Improving Chrome's Security Warnings

Adrienne Porter Felt

Chrome Security (Enamel)

The role of warnings:

Browser warnings stand between users and dangerous situations (malware, phishing, surveillance)

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

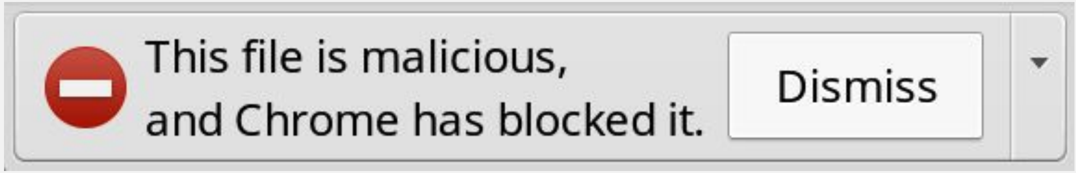
“~~Given a choice between dancing pigs and security the user will pick dancing pigs every time~~”

Challenges:

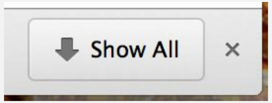
- Low false positive rate
- Users really want their content
- Highly technical situation
- No immediate consequences

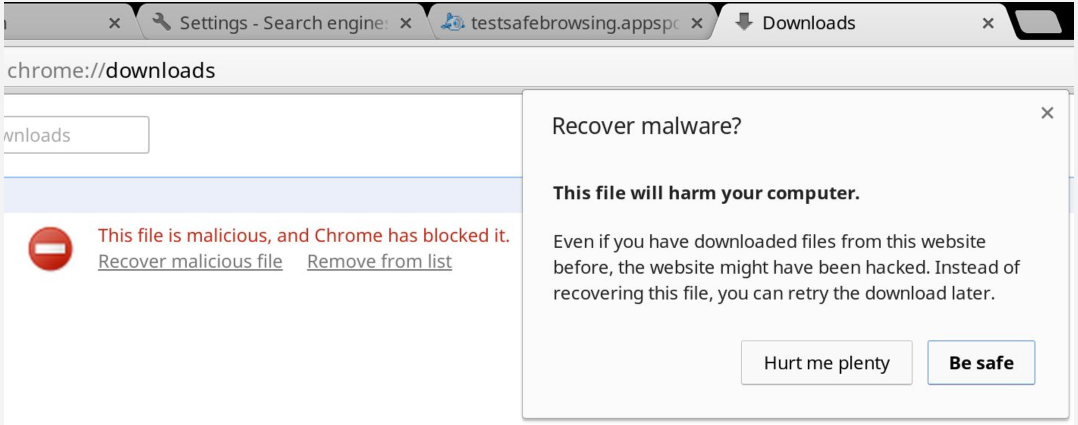
How well do warnings work?

MALICIOUS DOWNLOAD



This file is malicious, and Chrome has blocked it.





chrome://downloads

This file is malicious, and Chrome has blocked it.

Recover malicious file Remove from list

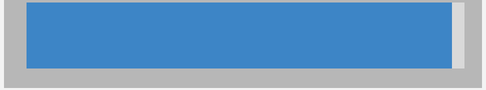
Recover malware?

This file will harm your computer.

Even if you have downloaded files from this website before, the website might have been hacked. Instead of recovering this file, you can retry the download later.

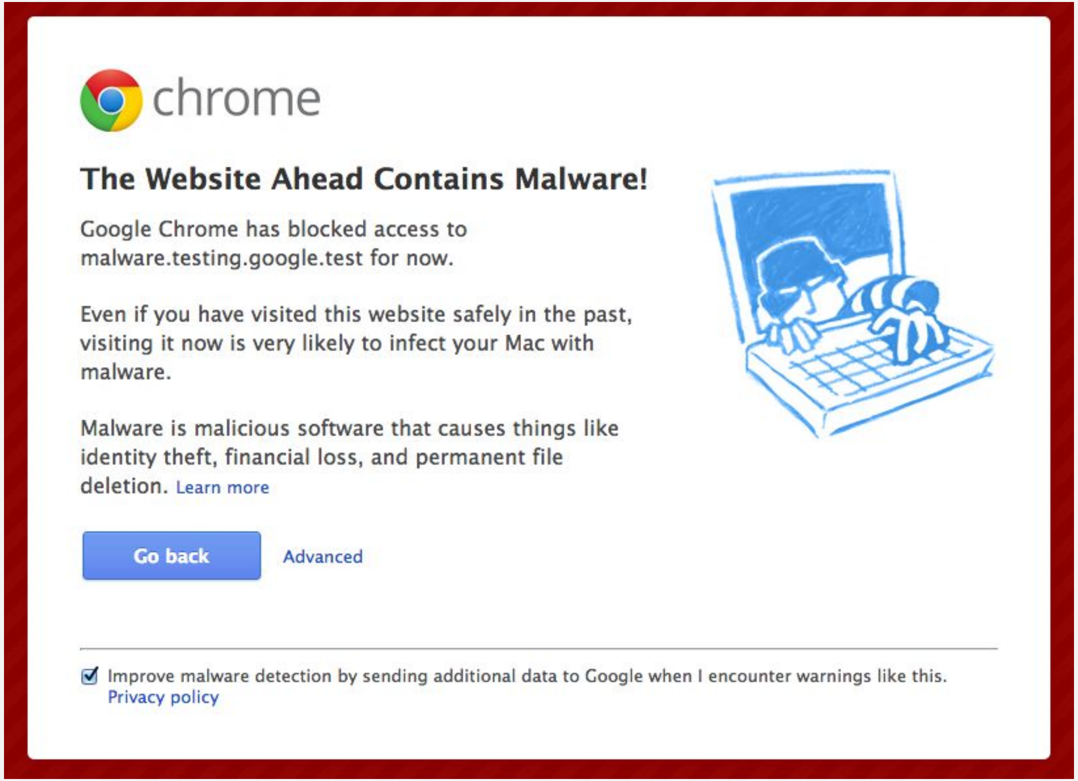
THREAT:
User tries to download & run bad binary

CONFIDENCE:



CTR: <5%

MALWARE INTERSTITIAL



The Website Ahead Contains Malware!

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

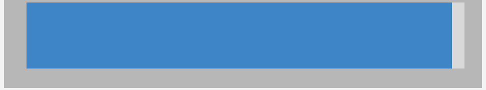
Even if you have visited this website safely in the past, visiting it now is very likely to infect your Mac with malware.

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

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

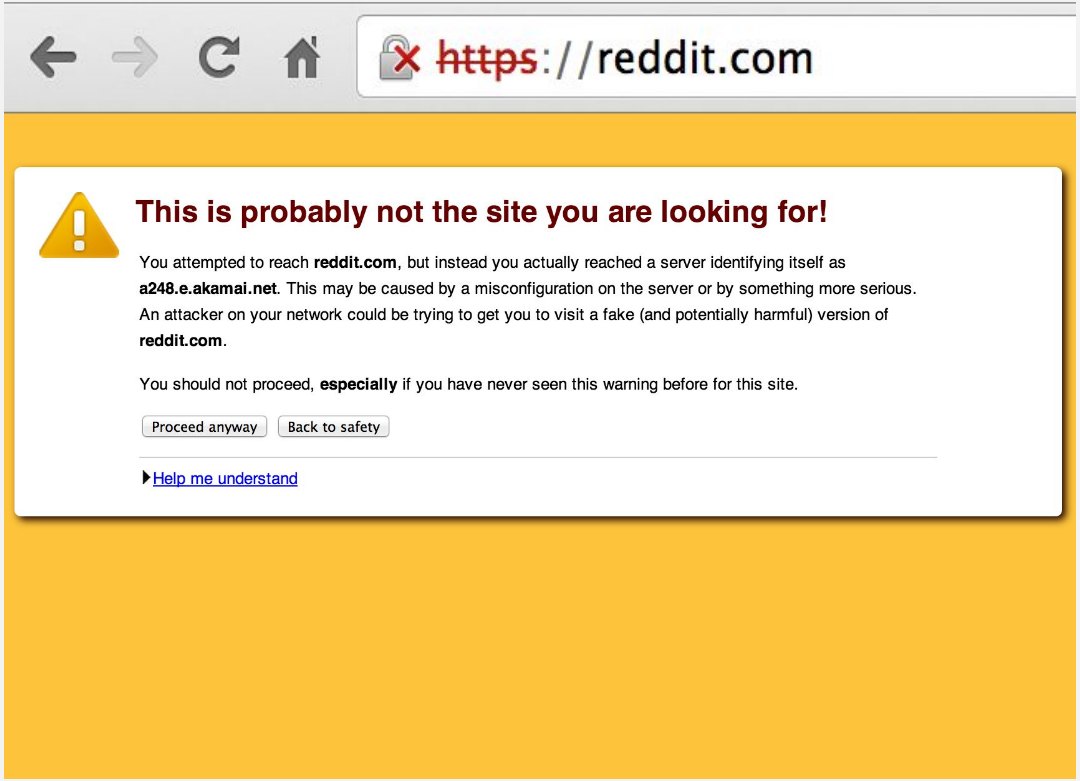
THREAT:
User at risk of drive-by download

CONFIDENCE:



CTR: ~18%

NON-FATAL SSL INTERSTITIAL



~~https~~://reddit.com

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.

THREAT:
Active network attacker

CONFIDENCE:

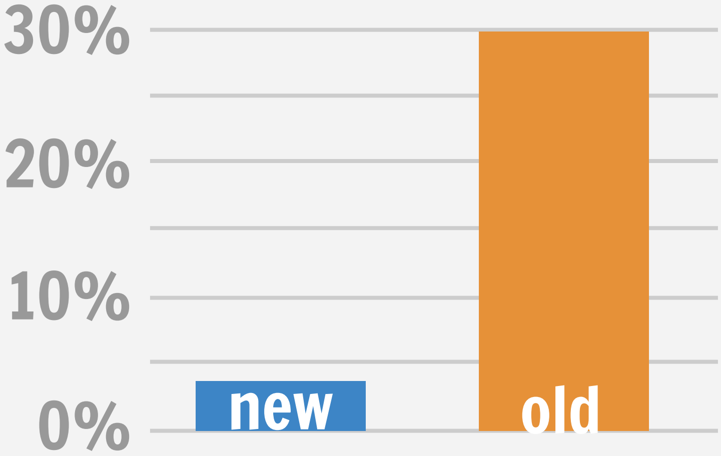
CTR: 68%

Takeaway:

- Warnings can be effective
- Some work better than others
- Room for improvement

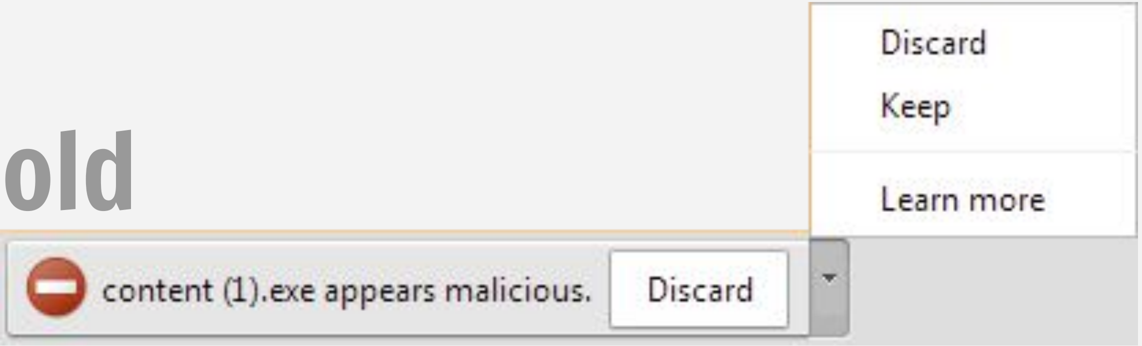
Case study: malicious downloads

We dramatically reduced the CTR with UX changes

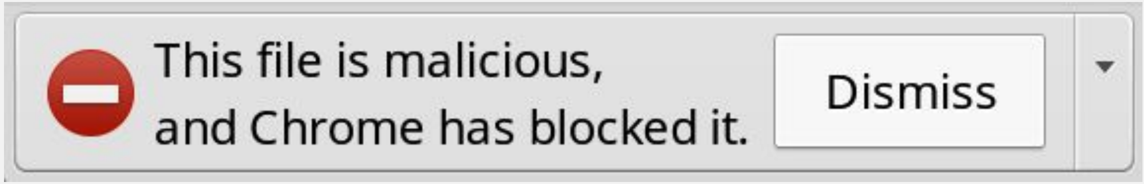


1: DOWNLOAD SHELF

old

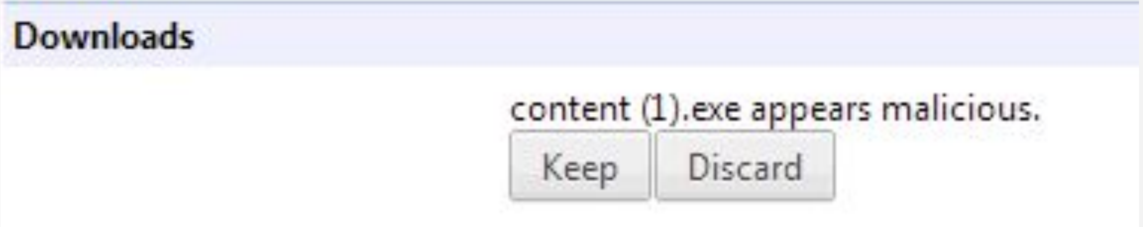

content (1).exe appears malicious.

new


This file is malicious, and Chrome has blocked it.

2: chrome://downloads

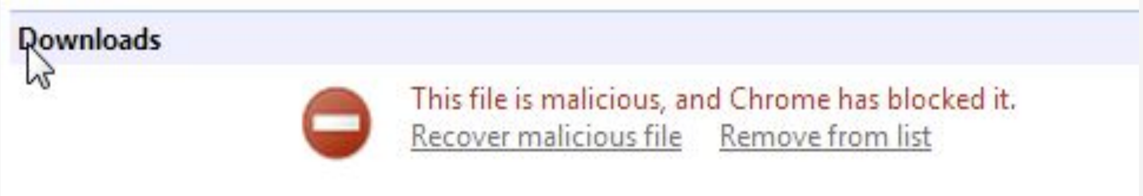
old



Downloads

content (1).exe appears malicious.

new

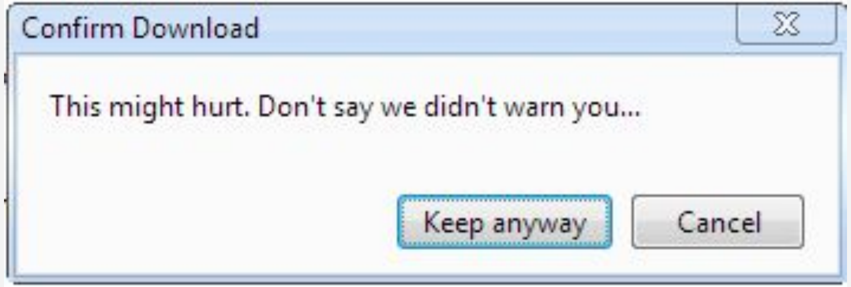


Downloads

This file is malicious, and Chrome has blocked it.

3: FINAL CONFIRMATION

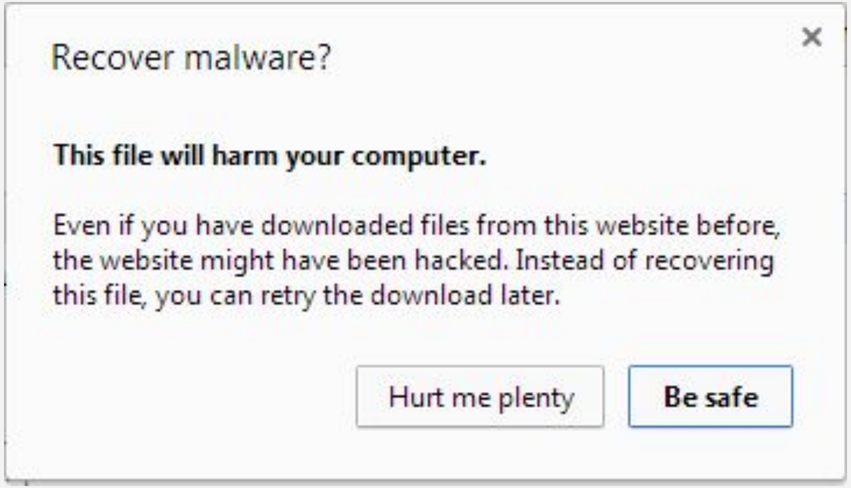
old



Confirm Download

This might hurt. Don't say we didn't warn you...

new



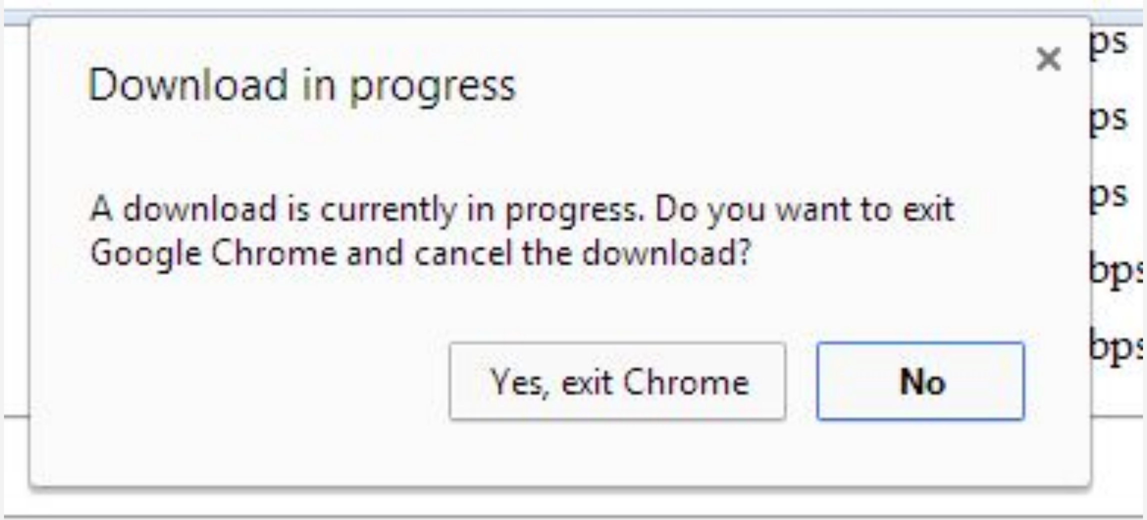
Recover malware?

This file will harm your computer.

Even if you have downloaded files from this website before, the website might have been hacked. Instead of recovering this file, you can retry the download later.

4: BROWSER SHUTDOWN

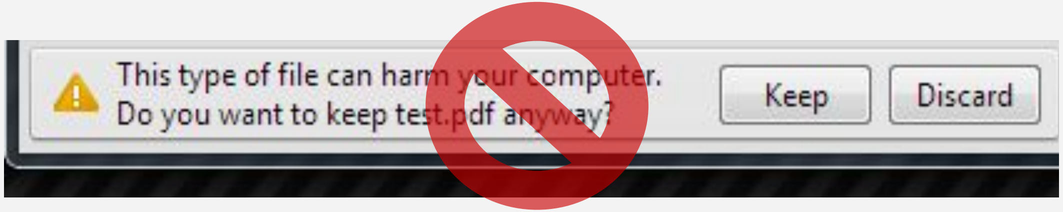
old



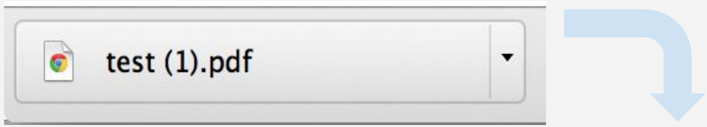
Download in progress

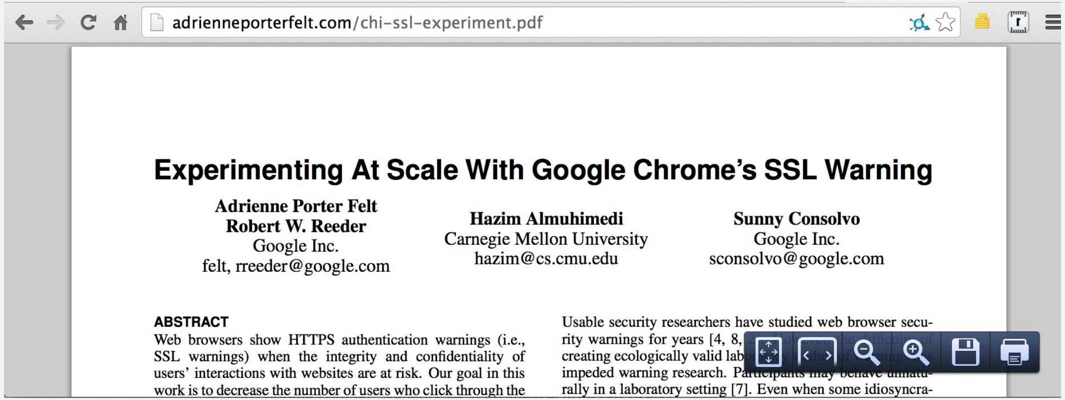
A download is currently in progress. Do you want to exit Google Chrome and cancel the download?

5: GENERIC PDF WARNINGS



This type of file can harm your computer.
Do you want to keep test.pdf anyway?





Experimenting At Scale With Google Chrome's SSL Warning

Adrienne Porter Felt
Robert W. Reeder
Google Inc.
felt, rreeder@google.com

Hazim Almuhimedi
Carnegie Mellon University
hazim@cs.cmu.edu

Sunny Consolvo
Google Inc.
sconsolvo@google.com

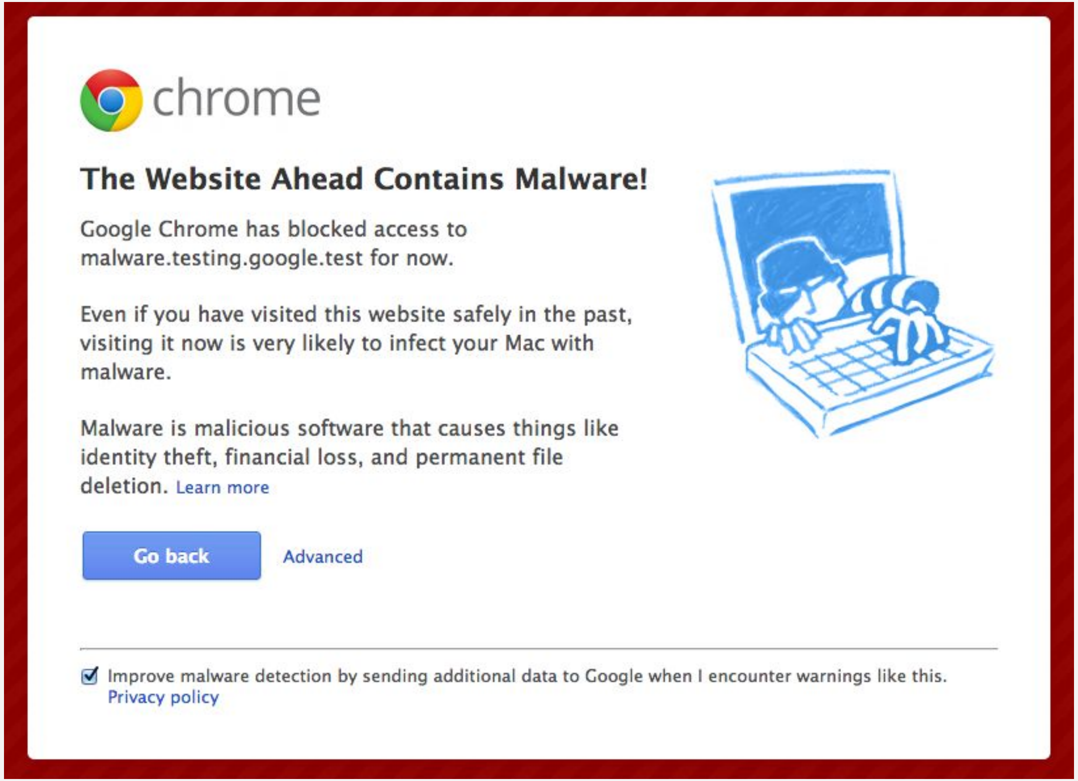
ABSTRACT

Web browsers show HTTPS authentication warnings (i.e., SSL warnings) when the integrity and confidentiality of users' interactions with websites are at risk. Our goal in this work is to decrease the number of users who click through the

Usable security researchers have studied web browser security warnings for years [4, 8, creating ecologically valid lab impeded warning research. Participants may behave unnaturally in a laboratory setting [7]. Even when some idiosyncra-

Case study: malware interstitial

MALWARE INTERSTITIAL



The Website Ahead Contains Malware!

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

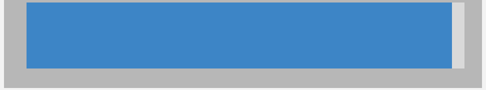
Even if you have visited this website safely in the past, visiting it now is very likely to infect your Mac with malware.

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

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

THREAT:
User at risk of drive-by download

CONFIDENCE:

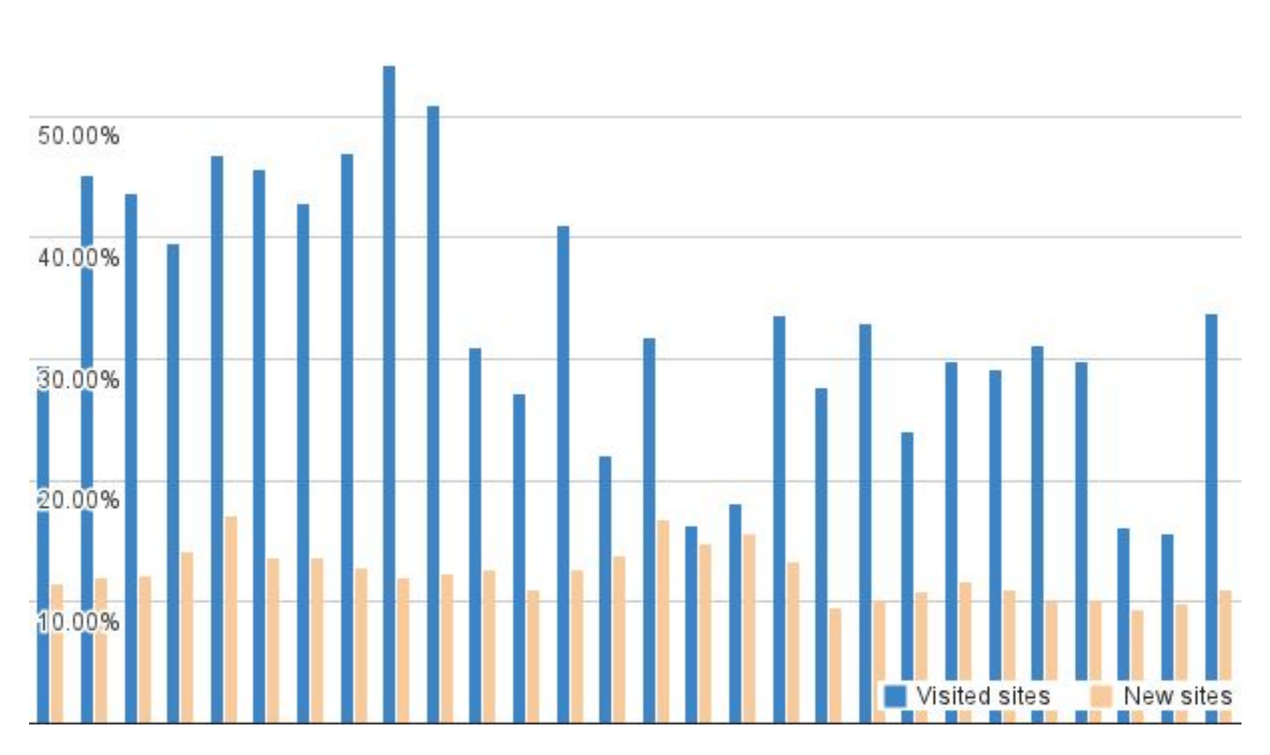


CTR: ~18%

FIELD STUDY: OCTOBER 2013

15%	15%	15%	16%	15%	15%	16%
17%	21%	21%	23%	15%	15%	18%
16%	18%	15%	11%	10%	12%	14%
21%	18%	24%	27%	14%	14%	15%

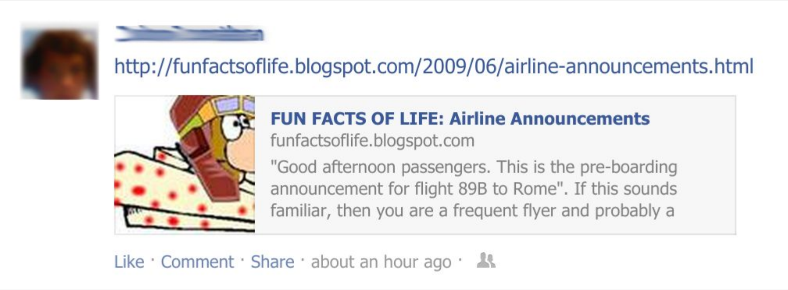
EFFECT OF PRIOR EXPERIENCE



Mechanical Turk experiment:

Does the reputation of the destination affect perception?

Low-reputation



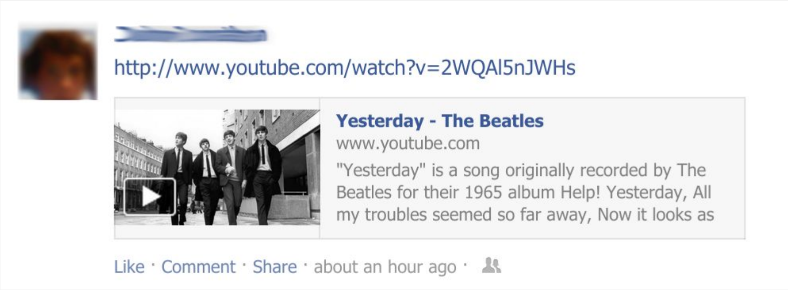
[redacted]

http://funfactsoflife.blogspot.com/2009/06/airline-announcements.html

FUN FACTS OF LIFE: Airline Announcements
funfactsoflife.blogspot.com
"Good afternoon passengers. This is the pre-boarding announcement for flight 89B to Rome". If this sounds familiar, then you are a frequent flyer and probably a

Like · Comment · Share · about an hour ago ·

High-reputation



[redacted]

http://www.youtube.com/watch?v=2WQAl5nJWHs

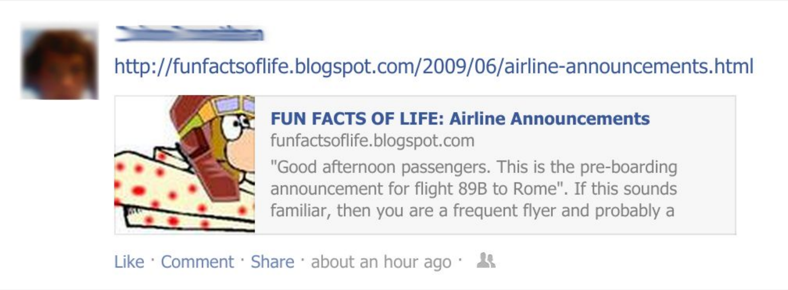
Yesterday - The Beatles
www.youtube.com
"Yesterday" is a song originally recorded by The Beatles for their 1965 album Help! Yesterday, All my troubles seemed so far away, Now it looks as

Like · Comment · Share · about an hour ago ·

Mechanical Turk experiment:

Does the reputation of the destination affect perception? Yes

Low-reputation 5% (471)



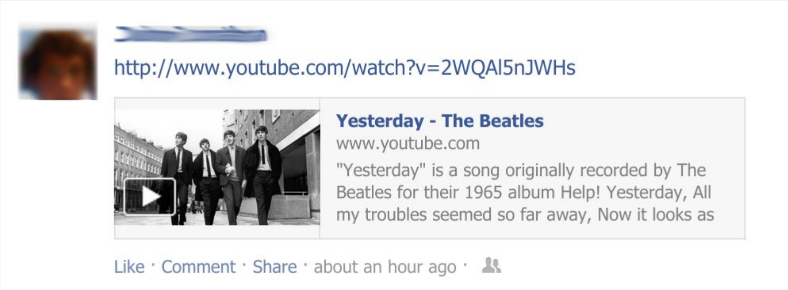
[redacted]

http://funfactsoflife.blogspot.com/2009/06/airline-announcements.html

FUN FACTS OF LIFE: Airline Announcements
funfactsoflife.blogspot.com
"Good afternoon passengers. This is the pre-boarding announcement for flight 89B to Rome". If this sounds familiar, then you are a frequent flyer and probably a

Like · Comment · Share · about an hour ago ·

High-reputation 38% (357)



[redacted]

http://www.youtube.com/watch?v=2WQAl5nJWHs

Yesterday - The Beatles
www.youtube.com
"Yesterday" is a song originally recorded by The Beatles for their 1965 album Help! Yesterday, All my troubles seemed so far away, Now it looks as

Like · Comment · Share · about an hour ago ·

I have never heard of this site so I wouldn’t trust it.

I frequent youtube.com a lot and I have never gotten any malware

Youtube is a well-known and highly trusted site.

REPUTATION

I use Linux I’m not afraid of anything

Because I own a mac and i don’t worry about that stuff

I would still proceed knowing I have an anti virus

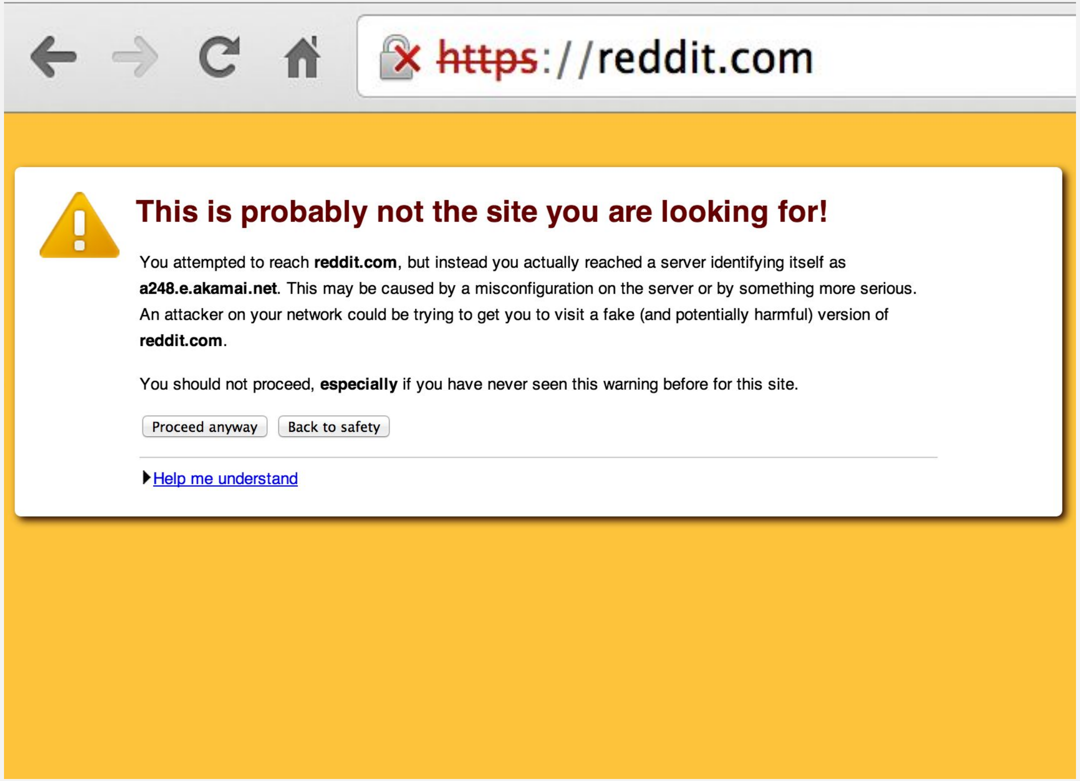
INVINCIBLE

Takeaway:

We need to figure out how to override normal indicators of trustworthiness

Case study: non-fatal SSL interstitial

NON-FATAL SSL INTERSTITIAL



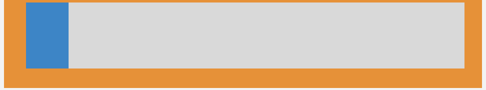
This is probably not the site you are looking for!

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.

THREAT:
Active network attacker

CONFIDENCE:



CTR: 68%

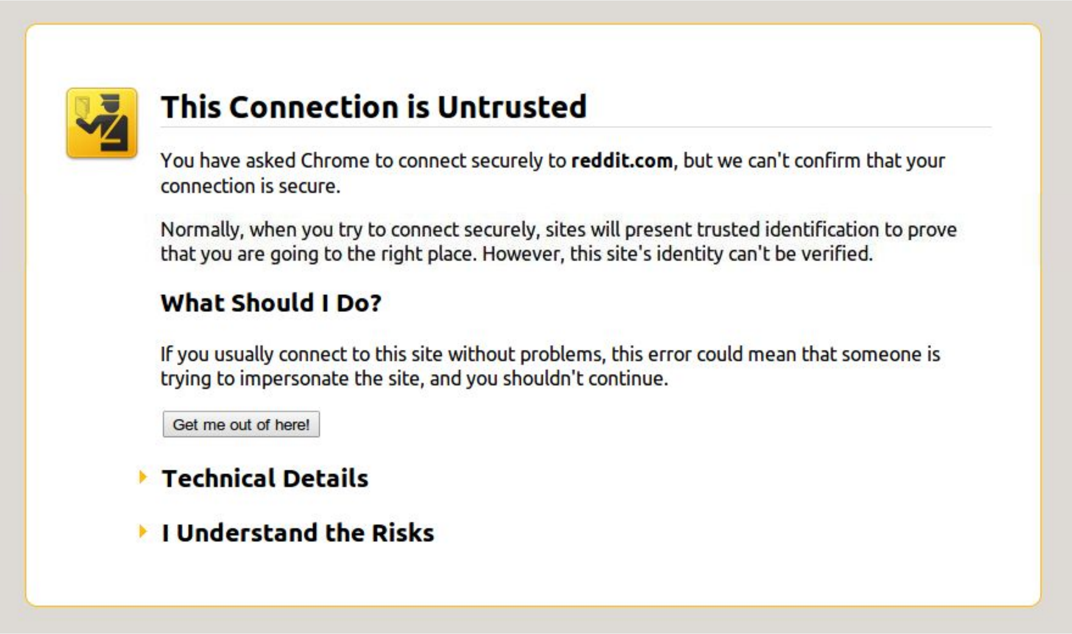
A few reasons for false positives:

- Developers use self-signed cert
- Enterprise deployment of certs
- Captive portals
- Subdomain name mismatch

Works in progress:

- Remember previously-seen certs
- Better integration with captive portal detection
- Categorize errors by severity

FIREFOX'S SSL ERROR



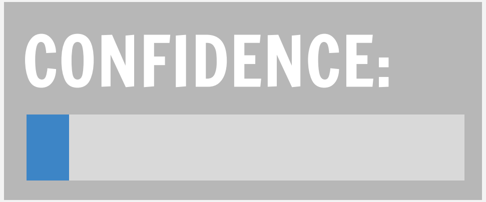
This Connection is Untrusted

You have asked Chrome to connect securely to **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.



CONFIDENCE:

CTR: 33%

Firefox experiment:

Is the Firefox warning UI better?

Conditions:

- Chrome warning
- Firefox warning in Chrome
- Firefox warning in Firefox

Firefox experiment:

Is the Firefox warning UI better?

Yes, but that’s not the whole story

Conditions:

- Chrome warning 68%
- Firefox warning in Chrome 56% (47%?)
- Firefox warning in Firefox 33%

Firefox experiment:

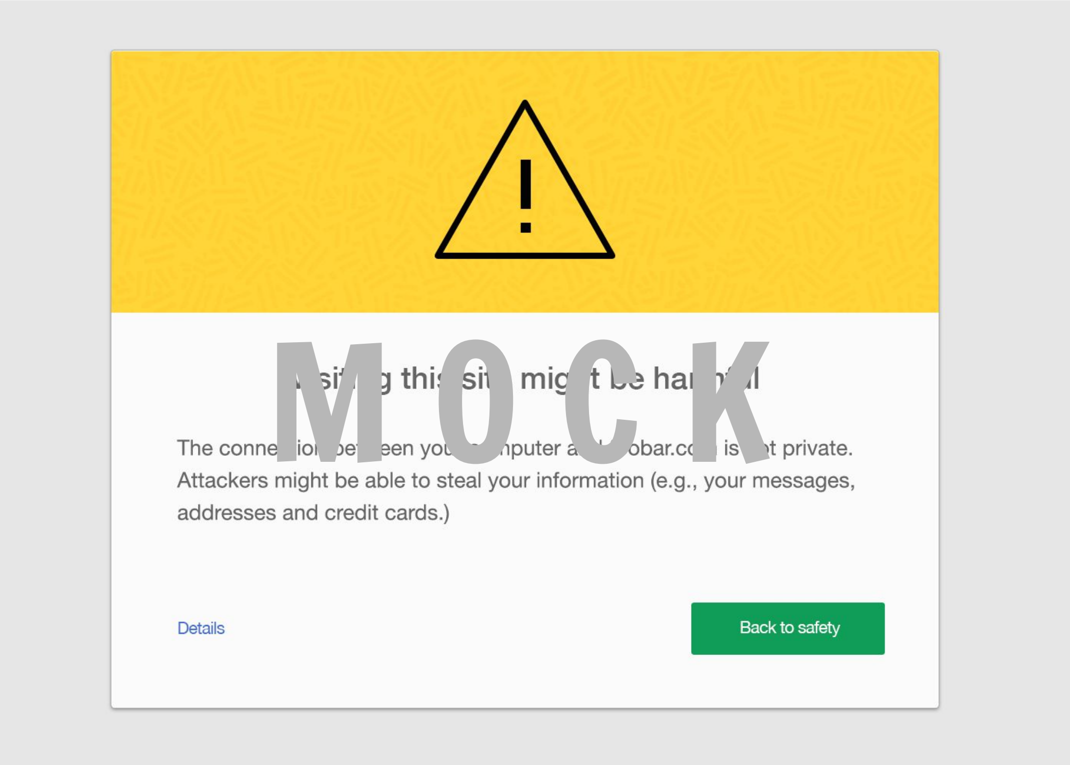
Is the Firefox warning UI better?

Yes, but that’s not the whole story

Conditions:

- Chrome warning 68%
- Firefox warning in Chrome 56% (47%?)
- Firefox warning in Firefox 33%

WORK IN PROGRESS



Visiting this site might be harmful

The connection between your computer and foobar.com is not private. Attackers might be able to steal your information (e.g., your messages, addresses and credit cards.)

Do warnings work?

Case study: malicious downloads

Case study: malware interstitial

Case study: non-fatal SSL interstitial

felt@chromium.org

CREDITS...

Mustafa Acer
Alex Ainslie
Alan Bettes
Sunny Consolvo
Hazim Almuhimedi

Robert Reeder
Chris Palmer
Somas Thyagaraja
Joel Weinberger