Alice in Warningland

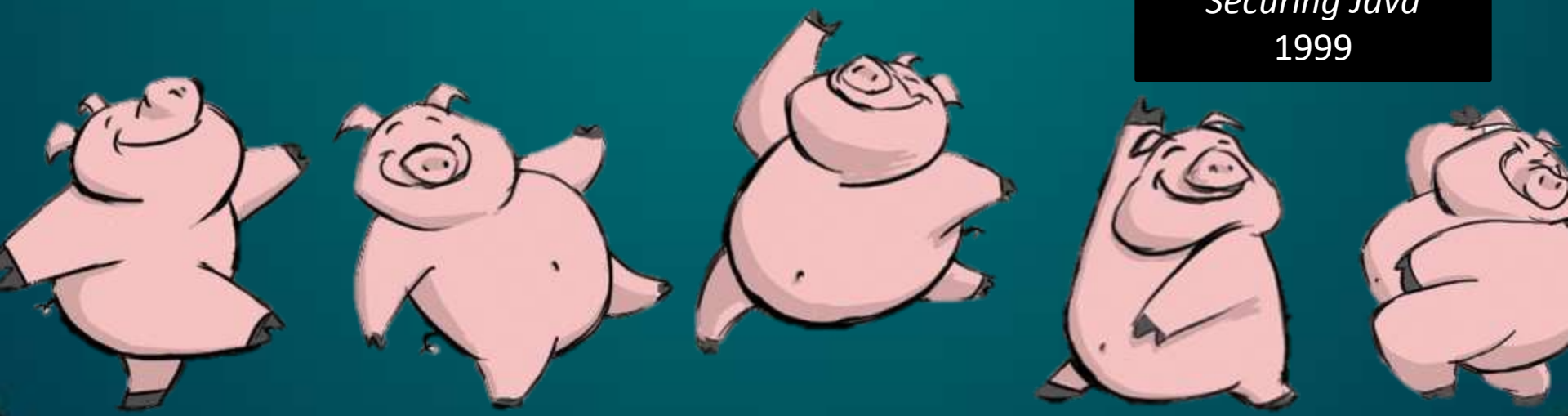
A Large-Scale Field Study of Browser Security Warning Effectiveness

Devdatta Akhawe
UC Berkeley

Adrienne Porter Felt
Google, Inc.

Given a choice between dancing pigs and security, the user will pick dancing pigs every time

Felten and McGraw
Securing Java
1999

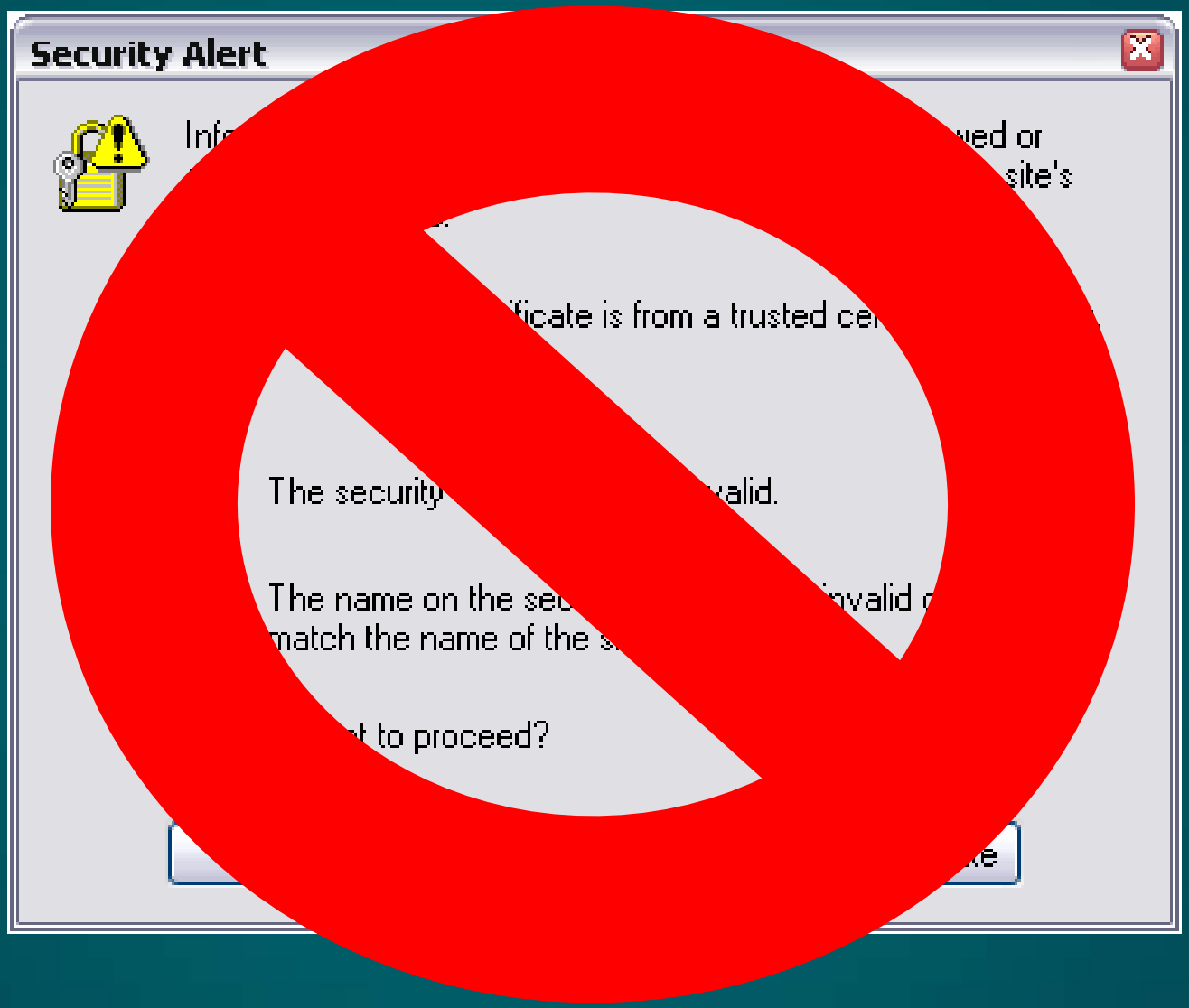


a growing body of measurement studies make clear that ...[users] are oblivious to security cues [and] ignore certificate error warnings

Herley
The Plight of The Targeted Attacker at Scale
2010

Evidence from experimental studies indicates that most people don't read computer warnings, don't understand them, or simply don't heed them, even when the situation is clearly hazardous.

Bravo-Lillo
Bridging the Gap in Computer Security Warnings
2011


Security Alert
ed or
site's
icate is from a trusted ce
The security
alid.
The name on the se
nvalid
match the name of the s
to proceed?

Malware Ahead!

malware.testing.google.test/testing/malware/

chrome

The Website Ahead Contains Malware!

Google Chrome has blocked access to malware.testing.google.test for now.

Even if you have visited this website safely in the past, visiting it now is very likely to infect your computer with malware.

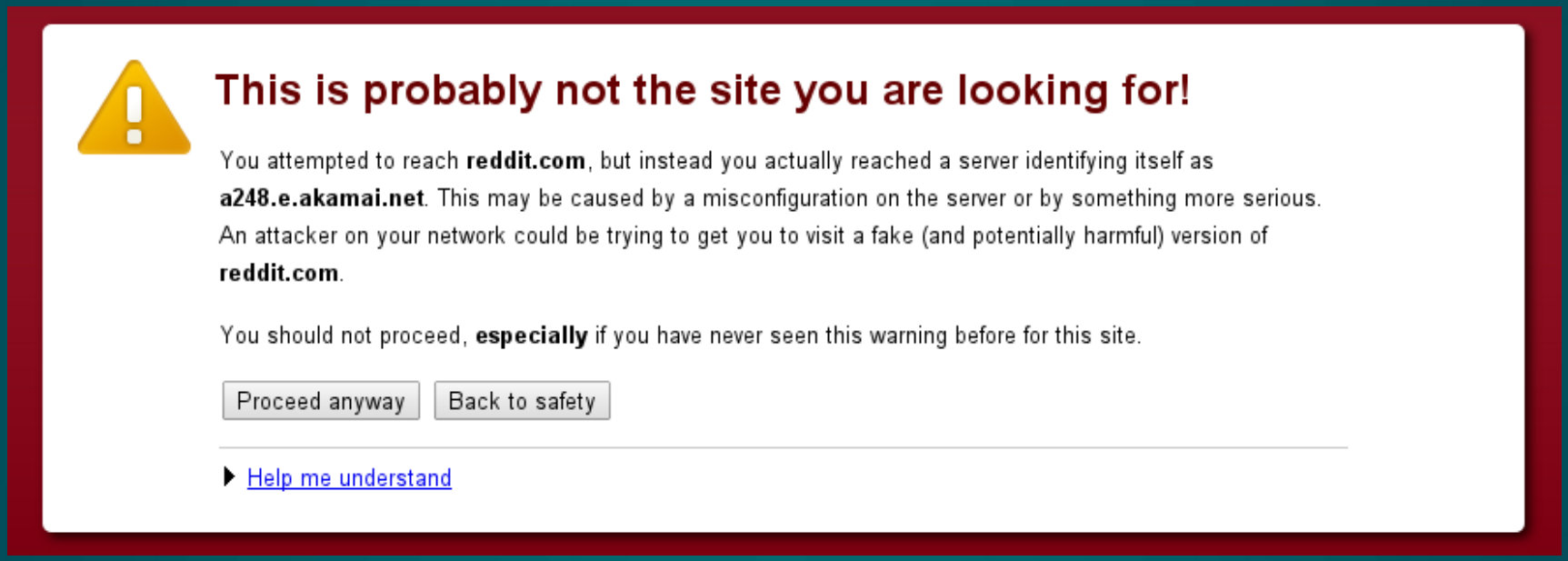
Malware is malicious software that causes things like identity theft, financial loss, and permanent file deletion. Learn more

Go back

Advanced

Firefox Malware Warning

Chrome SSL Warning



This is probably not the site you are looking for!

You attempted to reach **reddit.com**, but instead you actually reached a server identifying itself as **a248.e.akamai.net**. This may be caused by a misconfiguration on the server or by something more serious. An attacker on your network could be trying to get you to visit a fake (and potentially harmful) version of **reddit.com**.

You should not proceed, **especially** if you have never seen this warning before for this site.

Proceed anyway | Back to safety

Help me understand

Firefox SSL 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**

today

A large scale measurement of user responses to modern warnings *in situ*

today

A large scale measurement of user responses to modern warnings *in situ*

What did we measure?

Clickthrough Rate

$$\frac{\text{\# warnings ignored}}{\text{\# warnings shown}}$$

(across all users)

What is the ideal click through rate?

0%

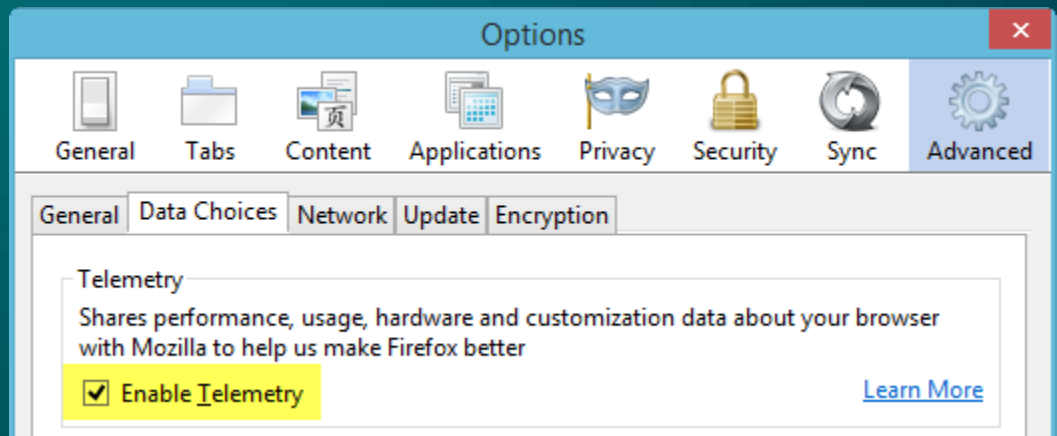
Why aim for a 0% rate?

- Low false positives => protecting users
  - The Google Safe Browsing list (malware/phishing warnings) has low false positives
- High false positives ? (SSL Warnings)
  - Low clickthrough incentivizes websites to fix their SSL errors
  - False positives annoy users and browsers should reduce the number of false warnings to achieve 0% clickthrough rate

How did we measure it?

Browser Telemetry

- A mechanism for browsers to collect pseudonymous performance and quality data from end users
- Users *opt-in* to sharing data with the browser vendors
  - Users have to opt-out in pre-release builds (e.g., Nightly)



Data Collection

- We implemented “probes” to measure number of times a warning shown and number of times ignored
- For both Google Chrome and Mozilla Firefox’s malware, phishing, and SSL warnings
- Data collected:
  - April 28-May 31 for Google Chrome
  - May 1-May 31 for Mozilla Firefox

Limitations

- No data on demographics or browsing habits of users except for OS and release channel
- Users might be biased towards clicking because they agreed to share data
- We present aggregate data across all users
  - Individual users could be over-represented
  - Over-represented users in Google Chrome still contribute fewer than 1% of the total warnings

Limitations: Iframes

- Our original Mozilla Firefox implementation did not ignore warnings in iframes
  - Since warnings in iframes might not be visible, this caused us to measure a lower click-through rate
  - Chrome never shows a warning in an iframe
- Bug fixed in Firefox 23, but we only have pre-release data
  - Impact is ~2 percentage points for Malware/phishing warnings so we use old numbers
  - Impact is ~25 percentage points for SSL warnings, so we use new numbers

Details about the data

- Google Chrome
  - ~6M malware warnings (~2.1M users)
  - ~386K phishing warnings (~204K users)
  - ~16.7M SSL Warnings (~4.5M users)
- Mozilla Firefox (nearly 1% of all users)
  - ~2.1M malware warnings
  - ~100K phishing warnings
  - 10,976 SSL Warnings (pre-release only)
  - ~2M “Add Exception” dialogs

What did we find?

Results

1. Malware/Phishing
2. SSL Warnings
3. SSL Warnings by Error Type
4. SSL Warning Times

7.2% (Firefox Malware)

23.2% (Chrome Malware)

Firefox rates < Chrome Rates

9.1% (Firefox Phishing)

18.0% (Chrome Phishing)

Firefox Malware Warning

User only needs to click on “Ignore”

chrome

The Website Ahead Contains Malware!

Google Chrome has blocked access to malware.testing.google.test for now.

Even if you have visited this website safely in the past, visiting it 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 additio
Privacy policy

User has to click "Advanced" and then "Ignore"

7.2% (Firefox)

1 click to ignore

23.2% (Chrome)

2 clicks to ignore

But higher clickthrough

7.2% (Firefox Malware)

23.2% (Chrome Malware)

9.1% (Firefox Phishing)

18.0% (Chrome Phishing)

7.2% (Firefox Malware)

This rate fluctuates a lot

Rational?

9.1% (Firefox Phishing)

18.0% (Chrome Phishing)

What about demographics?

Operating System & Release Channel

Operating System & Release Channel

Results by Release

- A release "channel" is a way for browsers and developers to test out bleeding edge features
  - Useful for developers, often unstable
- Different channels further ahead in release train
- For example, on May 27, 2013
  - Stable = Firefox v21, Beta = Firefox v22, Aurora (i.e., Dev) = Firefox v23, Nightly = Firefox v24
- **Hypothesis: Earlier channels correspond to greater technical skill of user**

Impact of Demographics

Operating System	Malware Firefox	Malware Chrome	Phishing Firefox	Phishing 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%

Channel	Malware Firefox	Malware Chrome	Phishing Firefox	Phishing 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%

Impact of Demographics

Operating System	Malware Firefox	Malware Chrome	Phishing Firefox	Phishing Chrome
Linux	18.2%	13.9%	34.8%	31.0%

Channel	Malware Firefox	Malware Chrome	Phishing Firefox	Phishing 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%

Linux clickthrough rates much higher (except Chrome malware)

Impact of Demographics

Clickthrough rates higher for Firefox developer releases

Operating System	Malware Firefox	Malware Chrome	Phishing Firefox	Phishing 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%

Channel	Malware Firefox	Malware Chrome	Phishing Firefox	Phishing 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%

Does a greater degree of technical skill corresponds to reduced risk aversion?

(if Linux /developer releases => more technical skill)

Results by Date

- For Google Chrome malware warnings, the clickthrough rates range from 11.2% to 24.9% for different weeks
- We do not see any such effect for Mozilla Firefox
- Possibly because Google Chrome shows a top-level warning for secondary resources
  - For example, malware ad on youtube.com causes Chrome to show warning for YouTube, while Mozilla silently blocks it

Results

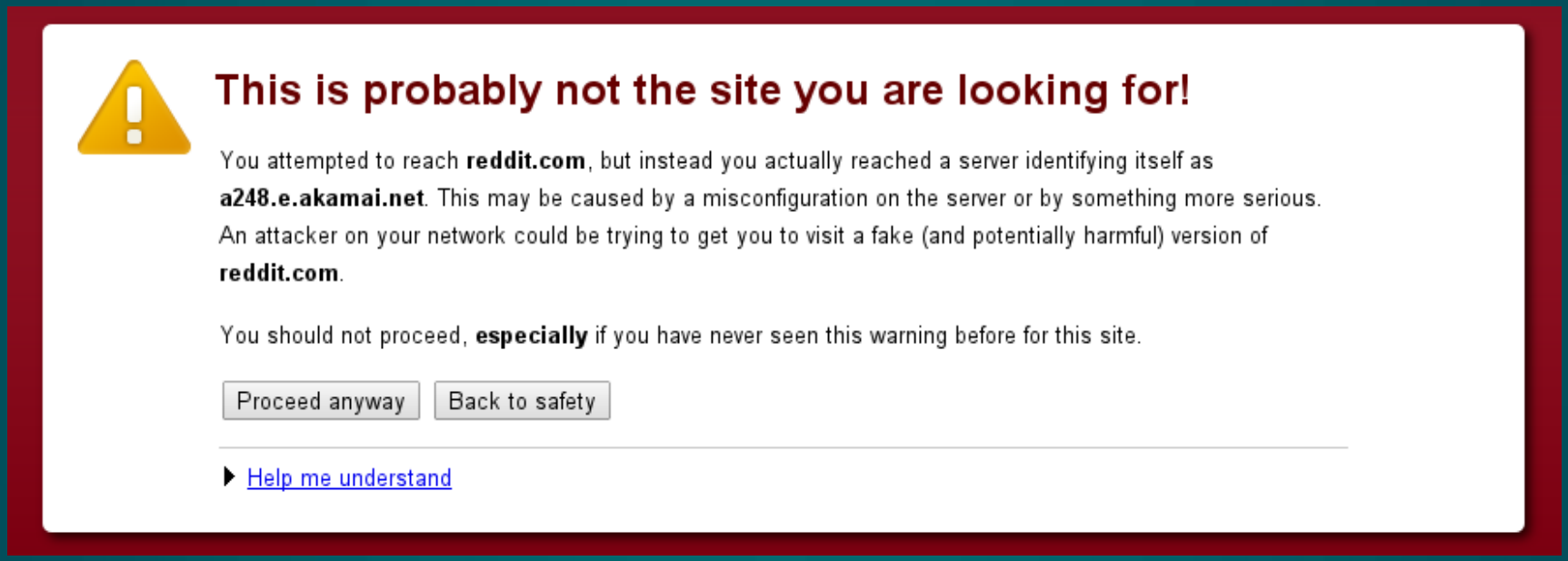
1. Malware/Phishing
2. SSL Warnings
3. SSL Warnings by Error Type
4. SSL Warning Times

33.0% (Firefox beta)

70.2% (Chrome stable)

Possible Reasons

1. Warning Appearance
2. Number of Clicks
3. Certificate Pinning
4. Remember Exception


This is probably not the site you are looking for!
You attempted to reach reddit.com, but instead you actually reached a server identifying itself as a248.e.akamai.net. This may be caused by a misconfiguration on the server or by something more serious. An attacker on your network could be trying to get you to visit a fake (and potentially harmful) version of reddit.com.
You should not proceed, especially if you have never seen this warning before for this site.
Proceed anyway
Back to safety
Help me understand

Firefox SSL 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.

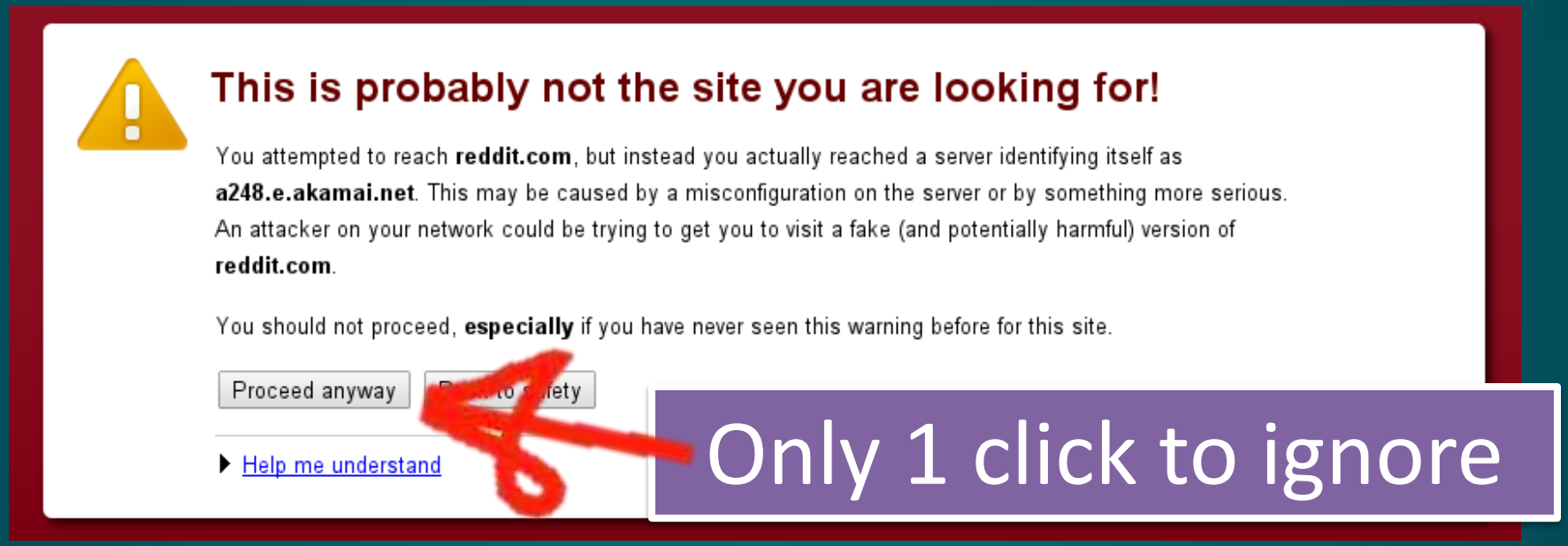
Get me out of here!

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

Possible Reasons

1. Warning Appearance
2. Number of Clicks
3. Certificate Pinning
4. Remember Exception

Chrome SSL Warning



Firefox SSL 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. Howe

Two clicks to ...

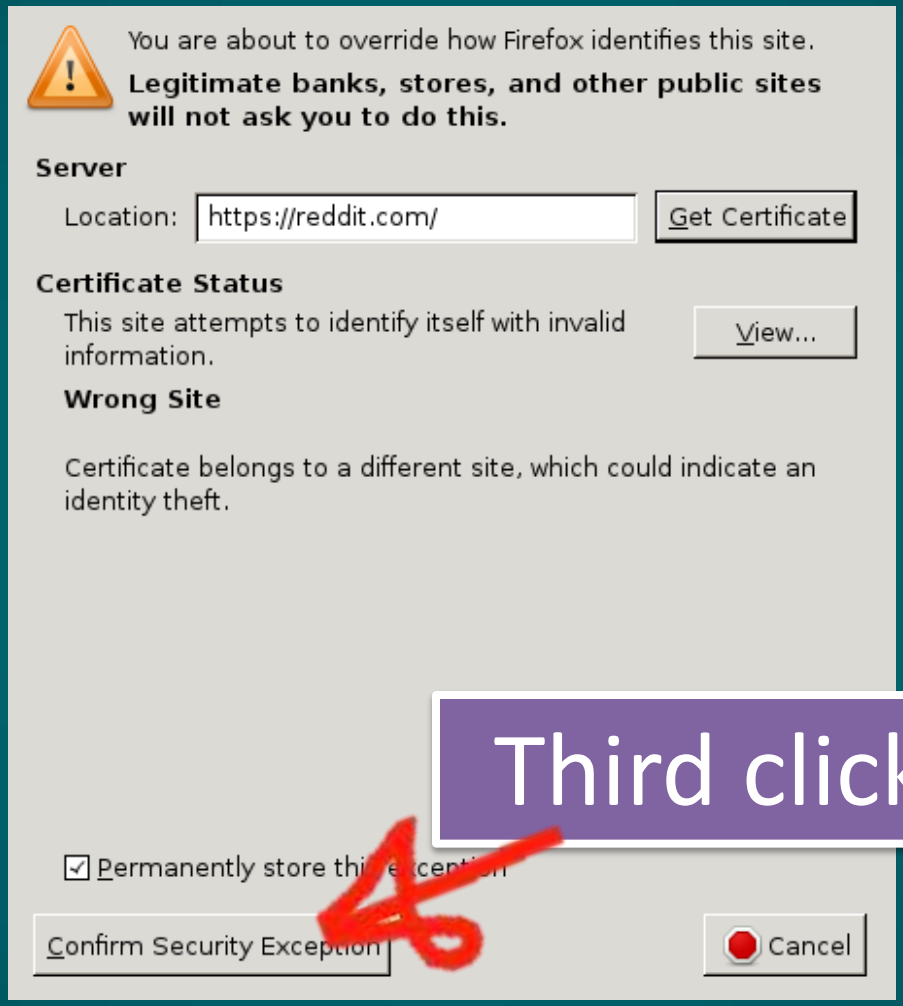
What Should I Do?

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

Get me out of here!

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

Firefox SSL “Add Exception” dialog



Third click to confirm

Firefox SSL warning requires more clicks and has lower clickthrough rate

But, previously…

7.2% (Firefox Malware)

1 click to ignore

23.2% (Chrome Malware)

2 clicks to ignore

Possible Reasons

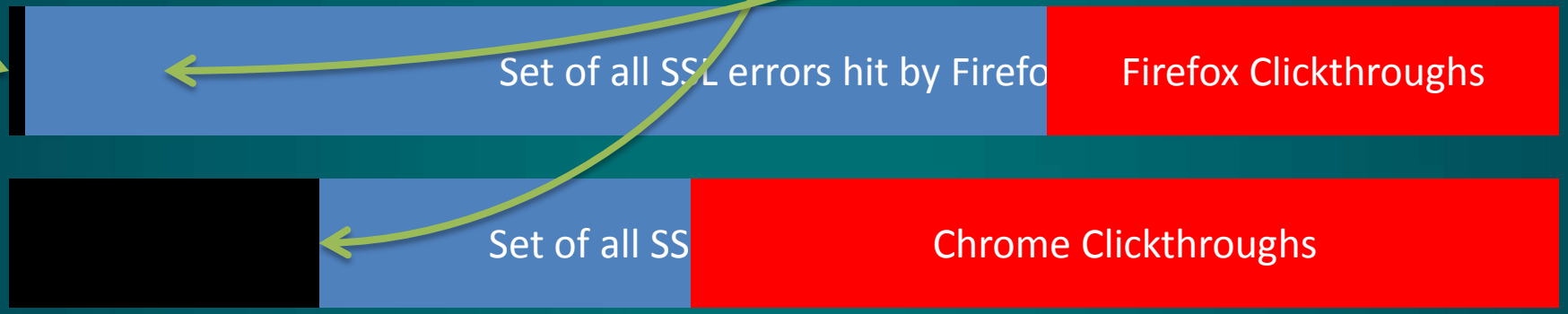
1. Warning Appearance
2. Number of Clicks
3. Certificate Pinning
4. Remember Exception

Certificate Pinning

- Browser does not allow user to bypass errors for high-profile “pinned” sites
- Chrome ships with a bigger list of such high-profile sites
- Nearly 20% of all warnings are non-bypassable on Chrome vs. 1% for Firefox

[redacted]

Firefox users heeding warnings for high profile sites?

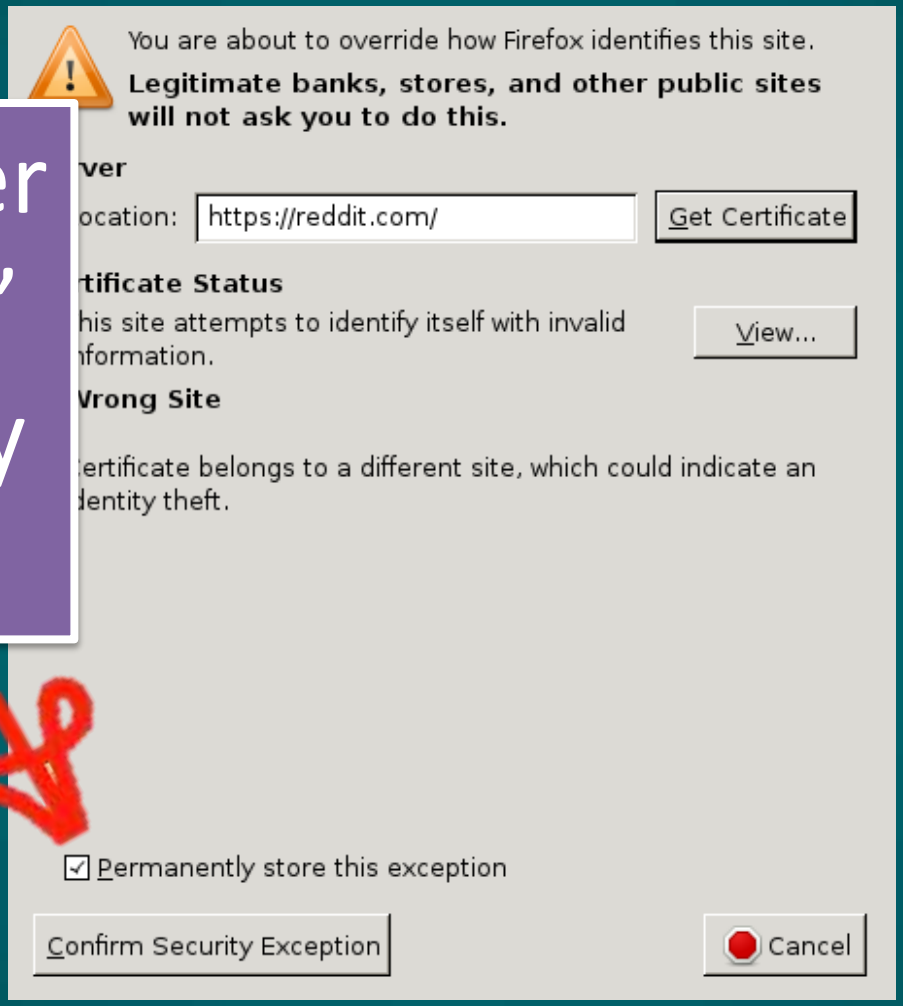


~56% of errors are ignored

Possible Reasons

1. Warning Appearance
2. Number of Clicks
3. Certificate Pinning
4. Remember Exception

“Remember Exception” checked by default



1 site with bad certificate

3 visits

33% clickthrough rate for Firefox

100% clickthrough rate for Chrome

Possible Reasons

1. Warning Appearance
2. Number of Clicks
3. Certificate Pinning
4. Remember Exception

What about demographics?

Results

Similar effect as for Firefox malware

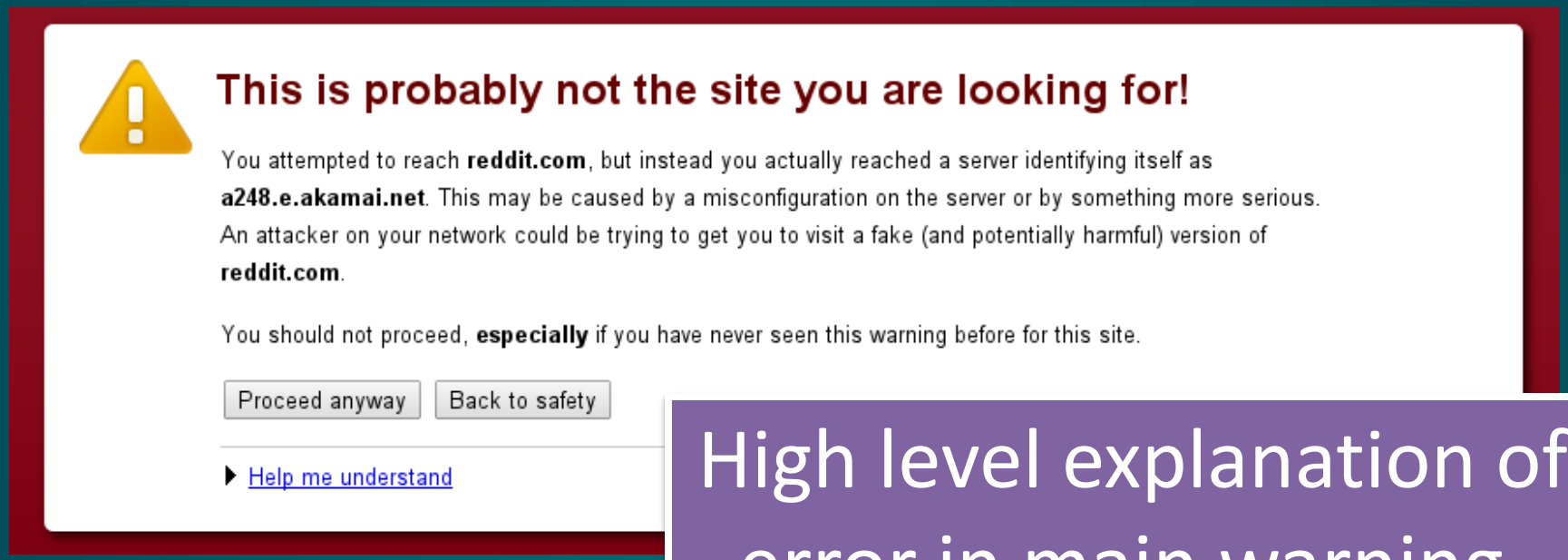
Operating System	Firefox	Chrome
Windows	32.5%	71.1%
MacOS	39.3%	68.8%
Linux	58.7%	64.2%
Android	NC	64.6%

Channel	Firefox	Chrome
Stable	NC	70.2%
Beta	32.2%	73.3%
Dev	35.0%	75.9%
Nightly	43.0%	74.0%

Results

1. Malware/Phishing
2. SSL Warnings
3. SSL Warnings by Error Type
4. SSL Warning Times

Chrome SSL Warning



High level explanation of error in main warning, more in “Help Me Understand”

Google Chrome

Network view systems can reduce SSL warnings by up to 75%

Error Type	Percentage of Total	Clickthrough Rate
Self-Signed Cert	56.0%	81.8%
Wrong Domain Name	25.0%	62.8%
Expired Certificate	17.6%	57.4%
Other	1.4%	--

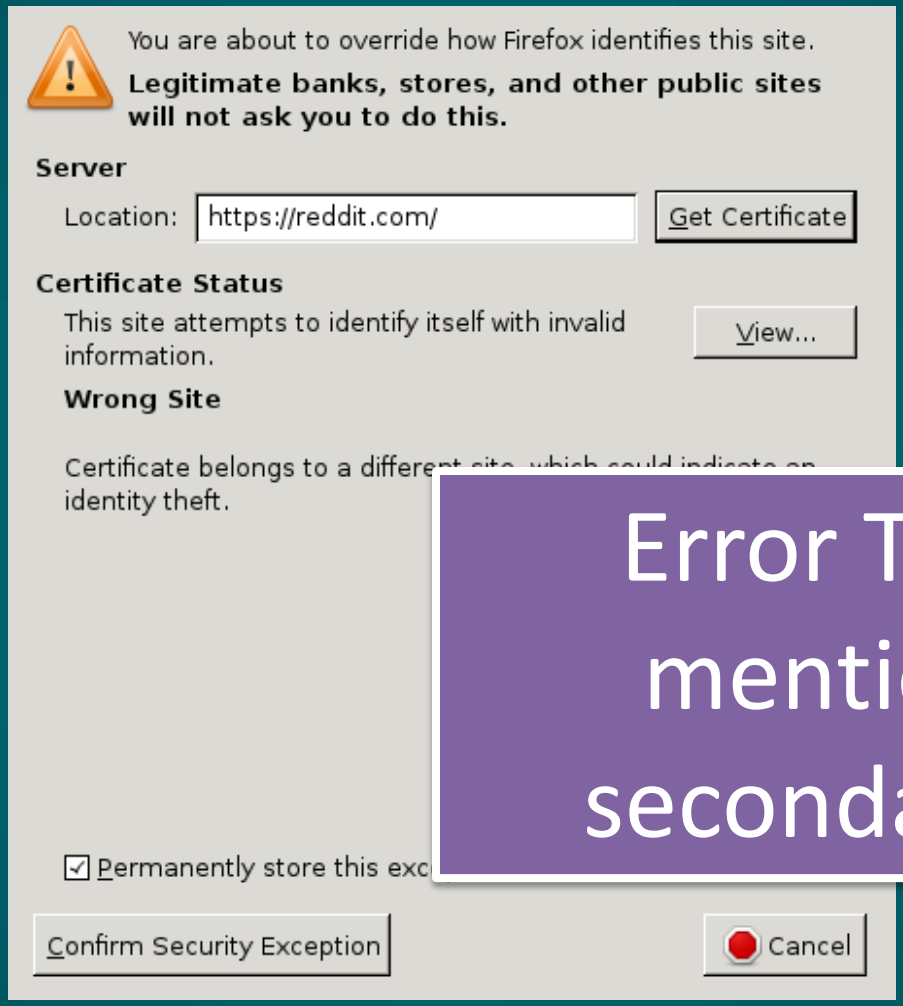
But not a panacea: name errors account for at least 25% of errors

Google Chrome

More common warnings have higher clickthrough rate

Error Type	Percentage of Total	Clickthrough Rate
Self-Signed Cert	56.0%	81.8%
Wrong Domain Name	25.0%	62.8%
Expired Certificate	17.6%	57.4%
Other	1.4%	--

Firefox SSL “Add Exception” dialog



Error Type only mentioned on secondary dialog

Mozilla Firefox

Not much difference by error type.

Maybe users make a decision at the very first click?

Error Type	Percentage of Total	Clickthrough Rate
Untrusted Issuer	38%	87.1%
Untrusted, Name Mismatch	26.4%	87.9%
Name Mismatch	15.7%	80.3%
Expired	5.1%	80.7%
Expired, Untrusted, Name	4.7%	87.6%
Expired, Untrusted	4.1%	83.6%
Expired, Name Mismatch	0.7%	85.2%
None of the above	<0.1%	77.9%

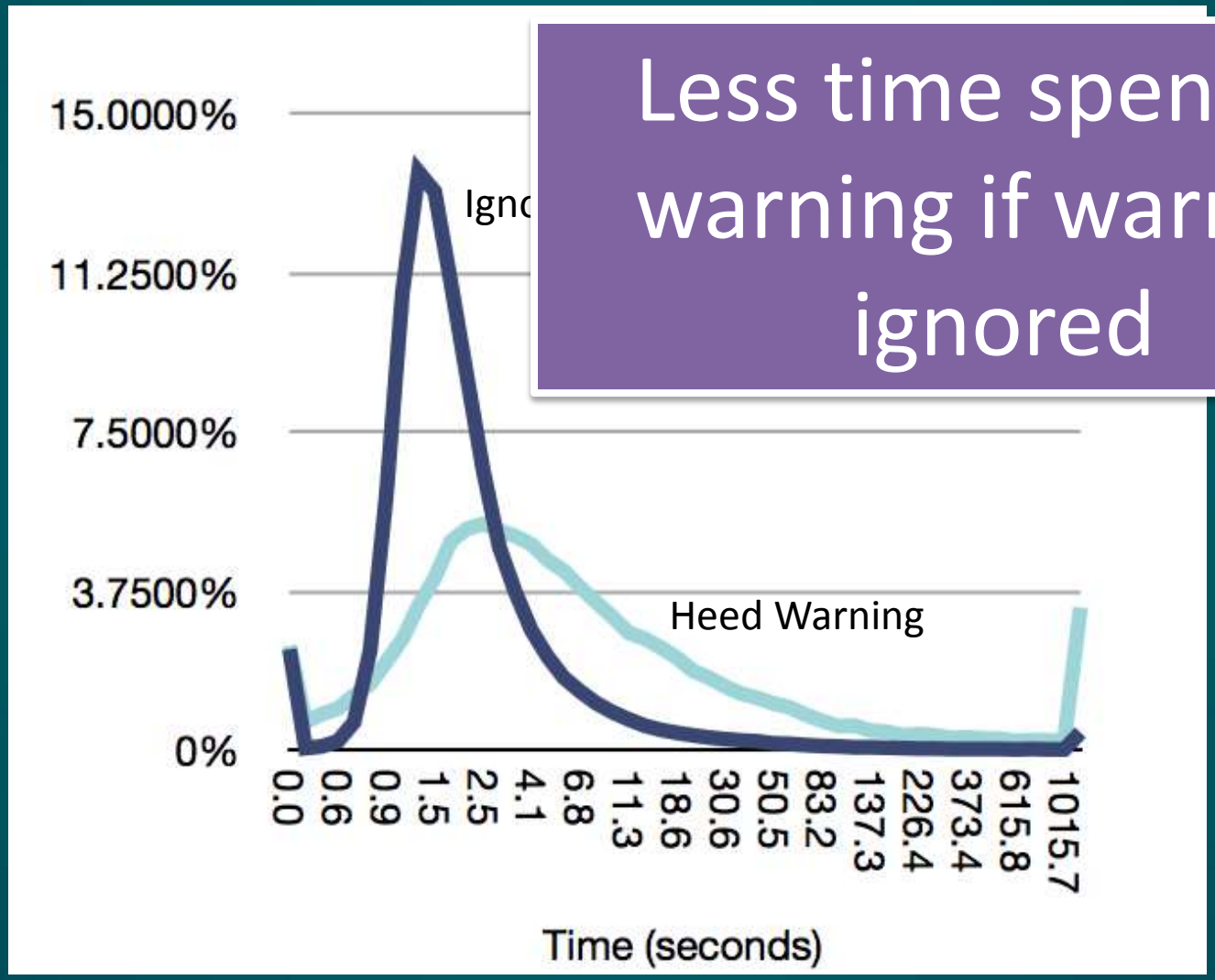
Discussion

- 24.4 point difference between clickthrough rates for expired & self-signed certs (Chrome)
- Maybe untrusted issuer errors only occur on unimportant sites
- Maybe expired certificates are a surprise to users and thus users are cautious
  - Lower clickthrough rate when site that used to work without warning shows a warning

Results

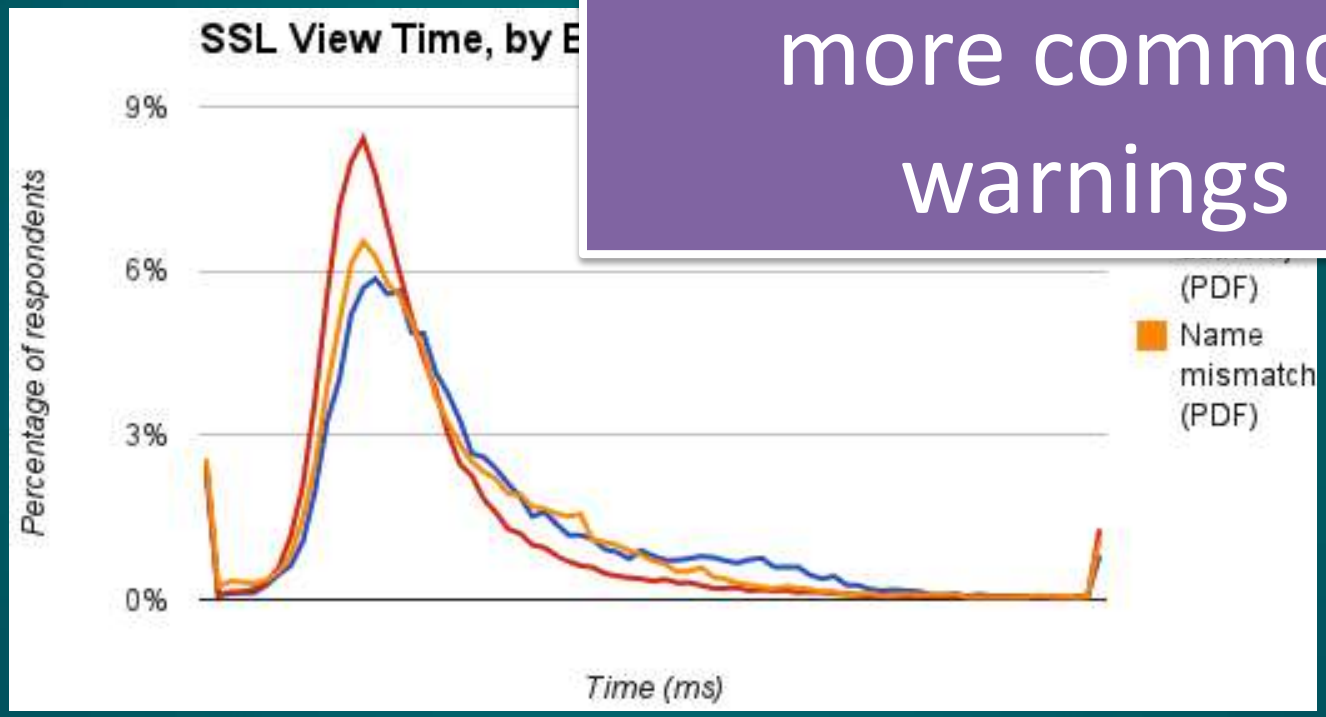
1. Malware/Phishing
2. SSL Warnings
3. SSL Warnings by Error Type
4. SSL Warning Times

Chrome: Time by outcome



Less time spent on warning if warning ignored

Chrome: Time by Error Type



Less time spent on more common warnings

Implications

Warning Effectiveness

- Save for the Chrome SSL Warning, all other warnings ignored only under 33% of times
- Chrome SSL Warning ignored 70.2% of times
  - Positive results with other warnings suggest this can be improved
- **Warning design can impact user behavior**
  - Security practitioners should not ignore the role of the user

User Attention

- Our data contradict the stereotype of wholly oblivious users with no interest in security.
  - 24 point difference between clickthrough rates for untrusted issuer and expired cert errors for Google Chrome
  - 21.3% of Mozilla Firefox users who clicked on “Add Exception” unticked “Permanently Store This Exception”

Comparison with Previous Work

- Difference between lab studies and field measurements
  - Lab studies focused on old warning designs
  - Or participant trust in lab environment affected results?

During our study we observed a strong disparity between our participants actions during the laboratory tasks and their self-reported "would be" actions during similar tasks in everyday computer practices. Our participants attributed this disparity to the laboratory environment and the security it offered

Sotirakopoulos et al.
On the challenges of Usable Security Lab Studies

Comparison with Previous Work

- Difference between lab studies and field measurements
  - Lab studies focused on old warning designs
  - Or participant trust in lab environment affected results?
- Renewed emphasis on field study needed
  - Experience Sampling
  - Network based measurements
  - Real world deception studies

Theory of Warning Fatigue

- We observe behavior consistent with theory of warning fatigue
  - Common errors clicked through faster and more frequently
  - Security practitioners should limit the number of warnings raised

In Conclusion

We find that browser security warnings can be effective, although they can be improved.

We also find evidence that warning mechanism design can have a tremendous impact on user behavior.

Thanks for Listening!

evil@berkeley.edu
www.cs.berkeley.edu/~devdatta