computer the next time you sign in, please check the **Yes** checkbox below. If not, please check **No**. Then click the **Continue** button.

An asterisk (*) indicates a required field.

What was your best childhood friend's first name?

*** Answer:** 1

(Not case sensitive)

*** Remember this computer next time you Sign in?**

Learn more

- (•) Yes, remember this computer
- ( ) No, don't remember this computer

Continue

Forgot the answer to your SiteKey Challenge Question?

Secure Area

- Otherwise, rely on challenge questions.

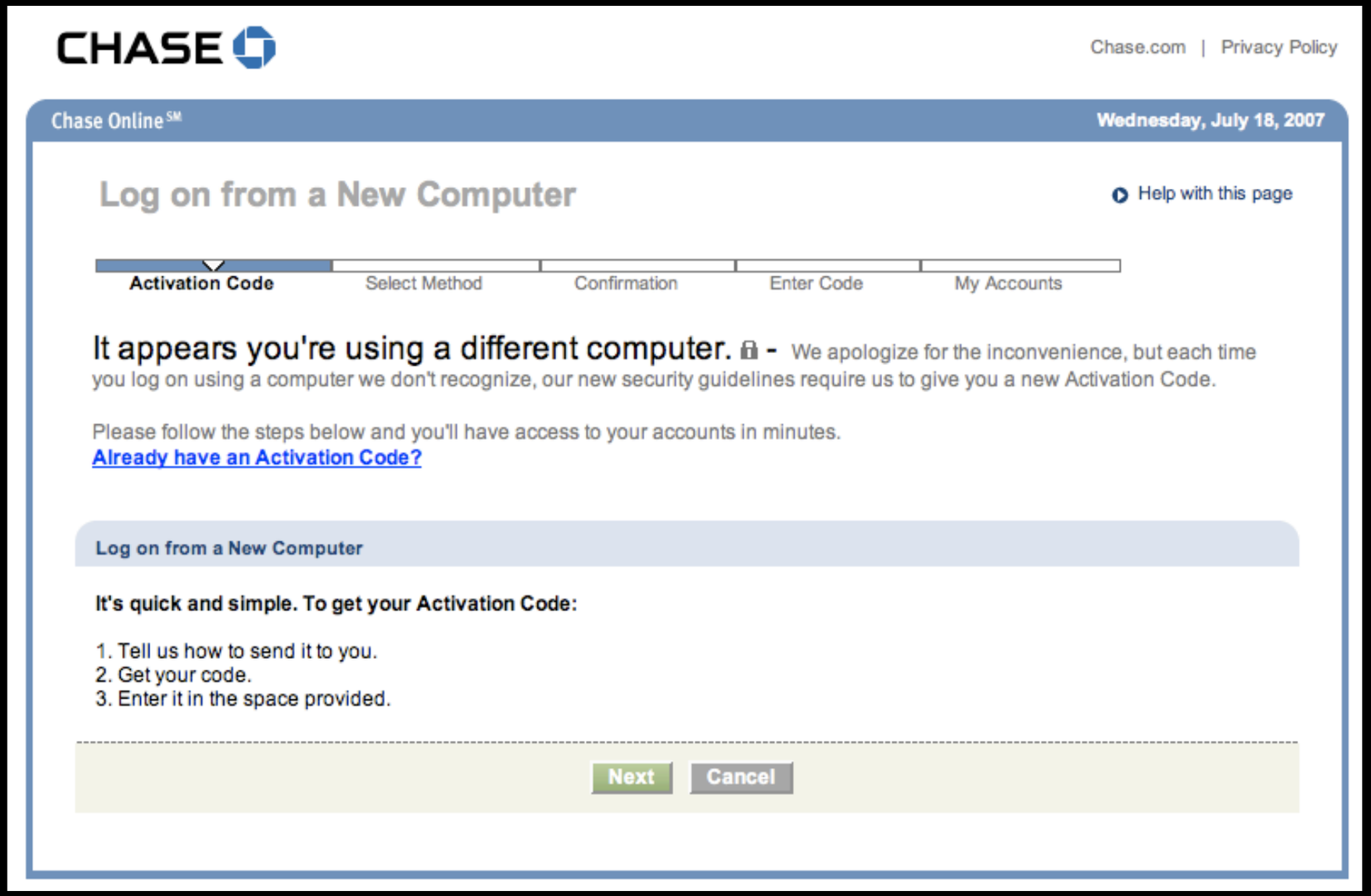
Knowledge Based Challenges

- Questions that only you should know the answer to?
  - Mother's Maiden Name
  - Your Elementary/Jr High/Sr High School
  - Pet's name
- Which questions are those exactly
- Used for *authentication* and Identity Reestablishment
- Which questions' answers can be data-mined
  - (i.e. facebook proof, etc....)

Out of Band Communication

- Use out-of-band communication to deliver authenticating secret
  - Cell-Phone Texting
  - Email
  - Voice Calls

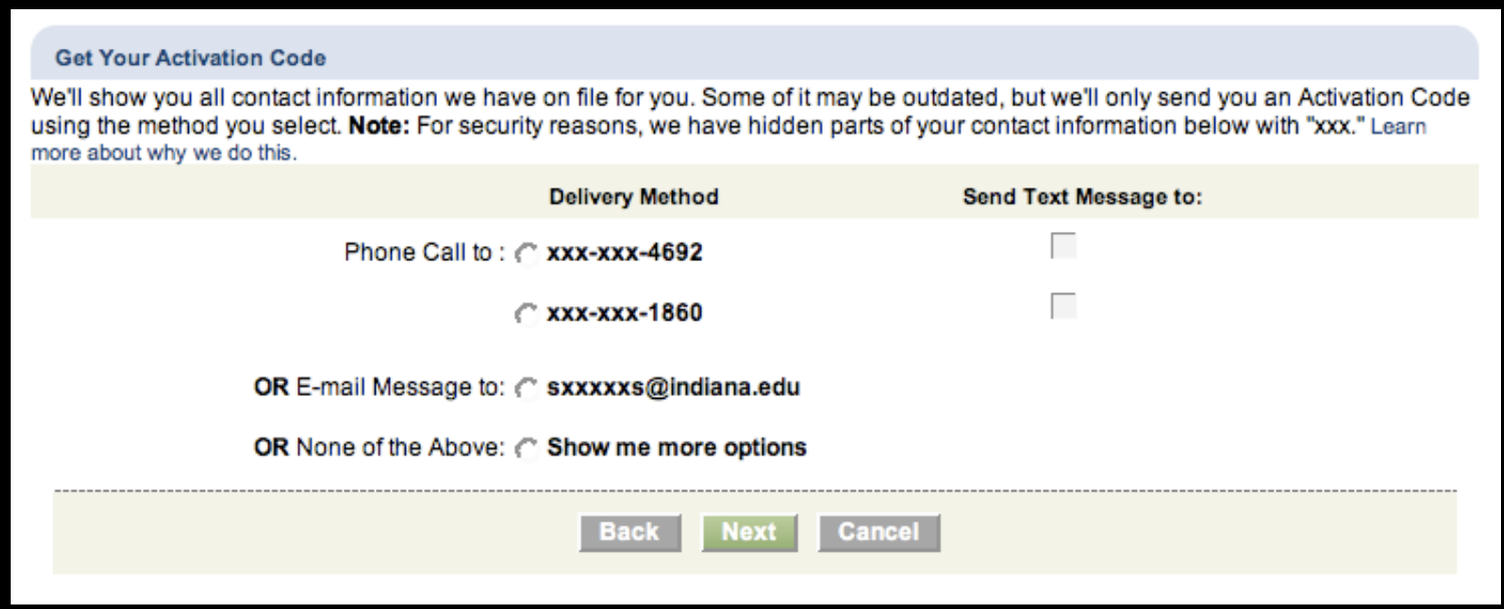
Chase Authentication System



Cookies are placed on users' computers based on out of band communication

Chase Authentication System Cont.

- Activation code delivered by choice of out-of-band communication
- Correct code and password places cookie on browser



Cookies

- A cookie is placed on computer, and attached to account.
- Only browsers with cookies can access account.
- Privacy concerned users turn off cookies/ mutliple browsers/computers/etc...
- Cookies can be stolen with pharming.

Biometrics

- Measuring some property of who you are:
  - Fingerprints
  - Facial Recognition
  - Voice Recognition
  - Keystroke Dynamics

Voice Recognition

- Low cost of entry/ pervasiveness of mics increasing

- Adaptive vs. Non-adaptive templates.

- Authenticator changes: puberty, colds, laryngitis.

- Operating System/Driver issues.

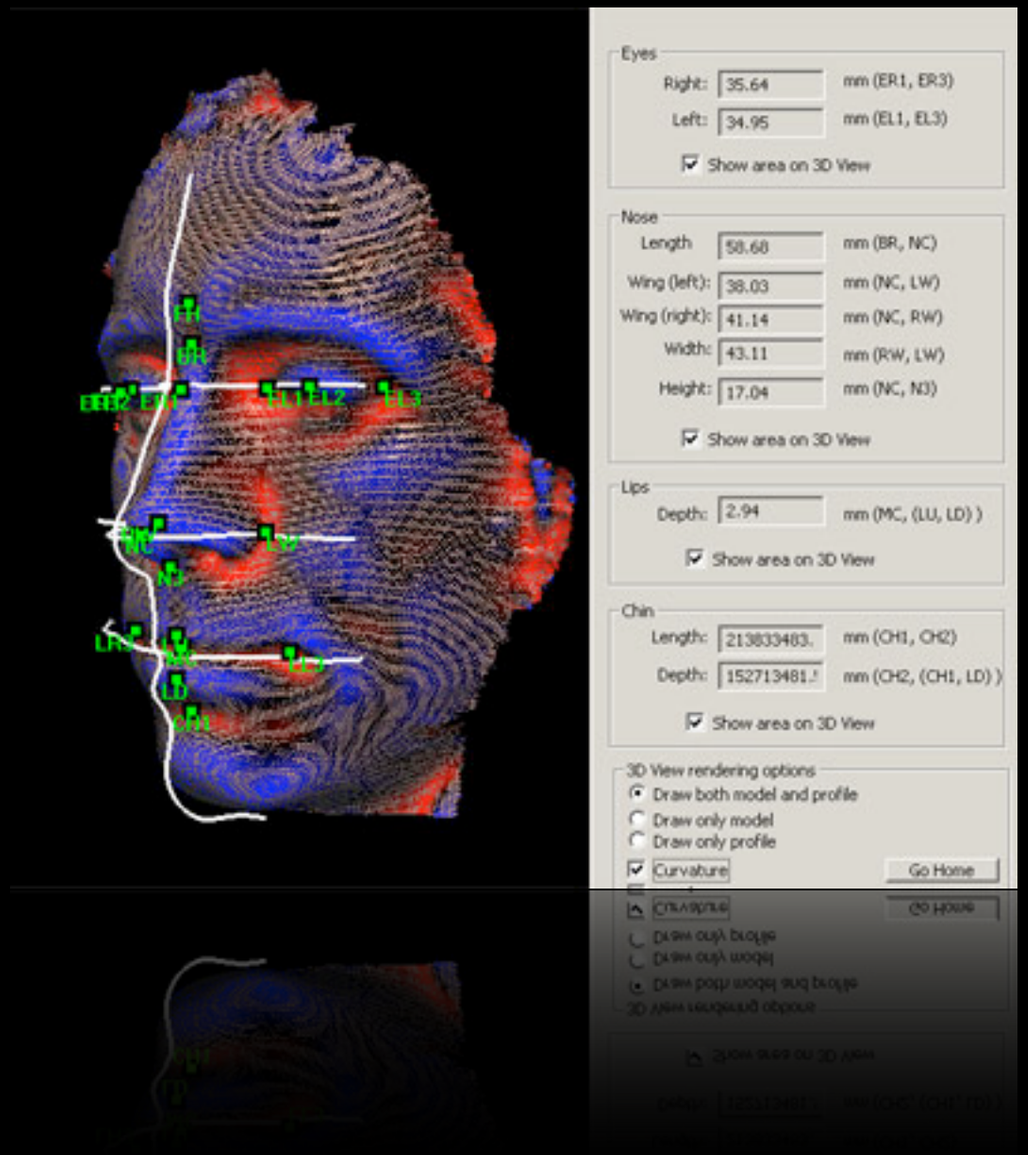
Facial Recognition

- Can web-cams be used/ prevalence is quickly growing.

- Template based on specific measurements on face & resilient to daily changes in appearance.

- Template changes: aging, plastic-surgery

- Processing & bandwidth requirements



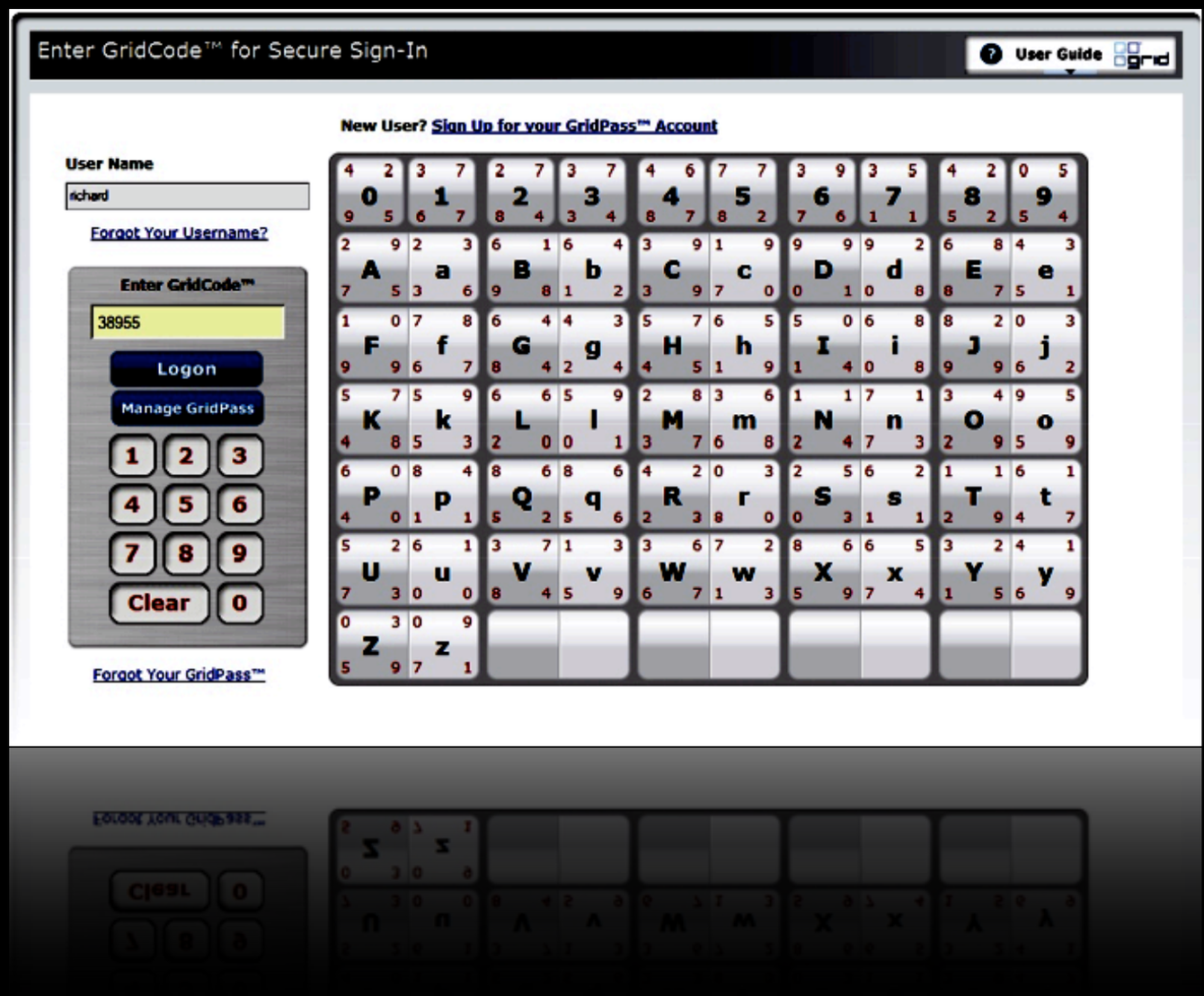
Facial Recognition Challenge Problem

Keyboard Dynamics

- Ubiquitous distribution of keyboards.
- Measure dynamics such as typing rates, speed between different keys, etc....
- Static vs. dynamic
- People use a number of different keyboards.
- OS/Driver Issues
- Unreliable if users are beginners, distracted, etc...

Visual Keyboard

- User specifies corner during account enrollment
- User enters numbers corresponding to password
- Screen capture or keyboard logger insufficient (unless done repeatedly & in conjunction)

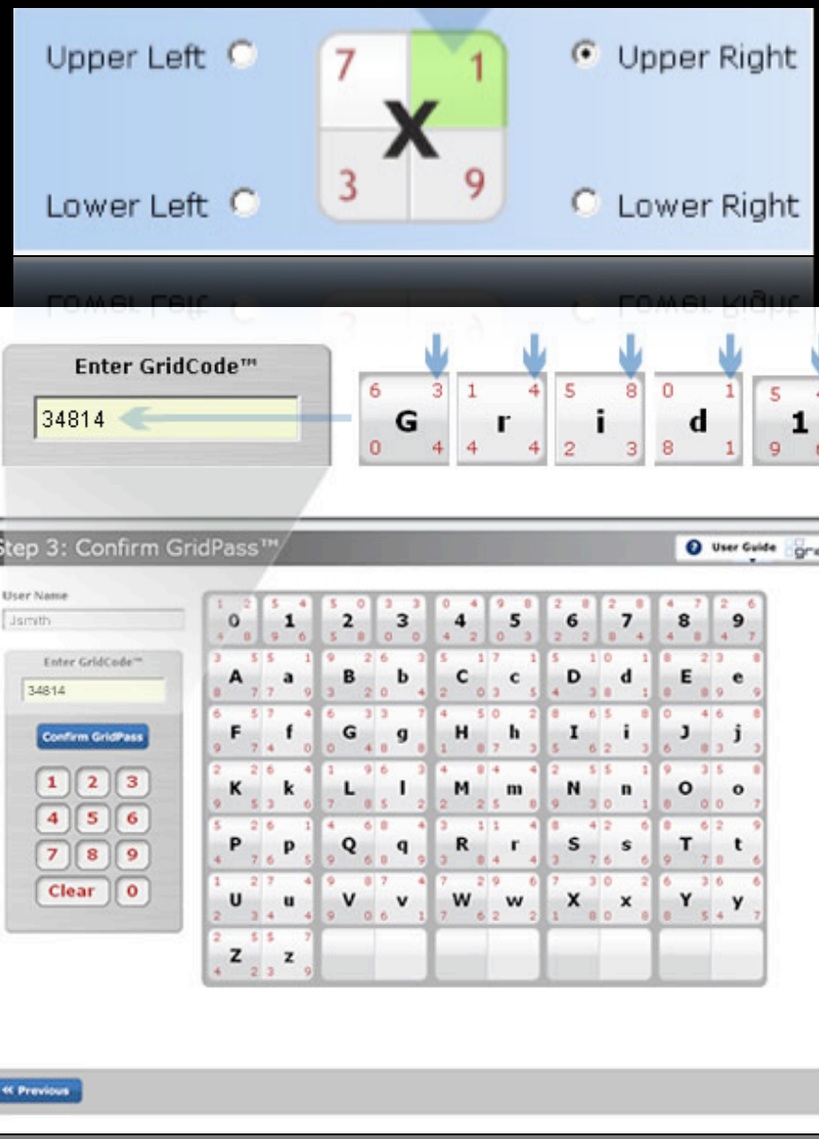


GridCode Keyboard

- Enrollment: user selects corner (this does not change)

- Password entry: user inputs numbers in specified corner, corresponding to password.

- Every new authentication attempt randomizes numbers in corners.



Extended Validation Certificates

- Primary difference between current certs is non-technical:

  Identity of certificate requested is stringently checked.

- Browsers will display different security indicators than previous certs.

- Users aren't currently being tricked because they are accepting bad certs.

What Do We Do?

- Banks need to implement something.
- It needs to be cost effective or they can shutdown Internet Banking
  - (Bank of New Zealand)
- They needed it last year, future research is useful, but not a viable answer.
- Think *risk management* not silver-bullets.

Research Questions

- How do we know if a security technology is unworkable or has simply been incarnated with a poor interface?
- How do we generate user studies that simulate calls to action, motivated behavior and non-suspicious users.