Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness (2013)

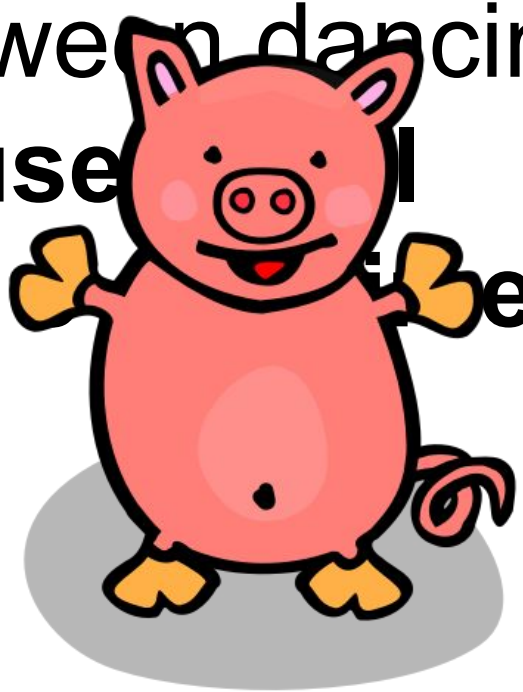
Written By: Devdatta Akhawe, University of California, Berkeley; Adrienne Porter Felt, Google, Inc.

Presented By: Allen Jue

Give a choice between dancing pigs and security, **use**[illegible]**l**

pi[illegible]**g pigs**[illegible]**e.**

- [illegible]lten



Goals

- Understand differences in browser warnings
- Analyze if browser warnings actually work in practice
- Recommendations to improve browser warnings

Background

- Browsers are ubiquitous, complex, and vulnerable
- SSL/TLS (MITM)
- Malware (MITB)
- Phishing

Your connection is not private

Attackers might be trying to steal your information from [redacted] (for example, passwords, messages or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

☑ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy Policy

ADVANCED

Back to safety

chrome

Danger: Malware Ahead!

Google Chrome has blocked access to this page on www.huffingtonpost.com.

Content from images.buddytv.com, a known malware distributor, has been inserted into this web page. Visiting this page now is very likely to infect your Mac with malware.

Malware is malicious software that causes things like identity theft, financial loss, and permanent file deletion. Learn more

Go back Advanced

☐ Improve malware detection by sending additional data to Google when I encounter warnings like this. Privacy policy


Reported Attack Page!
This web page at www.mozilla.org has been reported as an attack page and has been blocked based on your security preferences.
Attack pages try to install programs that steal private information, use your computer to attack others, or damage your system.
Some attack pages intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.
Get me out of here!
Why was this page blocked?
Ignore this warning

This Connection is Untrusted

You have asked Firefox to connect securely to **www.reddit.com**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

- **Technical Details**
- **I Understand the Risks**

Warnings

- Protect the user (**Danger** usually ahead!)
- Click-through rate
- Goal: 0% Click-through rate
- Why click-through?

Subtle differences between Chrome and Firefox

- Chrome requires 2 clicks to bypass warnings.
- Safe browsing list
  - Chrome loads, then blocks
  - Firefox automatically blocks
- Firefox SSL memory
- Iframe warnings

Previ

- Sc
- Dh
  cli
- Sc
  me
- Fri
  se

he

Methodology

- Collected with telemetry
- Release channels for browsers
- Ethics - consenting users allowed data to be collected
  - Private data demographics
  - Biased sample
  - Overrepresentation
  - Iframe warnings?

	Malware	Phish-ing	SSL	Add Exception
Release	1,968,707	89,948	NC	1,805,928
Beta	74,782	3,058	10,976	66,694
Dev	61,588	2,759	15,560	53,001
Nightly	58,789	4,239	18,617	64,725

Table 7: Warning impression sample sizes for Mozilla Firefox warnings, by channel, for all operating systems.

	Malware	Phish-ing	SSL	Add Exception
Mac	71,371	3,951	534	154,129
Win	1,892,285	85,598	10384	1,634,193
Linux	1,750	112	58	17,606

Table 8: Warning impression sample sizes for Mozilla Firefox warnings, by operating system. The malware, phishing, and the "Add Exception" samples are from the release channel, whereas the SSL samples are from the beta channel. The frame issue does not affect statistics that pertain only to the "Add Exception" dialog.

Operating System	Malware		Phishing	
	Firefox	Chrome	Firefox	Chrome
Windows	7.1%	23.5%	8.9%	17.9%
MacOS	11.2%	16.6%	12.5%	17.0%
Linux	18.2%	13.9%	34.8%	31.0%

Table 1: User operating system vs. clickthrough rates for malware and phishing warnings. The data comes from stable (i.e., release) versions.

Channel	Malware		Phishing	
	Firefox	Chrome	Firefox	Chrome
Stable	7.2%	23.2%	9.1%	18.0%
Beta	8.7%	22.0%	11.2%	28.1%
Dev	9.4%	28.1%	11.6%	22.0%
Nightly	7.1%	54.8%	25.9%	20.4%

Table 2: Release channel vs. clickthrough rates for malware and phishing warnings, for all operating systems.

SSL Warnings

- 33.0% Firefox
- 70.2% Google Chrome

Why?

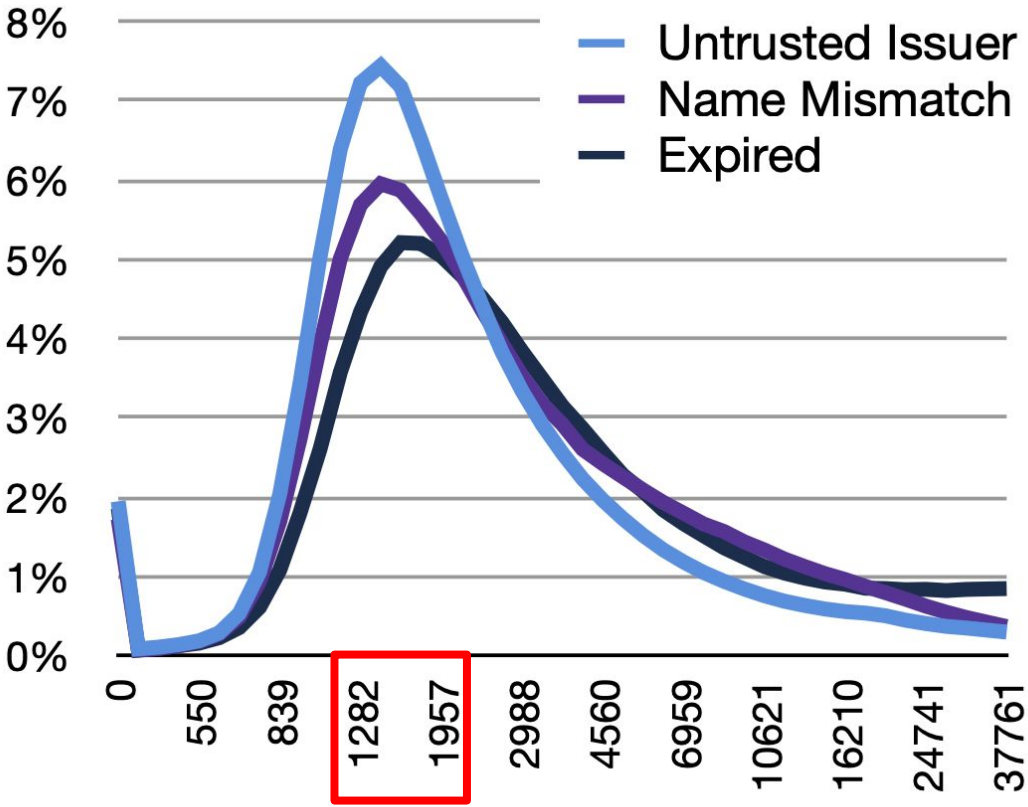
- Number of clicks (1 vs. 3)
- Warning Appearance
- Certificate Pinning (Un-bypassable in Chrome)
- Remembering Exceptions

Certificate Error	Percentage of Total	Clickthrough Rate
Untrusted Issuer	56.0%	81.8%
Name Mismatch	25.0%	62.8%
Expired	17.6%	57.4%
Other Error	1.4%	–
All Error Types	100.0%	70.2%

People are Cognizant

- People do not view more information
- They do not blindly skip exception

Time Spent on SSL



Implications

- Security warnings **are** effective
  - Chrome
    - Phishing: 18.0%
    - Malware: 23.2%
    - SSL: 70.2%
  - Firefox
    - Phishing: 9.1%
    - Malware: 7.2%
    - SSL: 33.0%

Recommendations

- Don’t click: towards an effective anti-phishing training. A comparative literature review[1]
- ”I am Definitely Manipulated, Even When I am Aware of it. It’s Ridiculous!” - Dark Patterns from the End-User Perspective.[2]
- *Design of Everyday Things* - Don Norman

1. (Jampen, D., Gür, G., Sutter, T. et al. 2020)
2. (Kerstin Bongard-Blanchy, Arianna Rossi, Salvador Rivas, Sophie Doublet, Vincent Koenig, and Gabriele Lenzini. 2021.)

Your clock is ahead

A private connection to **example.com** can't be established because your computer's date and time (Sunday, November 17, 2024 at 6:11:54 PM) are incorrect.

NET::ERR_CERT_DATE_INVALID

Turn on enhanced protection to get Chrome's highest level of security

Advanced

Update date and time

Conclusion

- Malware, Phishing, and SSL are all prominent browser attacks
- Google Chrome and Mozilla Firefox prevent most users from entering these sites
    - SSL is still relatively high
- Previous studies have ecological invalidity – this paper offers a more accurate way to test browser warning effectiveness in situ
- Human solutions