Do Users Attend to Highlighted Domains in Identifying Phishing Webpages?
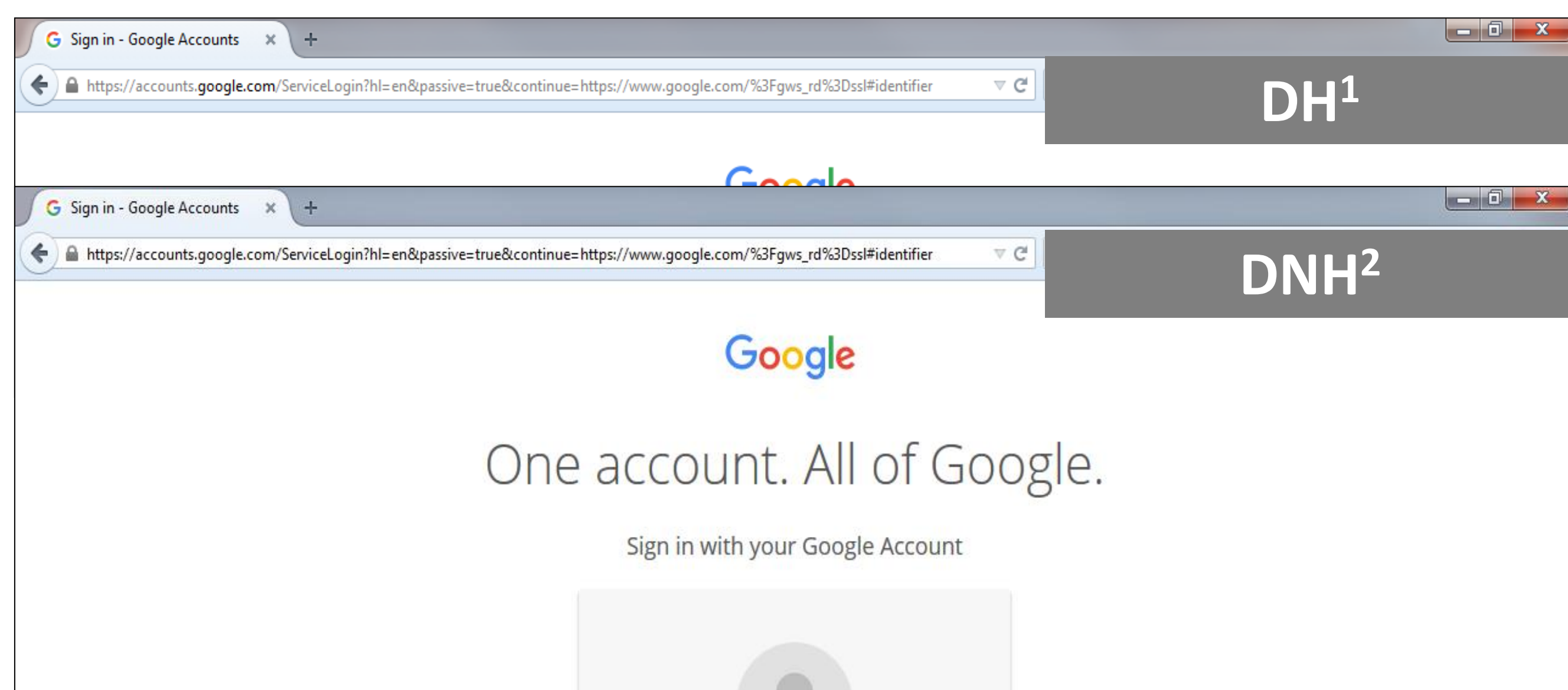
Aiping Xiong[1], Weining Yang[2], Robert W. Proctor[1], Ninghui Li[2]

[1]Department of Psychological Sciences, [2] Department of Computer Science

Domain Highlighting

DH[1]

DNH[2]

Note: 1: Domain Highlighting; 2: Domain Non-Highlighting

Research Questions:

1. Will users naturally attend to the address bar?
2. Will users use the domain name to judge the website's legitimacy?
3. Can users recognize the legitimate domain names?

Eye-Tracking Experiment
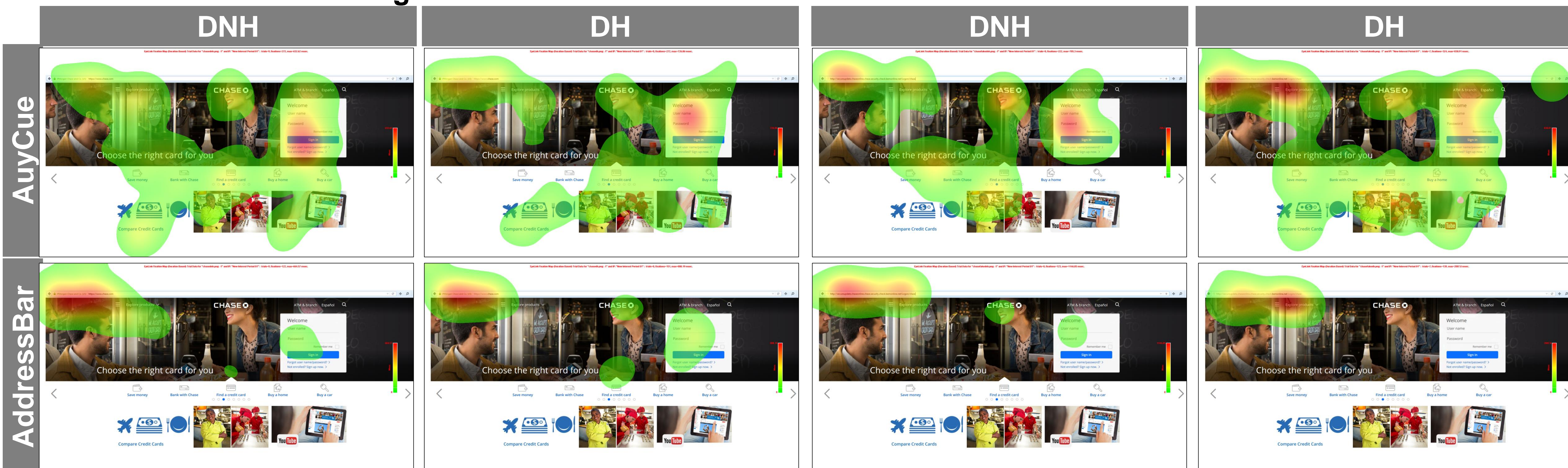
A laboratory Experiment

- 32 participants
- 2 groups of 6 frequently target phishing webpages (one set legitimate and the other fraudulent) based on a 5 point scale
- 2 phases: 1st phase AnyCue
  2nd phase AddressBar
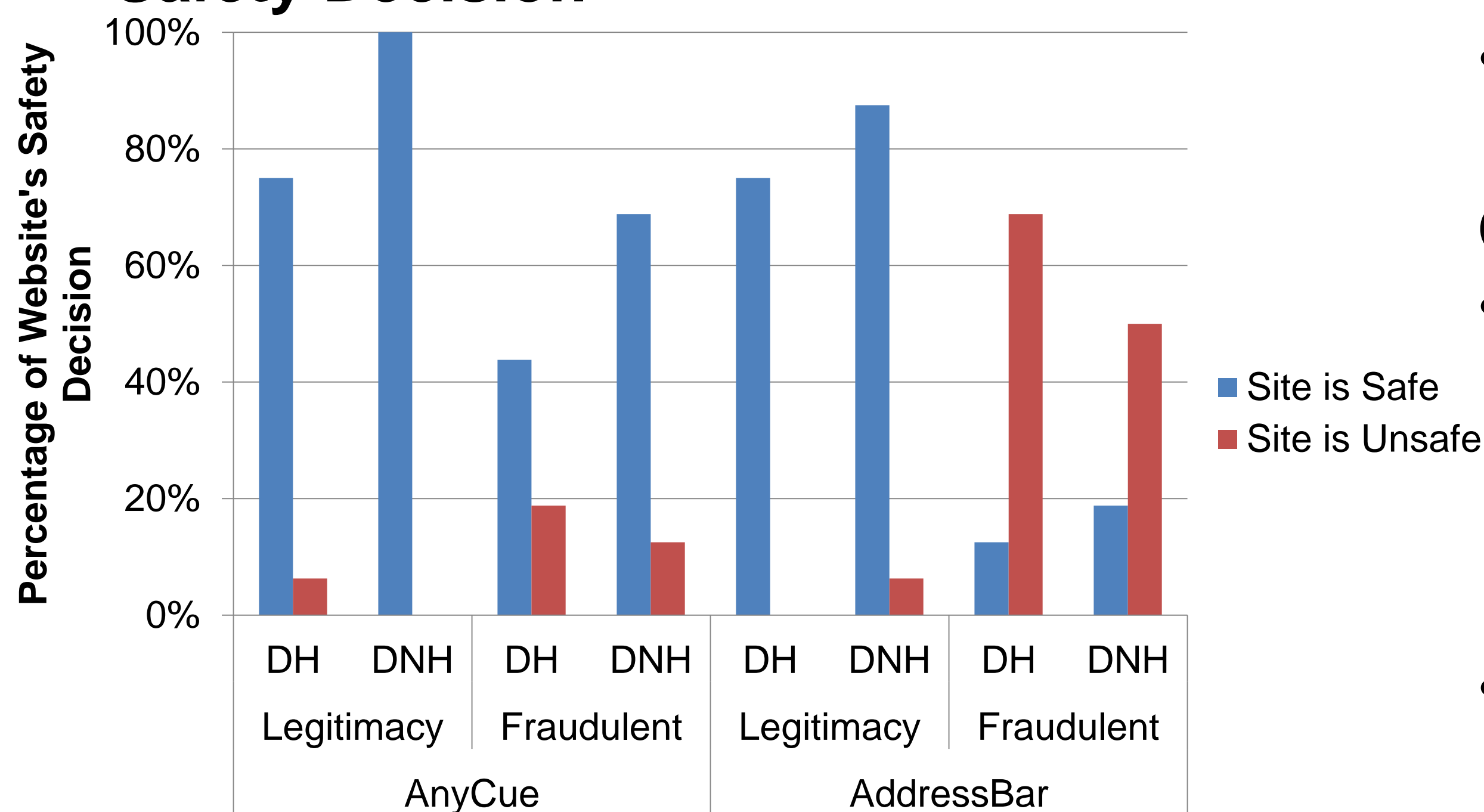- Domain highlighted (DH) or not (DNH) varied between-subjects

Results

Legitimate

DNH	DH

Fraudulent

DNH	DH

AnyCue
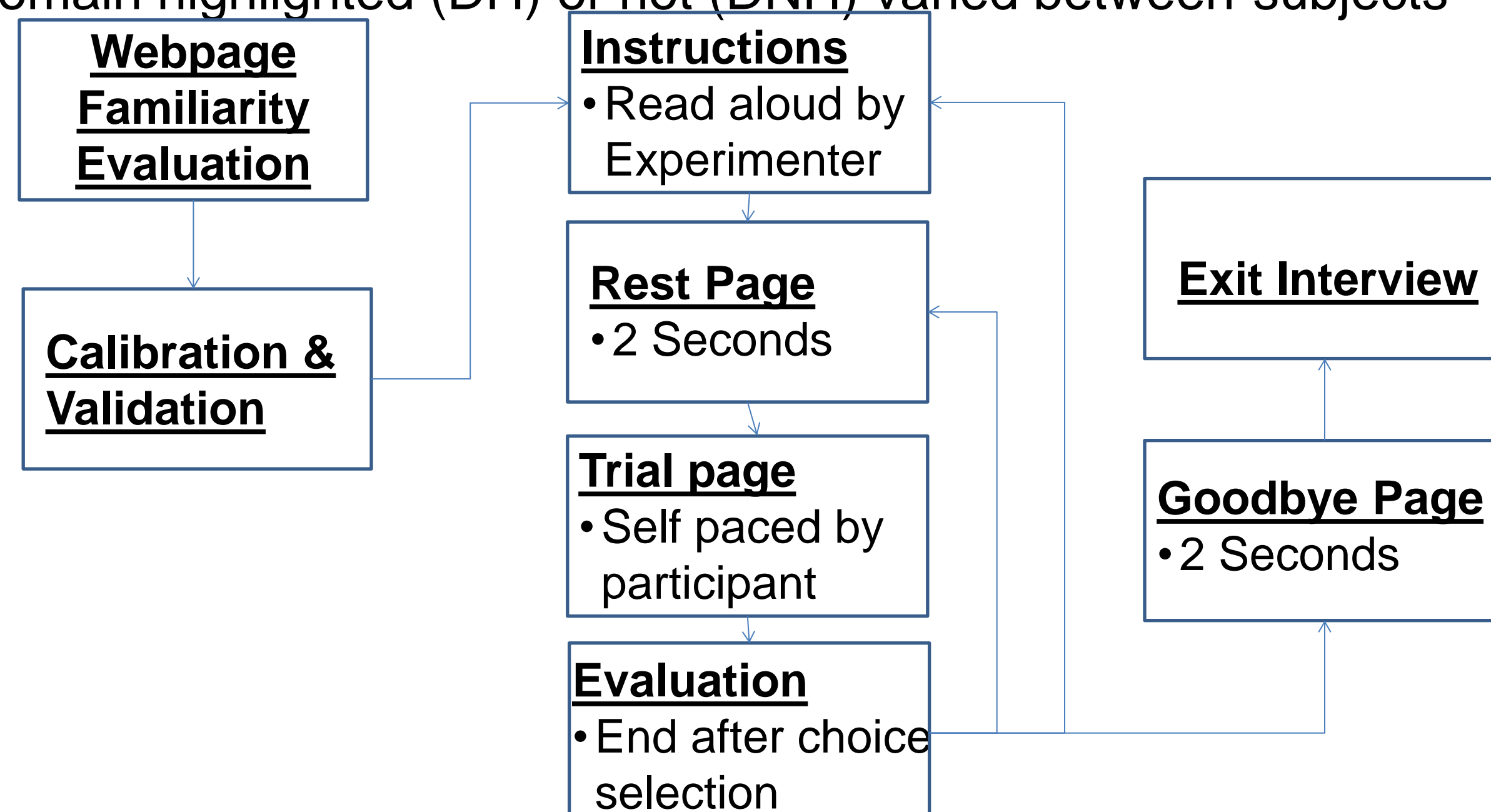
AddressBar

Safety Decision

Q1: Yes.
- Naturally, participants attended to the address bar but in a much less extent if compared to visual cues such as login and logos.

Q2 & Q3:   No.
- Although fixations were longer and concentrated on the highlighted domains for the fraudulent webpages, the non-significant differences between DH and DNH conditions revealed that participants did not mainly rely on the domain name for the legitimacy decision.
- Consequently, it suggests a lack of knowledge of the legitimate domain names for the participants.