Web Security Requirements: A Phishing Perspective

What is Usability? How are we failing?

Ian C. Fette, Norman Sadeh, Lorrie Cranor

March 15, 2006

{icf,sadeh,lorrie}@cs.cmu.edu

Carnegie Mellon

CMU Usable Privacy and Security Laboratory

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

The Phishing Problem

- It's easy to fake a page and collect user information

Chase OnlineSM - $20 Reward Survey - Mozilla

File Edit View Go Bookmarks Tools Window Help

Back Forward Reload Stop http://chaseonline.new-paid-survey.us/ Search Print

Home Bookmarks mozilla.org mozillaZine HP iPAQ hx4700 an... mozdev.org

usability of w... Program (Untitled) Citi Credit Car... U.S. Bank - Pe... MBNA.com - If... Bank of Ameri... Chase Online...

CHASE

Chase.com | Privacy Policy

Chase Online SM

Sunday, March 12, 2006

Online Survey

Help with this page

Chase Online SM $20 Reward Survey.

Chase Bank will add $20 credit to your account just for taking part in our quick 5 question survey. *

Reward Survey

Choose one question from each list below.

Have you recently noticed changes to Chase Bank Online web page surfing speed?	Yes - It's faster Yes - It's slower No - It's the same
How would you rate Chase Bank Online Website?	Outstanding Alright Could be Better Poor
Are you happy with the services Chase Bank provides compared with other banks?	Yes, Very happy Yes, But in some areas only No, But it's getting better No, Not at all
In the last 6 months have you considered changing banks?	Yes No

Run command: Adobe Reader - CH w3c06 - OpenOffice Mozilla-bin [3] ian@mentalis:/hom XMMS 5:37

Overview

- What does it mean for security to be usable?
- What security features do we currently have?
- Why what we have has failed (or will fail)
- Where our group is looking
- Concluding Remarks

What is usable security?

- Any interactions with the user should be at a level understandable by said user
- Required user interaction (both input and attention) should be kept minimal
- Should be “hard” for a user to commit a serious mistake
- Should be usable from wherever the user may be (public cafe, mobile device)
- Should consider users' disabilities

Current Security Features

- The Lock
  - Ignored by many
  - Confusion as to what it means
  - Mis-used by websites (next slides) so as to diminish power
- RSA SecurID
- PassMark SiteSecure
- Various chrome extensions

Chase Personal Banking Investments Credit Cards Home Auto Commercial Small Business Insurance - Mozilla

File Edit View Go Bookmarks Tools Window Help

Back Forward Reload Stop http://www.chase.com/ Search Print

Home Bookmarks mozilla.org mozillaZine HP iPAQ hx4700 an... mozdev.org

usability ... Program Chase P... Citi Credit... U.S. Bank... MBNA.co... Bank of A... Chase On... U.S. Bank... Slashdot:...

CHASE

Find ATM / Branches | Contact Us | Site Map | Search

Start banking online now
Get a User ID
GO

Consolidate your high interest bills with Chase and **save.**
0% APR for up to 12 Months*

Returning Users: Log On

User ID:

Password:

Remember my User ID

Forgot User ID/Password?

Log On

Protect Your Identity

Learn how to recognize and report fraudulent e-mail.

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
- Education Loans

Insurance & Investing
- Insurance
- Investing
- Retirement Planning

Tell me about...
- Premier Platinum Banking
  Exclusive banking and investment benefits for clients with higher balances

News & Announcements
- U.S. Armed Forces Overseas
  Please contact us if you need assistance with your Chase or Bank One accounts.
- Chase offers Zero-Fees!
  For academic year 2006-2007 the origination fee will be paid on all Federal Stafford Loans that Chase funds directly to students.

1 2 3 4 Run command: Adobe Reader - CH w3c06.odp - OpenO Mozilla-bin [3] ian@mentalis:/hom XMMS - 1.11 - blac 7:12

MBNA.com - If you're into it, we're into it. - Mozilla

File Edit View Go Bookmarks Tools Window Help

Back Forward Reload Stop http://www.mbna.com/ Search Print

Home Bookmarks mozilla.org mozillaZine HP iPAQ hx4700 an... mozdev.org

usability ... Program Chase Pe... Citi Credit... U.S. Bank... MBNA.co... Bank of A... Chase On... U.S. Bank... Slashdot:...

mbna

Log In | Contact Us | Search | En Español

MBNA: USA [Change]

Cards Loans Savings Business

Access Your Account

Login:

Password:

Log In » | Sign Up

» Forget Login or Password?

» Business Account Log In

MBNA Card Solutions » Apply Now

MBNA - Bank of America Agreement

Get the latest information about the Bank of America - MBNA agreement.

Featured Products

MBNA Cash Back® Card
The card that pays you back — in cash! — with every purchase.
Apply Now

Working Assets® Card
Everyday purchases generate donations for a better world.
Apply Now

Elite Rewards® Card

» Cards
Travel Rewards, Cash Back Rewards, Student, Business, Gift Cards, more...

» Savings
Money Market Deposit Accounts, High-Yield CDs, IRAs, more...

» Loans
Debt Consolidation, Home Improvement, Mortgage & Home Equity, Auto, more...

» Business
Business Credit Cards, Line of Credit, Practice Financing, more...

1 2 3 4 Run command: Adobe Reader - CH w3c06.odp - OpenO Mozilla-bin [3] ian@mentalis:/hom XMMS Gimp [5] 7:18

Bank of America | Home | Personal - Mozilla

File Edit View Go Bookmarks Tools Window Help

Back Forward Reload Stop http://www.bankofamerica.com/ Search Print

Home Bookmarks mozilla.org mozillaZine HP iPAQ hx4700 an... mozdev.org

usability ... Program Chase Pe... Citi Credit... U.S. Bank... MBNA.co... Bank of A... Chase On... U.S. Bank... Slashdot:...

Bank of America Higher Standards

Locations · Contact Us · Help · Sign In

Search

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

Online Banking Sign In

View demo | Learn more | Enroll

Enter Online ID:

Save this online ID

Enter Passcode:

Account in:

Dist. of Colum

Sign In

Forgot or need help with your ID?

Reset passcode

Your Security and Privacy Partner

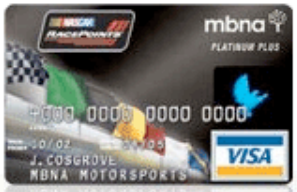
Learn how we're committed to your security

Protect yourself against fraud

Guard against scams with the free Bank of America

What moves you?

Get the card that rewards your passion.
Choose from hundreds of new cards, including NASCAR, football, travel, and more.



See all cards

Products & Services

- Online Banking
- Checking
- Savings & CDs
- Credit cards
- 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™ NEW!
- IRAs
- Buying a home
- Searching for a home
- Moving
- Planning for college
- Getting a student loan
- Planning for retirement
- More options >

1 2 3 4 Run command: Adobe Reader - CH w3c06.odp - OpenO Mozilla-bin [3] ian@mentalis:/hom XMMS Gimp [6] 7:20

We've Failed The Lock

- We started with something ill-designed
- We made it worse by confusing the issue "The lock means you're secure"
- We started using the indicator outside of its normal location, and now people look for it outside of its normal location.

RSA SecurID

- Moving beyond the browser to hardware assistance
- Usable at home or on the road
- ... but vulnerable to man in the middle attacks

Passmark SiteSecure

- Attempt at two-factor mutual authentication using properties of the computer as the second factor
- Enrollment process to 'sign up' a computer
- Once enrolled, user authenticates in part based on the computer they are using
- Bank authenticates itself by displaying a shared secret (picture)
- Enrollment process can be spoofed

Phishing Toolbars

- Overall, fail to protect users from high quality spoofs
- Users ignore indicators, as security is not their primary objective
- Pop-up warnings are slightly more effective, but overuse and false positives lead to the "just-click-ok" syndrome.

[1] M. Wu, R.C. Miller and S.L. Garfinkel, "Do security toolbars actually prevent phishing attacks?" in CHI (to appear), 2006. [Online]. Available: http://www.simson.net/ref/2006/CHI-security-toolbar-final.pdf

Where Our Group is Looking

- Heuristic Detection
  - Link Characteristics and HTML tricks
  - Header Information
  - Domain Age
  - “Inbox context”
- Collaborative Approaches
  - Leverage economies of scale
  - Publish warnings, or “vaccines” (think virus definitions)
  - Issues of trust in reporting, detecting misinformation

Where Our Group is Looking (2)

- Semantic Approaches
  - User's environment knows more about the user than the ISP does
  - Detect deviance from normal user behavior
  - Semantic approaches, including digital wallets or federated identity management systems
- Leveraging Out-Of-Band Communications
  - Salvaging PKI
  - Building on current relationship establishment procedures
  - Facilitating support technologies

Where Our Group is Looking (3)

- Understanding the Users: Interviews
  - People misunderstand many cues the browser provides:
    - Some are alarmed by 'warnings' that they are entering a secure site
    - Certificates, especially self-signed, and encryption are confusing to users: “I guess I'm not fully sure what 'encrypted' means.” - user
  - Some are highly affected by targeted attacks
  - Past “experience” doesn't necessarily help

Where Our Group is Looking (4)

- Educating the User
  - Providing training in the context of the user's inbox
  - Tailoring the training to the specific user's needs, adapting to strengths and weaknesses
  - Creating an educational game to teach anti-phishing skills

Concluding Remarks

- New solutions must take usability into account
- Security should be analyzed from a holistic perspective, including user analysis
  - What do we rely upon the user doing?
  - Can the user be tricked into doing a “bad” action at any stage?
- Expectations for user action should be minimal
- Active, positive indicators of problems

Questions?

- Thank you
- Ian Fette, Norman Sadeh, Lorrie Cranor
Carnegie Mellon University
School of Computer Science – COS
5000 Forbes Ave.,
Pittsburgh PA 15217

{icf,sadeh,lorrie}@cs.cmu.edu