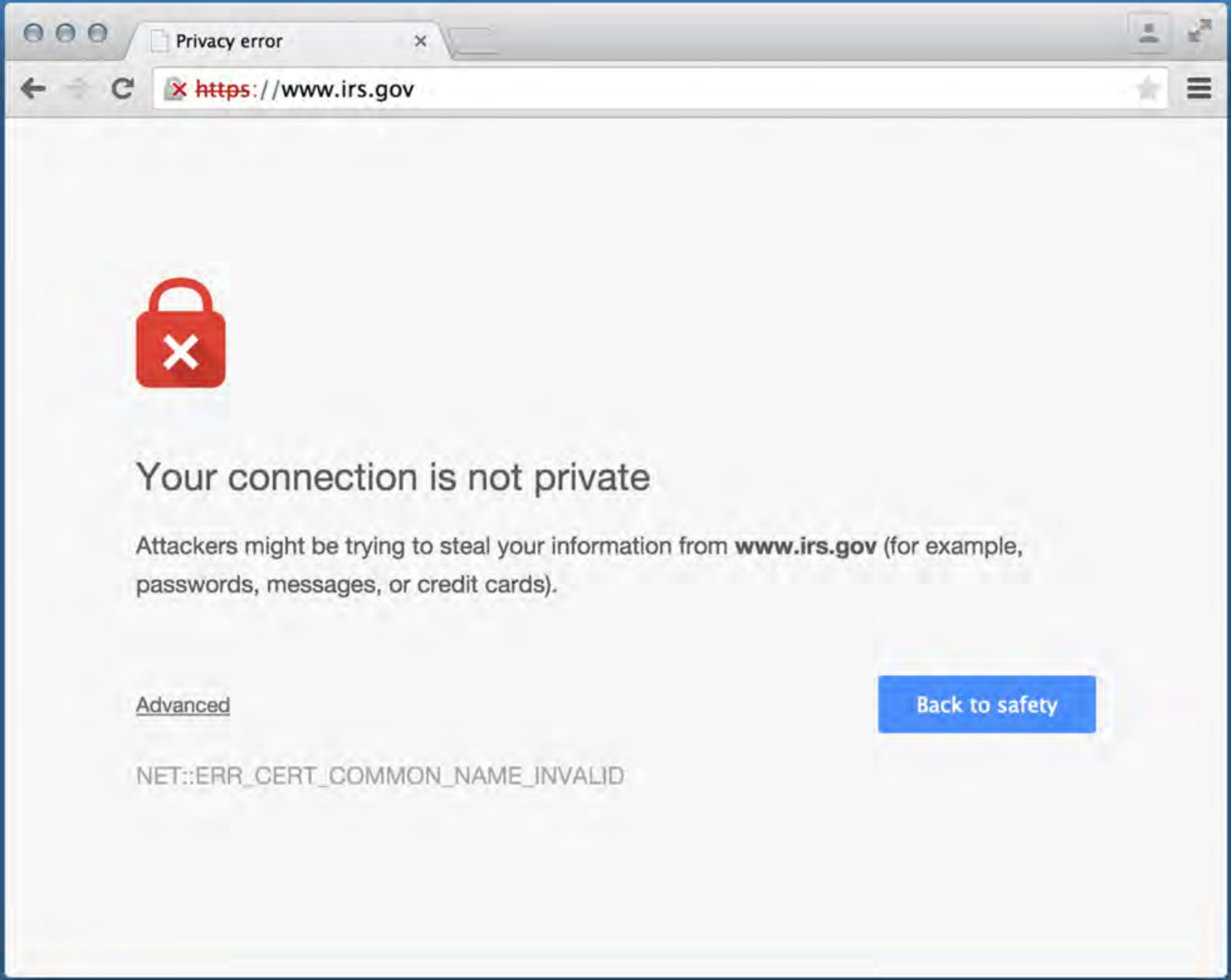
Improving SSL warnings

Adrienne Porter Felt
Chrome security team
felt@chromium.org



Your connection is not private

Attackers might be trying to steal your information from **www.irs.gov** (for example, passwords, messages, or credit cards).

NET::ERR_CERT_COMMON_NAME_INVALID

THE HOLY GRAIL

1. Warn only when under attack

THE HOLY GRAIL

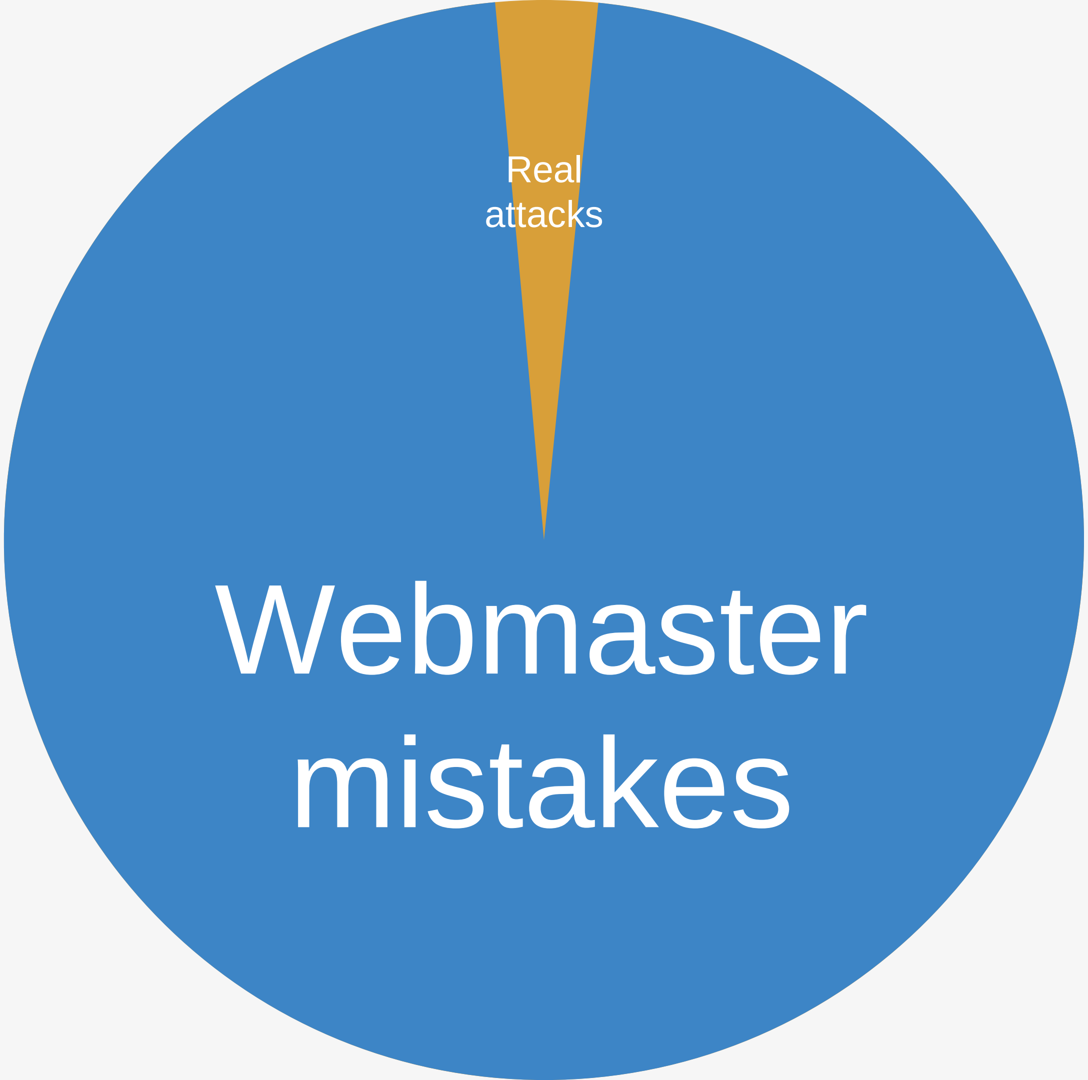
2. Users understand warnings

THE HOLY GRAIL

3. Users follow warning advice

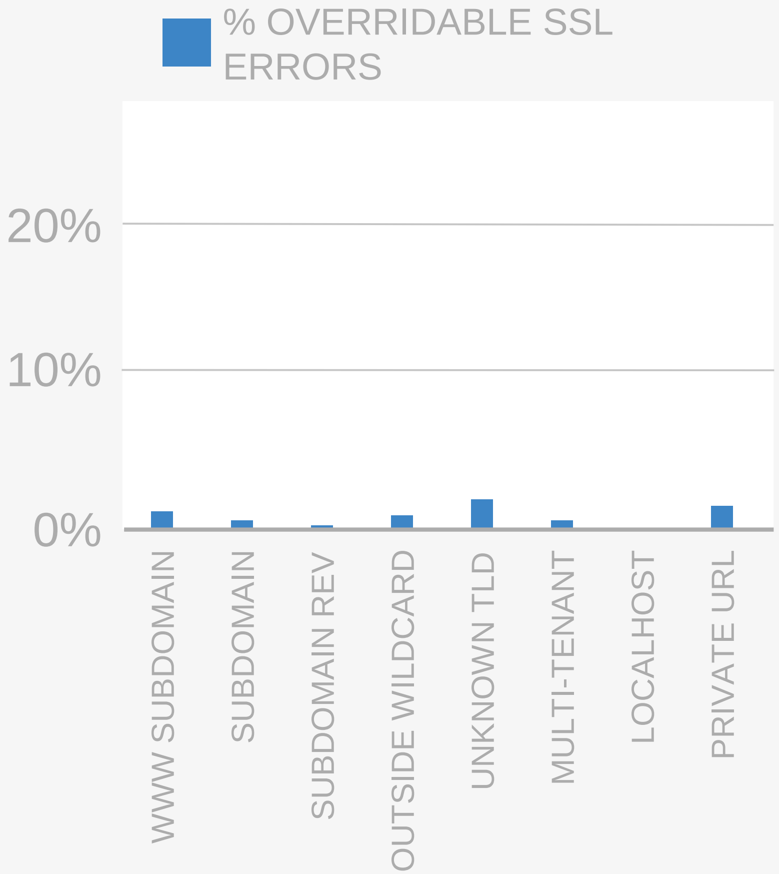
How can browsers stop crying wolf?

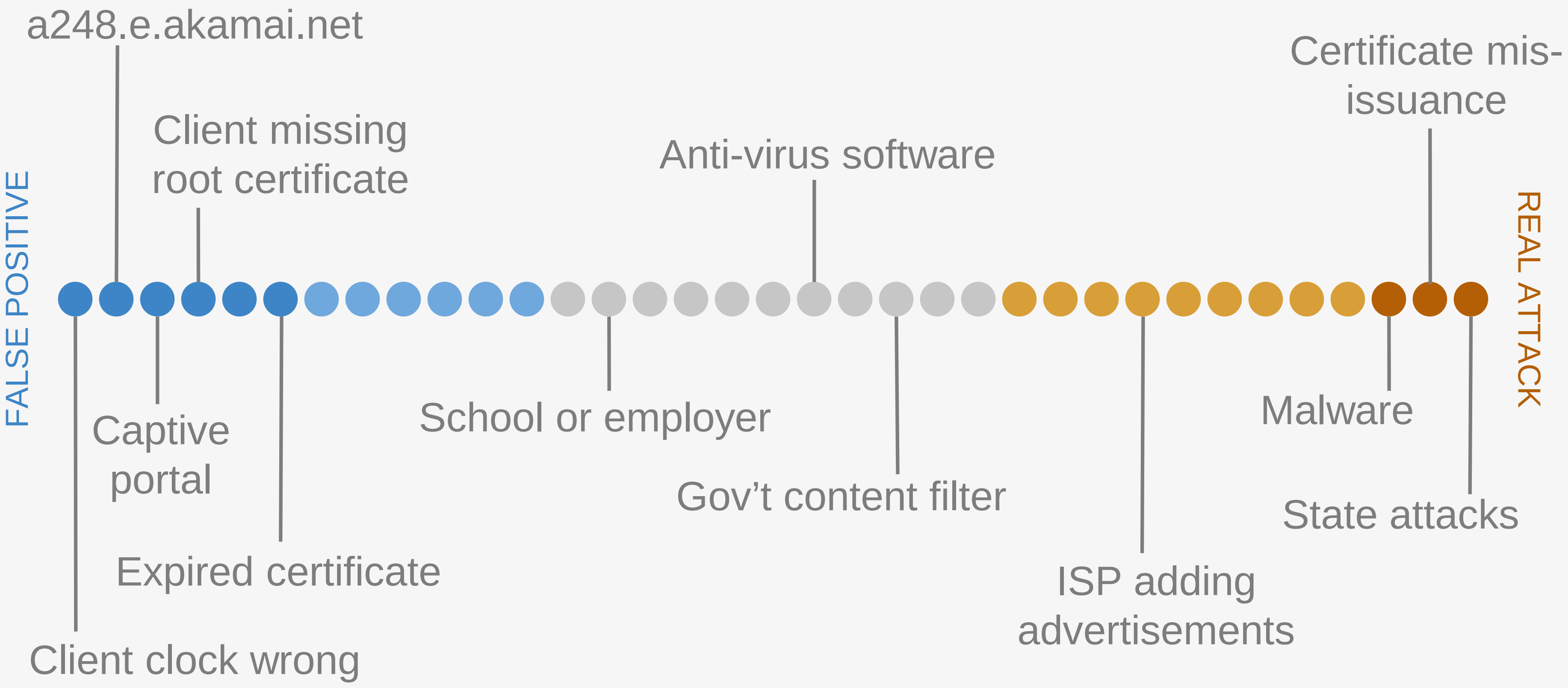
Photo credit: https://www.flickr.com/photos/tambako



HOW I IMAGINED ERRORS

DEVELOPER SSL ERRORS, MEASURED





FALSE POSITIVE

Client clock wrong

a248.e.akamai.net

Captive portal

Client missing root certificate

Expired certificate

School or employer

Anti-virus software

Gov’t content filter

ISP adding advertisements

Malware

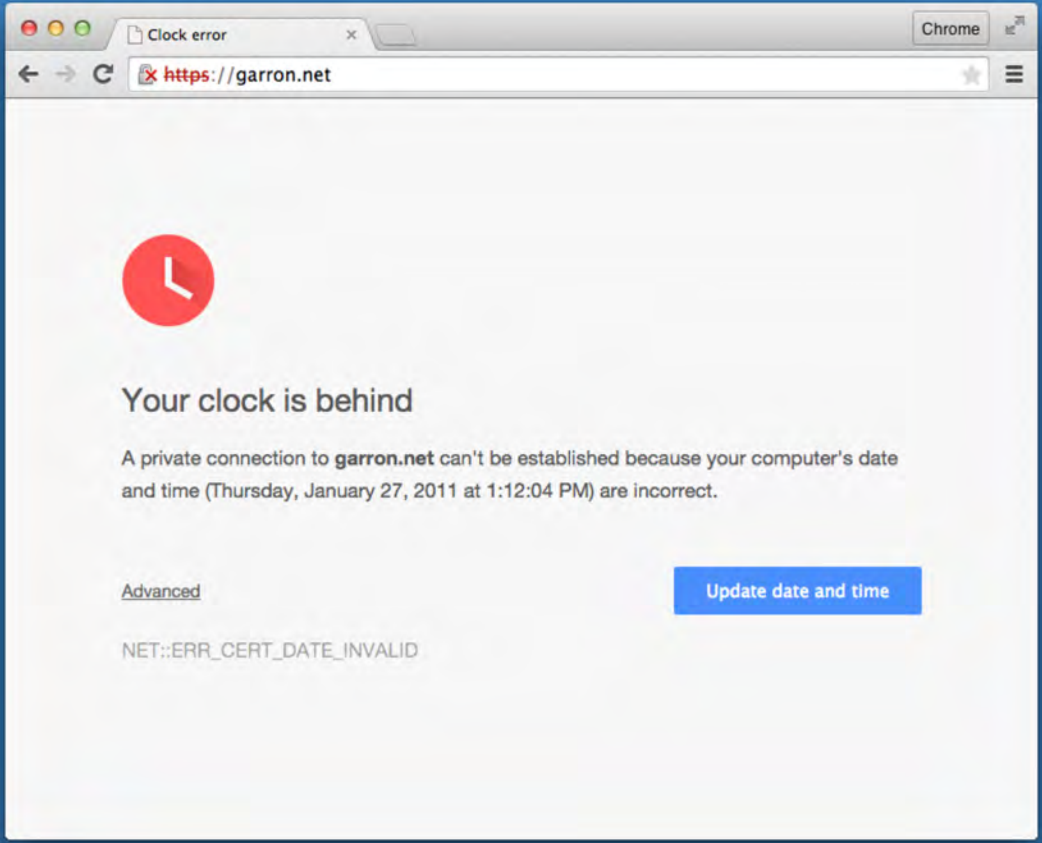
Certificate mis-issuance

State attacks

REAL ATTACK

Blame the clock

Wrong clocks cause **20%** of HSTS errors



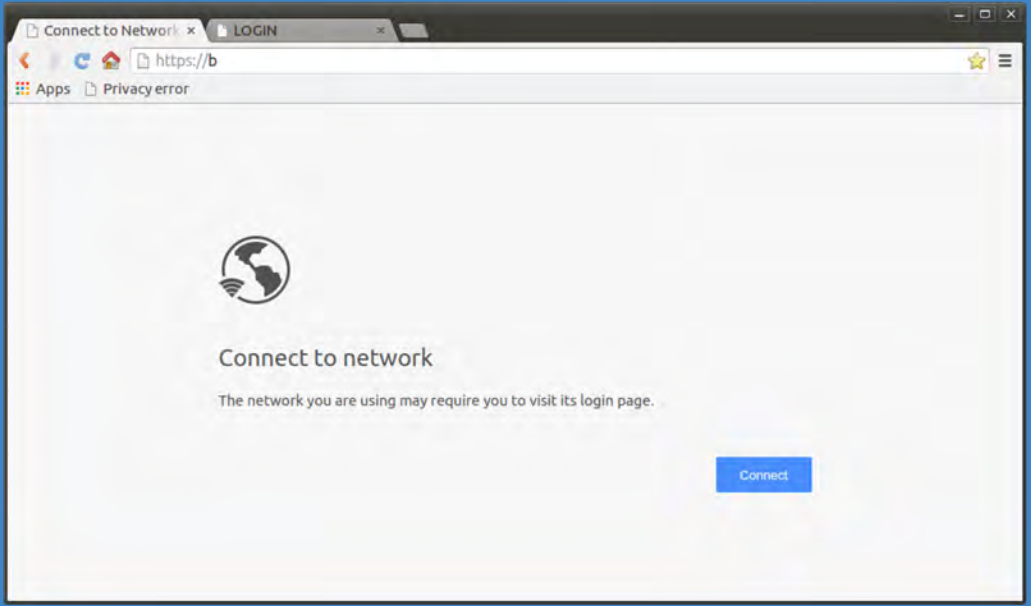
Your clock is behind

A private connection to **garron.net** can't be established because your computer's date and time (Thursday, January 27, 2011 at 1:12:04 PM) are incorrect.

NET::ERR_CERT_DATE_INVALID

Captive portals

4.5% of all errors caused by redirects

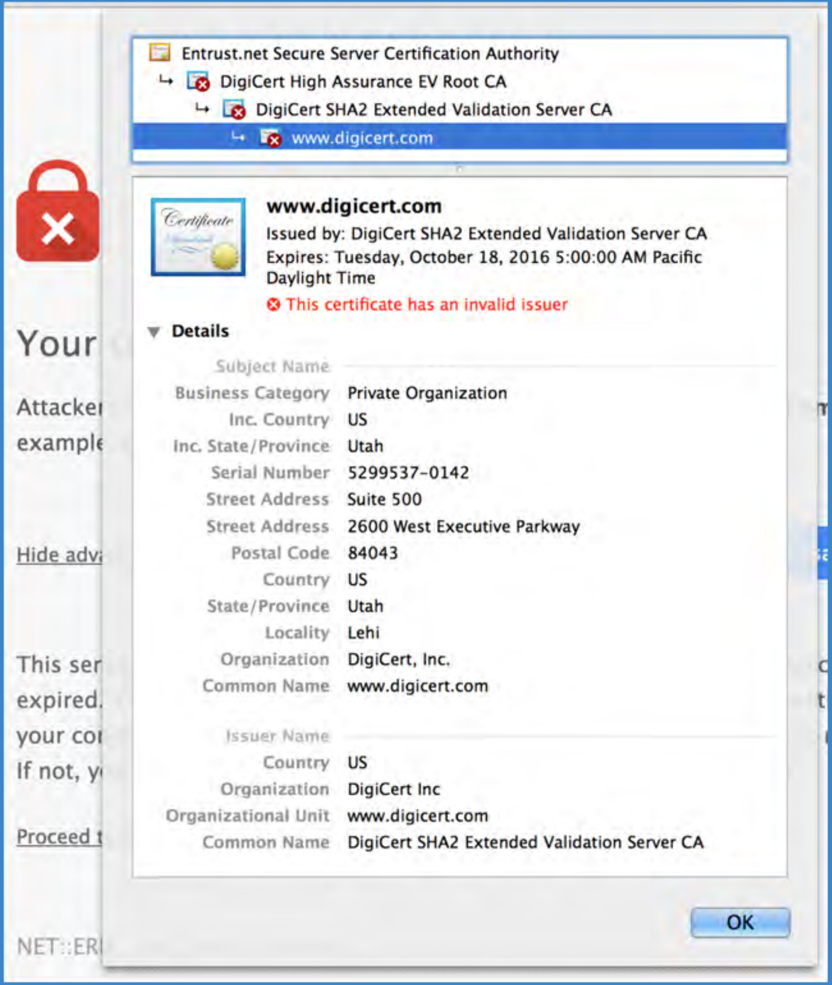


Connect to network

The network you are using may require you to visit its login page.

Wonky trust stores

Expired and missing certificates



Entrust.net Secure Server Certification Authority
↳ DigiCert High Assurance EV Root CA
↳ DigiCert SHA2 Extended Validation Server CA
↳ www.digicert.com

www.digicert.com

Issued by: DigiCert SHA2 Extended Validation Server CA

Expires: Tuesday, October 18, 2016 5:00:00 AM Pacific Daylight Time

⊗ This certificate has an invalid issuer

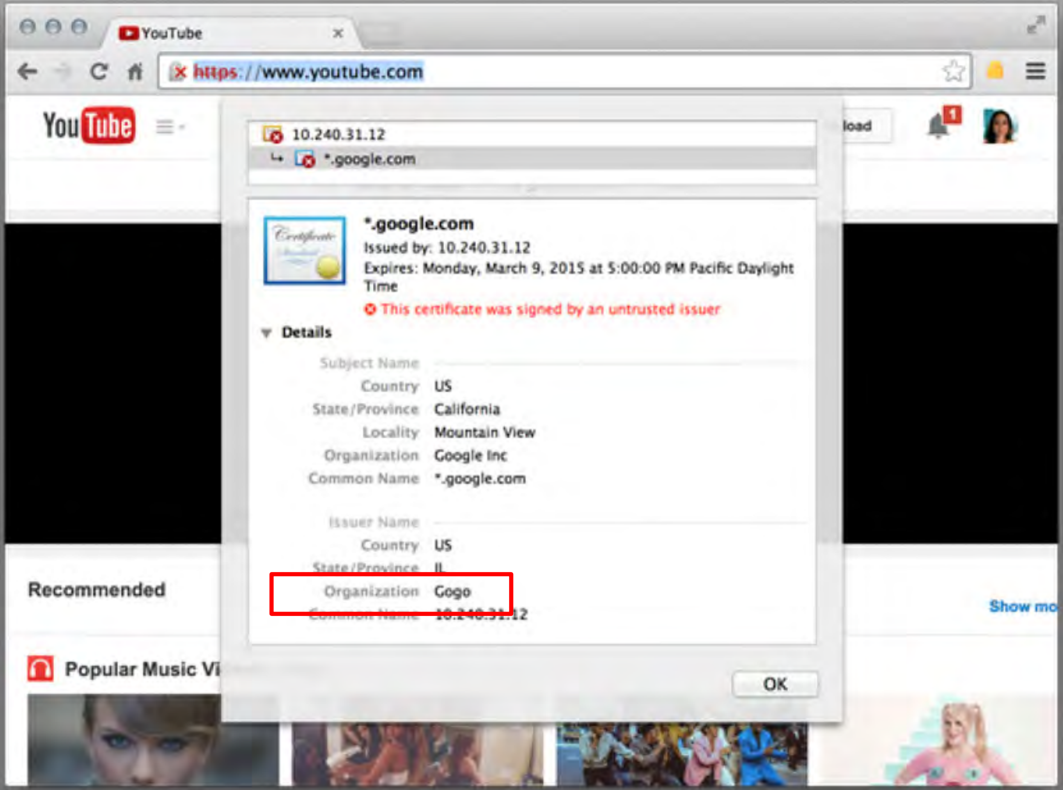
▼ **Details**

Subject Name	
Business Category	Private Organization
Inc. Country	US
Inc. State/Province	Utah
Serial Number	5299537-0142
Street Address	Suite 500
Street Address	2600 West Executive Parkway
Postal Code	84043
Country	US
State/Province	Utah
Locality	Lehi
Organization	DigiCert, Inc.
Common Name	www.digicert.com

Issuer Name	
Country	US
Organization	DigiCert Inc
Organizational Unit	www.digicert.com
Common Name	DigiCert SHA2 Extended Validation Server CA

Traffic shaping

Throttle or block expensive streaming



10.240.31.12

↳ *.google.com

***.google.com**

Issued by: 10.240.31.12

Expires: Monday, March 9, 2015 at 5:00:00 PM Pacific Daylight Time

This certificate was signed by an untrusted issuer

▼ **Details**

Subject Name

Country US

State/Province California

Locality Mountain View

Organization Google Inc

Common Name *.google.com

Issuer Name

Country US

State/Province IL

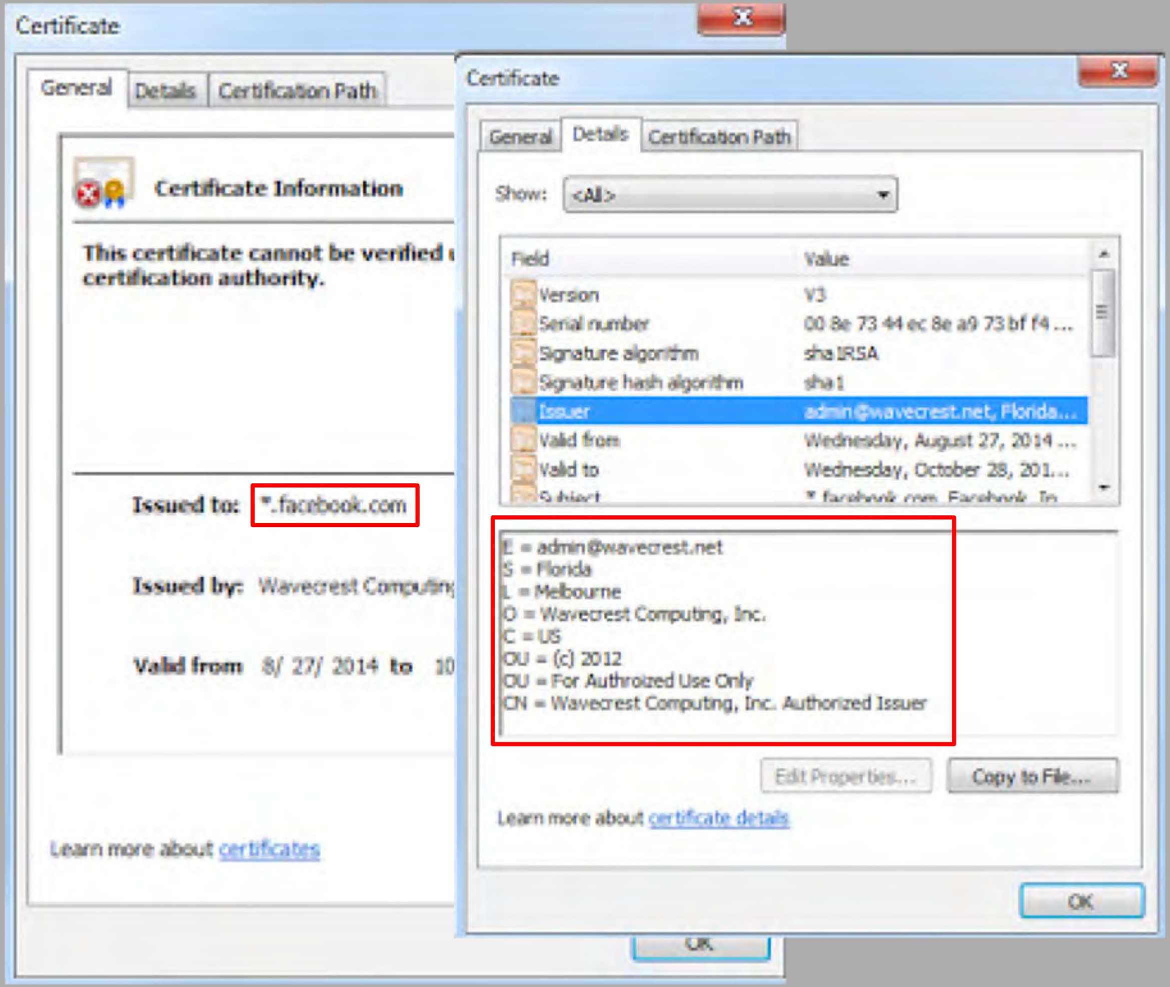
Organization Gogo

Common Name 10.240.31.12

OK

Schools & employers

Network admins want to filter content



This certificate cannot be verified u
certification authority.

Issued to: *.facebook.com

Issued by: Wavecrest Computing

Valid from 8/ 27/ 2014 to 10

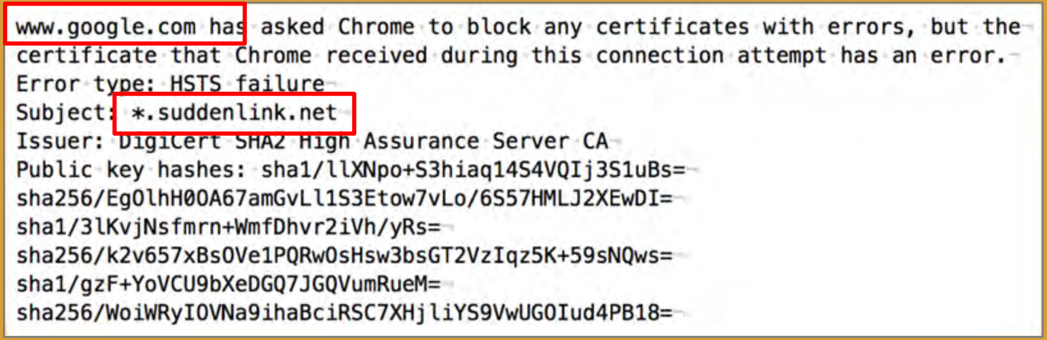
Show: <All>

Field	Value
Version	V3
Serial number	00 8e 73 44 ec 8e a9 73 bf f4 ...
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	admin@wavecrest.net, Florida...
Valid from	Wednesday, August 27, 2014 ...
Valid to	Wednesday, October 28, 201...
Subject	*.facebook.com, Facebook, In...

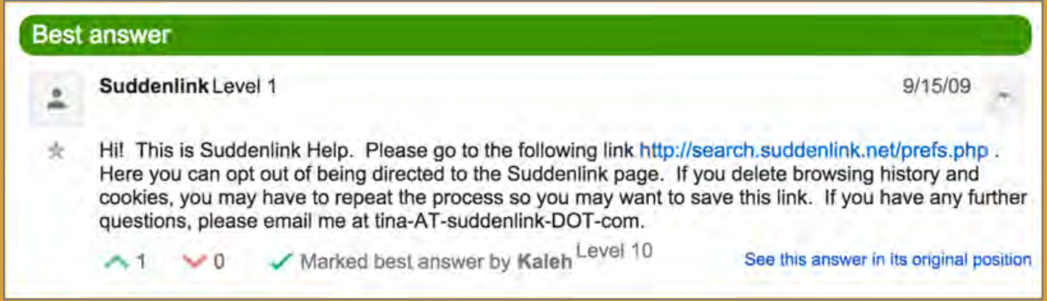
E = admin@wavecrest.net
S = Florida
L = Melbourne
O = Wavecrest Computing, Inc.
C = US
OU = (c) 2012
OU = For Authroized Use Only
CN = Wavecrest Computing, Inc. Authorized Issuer

Traffic is $$$$$

Monetizing traffic with ads, search, etc.



```
www.google.com has asked Chrome to block any certificates with errors, but the
certificate that Chrome received during this connection attempt has an error.
Error type: HSTS failure
Subject: *.suddenlink.net
Issuer: DigiCert SHA2 High Assurance Server CA
Public key hashes: sha1/llXNpo+S3hiaq14S4VQIj3S1uBs=
sha256/Eg0lhH00A67amGvLl1S3Etow7vLo/6S57HMLJ2XEwDI=
sha1/3lKvjNsfmrn+WmfDhvr2iVh/yRs=
sha256/k2v657xBsOVe1PQRwOsHsw3bsGT2VzIqz5K+59sNQws=
sha1/gzF+YoVCU9bXeDGQ7JGQVumRueM=
sha256/WoiWRyIOVNa9ihaBciRSC7XHjliYS9VwUGOIud4PB18=
```



Best answer

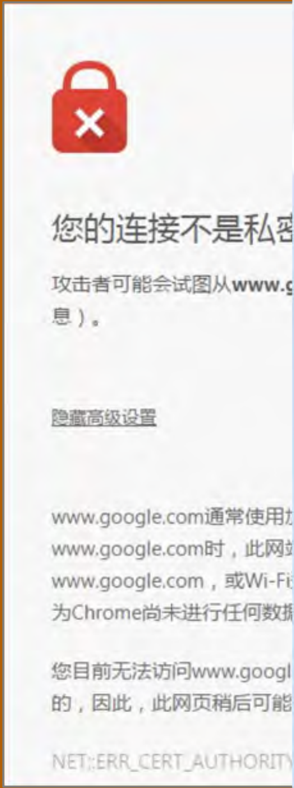
Suddenlink Level 1 9/15/09

Hi! This is Suddenlink Help. Please go to the following link http://search.suddenlink.net/prefs.php . Here you can opt out of being directed to the Suddenlink page. If you delete browsing history and cookies, you may have to repeat the process so you may want to save this link. If you have any further questions, please email me at tina-AT-suddenlink-DOT-com.

^ 1
∨ 0
✓ Marked best answer by Kaleh Level 10
See this answer in its original position

Clear-cut attack

More common than we think?



您的连接不是私

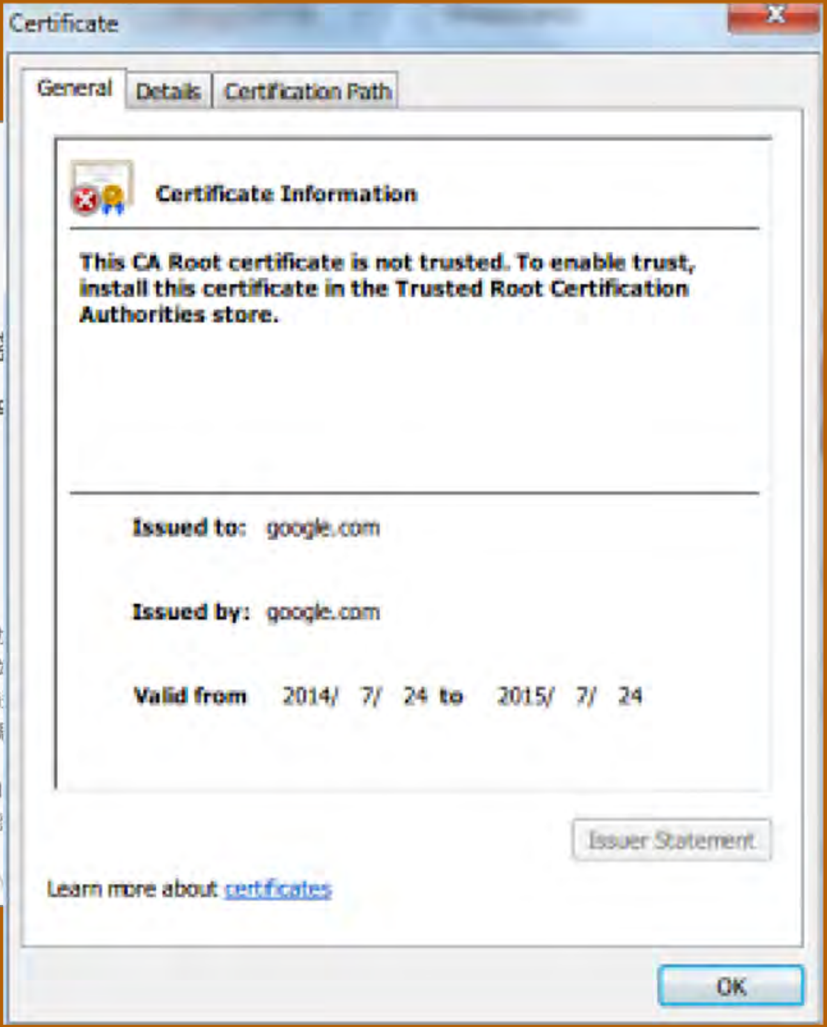
攻击者可能会试图从www.g
息）。

隐藏高级设置

www.google.com通常使用
www.google.com时，此网
www.google.com，或Wi-Fi
为Chrome尚未进行任何数据

您目前无法访问www.googl
的，因此，此网页稍后可能

NET::ERR_CERT_AUTHORITY



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: google.com

Issued by: google.com

Valid from 2014/ 7/ 24 **to** 2015/ 7/ 24

Learn more about certificates

define,

identify,

fix

How do we explain this to users?

Photo credit: https://www.flickr.com/photos/sandras_weeds

WHAT WE WANT TO CONVEY

Threat source: the attacker is on the network, not a malicious website

WHAT WE WANT TO CONVEY

Data risk: the data on foo.com is at risk (and no other data)

WHAT WE WANT TO CONVEY

False positives: be more concerned about errors on well-regarded sites

- Non-technical language
- Sixth grade reading level
- As brief as possible
- Specific about risk
- Enough information

“...the server presented a certificate issued by an entity that is not trusted by your computer’s operating system.”

> “The security certificate presented by this website was not issued by a trusted certificate authority.”

...security is
up to date on
your computer

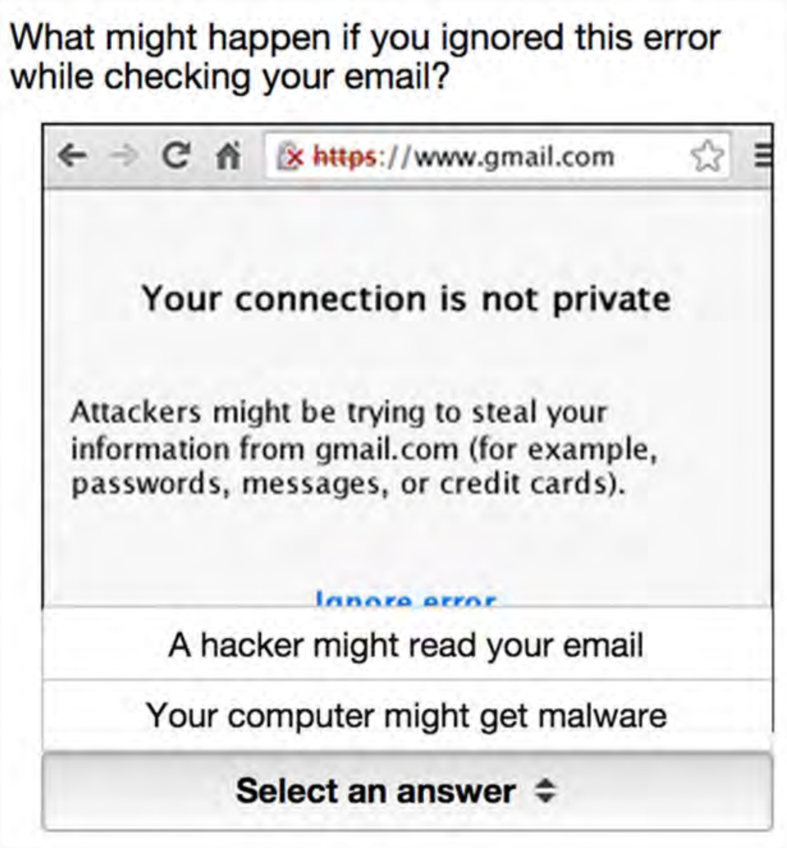
...security is up to date on your computer

I don’t know if my information is safe… I don’t know what encrypted means

Non-technical language	F
Sixth grade reading level	F
As brief as possible	B
Specific about risk	A
Enough information	A

“Your connection is not private. Attackers might be trying to steal your information from www.irs.gov (for example, passwords, messages, or credit cards).”

Non-technical language	A
Sixth grade reading level	A
As brief as possible	A
Specific about risk	C
Enough information	D



What might happen if you ignored this error while checking your email?

Your connection is not private

Attackers might be trying to steal your information from gmail.com (for example, passwords, messages, or credit cards).

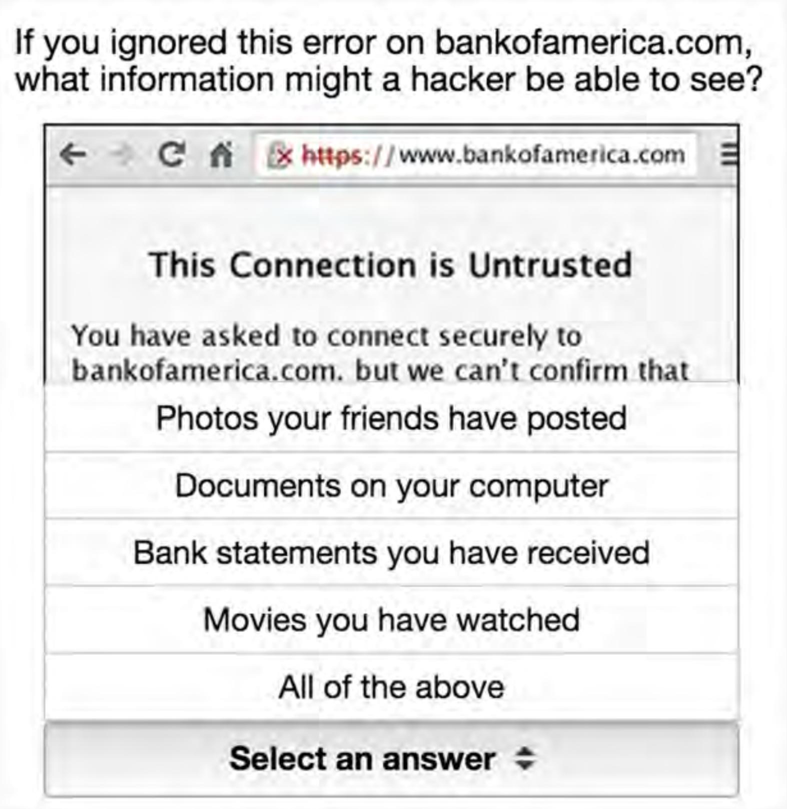
A hacker might read your email

Your computer might get malware

Select an answer

Threat source

	CORRECT
Chrome 37	49%
Chrome 36	38%
Safari	36%
Firefox	39%
IE	39%



If you ignored this error on bankofamerica.com, what information might a hacker be able to see?

https://www.bankofamerica.com

This Connection is Untrusted

You have asked to connect securely to bankofamerica.com. but we can't confirm that

Photos your friends have posted

Documents on your computer

Bank statements you have received

Movies you have watched

All of the above

Select an answer

Data risk

	BANK	ALL
Chrome 37	**18%**	65%
Chrome 36	**18%**	62%
Safari	**14%**	67%
Firefox	**20%**	69%
IE	**19%**	51%

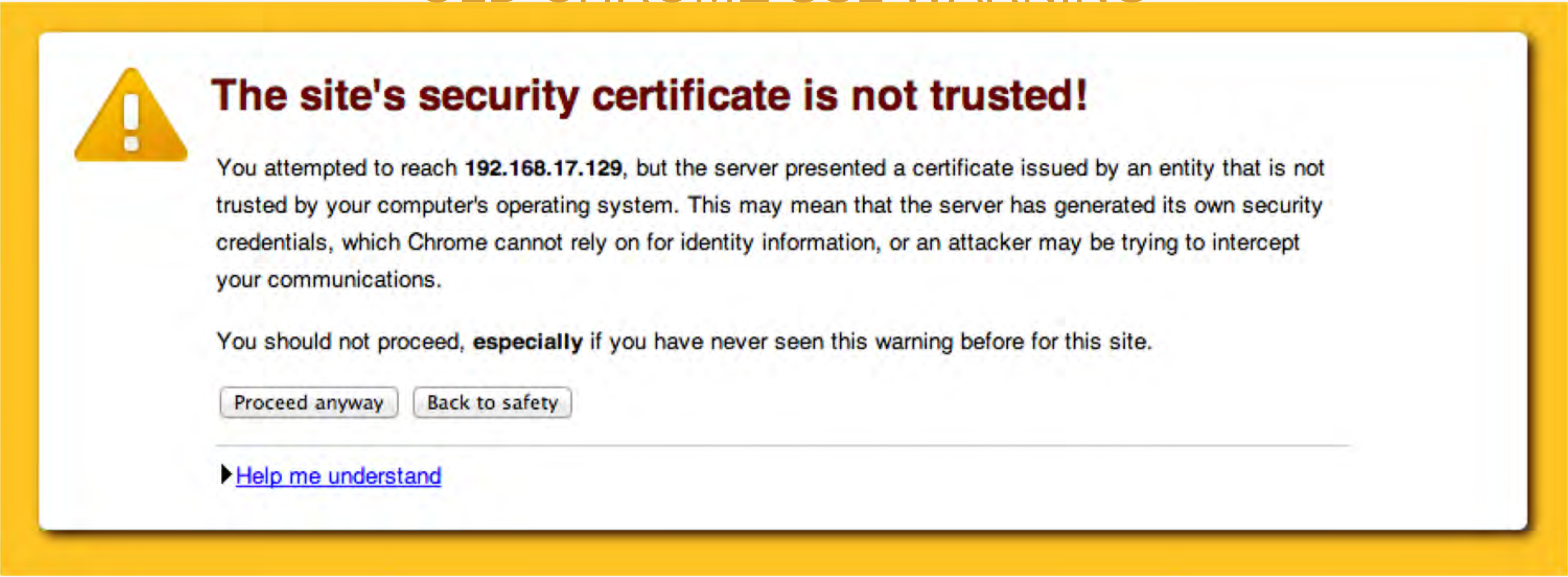
None succeed yet; how do we do better?

Can we nudge users to heed our advice?

Photo credit: https://www.flickr.com/photos/lara604/

- Clear instruction
- Attractive preferred choice
- Unattractive other choice

OLD CHROME SSL WARNING

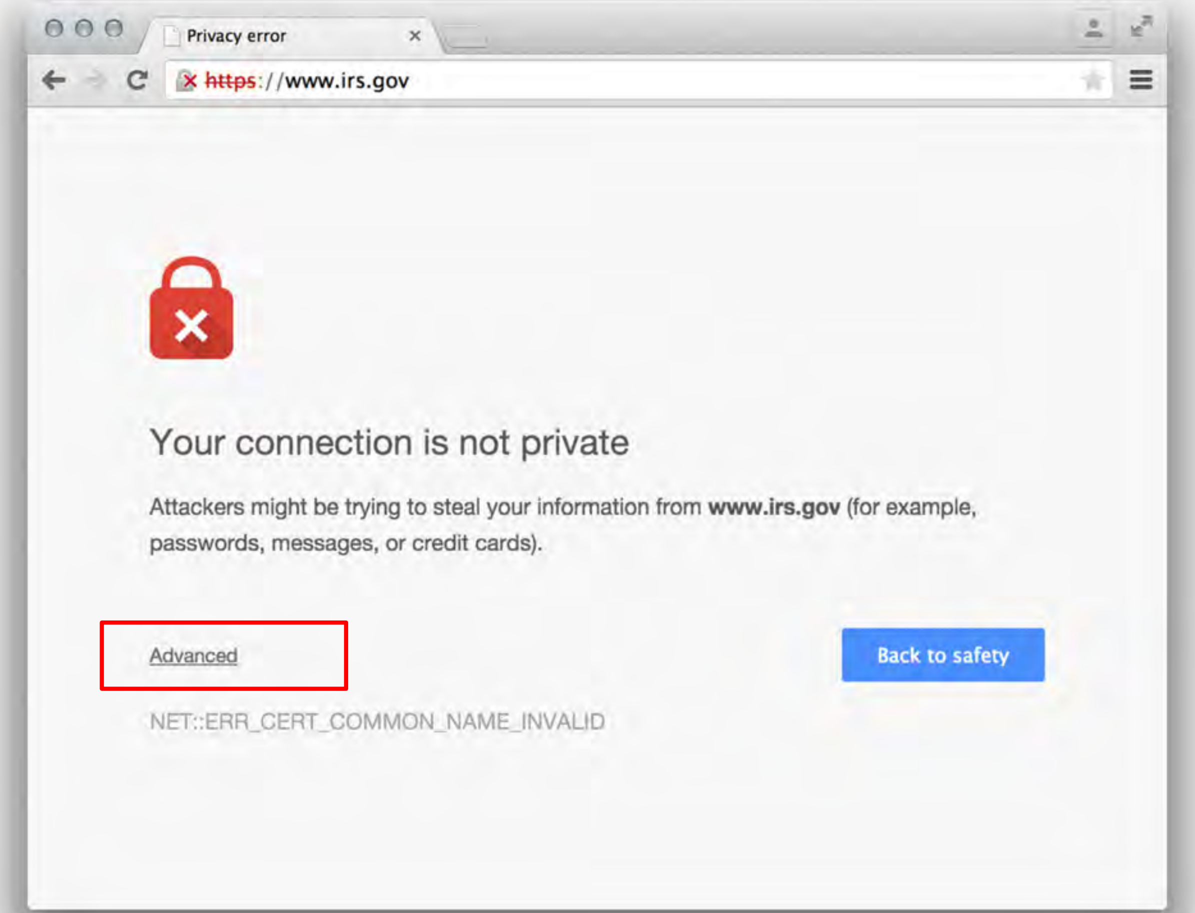


The site's security certificate is not trusted!

You attempted to reach **192.168.17.129**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications.

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

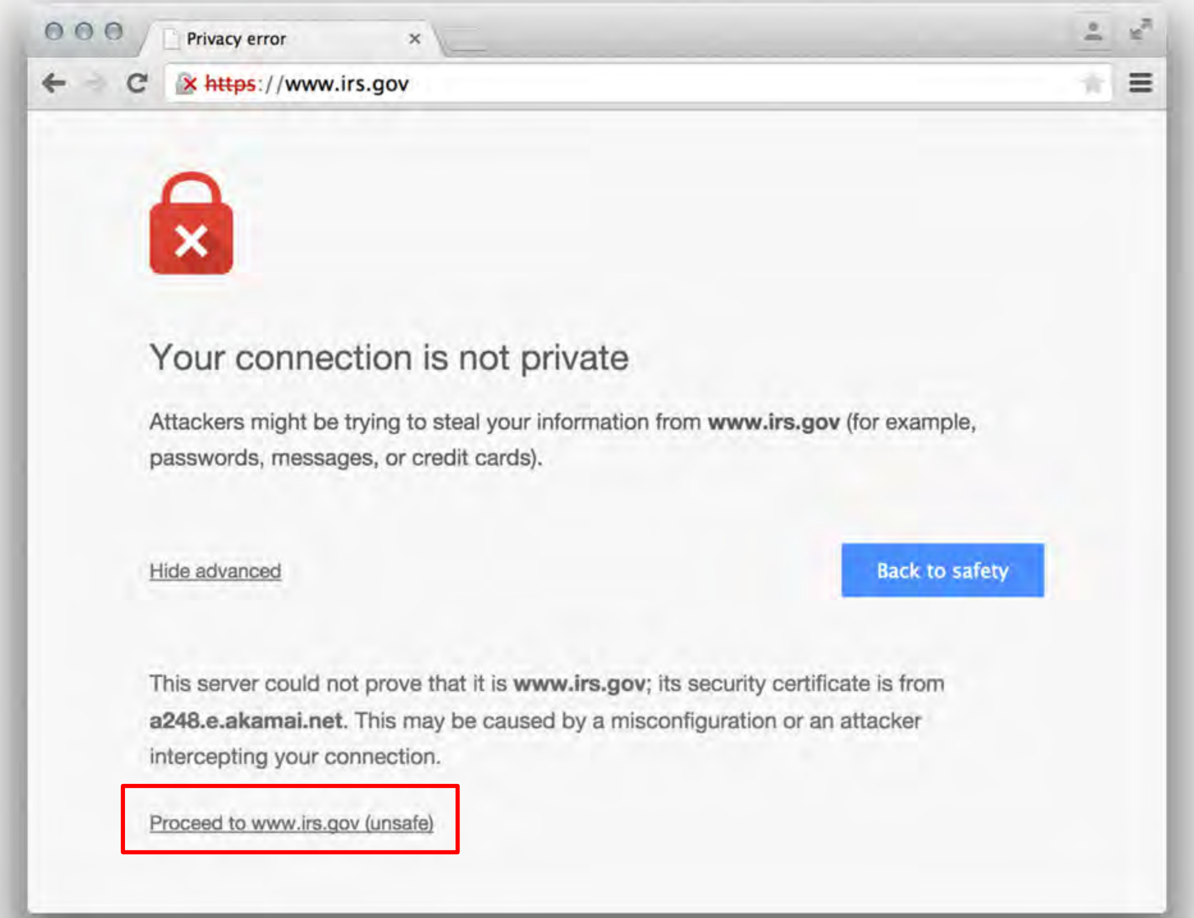
● Clear instruction	B
● Attractive preferred choice	F
● Unattractive other choice	F



Your connection is not private

Attackers might be trying to steal your information from **www.irs.gov** (for example, passwords, messages, or credit cards).

NET::ERR_CERT_COMMON_NAME_INVALID

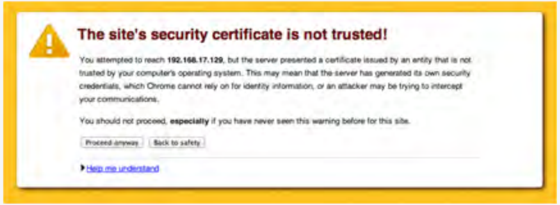


Your connection is not private

Attackers might be trying to steal your information from **www.irs.gov** (for example, passwords, messages, or credit cards).

This server could not prove that it is **www.irs.gov**; its security certificate is from **a248.e.akamai.net**. This may be caused by a misconfiguration or an attacker intercepting your connection.

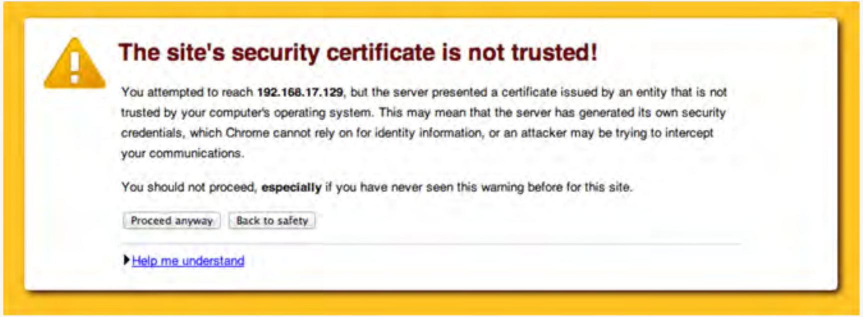
Clear instruction	C
Attractive preferred choice	A
Unattractive other choice	A



The site's security certificate is not trusted!

You attempted to reach **192.168.17.129**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications.

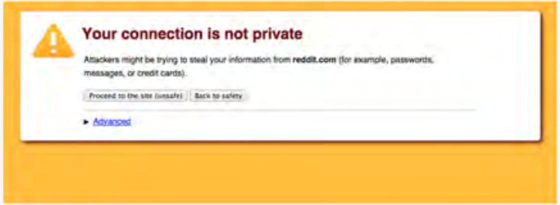
You should not proceed, **especially** if you have never seen this warning before for this site.



The site's security certificate is not trusted!

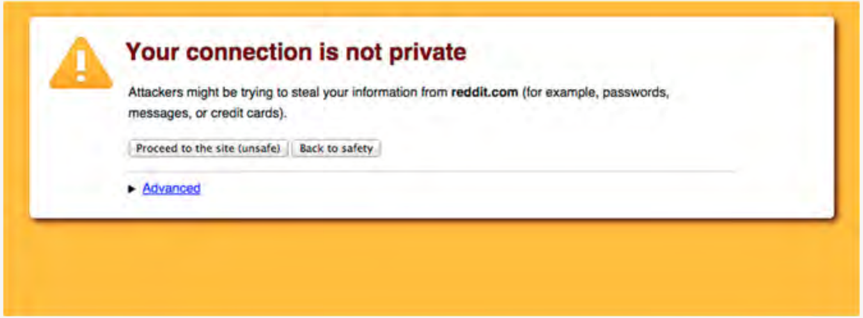
You attempted to reach **192.168.17.129**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications.

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



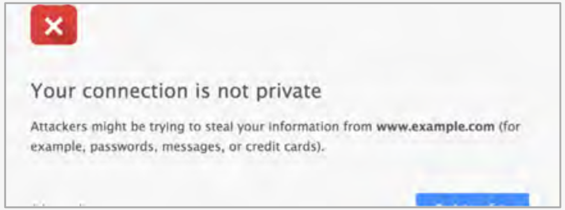
Your connection is not private

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



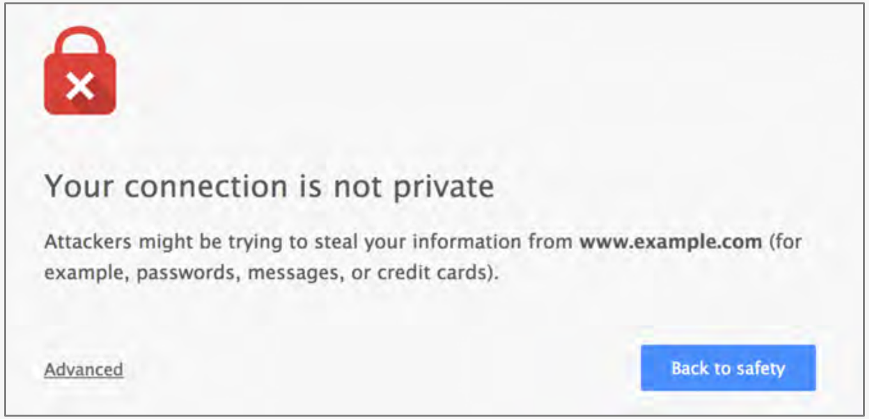
Your connection is not private

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



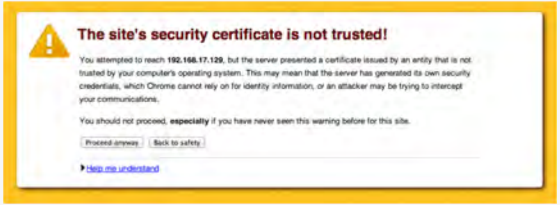
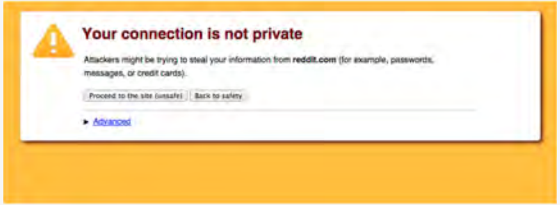
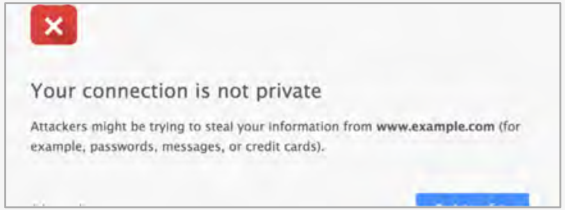
Your connection is not private

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



Your connection is not private

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

	ADHERENCE	N
 **The site's security certificate is not trusted!** You attempted to reach **192.168.17.129**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications. You should not proceed, **especially** if you have never seen this warning before for this site. Proceed anyway · Back to safety ▸ Help me understand	30.9%	4,551
 **Your connection is not private** Attackers might be trying to steal your information from **reddit.com** (for example, passwords, messages, or credit cards). Proceed to the site (unsafe) · Back to safety ▸ Advanced	32.1%	4,075
 Your connection is not private Attackers might be trying to steal your information from **www.example.com** (for example, passwords, messages, or credit cards).	**58.3%**	4,644

Opinionated design works where text fails

So in conclusion...

Photo credit: https://www.flickr.com/photos/sandras_weeds

TODO LIST

- Warn only when under attack
- Users understand warnings
- ~~Users follow warning advice~~

Adrienne Porter Felt
felt@chromium.org

In collaboration with...

Mustafa Acer
Alex Ainslie
Alan Bettes
Radhika Bharghava
Sunny Consolvo
Lucas Garron
Helen Harris
Elisabeth Morant
Chris Palmer
Robert W. Reeder
Ryan Sleevi
Parisa Tabriz
Somas Thyagaraja
Joel Weinberger