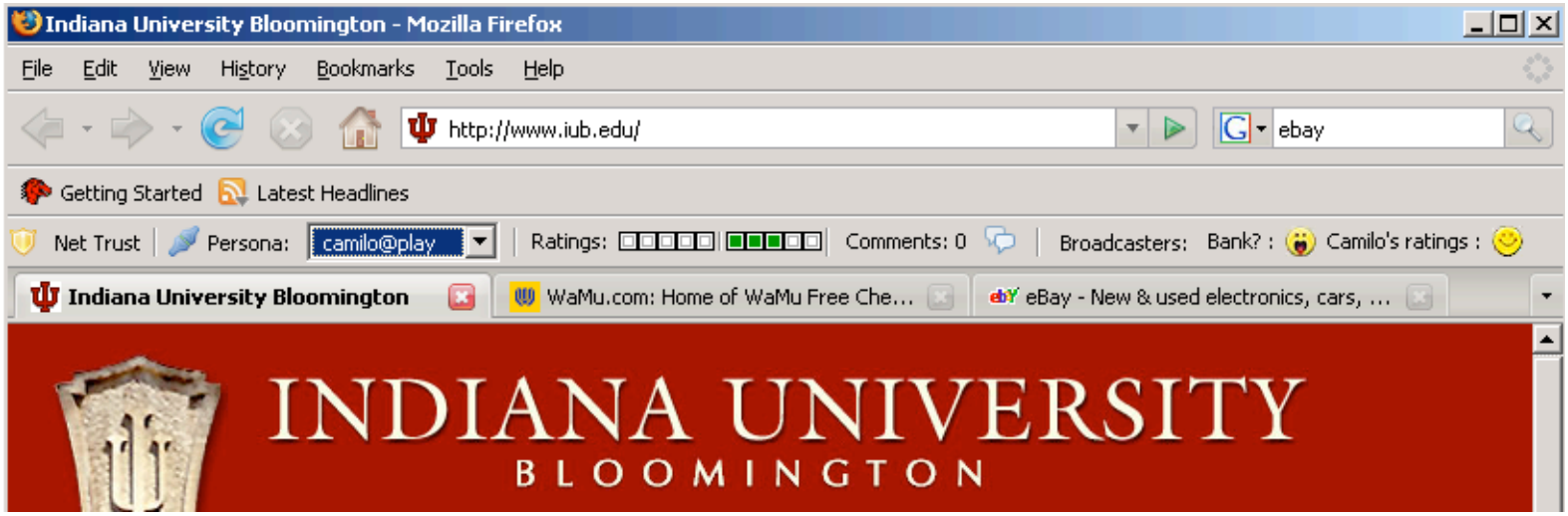
Net Trust

www.ljean.com/NetTrust

L Jean Camp

{ljcamp, bpstephe}@indiana.edu



Google™

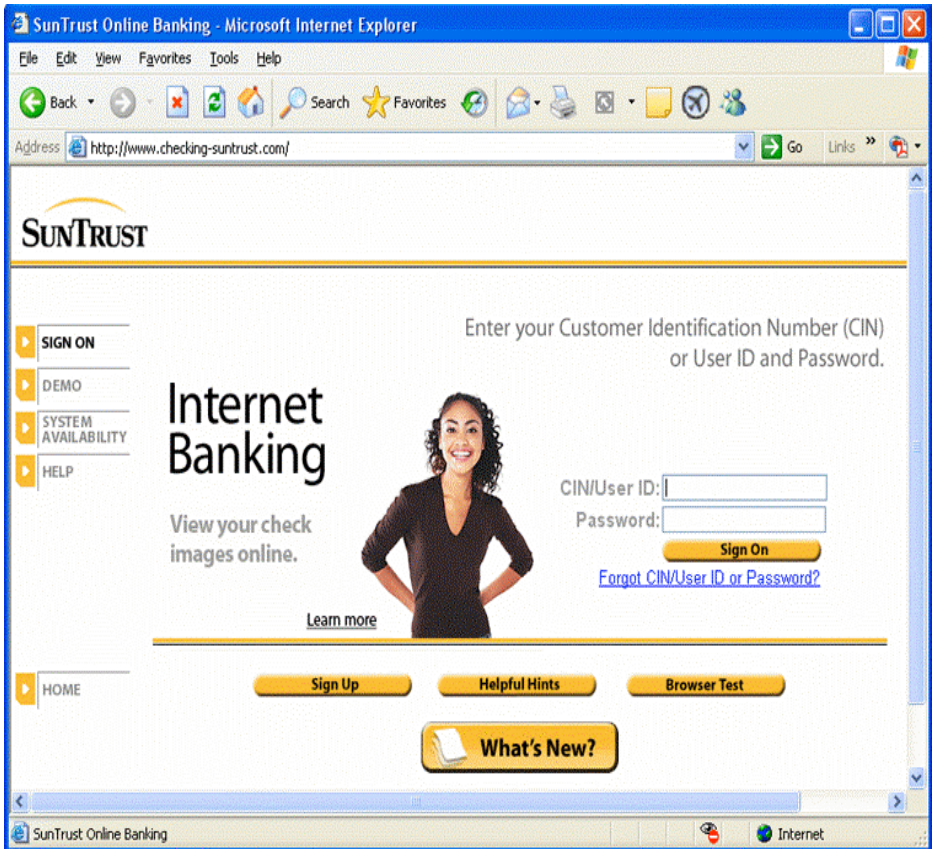
Trust and Context Offline

vs.

Resource Verification

Resources are often fairly easy to identify as highly reliable or high risk in the physical realm

Trust and Context



Contextual Information is not available on the web.

Avoiding Malicious Sites

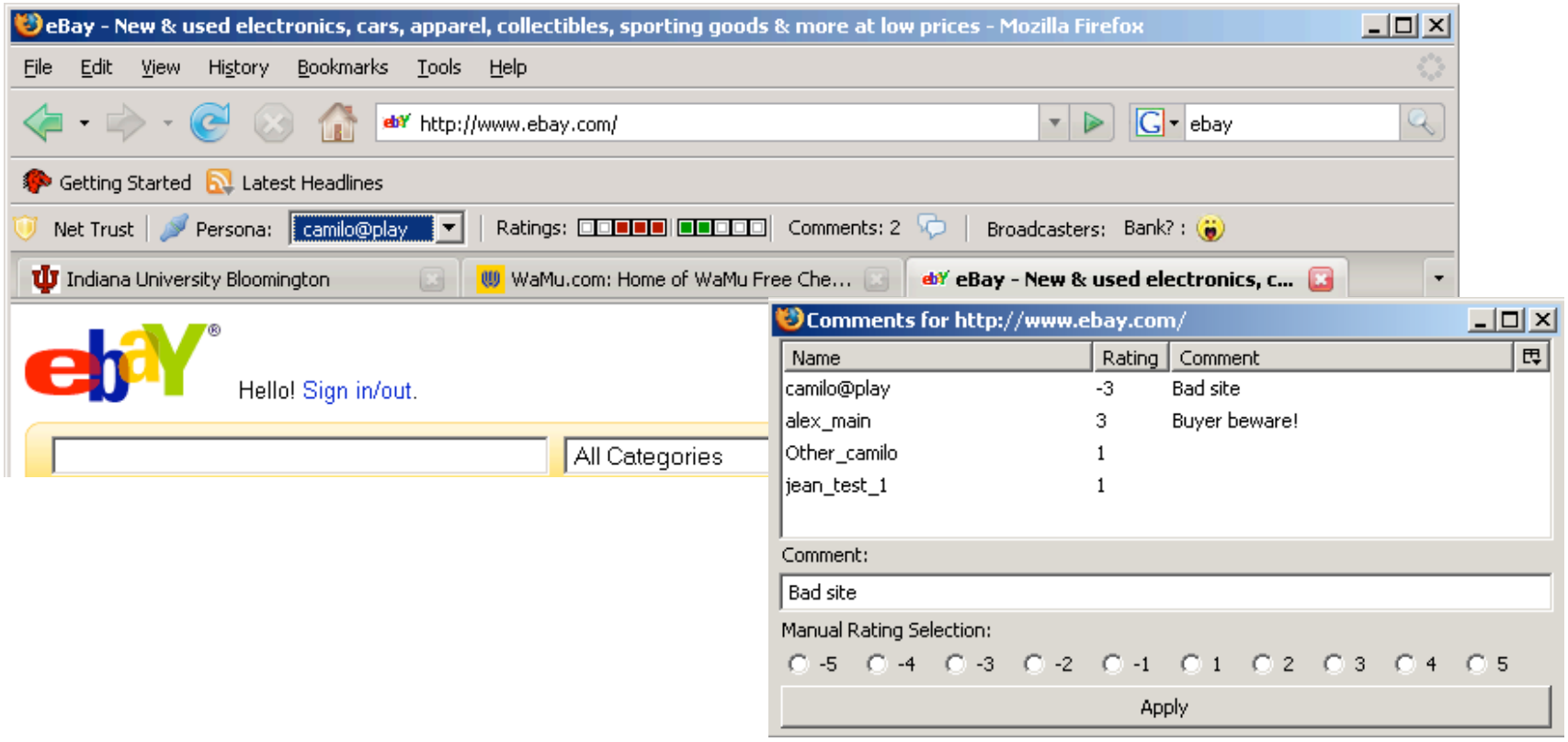
- Current Phishing and malicious site detection
  - Post-hoc detection, or
  - Depends on characteristics of the site, which is provided by the phisher
- Net Trust
  - This requires variables that cannot be controlled by the phisher
  - Includes "do NOT trust" signals
  - Includes other "quality of site" signals
  - Design goal: Minimize trust required for toolbar

Social Reputation

- Reputation based on
- Implicit based on behavior
  - First visit results in delayed rating
    - Time delay is roughly equivalent to lifetime of phishing sites 72hrs
  - 1-nth visit increased by one
  - Increases up to nth visit, decreases to as low as n/2 after a delay
    - Trust fades over time
- Explicit based on direct entry
  - Rating and comments do not change
  - Set by user
  - Combine peer and centralized ratings sources
  - Minimize explicit user-rating actions

Net Trust View

Using a user's **social network** (known as a buddy list) as well as user-selected **centralized authorities** (known as broadcasters) the Net Trust system displays meaningful information to the user so they can make an educated decision about the trustworthiness of a website.

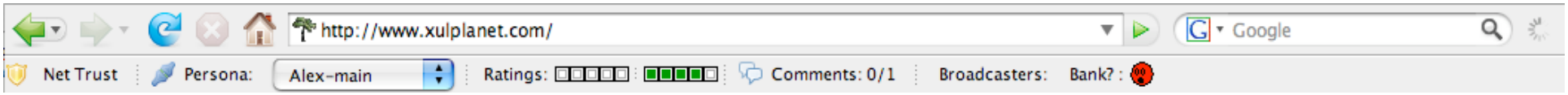


Alternative Interface

- Elderly testing
  - Too much cognitive load
  - Unaware of risks
  - In denial about privacy issues
  - No understanding of social networks

The Social Network

- NOT the centralized network
- Correlation of information
  - Socially meaningful information
  - History
  - Individual choice
    - Where do you buy shoes?
- Enabling informed resource location and information sharing
- A complement to not a substitute for search



Architectural Overview

Peer Client

Toolbar UI

Rating Engine

Social Network

Peer Email Invitations

Other Peer Clients

Synchronization

File System

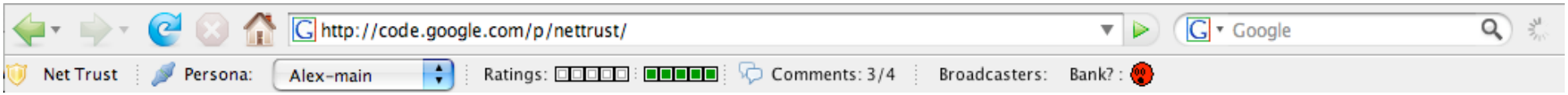
Server

CGI Web End

Peer Ratings Store

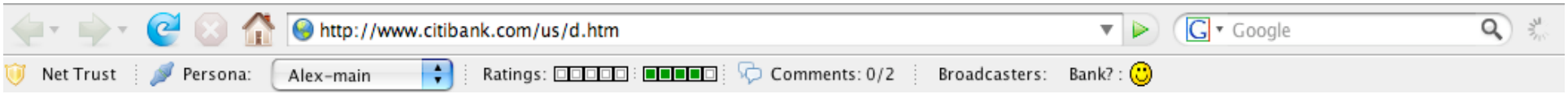
Third-Party Store

Third-Party Rating Producers



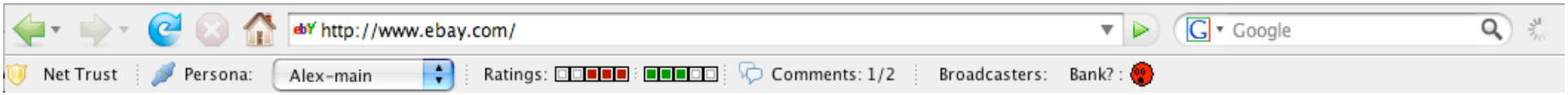
Done & Working

- Ratings Engine
  - Implicit ratings (history-based)
  - Explicit ratings (manual interaction), comments
  - Local evaluation with age threshold adjustment
- Toolbar UI
  - Correct updates; coherent over tabs & windows
- Social Network
  - Manual email invitation and buddy ID entry
  - Self-enforcement of rating partition over personas
- Synchronization
  - Local ratings storage
  - Immediate server read/write on persona load/unload



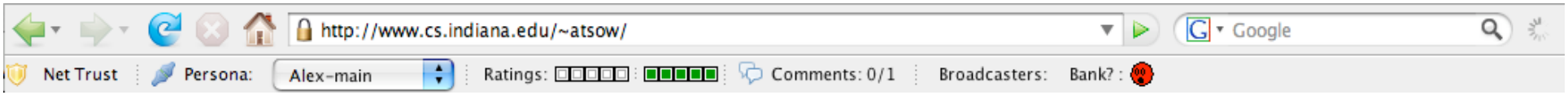
Security & Privacy Properties

- Sybil attack resistance
- Web scripting resistance
- Server authentication (anti-spoofing)
- Write authentication for peer records
- NT ID to email address commitment
- NT ID deniability ("That's not *my* ID")
- Linking resistance (NT ID and personal info)
- Social network confidentiality



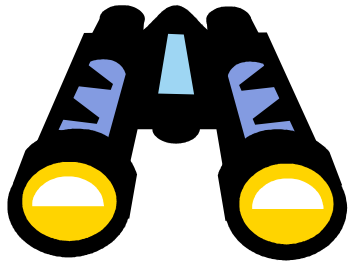
Short Term Objectives

- Synchronization (protecting social network)
  - Time delays for server access on persona change
  - Anonymous server access via Tor
- Third-Party rating assurance
  - Net Trust Certificate Authority
  - Signed rating lists
- Social Network
  - Mandatory history partition over multiple personas
  - Invite automation & validation
  - Shared key generation and perfect forward encryption in social network



Longer Term Initiatives

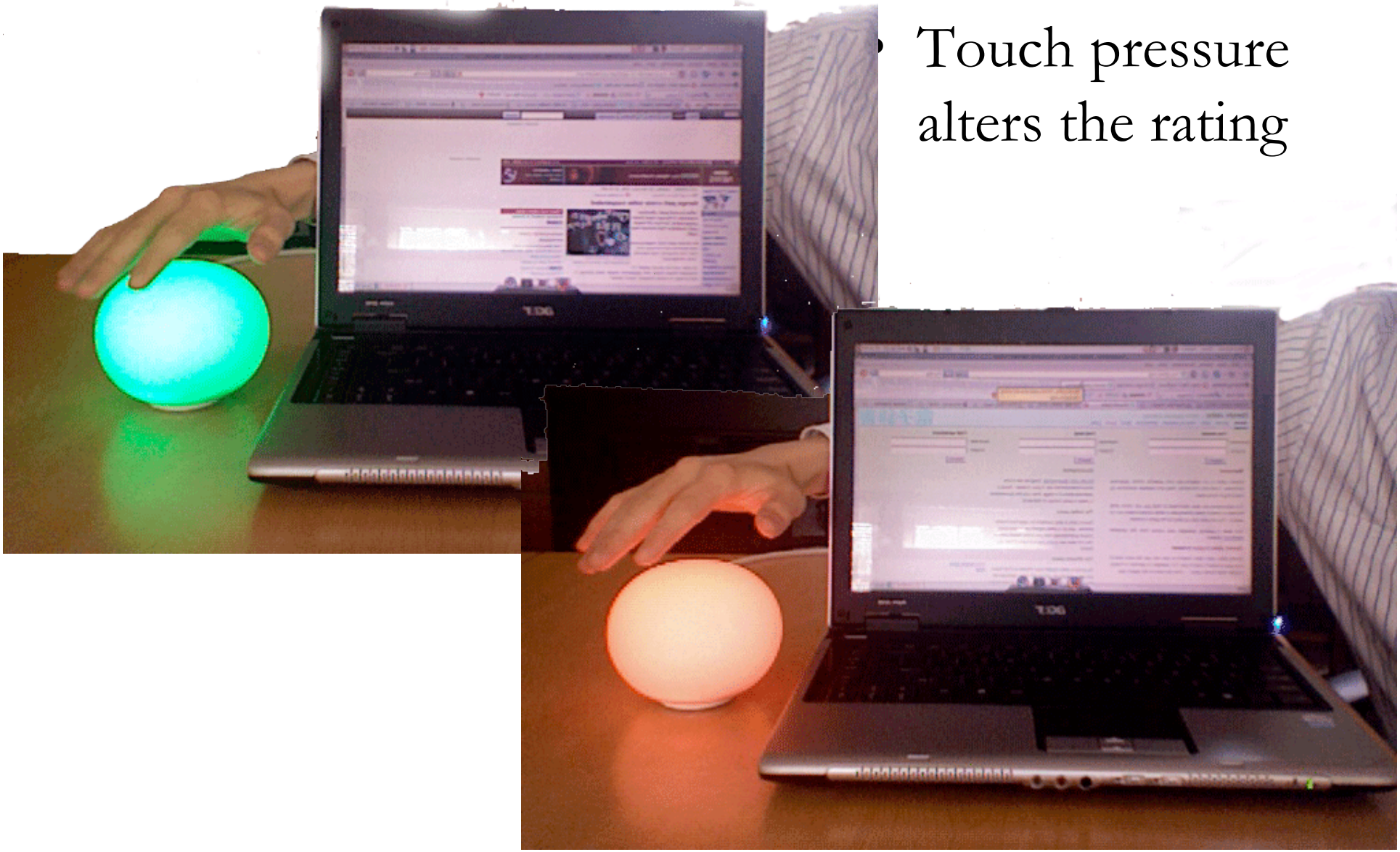
- Expand rating sets for client-side pharming detection
  - Include hashes of server IP address & certs in history
- Blend rating sets across social networks
  - Deter unauthorized sharing of NT IDs
  - Improves ID deniability
    - Came from a friend of a friend
  - Improves information diffusion
  - Enable server intersection attack on social network
- Narrative risk communication
  - Rich warnings: cartoons, video, animation
  - Preliminary research extremely effective
    - But HSD prevents us telling you …..



Ambient Trust Orb

- All ratings are added together with third party dominance or integration

SWAT: Surfing With Ambient Trust



- Touch pressure alters the rating

Conclusion

- No inherent trade-off between additional security information and usability
- Users like having history and shared information
  - Leveraging this for other purposes keeps attention span
  - Integrating in search increases value can enhance security as a benefit to increased usabilitys
- Users have in their histories information to detect phishing and pharming
  - The information infrastructure has the least contextual information of any communication.
- The goal is *to inform user behaviors* when decision-making under uncertainty

Acknowledgements

- Alla Genkina Ayre, MS HCI 2005
- Alex Tsow, PhD CS 2007
- Camilo Viecco, PhD CS August 2008
- Allan Friedman, PhD Public Policy, 2008
- Brandon Stephens, MS HCI 2009
- Shreyas Kamath, MS CS 2007
- Preeti Hariharan MS CS 2007
- Farzaneh Asghapour MS HIC/Security 2007