

05. Phishing; Robust and Ethical Experiments

Blase Ur

April 16th, 2019

CMSC 23210 / 33210



THE UNIVERSITY OF
CHICAGO



**Security, Usability, & Privacy
Education & Research**

Why John Can't Protect His Emails

Someone has your password

Inbox

Google <no-reply@accounts.googlemail.com>

to me

12:02 (1 hour ago)

Google

Someone has your password

Hi John

Someone just used your password to try to sign in to your Google Account john.podesta@gmail.com.

Details:

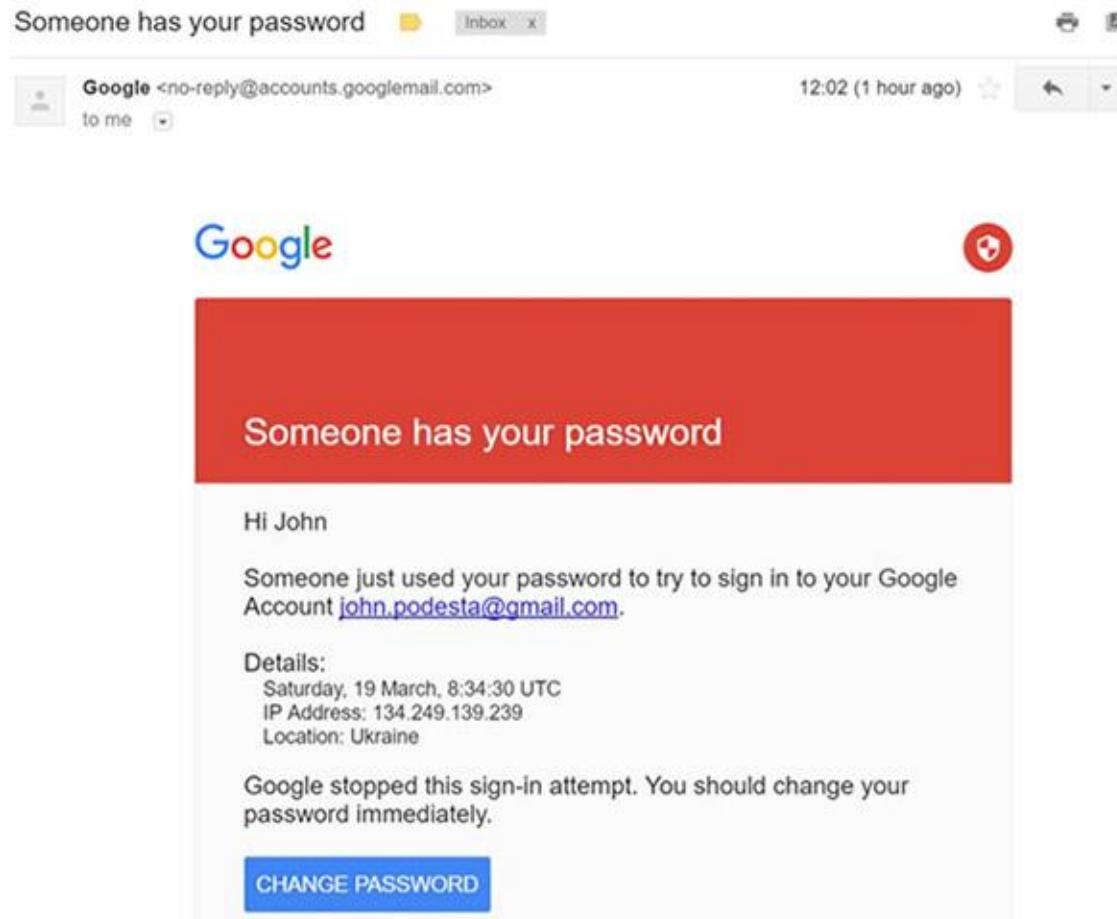
Saturday, 19 March, 8:34:30 UTC

IP Address: 134.249.139.239

Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

CHANGE PASSWORD



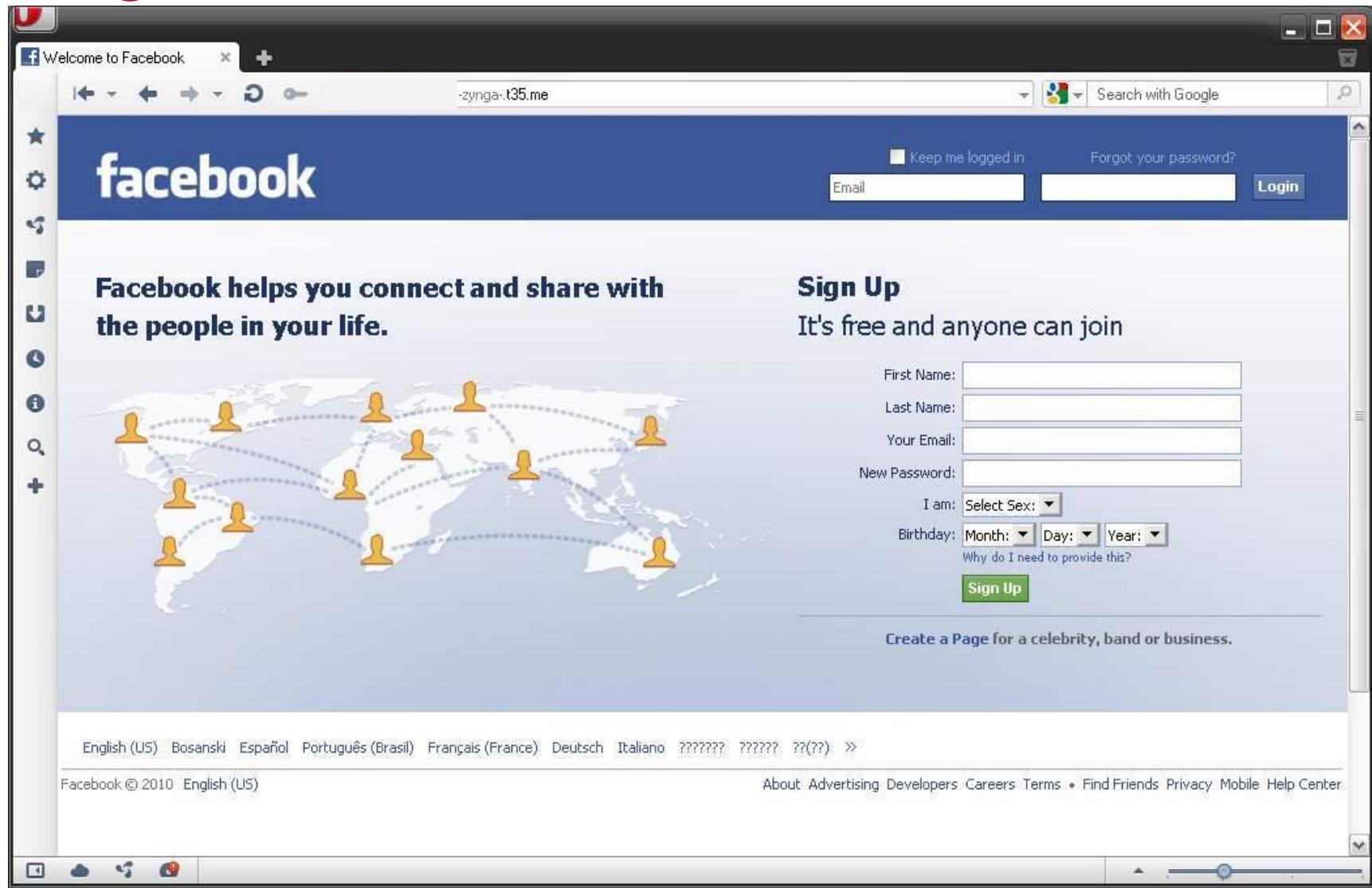
Phishing

- Phish: Fraudulent email that looks real
 - Usually try to extract credentials (e.g., password), financial information (e.g., bank account), or other private information
- Spear phish: Targeted phishing email

Why Does Phishing Work?

- Rachna Dhamija, J.D. Tygar, Marti Hearst.
Why Phishing Works. CHI 2006.
- How do you tell if a site is legitimate?
- How do you tell if an email is legitimate?

Legitimate or Phish?



Welcome to Facebook

zynga-t35.me

facebook

Keep me logged in

Forgot your password?

Email

Login

Facebook helps you connect and share with the people in your life.

Sign Up

It's free and anyone can join

First Name:

Last Name:

Your Email:

New Password:

I am:

Birthday:

Why do I need to provide this?

Sign Up

Create a Page for a celebrity, band or business.

English (US) Bosanski Español Português (Brasil) Français (France) Deutsch Italiano ??????? ??????? ??(??) >>

Facebook © 2010 English (US)

About Advertising Developers Careers Terms • Find Friends Privacy Mobile Help Center

Legitimate or Phish?

Bank of the West |

Back Forward Reload Stop Home <http://www.bankofthewest.com/BOW/home/index.html> Go

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:

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



Locations

State:

ZIP code:

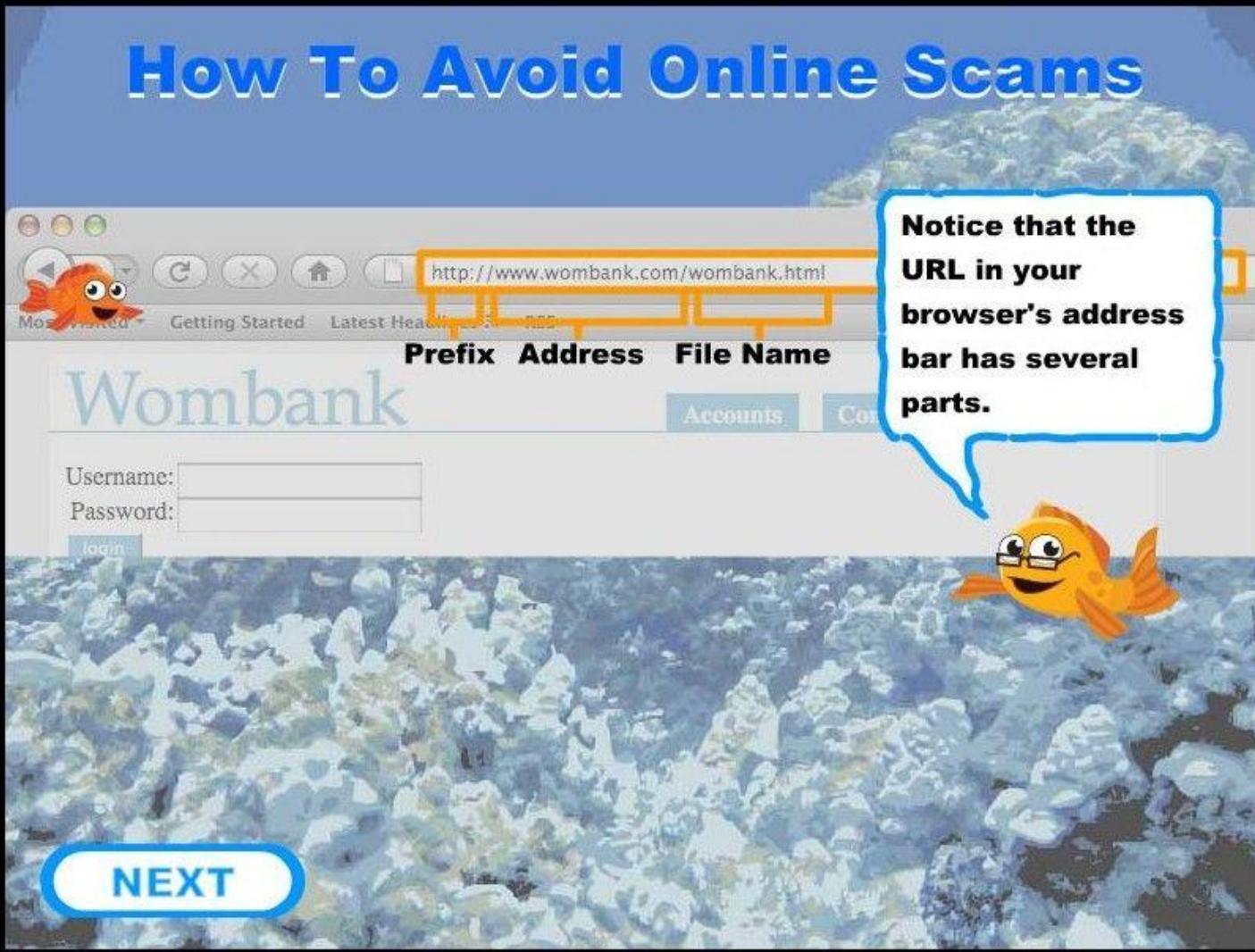
Personal Banking

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

Anti-Phishing Phil / PhishGuru



How To Avoid Online Scams

Notice that the URL in your browser's address bar has several parts.

NEXT

Social phishing (Jagatic et al., 2007)

- Use social networking sites to get information for targeted phishing
 - “In the study described here we simply harvested freely available acquaintance data by crawling social network Web sites.”
- “We launched an actual (but harmless) phishing attack targeting college students aged 18–24 years old.”

Social phishing (Jagatic et al., 2007)

- Control group: message from stranger
- Experimental group: message from a friend
- Used university's sign-on service to verify passwords phished

Ethics (Jagatic et al., 2007)

- How did they obtain consent?
- What ethical concerns are there?
 - What seemed to be done well?
 - What could have been done better?
- Who was potentially affected by the study?
- “The number of complaints made to the campus support center was also small (30 complaints, or 1.7% of the participants).”

HCI Experimental Methods

Human-Computer Interaction (HCI)

- You are not the user! You know too much!
- Think about the user throughout design
- Involve the user



What is usable?

- Intuitive / obvious
- Efficient
- Learnable
- Memorable
- Few errors
- Not annoying
- Status transparent



THE AUTHOR OF THE WINDOWS FILE
COPY DIALOG VISITS SOME FRIENDS.

Image from <http://www.xkcd.com>

Determine use cases and goals

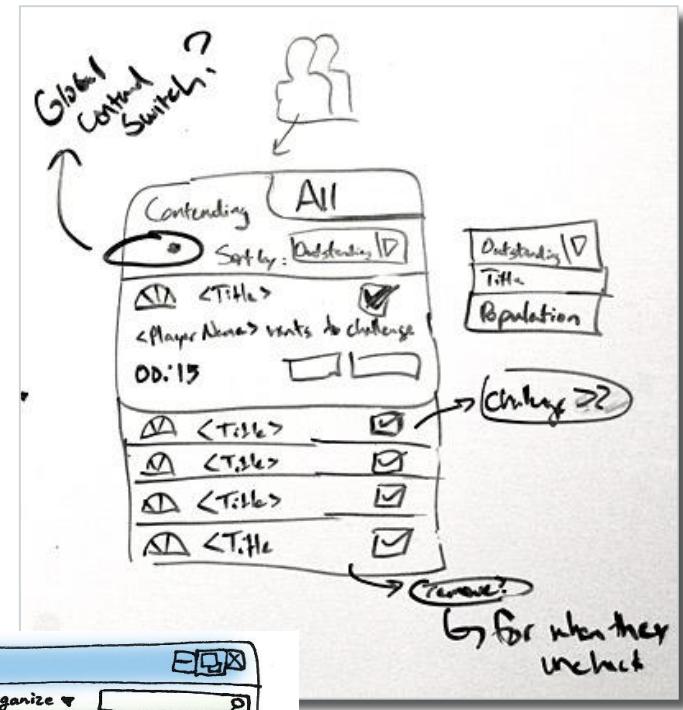
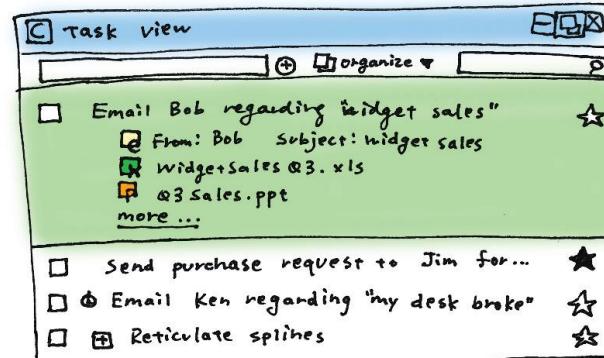
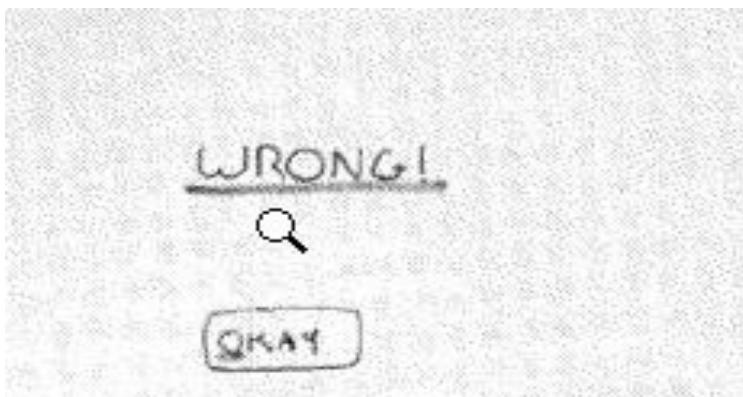
- What are the concrete tasks users should be able to accomplish?
 - Based on understanding of users!
- Set realistic metrics

Example: paper prototypes

- Don't overthink. Just make it.
- Draw a frame on a piece of paper
- Sketch anything that appears on a card
- Make all menus, etc.
- Redesign based on feedback
- “Think aloud”

Iterative prototyping is crucial!

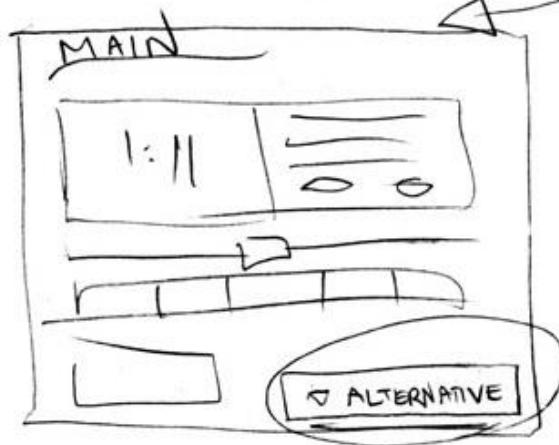
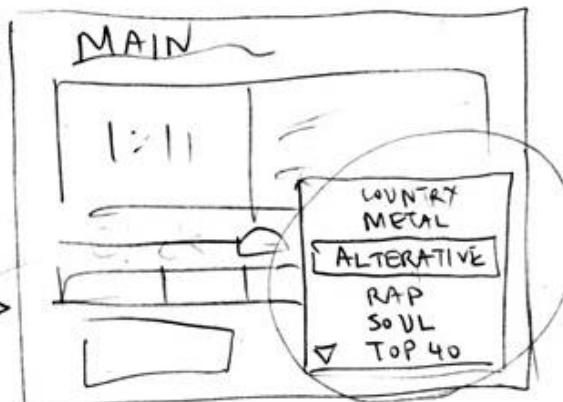
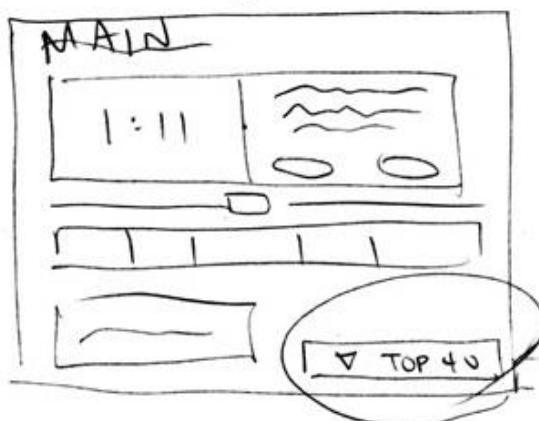
High-fidelity, “Wizard of Oz,” low-fidelity



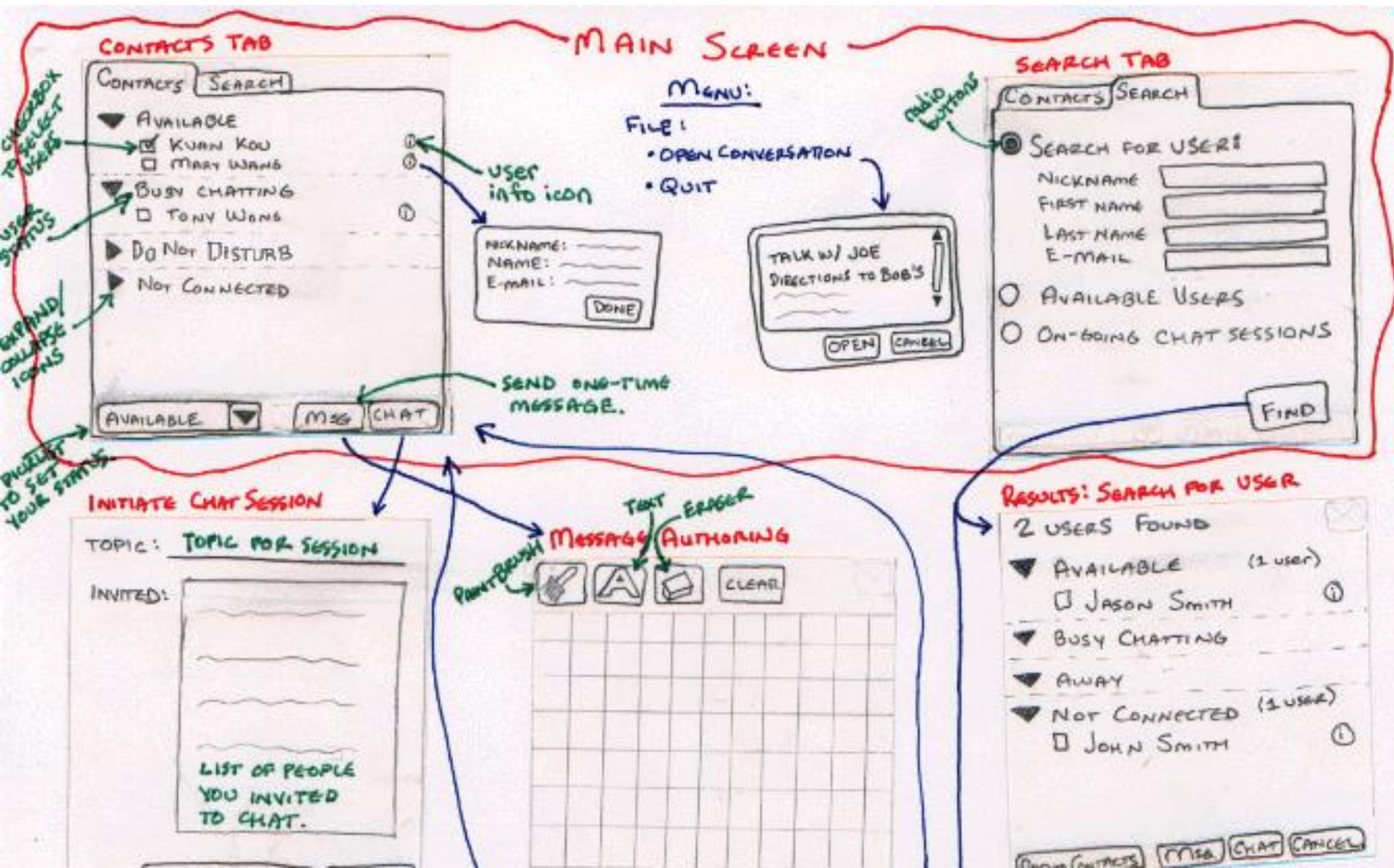
Example: low-fidelity paper prototype

SCENARIO 1

"I want to listen to alternative music"



Example: paper prototype



Example: think aloud

- Download and install software that lets you encrypt your email
 - “Think aloud” of whatever’s on your mind
 - Give them an example
- Additional things you can ask:
 - What are you thinking now?
 - What do you expect to happen if you do X?
 - How did you decide to do that?

Research Studies and Methods

Research studies: purpose and goals

- What are you hoping to learn?
- What are your hypotheses?
 - Often listed explicitly in a paper
- What are your metrics for success?
 - More secure, quicker to use, more fun, etc.
- What are you comparing to?
- What data might be helpful?

Broad types of studies

- Descriptive study
- Relational study
- Experimental study
- Formative (initial) vs. summative (validate)

STAND BACK



**I'M GOING TO TRY
SCIENCE**

Quantitative vs. Qualitative

- Quantitative: you have numbers (timing data, ratings of awesomeness)
- Qualitative: you have non-numerical data (thoughts, opinions, types of errors)

Types of studies (1)

- What people want/think/do overall:
 - Surveys
 - Interviews
 - Focus groups
- What people want/think in context:
 - Contextual inquiry (interviews)
 - Diary study (prompt people)
 - Observations in the field

Types of studies (2)

- Expert evaluation of usability:
 - Cognitive walkthrough
 - Heuristic evaluation
- Usability test:
 - Laboratory (“think aloud”)
 - Online study
 - Log analysis

Types of studies (3)

- Controlled experiments to test causation
- Varying different conditions
 - Full-factorial design or not
 - Independent and dependent variables
- Many methods apply (e.g., surveys can be designed to test causation)
 - Role-playing studies
 - Field studies

Study designs

- Within subjects
 - Every participant tests everything
 - Crucial to randomize order! (learning effect)
 - Fewer participants
- Between subjects
 - Each participant tests 1 version of the system
 - You compare these groups
 - Groups should be similar (verify!)
 - Still randomize!