Your connection is not private

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

Advanced

Back to safety

NET::ERR_CERT_COMMON_NAME_INVALID
THE HOLY GRAIL

1. Warn only when under attack
2. Users understand warnings
3. Users follow warning advice
How can browsers stop crying wolf?
Webmaster mistakes

Real attacks

HOW I IMAGINED ERRORS
DEVELOPER SSL ERRORS, MEASURED
Client clock wrong
Client missing root certificate
Captive portal
Expired certificate
Anti-virus software
School or employer
Gov’t content filter
ISP adding advertisements
Malware
State attacks
Certificate misissuance
FALSE POSITIVE
REAL ATTACK
Blame the clock
Wrong clocks cause 20% of HSTS errors
Captive portals
4.5% of all errors caused by redirects
Wonky trust stores
Expired and missing certificates
Traffic shaping
Throttle or block expensive streaming
Schools & employers
Network admins want to filter content
Traffic is $$$$$

Monetizing traffic with ads, search, etc.
Clear-cut attack
More common than we think?
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
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
● Sixth grade reading level
● As brief as possible
● Specific about risk
● Enough information
**Threat source**

<table>
<thead>
<tr>
<th>Source</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chrome 37</td>
<td>49%</td>
</tr>
<tr>
<td>Chrome 36</td>
<td>38%</td>
</tr>
<tr>
<td>Safari</td>
<td>36%</td>
</tr>
<tr>
<td>Firefox</td>
<td>39%</td>
</tr>
<tr>
<td>IE</td>
<td>39%</td>
</tr>
</tbody>
</table>
If you ignored this error on bankofamerica.com, what information might a hacker be able to see?

<table>
<thead>
<tr>
<th>Browser</th>
<th>Bank</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chrome 37</td>
<td>18%</td>
<td>65%</td>
</tr>
<tr>
<td>Chrome 36</td>
<td>18%</td>
<td>62%</td>
</tr>
<tr>
<td>Safari</td>
<td>14%</td>
<td>67%</td>
</tr>
<tr>
<td>Firefox</td>
<td>20%</td>
<td>69%</td>
</tr>
<tr>
<td>IE</td>
<td>19%</td>
<td>51%</td>
</tr>
</tbody>
</table>
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
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.

[button] Proceed anyway  [button] Back to safety
● Clear instruction  
● Attractive preferred choice  
● Unattractive other choice
Your connection is not private

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

Advanced
Back to safety

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).

Hide advanced

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.

Proceed to www.irs.gov (unsafe)
● 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.

Proceed anyway  Back to safety

Help me understand
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 site (unsafely)  Back to safety

Advanced
Your connection is not private

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

Advanced

Back to safety
<table>
<thead>
<tr>
<th>Adherence</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>30.9%</td>
<td>4,551</td>
</tr>
<tr>
<td>32.1%</td>
<td>4,075</td>
</tr>
<tr>
<td>58.3%</td>
<td>4,644</td>
</tr>
</tbody>
</table>
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        Elisabeth Morant
Alex Ainslie        Chris Palmer
Alan Bettes         Robert W. Reeder
Radhika Bharghava   Ryan Sleevi
Sunny Consolvo      Parisa Tabriz
Lucas Garron        Somas Thyagaraja
Helen Harris         Joel Weinberger