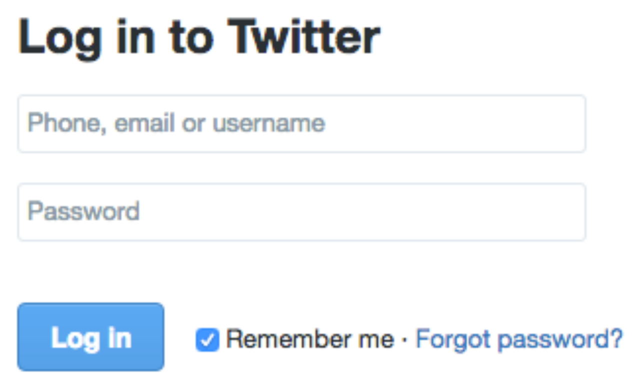
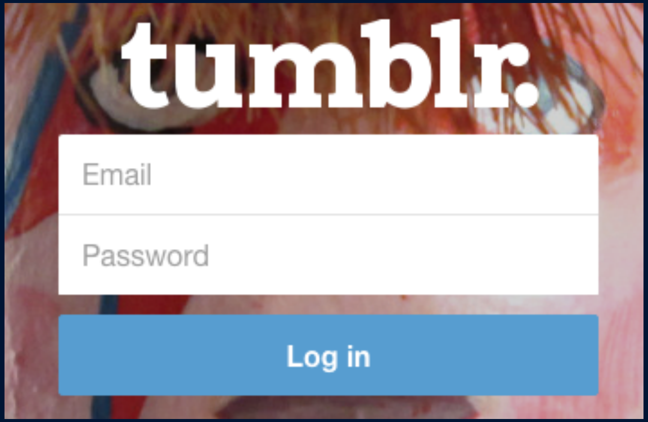
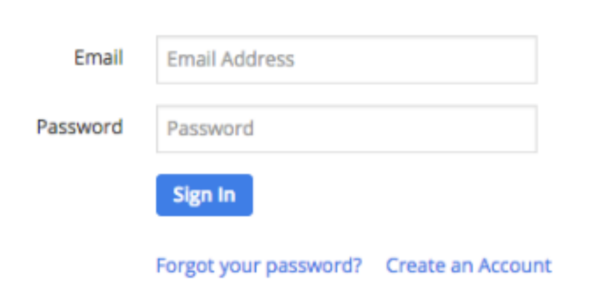
Strengthening Password-based Authentication

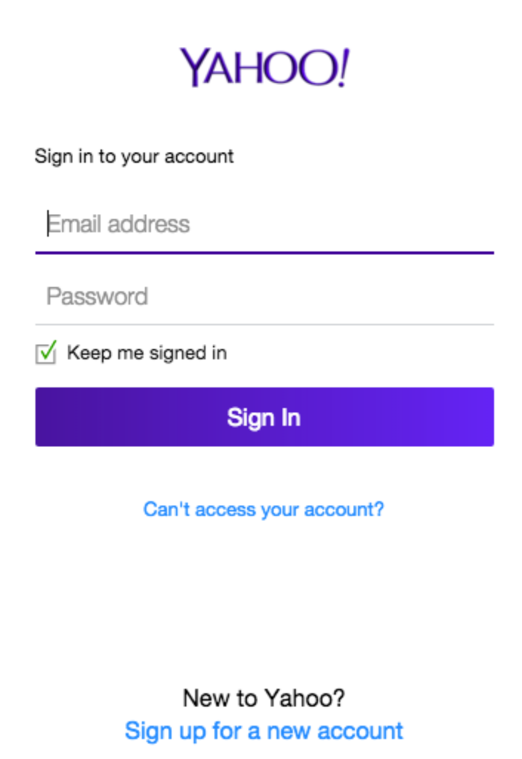
SCOTT RUOTI
JEFF ANDERSEN
KENT SEAMONS

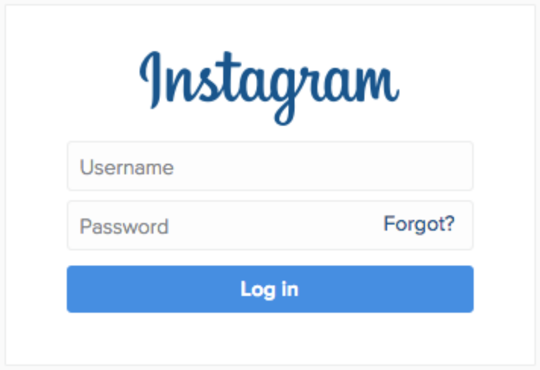
BRIGHAM YOUNG UNIVERSITY

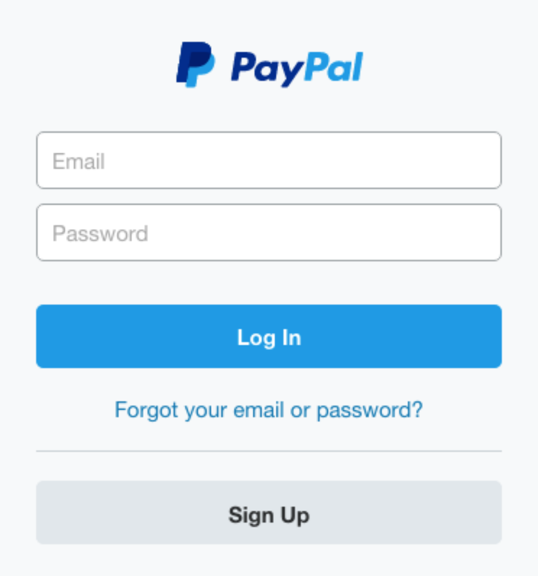


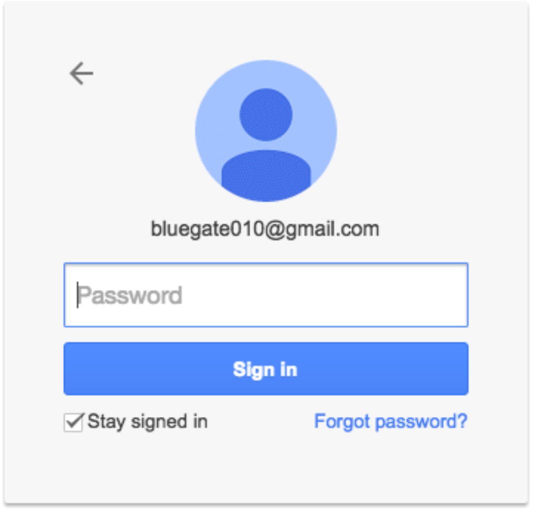


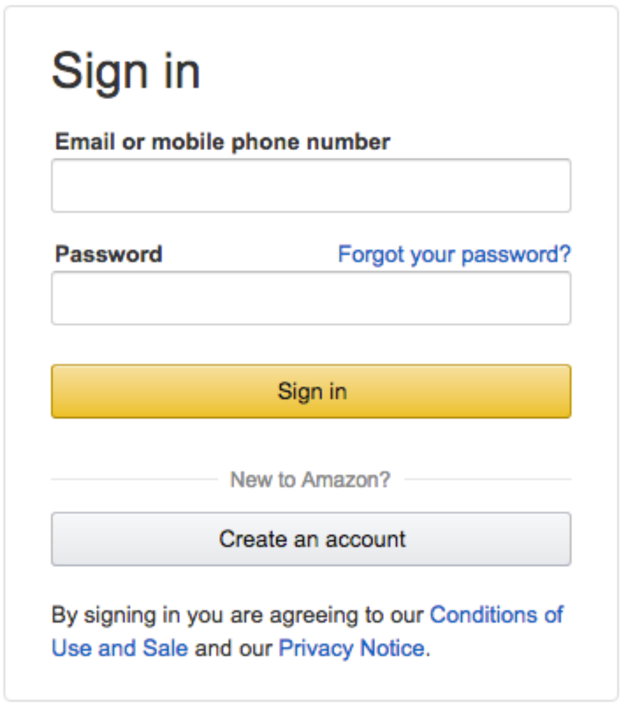




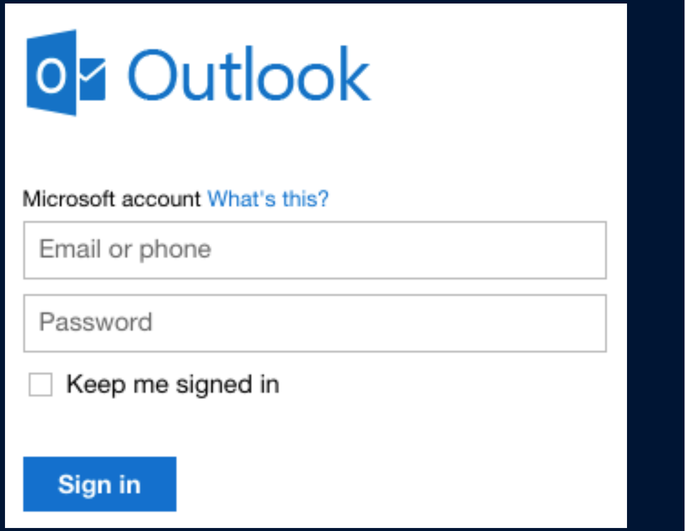


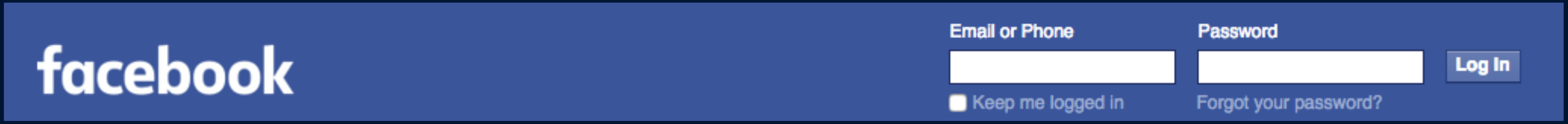



bluegate010@gmail.com



By signing in you are agreeing to our Conditions of Use and Sale and our Privacy Notice.





Problems with Passwords

POOR SECURITY AT THE SERVER

- Servers have access to password plaintext
- Users trust that servers salt+hash before storage
- Many servers are vulnerable to password theft

VULNERABILITY TO PHISHING

- Web pages have access to password plaintext
- Phishers impersonate legitimate site
- Credentials immediately vulnerable

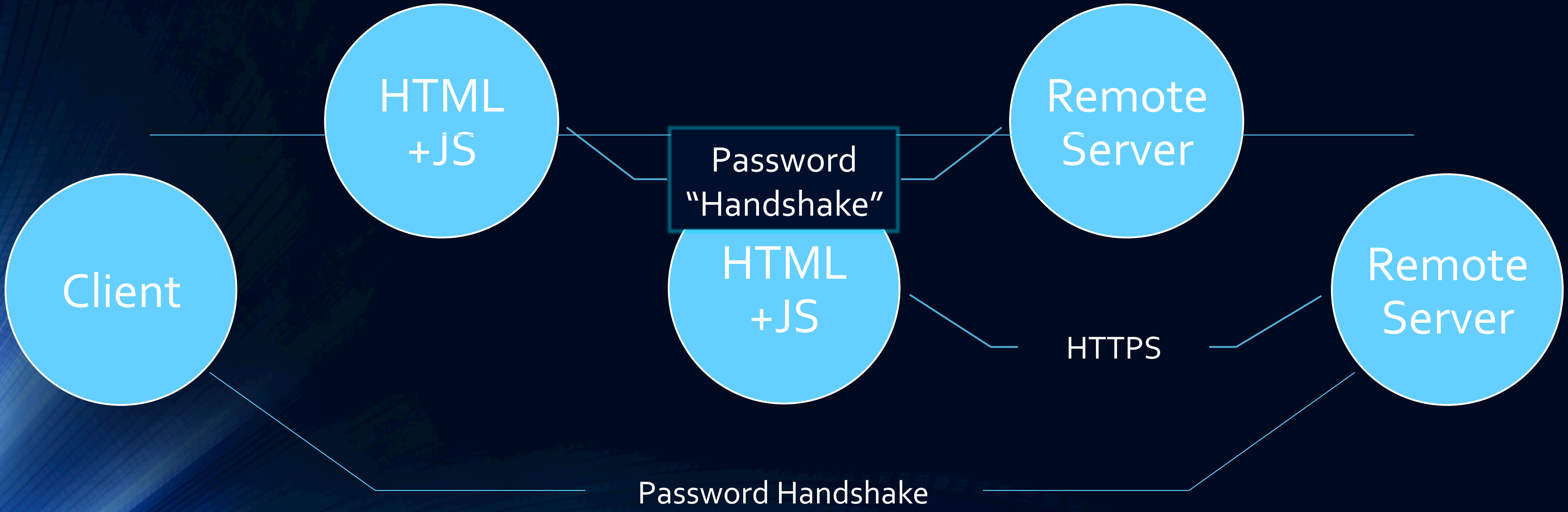
Password re-use compounds both problems

What can be done?

STRONG PASSWORD PROTOCOLS

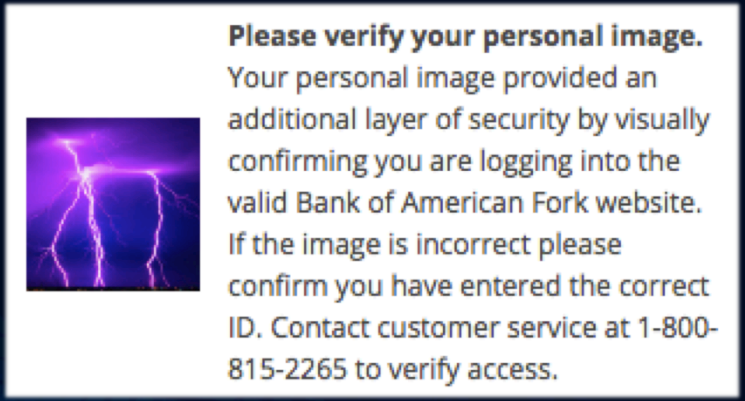
SAFE PASSWORD ENTRY

Strong Password Protocols



Safe Password Entry

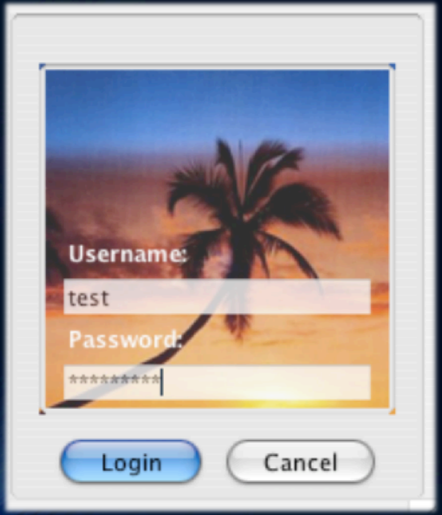
- Spoof-resilient password-entry interfaces
- Interfaces that indicate they are privileged
  - Position on screen
  - OS features
  - SiteKey



Please verify your personal image. Your personal image provided an additional layer of security by visually confirming you are logging into the valid Bank of American Fork website. If the image is incorrect please confirm you have entered the correct ID. Contact customer service at 1-800-815-2265 to verify access.

Dynamic Security Skins, Dhamija [2005]

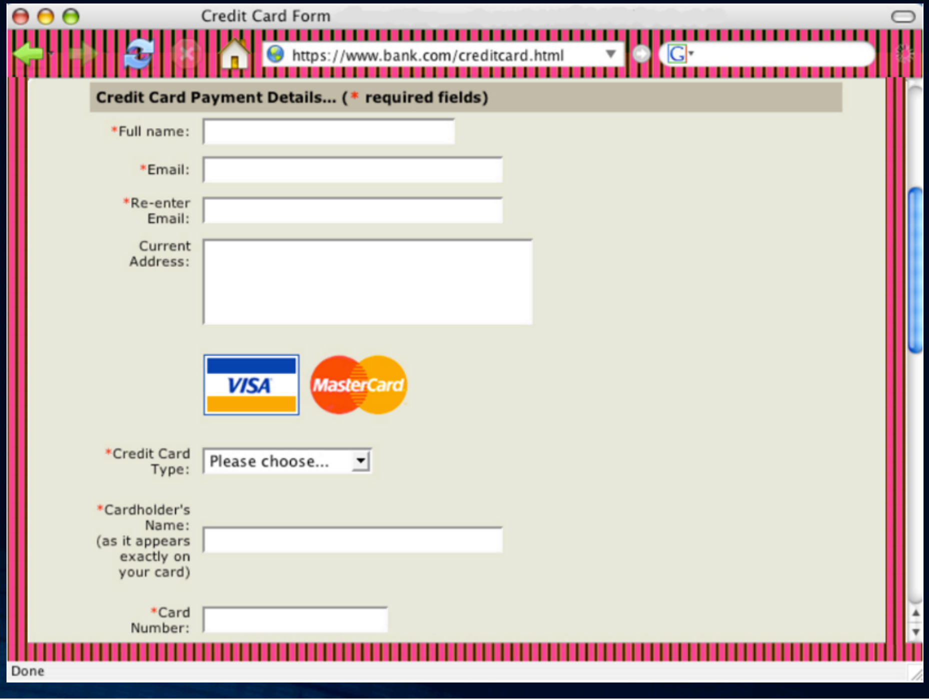
- Over 500 citations
- SiteKey



Username: test

Password: **********

- Strong password protocol
- Visual hashes provide site authentication



Credit Card Payment Details... (* required fields)

*Full name:

*Email:

*Re-enter Email:

Current Address:

*Credit Card Type: Please choose...

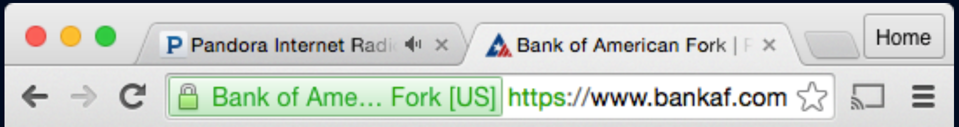
*Cardholder's Name: (as it appears exactly on your card)

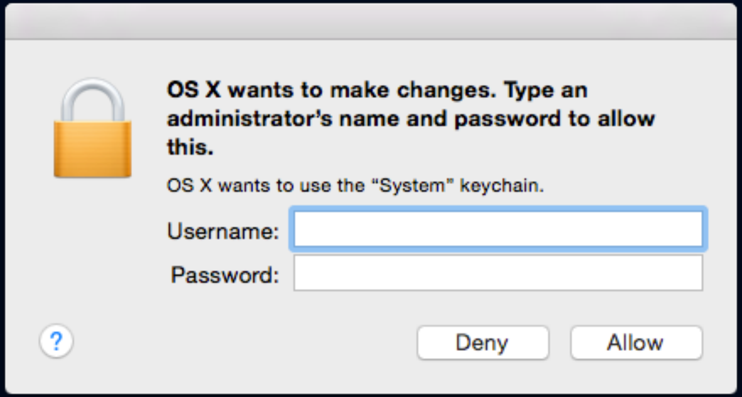
*Card Number:

Our Ideas

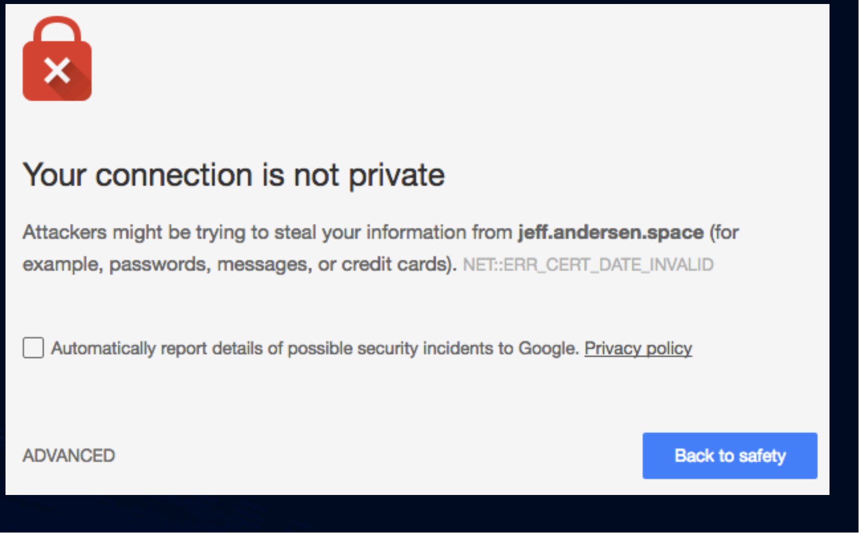
- Safe Password Entry
  - Browser chrome
  - Operating system prompt

- Site Authentication
  - Browser detects handshake failure




OS X wants to make changes. Type an administrator's name and password to allow this.

OS X wants to use the “System” keychain.


Your connection is not private

Attackers might be trying to steal your information from **jeff.andersen.space** (for example, passwords, messages, or credit cards). NET::ERR_CERT_DATE_INVALID

☐ Automatically report details of possible security incidents to Google. Privacy policy

Next Steps

1. Build our systems

2. ~~Test them~~ Design a user study Not good methodologies

Improving User Studies

PRESENT METHODOLOGY

- Too short
- Occurs in a lab
- Participants are primed
- Lab-assigned credentials

PROPOSED METHODOLOGY

- Long-term
- “Take-home”
- Deception
- Personal credentials

Preliminary Study Design

- Assign user to one safe password entry tool
- Playtesting a new game suite
  - Access via BYU Single Sign-On
- Daily testing, over 10-day period
  - Game links delivered over email
- On day 7, users are phished for their SSO password

Work Needed

- Introduce safe password entry without priming for security
- Ensure study is safe for participants

Points of Discussion

- Where should safe password entry be implemented?
  - Browser window, browser chrome, or operating system

- How can safe password entry effectiveness be accurately evaluated?
  - Ensuring both deception and safety for users