Reinforcing bad behaviour: the misuse of security indicators on popular websites

Douglas Stebila
stebila@qut.edu.au

OZCHI 2010 – November 25, 2010
How can users tell when a website is secure?

“secure” = “safe to enter personal information”
Facebook helps you connect and share with the people in your life.

Sign Up
It's free, and always will be.

First Name: 
Last Name: 
Your Email: 
Re-enter Email: 
New Password: 
I am: Select Sex: 
Birthday: Month: Day: Year: 

Sign Up

Create a Page for a celebrity, band or business.
PayPal

Search PayPal
Search

- Sign Up
- Log In
- Help
- Safety Advice

Skip to main content

- Home
- Individuals
- Business
- Products & Services

Secure Log In

**Member Login**

**Account login**

Member Login

Email address: 
PayPal password: 
Go to My account

Log In
What criteria do people use to decide if a website is secure?

Consider criteria identified by Whalen and Inkpen through eye-tracking and subject interviews.

---

Criteria people use to decide if a website is secure

“type of site” – 88%
Criteria people use to decide if a website is secure

“lock or key icon” – 75%

D. Stebila » Reinforcing bad behaviour: the misuse of security indicators on popular websites
Criteria people use to decide if a website is secure

“type of information” – 69%
Criteria people use to decide if a website is secure

“site statements” – 50%

Reinforcing bad behaviour: the misuse of security indicators on popular websites
Criteria people use to decide if a website is secure

“https” – 50%

D. Stebila » Reinforcing bad behaviour: the misuse of security indicators on popular websites
Criteria people use to decide if a website is secure

“certificate” – 19%
Criteria people use to decide if a website is secure

“certificate” – 19%
What criteria should people use to decide if a website is secure?

Narrow focus from a cryptographer’s perspective:

- What criteria accurately convey the known security properties of the connection?
  - Use of the SSL / HTTPS protocol which encrypts all data and gives server-to-client authentication.
We can’t trust anything provided by the server.
We can’t trust anything provided by the server
Security indicators

Security indicator: “https” in location bar

![PayPal login page with HTTPS indicated](image-url)
Security indicators

Security indicator: lock icon in browser chrome

Reinforcing bad behaviour: the misuse of security indicators on popular websites
Security indicators

D. Stebila » Reinforcing bad behaviour: the misuse of security indicators on popular websites
Security indicator: lock icon in browser chrome

D. Stebila » Reinforcing bad behaviour: the misuse of security indicators on popular websites
Security indicator: domain name correct

Security indicators

D. Stebila » Reinforcing bad behaviour: the misuse of security indicators on popular websites
Security indicators

Security indicator: extended validation certificate

Reinforcing bad behaviour: the misuse of security indicators on popular websites
Facebook helps you connect and share with the people in your life.

Sign Up
It's free, and always will be.

First Name:

Last Name:

Your Email:

Re-enter Email:

New Password:

I am: Select Sex:

Birthday: Month: Day: Year:

Why do I need to provide this?

Sign Up

Create a Page for a celebrity, band or business.
Criteria people use vs. security indicators

Criteria people use:
- “type of site” – 88%
- “lock or key icon” – 75%
- “type of information” – 69%
- “site statements” – 50%
- “https” – 44%
- “certificate” – 19%

Security indicators:
- https in location bar
- lock icon in browser chrome
- domain name correct
- extended validation certificate
To what extent are security criteria and indicators misused on websites?

Widespread misuse of security criteria and indicators suggests users will become habituated to making bad security decisions.
Methodology

- Identified security criteria and indicators from previous studies and expert analysis.
- Assembled list of 125 popular websites:
  - top 100 sites by traffic (as ranked by Alexa Topsites)
  - top banks in USA, UK, Canada, Australia
  - top 4 webmail services (Yahoo!, Hotmail, Gmail, AOL)
- Visited the website by typing in the domain name (hotmail.com).
- Checked for presence/absence of security criteria/indicators.
Study goals, methodology, and results

Misused indicator: login protocol vs. form protocol
Misused indicator: login protocol vs. form protocol

D. Stebila » Reinforcing bad behaviour: the misuse of security indicators on popular websites
## Misused indicator: login protocol vs. form protocol

<table>
<thead>
<tr>
<th>Login page</th>
<th>Form submission</th>
<th>Percentage</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>HTTP</td>
<td>45%</td>
<td>*</td>
</tr>
<tr>
<td>HTTPS</td>
<td>HTTPS</td>
<td>10%</td>
<td>✗</td>
</tr>
<tr>
<td>HTTPS w/EV cert.</td>
<td>HTTPS w/EV cert.</td>
<td>5%</td>
<td>✗</td>
</tr>
<tr>
<td>HTTPS</td>
<td>HTTPS</td>
<td>32%</td>
<td>✓</td>
</tr>
<tr>
<td>HTTPS w/EV cert.</td>
<td>HTTPS w/EV cert.</td>
<td>8%</td>
<td>✓</td>
</tr>
</tbody>
</table>

* HTTP form submission provides no protection whatsoever for usernames or passwords.
Misused indicator: lock icon on page or as favicon
study goals, methodology, and results

misused indicator: lock icon on page or as favicon

D. Stebila » Reinforcing bad behaviour: the misuse of security indicators on popular websites
Study goals, methodology, and results

Misused indicator: lock icon on page or as favicon

D. Stebila » Reinforcing bad behaviour: the misuse of security indicators on popular websites
Misused indicator: lock icon on page or as favicon

- lock icon on HTTP pages 5% × ×
- lock icon on HTTPS pages 15% ×
- banks with lock icon on HTTPS pages 70% ×
- lock icon as favicon 2% × ×
Misused indicator: mismatched domain name
Study goals, methodology, and results

**Misused indicator: mismatched domain name**

D. Stebila » Reinforcing bad behaviour: the misuse of security indicators on popular websites
Misused indicator: mismatched domain name
Misused indicator: mismatched domain name

Is secure.partyaccount.com the right domain name to login to partypoker.com?

- Apparently, yes.
Misused indicator: mismatched domain name

What about partypoker-account.com?
Misused indicator: mismatched domain name

What about partypoker-account.com?

- Definitely not! I could buy this domain name right now.
Misused indicator: mismatched domain name
### Misused indicator: mismatched domain name

<table>
<thead>
<tr>
<th>Match?</th>
<th>Example typed domain → login domain</th>
<th>Matches?</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exact match</td>
<td>google.com → <a href="http://www.google.com">www.google.com</a></td>
<td>✓</td>
<td>57%</td>
</tr>
<tr>
<td>Close match</td>
<td>yahoo.com → login.yahoo.com</td>
<td></td>
<td>30%</td>
</tr>
<tr>
<td>No match</td>
<td>hotmail.com → login.live.com</td>
<td>×</td>
<td>13%</td>
</tr>
</tbody>
</table>
Study goals, methodology, and results

**Misused indicator: complicated URL**

- Complicated URL makes checking domain name harder
- “URL as UI”\(^2\)

<table>
<thead>
<tr>
<th>Complexity</th>
<th>Example</th>
<th>Avg. Len.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain only</td>
<td><a href="https://www.chase.com/">https://www.chase.com/</a></td>
<td>21.9</td>
</tr>
<tr>
<td>One path</td>
<td><a href="https://www.blogger.com/start">https://www.blogger.com/start</a></td>
<td>32.9</td>
</tr>
<tr>
<td>More than one path component</td>
<td><a href="https://www.google.com/accounts/ServiceLogin?uilel=3&amp;service=youtube&amp;passive=true&amp;continue=http%3A%2F%2Fwww.youtube.com%2Fsigin%3Faction_handle_signin%3Dtrue%26nomobil">https://www.google.com/accounts/ServiceLogin?uilel=3&amp;service=youtube&amp;passive=true&amp;continue=http%3A%2F%2Fwww.youtube.com%2Fsigin%3Faction_handle_signin%3Dtrue%26nomobil</a> etemp%3D1%26hl%3Den_US%26next%3D%252F&amp;hl=en_US&amp;tmpl=sso</td>
<td>110.1</td>
</tr>
</tbody>
</table>


D. Stebila » Reinforcing bad behaviour: the misuse of security indicators on popular websites
Summary of results

<table>
<thead>
<tr>
<th>Misused security indicators</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP login page with HTTPS form submission</td>
<td>15%</td>
</tr>
<tr>
<td>Lock icon on page or as favicon</td>
<td>23%</td>
</tr>
<tr>
<td>Hidden location bar</td>
<td>2%</td>
</tr>
<tr>
<td>Mismatched domain name</td>
<td>13%</td>
</tr>
<tr>
<td>Very complicated URL</td>
<td>42%</td>
</tr>
</tbody>
</table>

“Of the 125 sites we evaluated, only 5 avoided all misleading security indicators. Hence, a typical user will, much more often than not, be asked to make security decisions against best-practice recommendations on security indicators.”
Design recommendations

- Deliver the page containing the login form over HTTPS.
- Don’t try to hide the location bar.
- Ensure the domain name of the login page matches the domain name of the site in question.
- Don’t use lock icons anywhere in the web page content.
- Try to use simple URLs, especially for the login page.
To improve security, we need...

- better user education.
  - Security indicators to look for
  - 
  - better web designer/programmer education.
  - 

- better web browser design (and evaluation of those designs!).
- stronger / simpler error messages.
- more / simpler / different security messages.
- better web security technologies.
  - single sign-on (with browser support?).
  - cryptographically strong password-based mutual authentication.

D. Stebila » Reinforcing bad behaviour: the misuse of security indicators on popular websites
To improve security, we need...

- ... better user education.
  - Security indicators to look for

- ... better web designer/programmer education.
  - Design recommendations to follow
To improve security, we need...

- better user education.
  - Security indicators to look for

- better web designer/programmer education.
  - Design recommendations to follow

- better web browser design (and evaluation of those designs!).
  - Stronger / simpler error messages.
  - More / simpler / different security messages.
To improve security, we need...

- ... better user education.
  - Security indicators to look for

- ... better web designer/programmer education.
  - Design recommendations to follow

- ... better web browser design (and evaluation of those designs!).
  - Stronger / simpler error messages.
  - More / simpler / different security messages.

- ... better web security technologies.
  - Single sign-on (with browser support?).
  - Cryptographically strong password-based mutual authentication.
Reinforcing bad behaviour: the misuse of security indicators on popular websites

Douglas Stebila
stebila@qut.edu.au

Misused security indicators

<table>
<thead>
<tr>
<th>Misused Indicator</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP login page with HTTPS form submission</td>
<td>15%</td>
</tr>
<tr>
<td>Lock icon on page or as favicon</td>
<td>23%</td>
</tr>
<tr>
<td>Hidden location bar</td>
<td>2%</td>
</tr>
<tr>
<td>Mismatched domain name</td>
<td>13%</td>
</tr>
<tr>
<td>Very complicated URL</td>
<td>42%</td>
</tr>
</tbody>
</table>

Of the 125 sites we evaluated, only 5 avoided all misleading security indicators. Hence, a typical user will, much more often than not, be asked to make security decisions against best-practice recommendations on security indicators.