A Research Framework and Initial Study of Browser Security for the Visually Impaired

Elaine Lau Zachary Peterson

Cal Poly, San Luis Obispo

Your connection is not private

Attackers might be trying to steal your information from **expired.badssl.com** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_DATE_INVALID

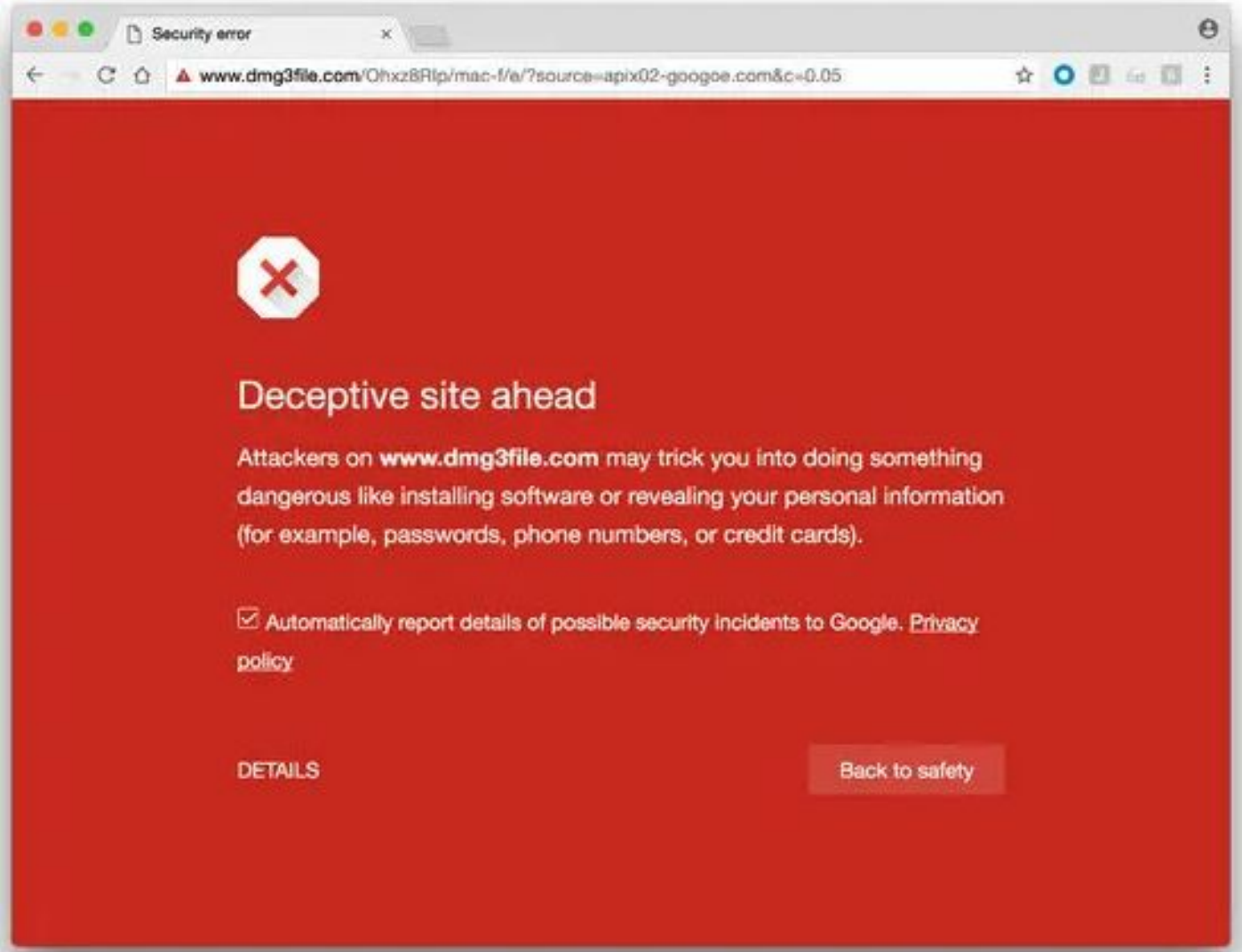
To get Chrome's highest level of security, turn on enhanced protection

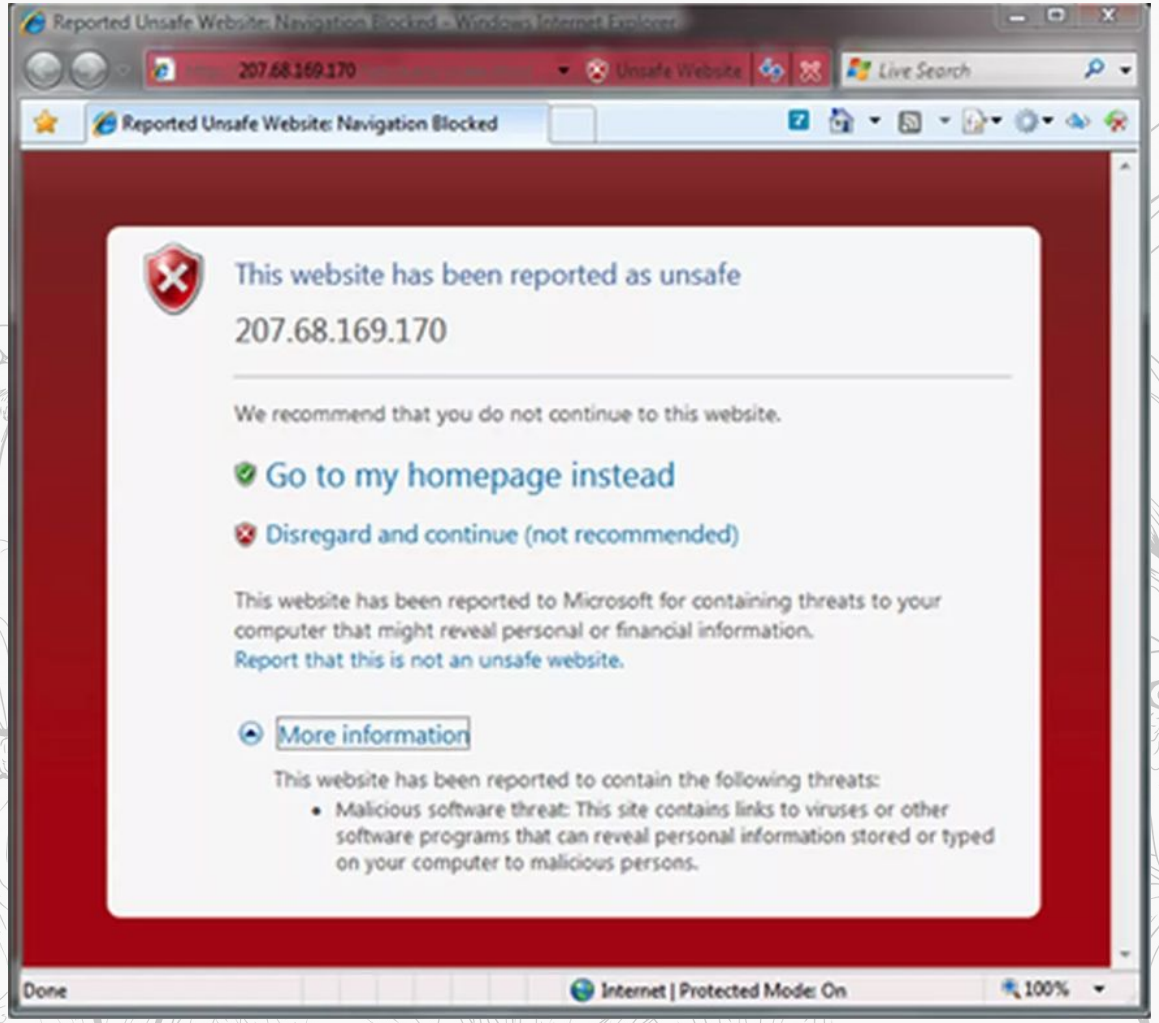
Hide advanced

Back to safety

This server could not prove that it is **expired.badssl.com**; its security certificate expired 2,581 days ago. This may be caused by a misconfiguration or an attacker intercepting your connection. Your computer's clock is currently set to Thursday, May 5, 2022. Does that look right? If not, you should correct your system's clock and then refresh this page.

Proceed to expired.badssl.com (unsafe)


Security error
www.dmg3file.com/Ohxz8Rlp/mac-f/e/?source=apix02-googoe.com&c=0.05
Deceptive site ahead
Attackers on www.dmg3file.com may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards).
Automatically report details of possible security incidents to Google. Privacy policy
DETAILS
Back to safety


Reported Unsafe Website: Navigation Blocked - Windows Internet Explorer
207.68.169.170
Unsafe Website
Live Search
Reported Unsafe Website: Navigation Blocked
This website has been reported as unsafe
207.68.169.170
We recommend that you do not continue to this website.
Go to my homepage instead
Disregard and continue (not recommended)
This website has been reported to Microsoft for containing threats to your computer that might reveal personal or financial information.
Report that this is not an unsafe website.
More information
This website has been reported to contain the following threats:
Malicious software threat: This site contains links to viruses or other software programs that can reveal personal information stored or typed on your computer to malicious persons.
Done
Internet | Protected Mode: On
100%

Suspected Phishing Site

The website you are visiting has been reported as a “phishing” website.

These websites are designed to trick you into disclosing personal or financial information, usually by creating a copy of a legitimate website, such as a bank.
Learn more...

Ignore Warning | Go Back

Report an error...

Motivation

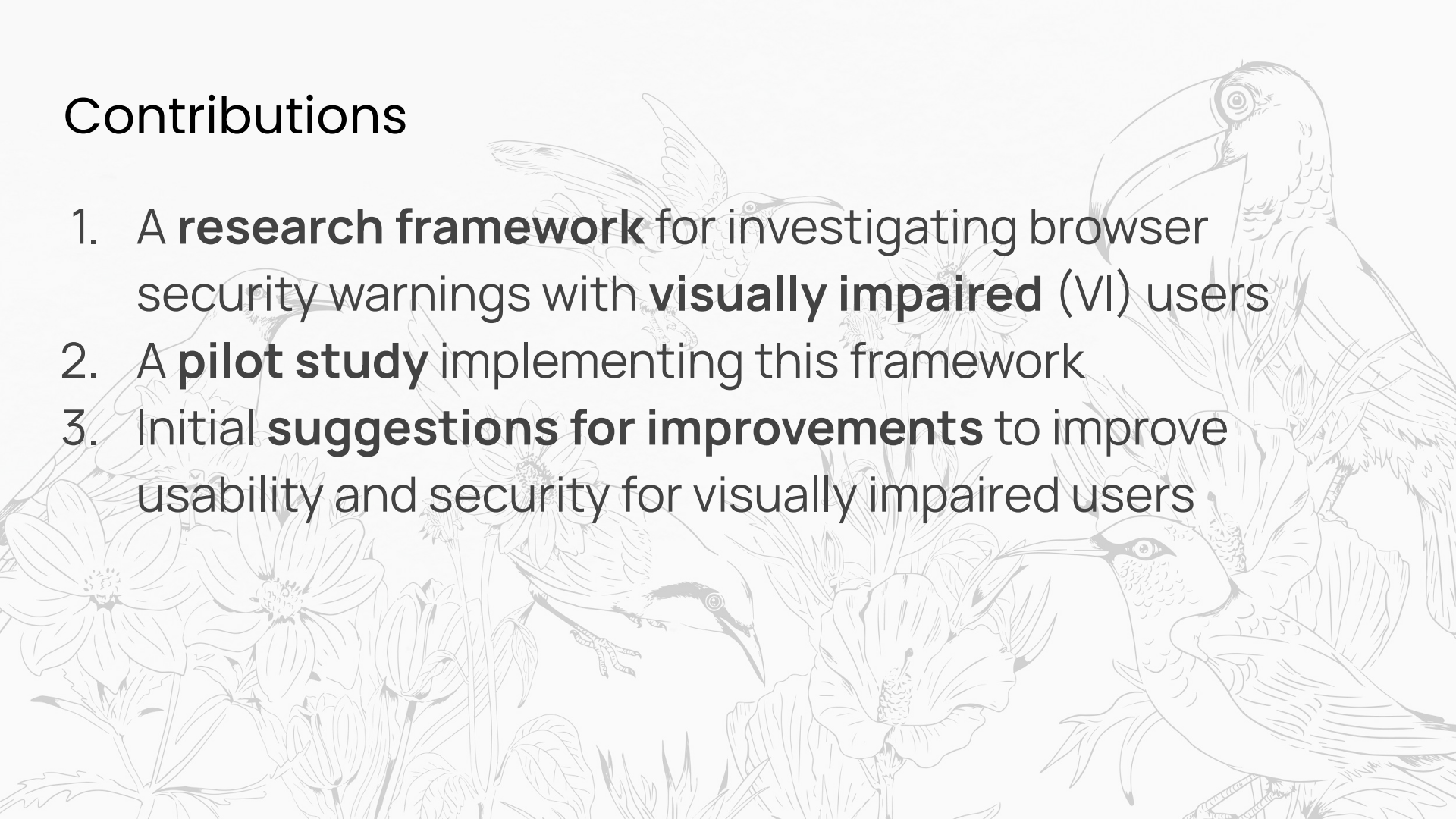
Browser warnings employ **visual techniques** to deter users away from the unsafe option, while drawing attention towards the “safe” choice.

- Icons
- Text size
- Color
- Images

- **Warning appearance** is a contributing factor to compliance (Akhawe and Felt [1])
- This is not effective for screen reader users

Contributions

1. A **research framework** for investigating browser security warnings with **visually impaired** (VI) users
2. A **pilot study** implementing this framework
3. Initial **suggestions for improvements** to improve usability and security for visually impaired users

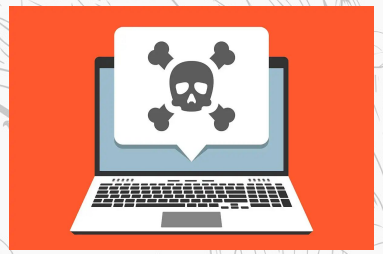


Methodology

1. Generic qualitative inquiry
2. Natural setting in users' home or work place
3. Three warning types (Akhawe and Felt)

Phishing Warning

Malware Warning

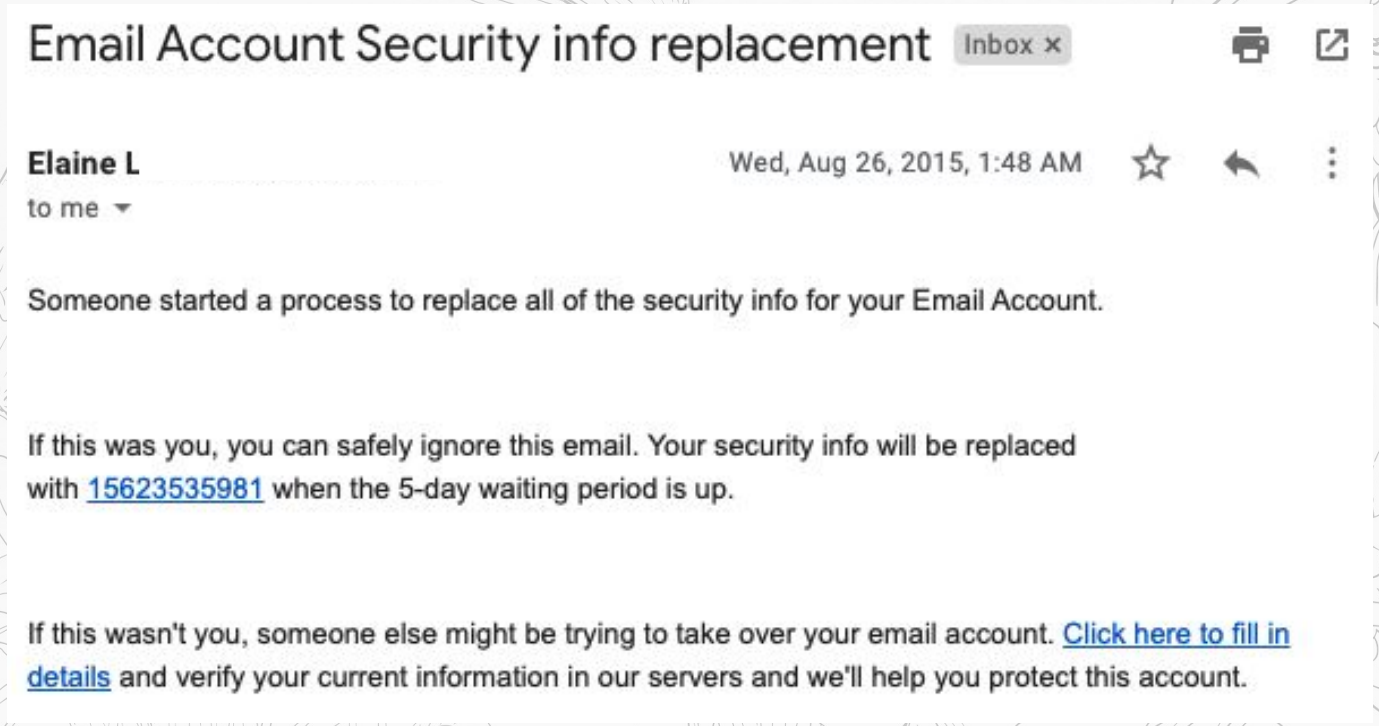


SSL Warning

Methodology

1. Participant recruitment via **email lists**
2. Section 508-compliant initial **questionna**
3. Video recorded contextual interviews
    a. Subjects **navigated directly** to **example page** of SSL or malware warnings
    b. A **phishing warning email example** was used

Phishing Email Example



Email Account Security info replacement Inbox ×

Elaine L Wed, Aug 26, 2015, 1:48 AM

to me

Someone started a process to replace all of the security info for your Email Account.

If this was you, you can safely ignore this email. Your security info will be replaced with 15623535981 when the 5-day waiting period is up.

If this wasn't you, someone else might be trying to take over your email account. Click here to fill in details and verify your current information in our servers and we'll help you protect this account.

Taken from Cornell University's "Phish Bowl".

Methodology

Ethical considerations

a. Announcing any **alterations to their environment**
b. Alerting participant to **video recording** actions and content
c. Protecting **participant privacy**

Thematic analysis

d. Open qualitative coding scheme

Results Participants

ID	Sex	Age	OS	Screen Reader	Browser
U01	F	35 to 44	Windows	JAWS	IE 9+
U04	M	55 to 64	Windows	Windows-Eyes	IE 8
U07	M	45 to 54	Mac	VoiceOver	Safari
U08	M	25 to 34	Mac	NaturalReader	Safari
U09	M	35 to 44	Windows	JAWS	IE 9+
U10	M	18 to 24	Windows	Windows-Eyes	IE 9+
U11	M	45 to 54	Windows	JAWS	Firefox
U12	F	45 to 54	Windows	JAWS	IE 9+

Results Common Themes

- The user's action depended on their **familiarity** with the website they were trying to visit
- This theme is consistent with Almuhimedi and Felt's work involving sighted users investigating the correlation between website reputation and warning adherence

U04: "*If it was something that I had been to before…I would probably either read the information or just go to the website.*"
(re: Malware warning, IE 8)

Results Common Themes

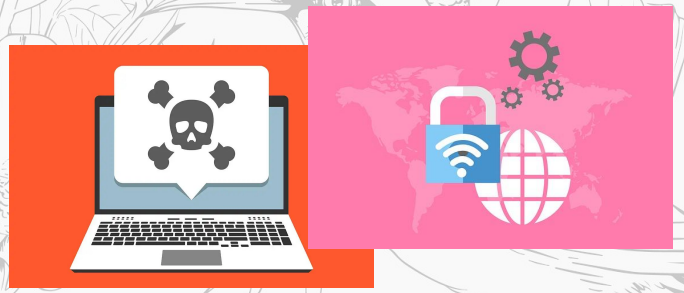
- The user's action depended on their familiarity with the website they were trying to visit
- This theme is also consistent with prior work

U08: "*If I was familiar with the site and knew that it was a safe site…I'd ignore the warning*."
(re: Malware warning, IE 8)

Results Common Themes

- There was confusion between the malware warning and SSL warning
- This theme is also consistent with prior work

U01: "*I get a lot of certificate errors and things like that.*"
(re: **Malware** warning, IE 8)



Results Common Themes

Participants suggested more uniform warning phrases

U01: "*Sometimes it's skip, sometimes it's don't warn me about this in the future. There should be some kind of uniform message…phrasing should be similar.*
I think at least something specific to look for, hey, if I come across this kind of security warning, how do I get past it."
(re: Malware warning, IE 9+)

Results Common Themes

Participants needed clarification of the destination resulting in clicking a button or link

U07: “*I am trying to think of what ‘report error’ would mean. The more things you click, the more trouble you may get into. Report an error to whom? Where is the error coming from?*”

(re: Phishing warning, Safari)

Results Common Themes

Participants needed clarification of the destination resulting in clicking a button or link

U12: “*The only thing that I would wonder is where am I gonna go, like am I gonna go back to my blank screen, where I start from, my home page, or am I gonna go back to where I came from, where would I go?*”

(re: SSL warning, IE 9+)

Results Common Themes

Participants needed clarification of the destination resulting in clicking a button or link

U11: "*Click here to close this webpage, I'm not sure what it'll do, let's find out!*"
(re: SSL warning, IE 9+)

Results Common Themes

- Participants trusted their antivirus software in any scenario - this provides a false sense of security
- This theme is also consistent with prior work

U04: "*I'm going on to the website because I trust Microsoft Security Essentials and whatever anti-malware stuff is in Windows 8.*"
(re: SSL warning, IE 8)

Results Common Themes

- Participants trusted their antivirus software in any scenario, providing a false sense of security
- This theme is also consistent with prior work

U09: "*Trusting that I have my malware and antivirus stuff up-to-date, then I'll just continue on to the site…usually you trust your antivirus software will detect anything malicious.*"
(re: SSL warning, IE 8)

Results Screen Reader Interactions

- Participants use **exhaustive scanning** and **probing** techniques when navigating warnings via screen reader
- This confirms prior work on VI users' coping tactics on the web

U11: "*I'm going to Insert +F7 to get to the links*."
(re: Malware warning, JAWS)

Results Screen Reader Interactions

- The screen reader narrates **blank lines** multiple times throughout the warning page
- This is not specific to security warnings

SR: “*Blank*.”

SR: “*Blank*.”
(Multiple scenarios)

Results Screen Reader Interactions

The screen reader narrates the same text multiple times in a row

SR: “*Reported unsafe website, navigation blocked*.”
SR: “*Reported unsafe website, navigation blocked*.”
SR: “*Reported unsafe website, navigation blocked*.”
SR: “*Page has 5 headings and 3 links*.”

(U11, Malware warning, IE 9+)

Results Screen Reader Interactions

The screen reader narrates the existence of graphics, without much context

SR: “*Graphic recommended icon*.”

U12: “*I guess it’s just a graphic with alt text, nothing to activate*.”

(re: Malware warning,IE 9+)

Discussion

- Browser security warning interface standards could include **standardized warning language** depending on warning type
- Warning design guidelines can aim to strike a balance of promoting safety (by creating inconsistencies) while **avoiding undue confusion or frustration**

Discussion

- Further research is required to determine impact of screen reader behavior on **warning habituation** for this population.
- Future work can explore methodologies that are more ecologically valid, i.e. reflect reality better without posing harm.

Thank you for coming to this talk!

Scan this code to read the paper:

References

1. D. Akhawe and A. P. Felt. Alice in warningland: A large-scale field study of browser security warning effectiveness. In USENIX Security Symposium, pages 257–272, Washington, D.C., Aug. 2013. USENIX Association.
2. S. Egelman, L. F. Cranor, and J. Hong. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pages 1065–1074. ACM, 2008.
3. C. Bravo-Lillo, L. F. Cranor, J. S. Downs, and
4. S. Komanduri. Bridging the gap in computer security warnings: A mental model approach. IEEE Security & Privacy, 9(2):0018–26, 2011.
5. A. Sotirakopoulos, K. Hawkey, and K. Beznosov. On the challenges in usable security lab studies: Lessons learned from replicating a study on SSL warnings. In Symposium on Usable Privacy and Security (SOUPS), pages 1–18, 2011.
6. M. Vigo and S. Harper. Coping tactics employed by visually disabled users on the web. Int. J. Hum.-Comput. Stud., 71(11):1013–1025, Nov. 2013.
7. B. Dosono, J. Hayes, and Y. Wang. "I'm Stuck!": A
8. Contextual Inquiry of People with Visual Impairments in Authentication. In Symposium On Usable Privacy and Security (SOUPS). USENIX Association, 2015.
9. E. Gerber. Surfing by ear: Usability concerns of computer users who are blind or visually impaired. In The 17th Annual International Conference of California State University Northridge (CSUN) "Technology and Persons with Disabilities, 2002.
10. H. Almuhimedi, A. P. Felt, R. W. Reeder, and S. Consolvo. Your reputation precedes you: History, reputation, and the chrome malware warning. In Symposium on Usable Privacy and Security (SOUPS), 2014.

Related Work

1. Akhawe and Felt found that **warning appearance** was a contributing factor to adherence rates [1]
2. Bravo et al. observed that users make security judgements based on whether a warning **appeared authentic** [3]