

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

**Douglas Stebila**

stebila@qut.edu.au



Indiana University – April 26, 2011

## How can users tell when a website is secure?

“secure” = “safe to enter personal information”

facebook

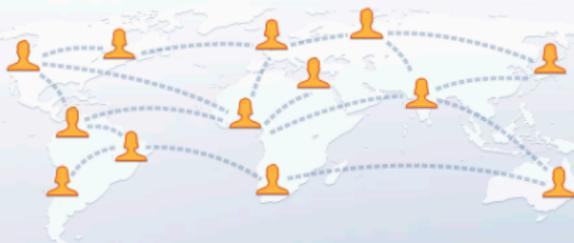
Email

Password

Login

 Keep me logged in[Forgot your password?](#)

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:

Birthday:



[Why do I need to provide this?](#)

Sign Up

[Create a Page](#) for a celebrity, band or business.
[English \(US\)](#)
[Español](#)
[Português \(Brasil\)](#)
[Français \(France\)](#)
[Deutsch](#)
[Italiano](#)
[العربية](#)
[हिन्दी](#)
[中文\(简体\)](#)
[日本語](#)

# PayPal

Search PayPal

Search

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

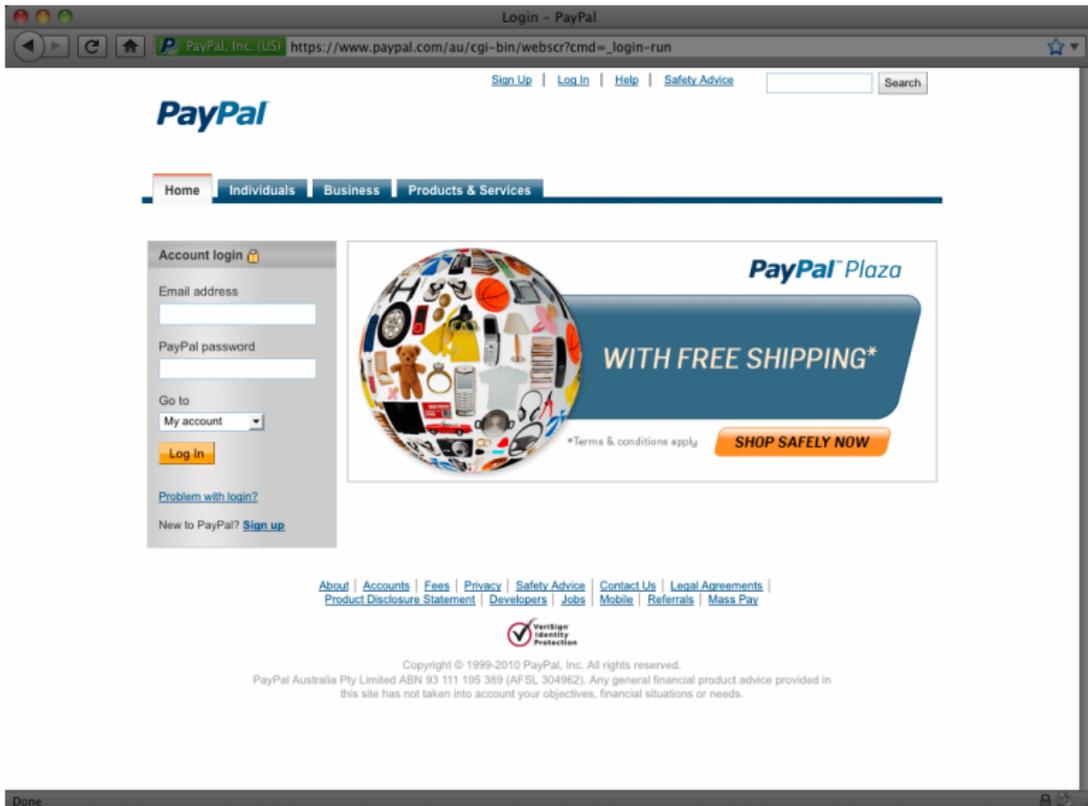
## What criteria do people use to decide if a website is secure?

Consider criteria identified by Whalen and Inkpen<sup>1</sup> through eye-tracking and subject interviews.

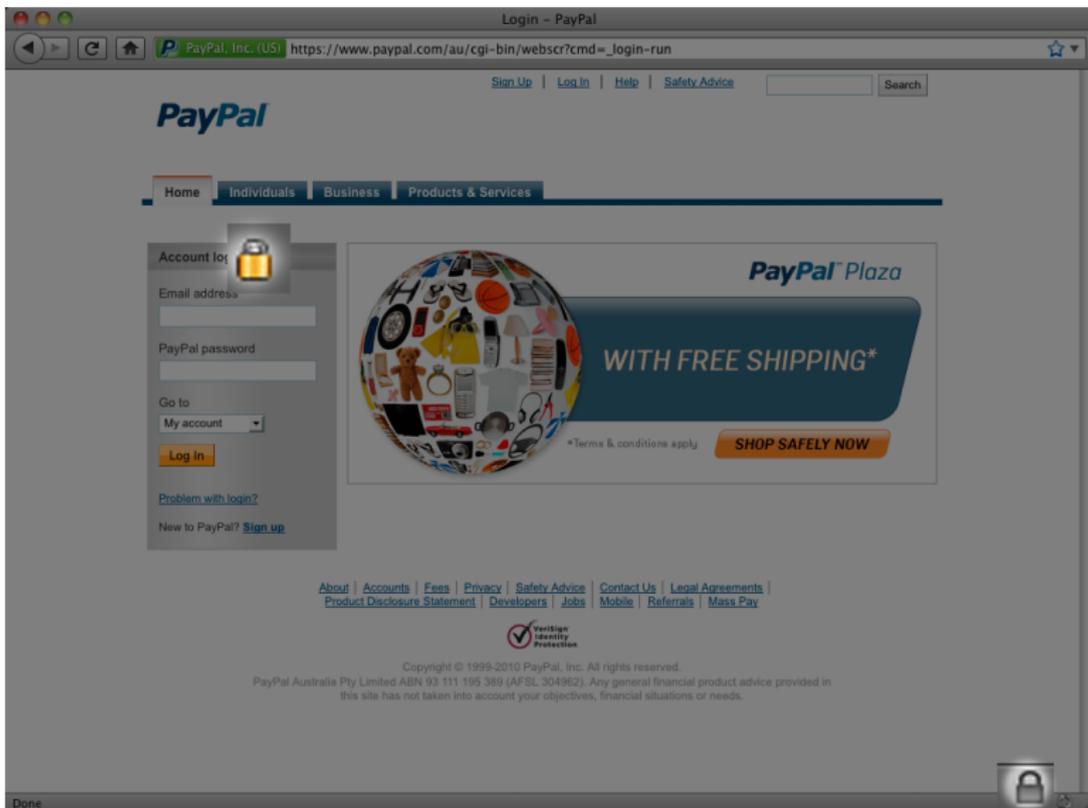
---

<sup>1</sup>Whalen, Inkpen. Gathering evidence: use of visual security cues in web browsers. *Graphics Interface*, 112:137-144 (2005)

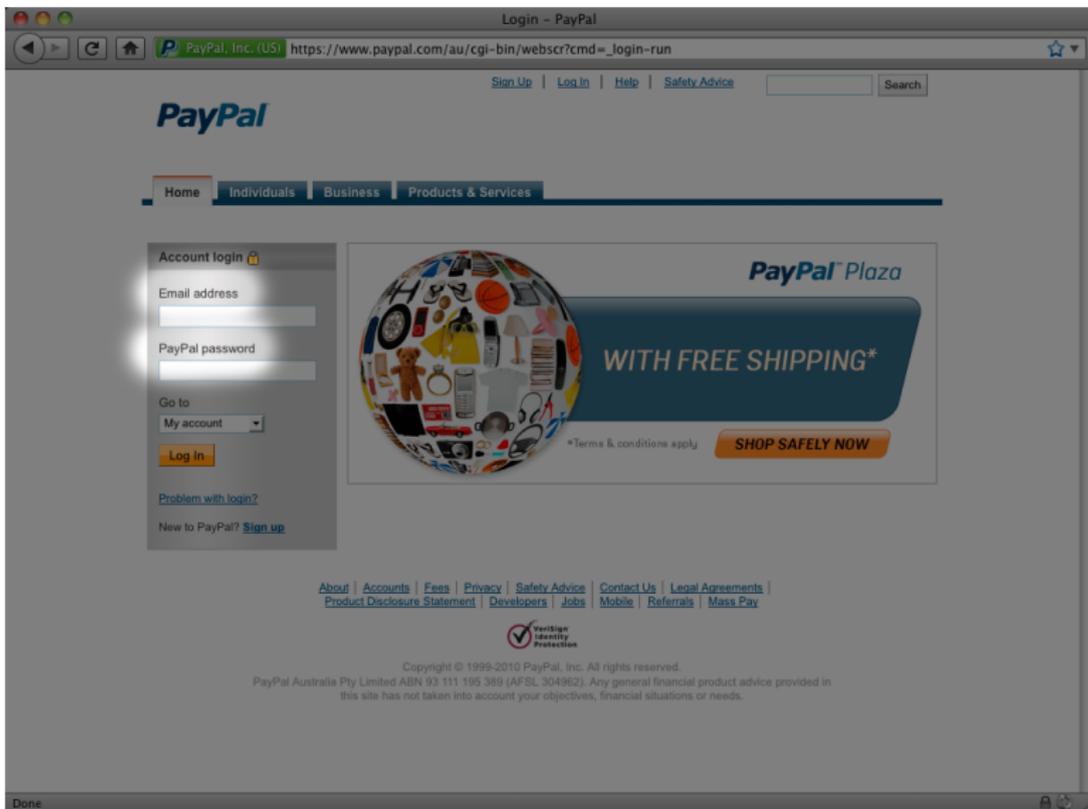
# “type of site” – 88%



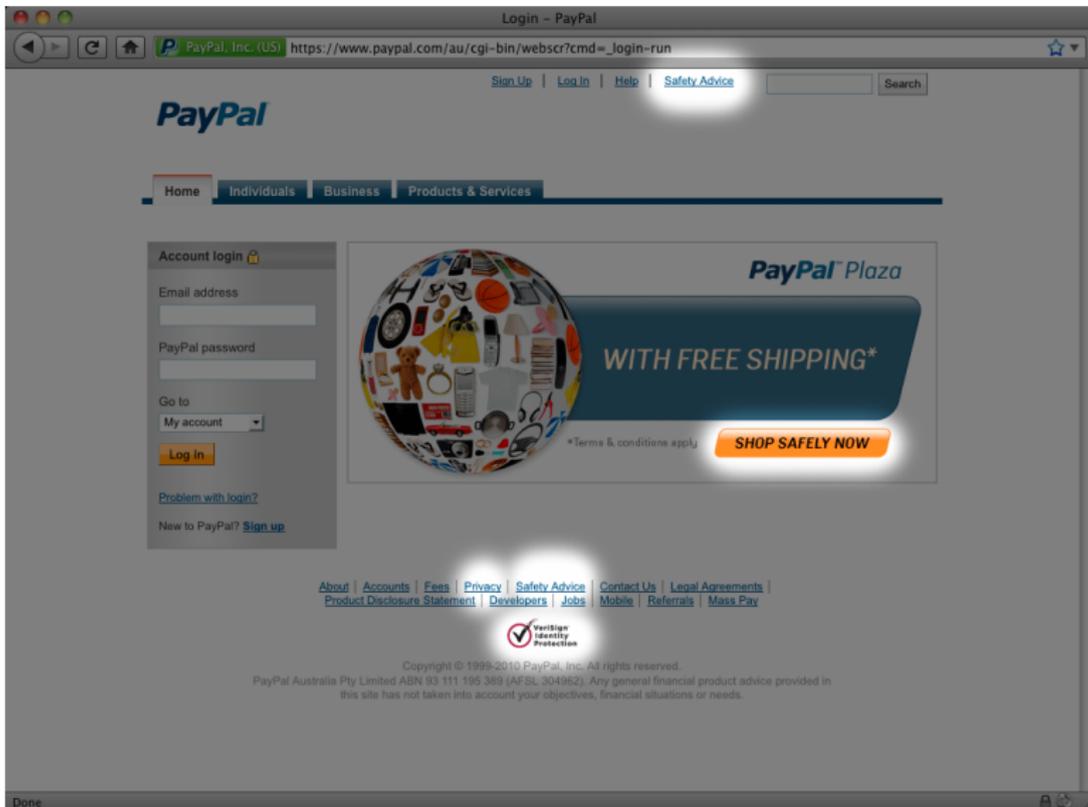
# “lock or key icon” – 75%



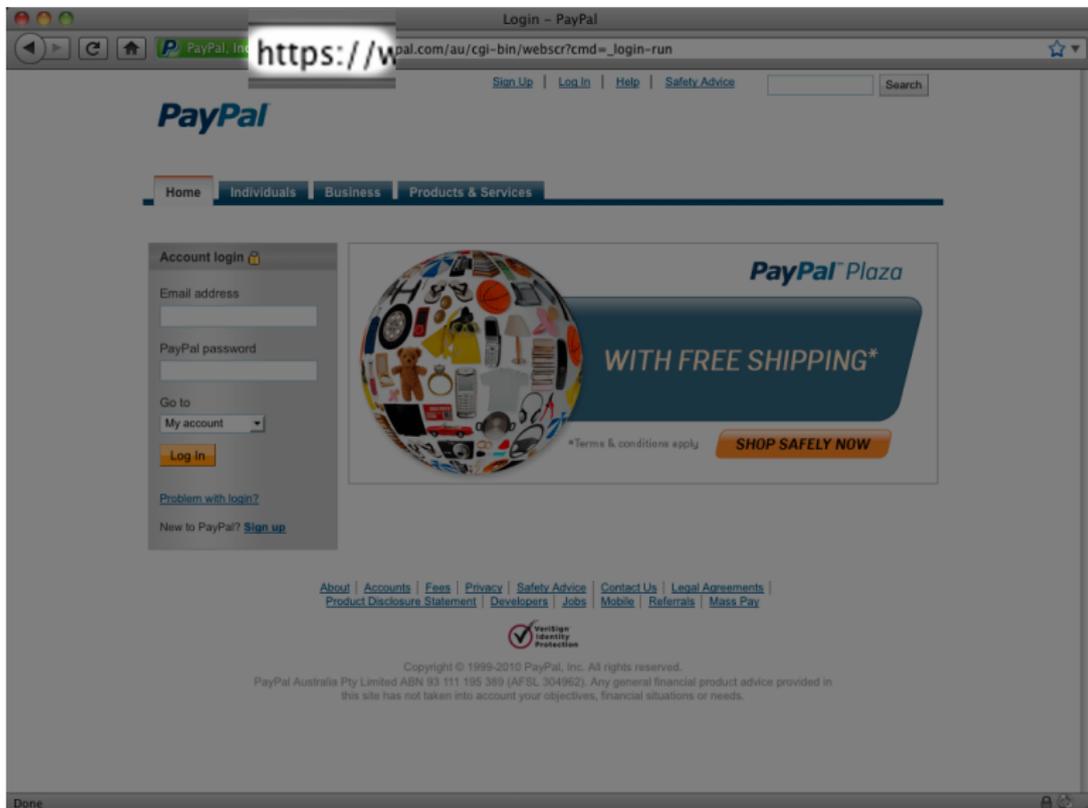
# “type of information” – 69%



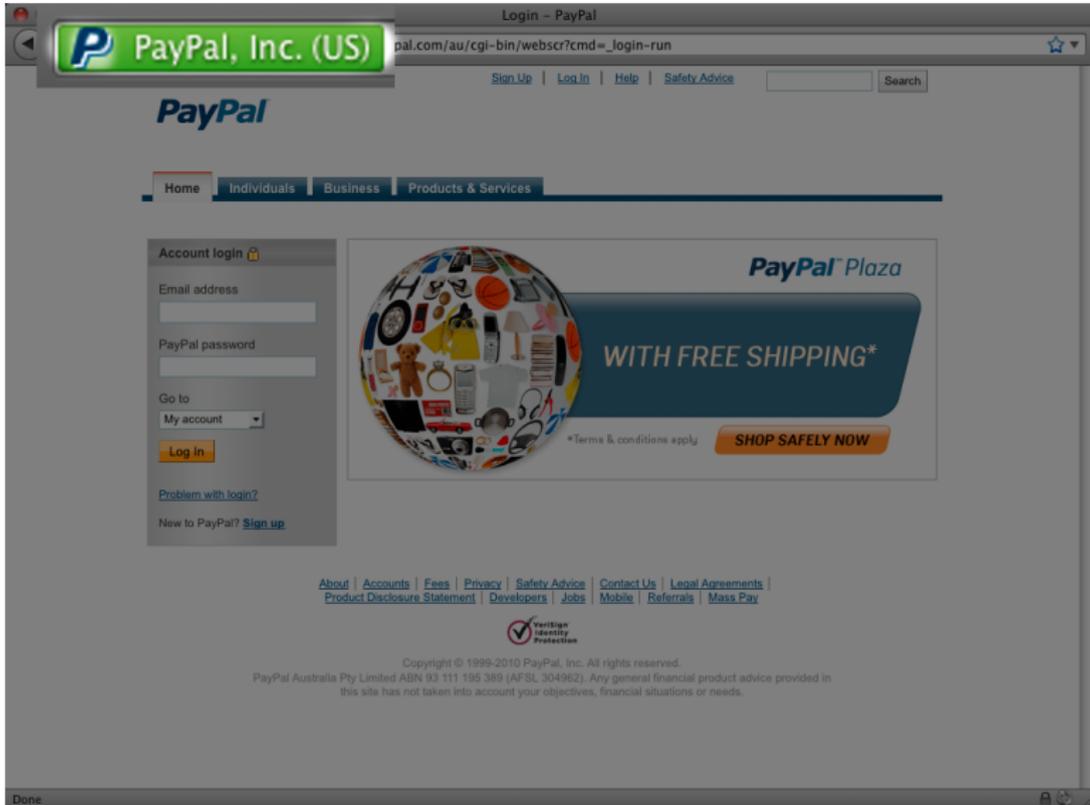
# “site statements” – 50%



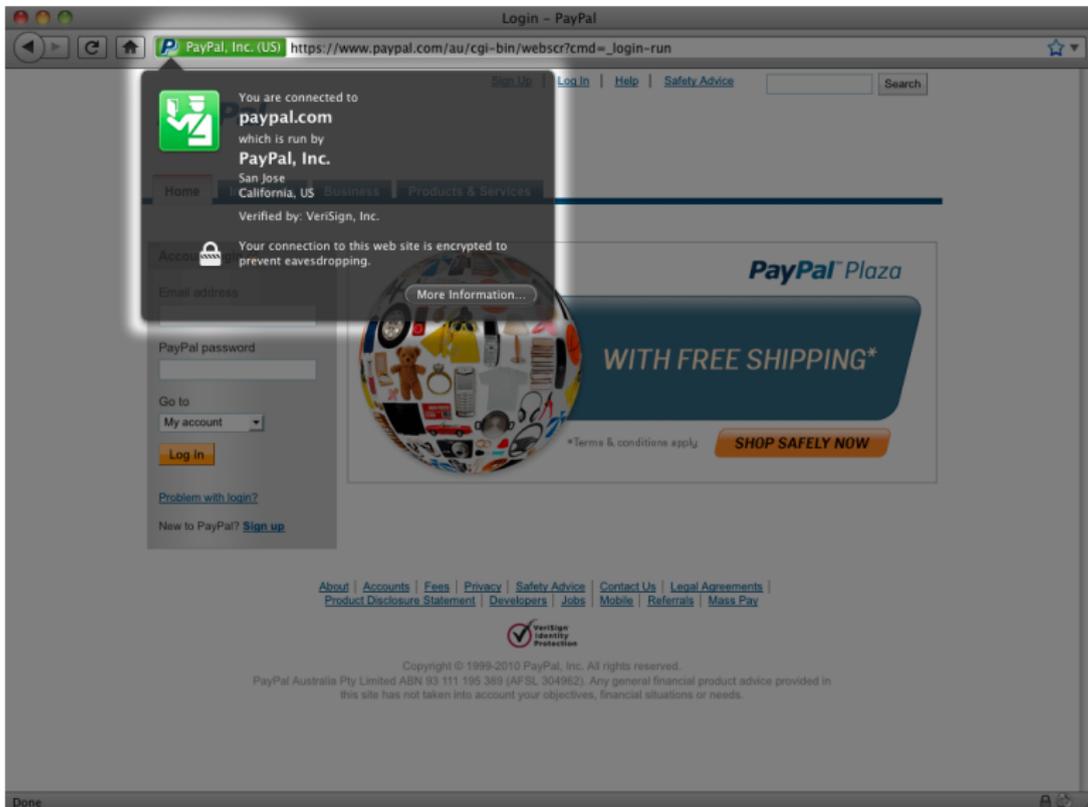
# “https” – 50%



# “certificate” – 19%



# “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

Browser window: Login - PayPal  
Address bar: https://www.paypal.com/au/cgi-bin/webscr?cmd=\_login-run

Navigation: [Sign Up](#) | [Log In](#) | [Help](#) | [Safety Advice](#) [Search]

PayPal

Home | Individuals | Business | Products & Services

Account login

Email address

PayPal password

Go to  
My account

[Problem with login?](#)

New to PayPal? [Sign up](#)

PayPal Plaza  
WITH FREE SHIPPING\*

\*Terms & conditions apply

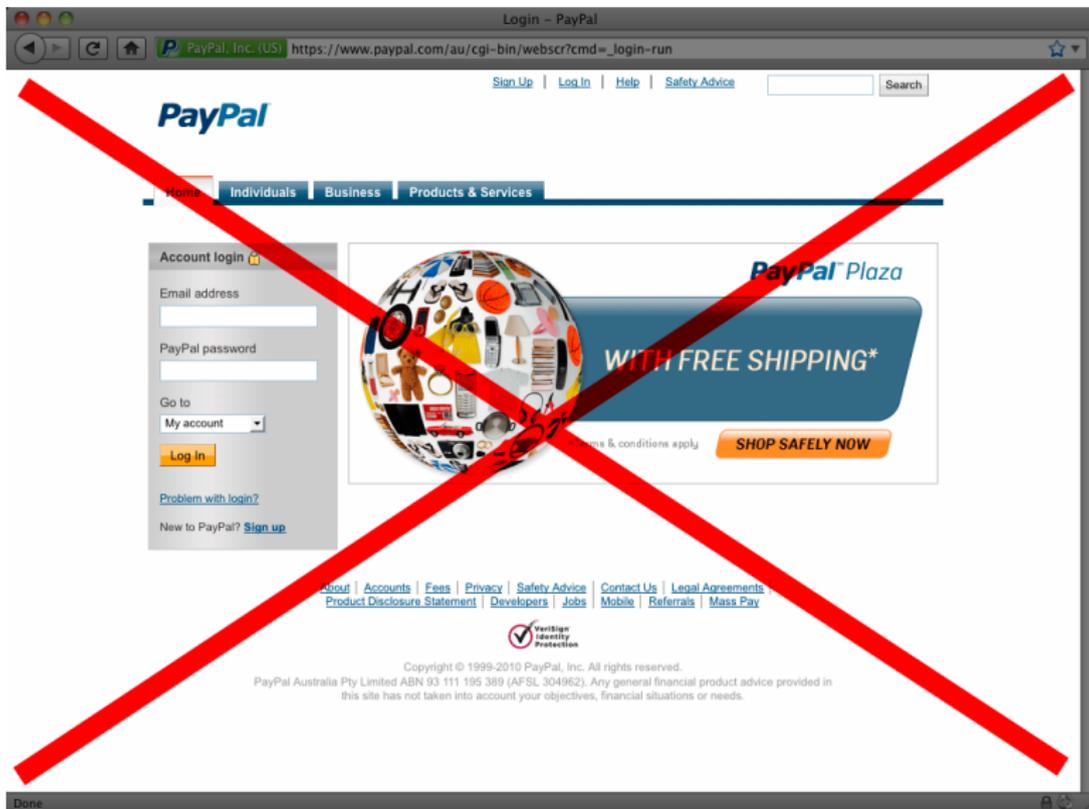
[About](#) | [Accounts](#) | [Fees](#) | [Privacy](#) | [Safety Advice](#) | [Contact Us](#) | [Legal Agreements](#) |  
[Product Disclosure Statement](#) | [Developers](#) | [Jobs](#) | [Mobile](#) | [Referrals](#) | [Mass Pay](#)

VeriSign Identity Protection

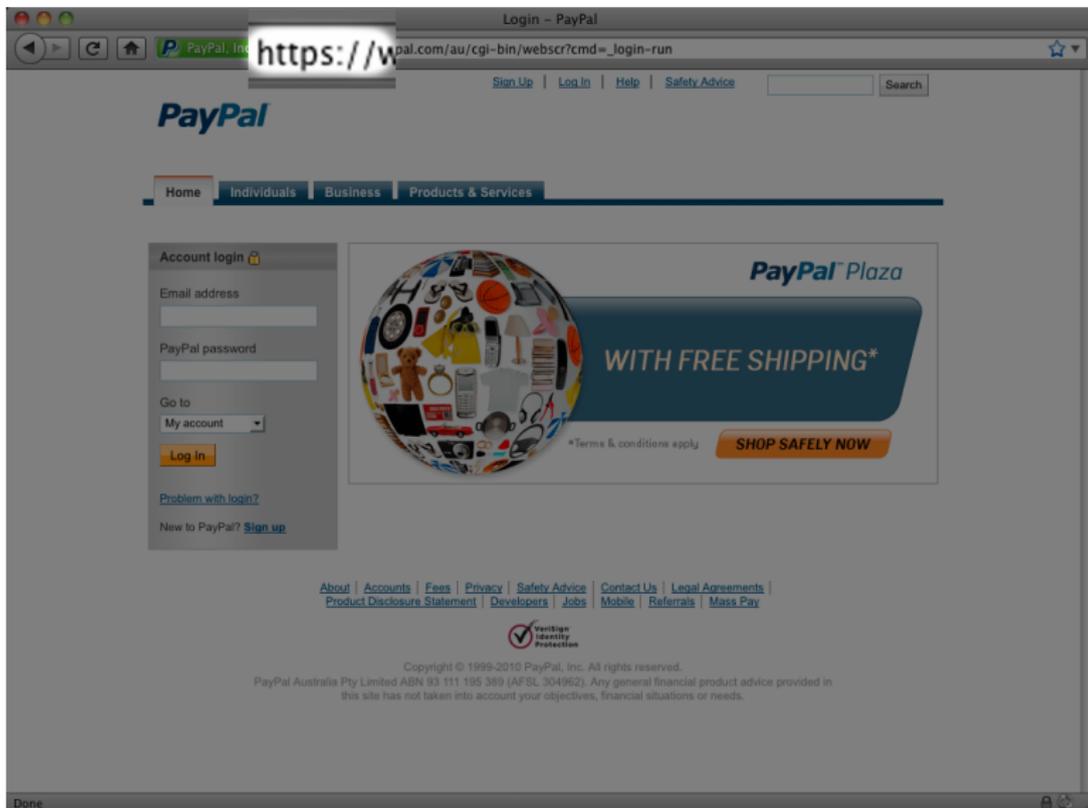
Copyright © 1999-2010 PayPal, Inc. All rights reserved.  
PayPal Australia Pty Limited ABN 93 111 195 389 (AFSL 304962). Any general financial product advice provided in this site has not taken into account your objectives, financial situations or needs.

Done

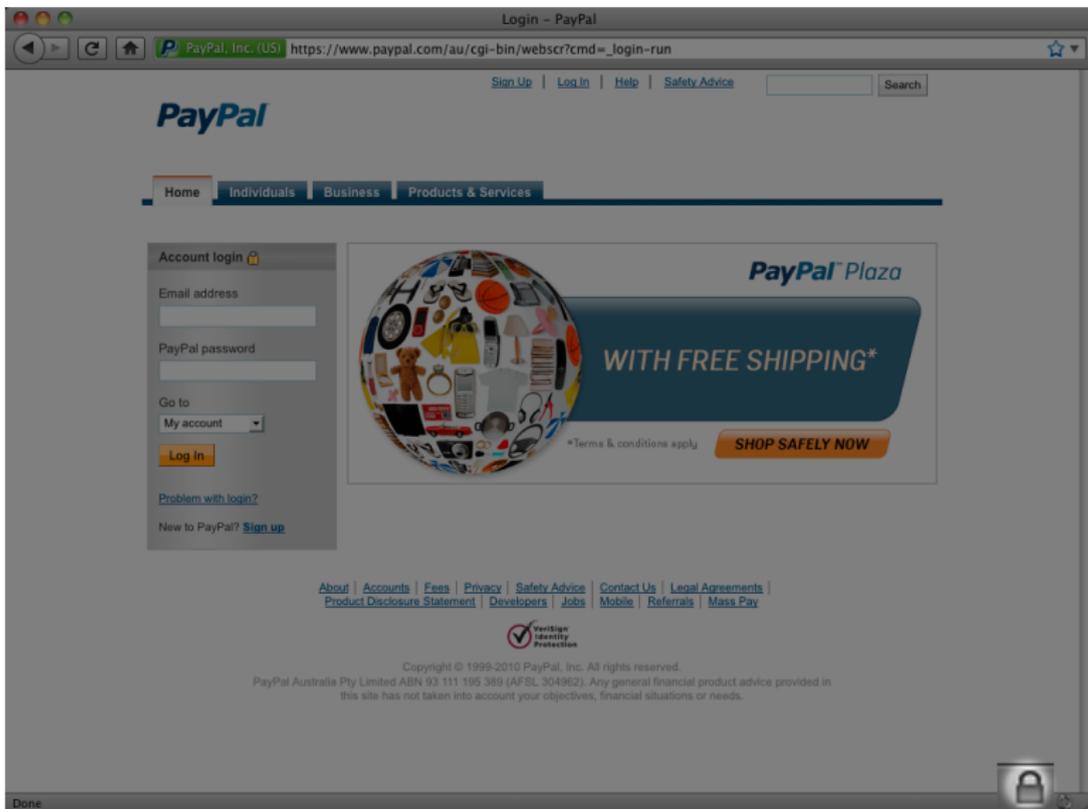
# We can't trust anything provided by the server



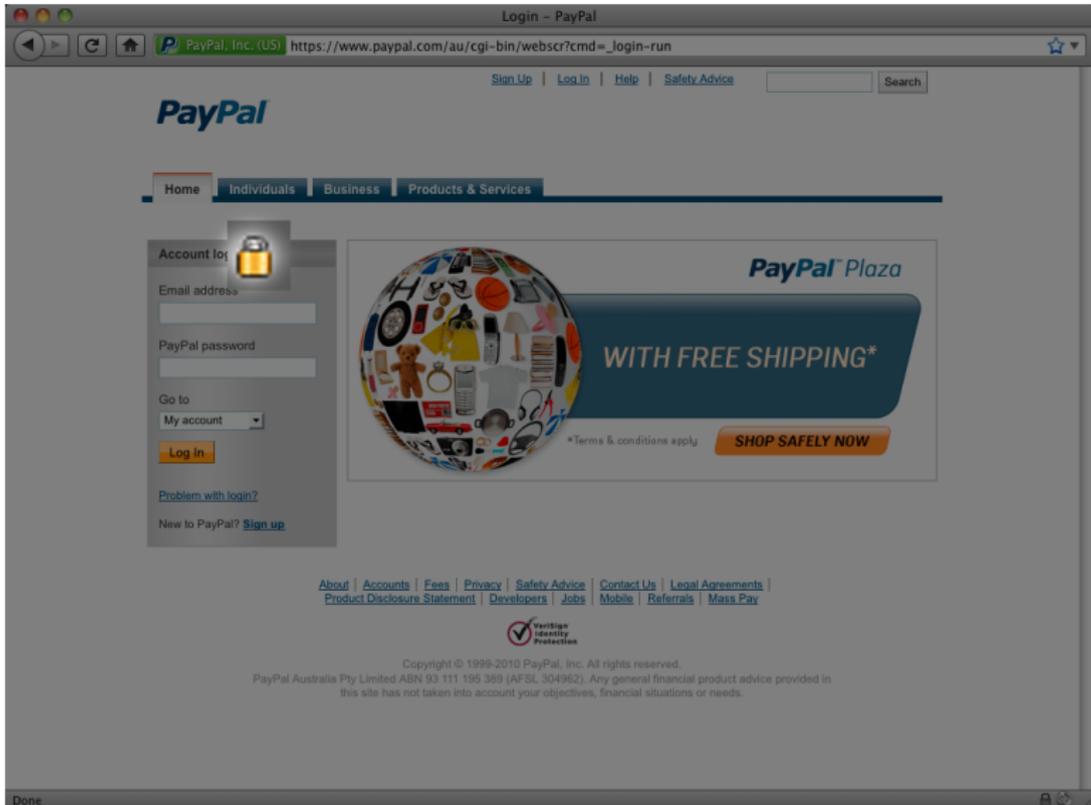
# Security indicator: “https” in location bar



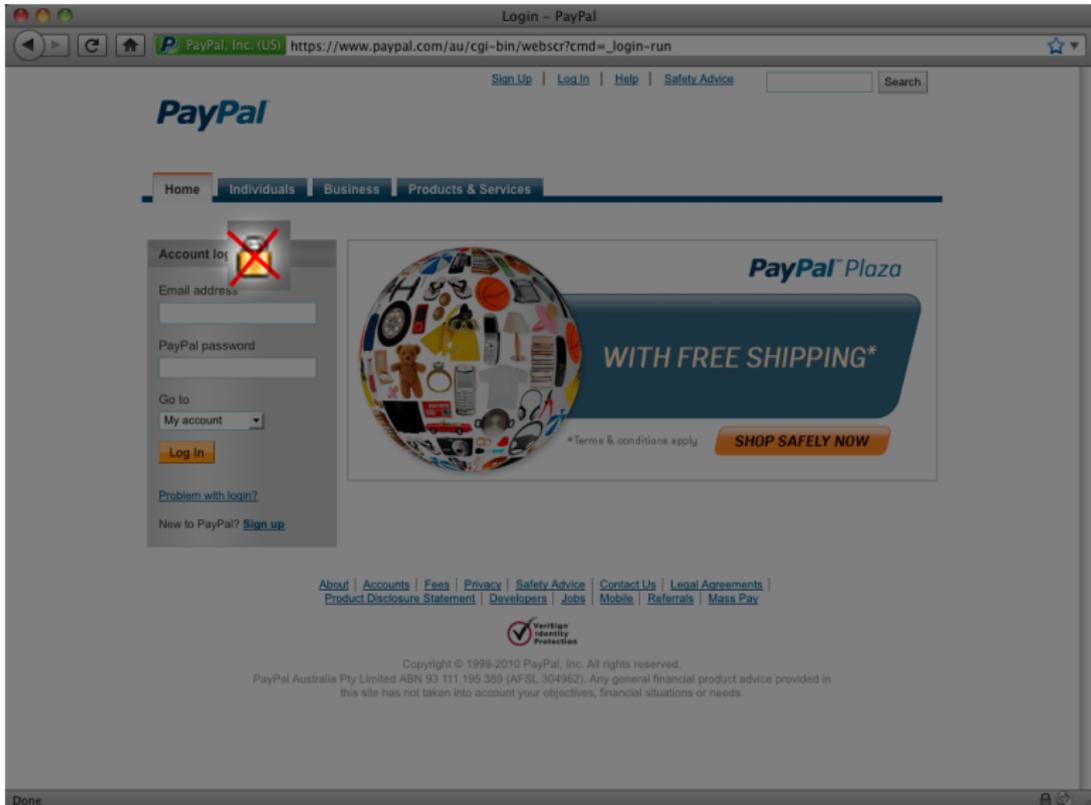
# Security indicator: lock icon in browser chrome



# Security indicator: lock icon in browser chrome



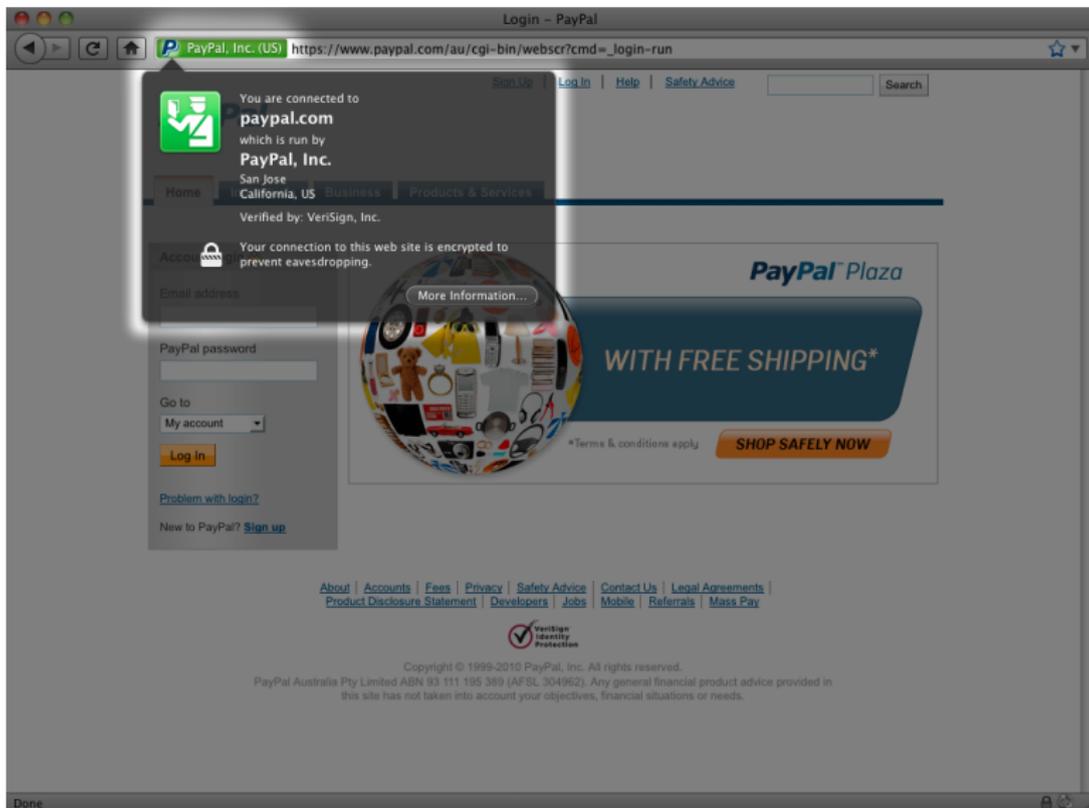
# Security indicator: lock icon in browser chrome



# Security indicator: domain name correct



# Security indicator: extended validation certificate





PayPal, Inc. (US)

https://www.paypal.com/a



# 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

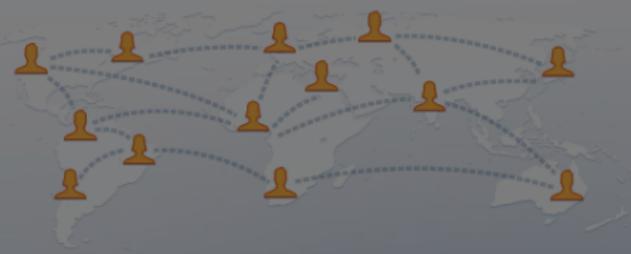
Email address

PayPal password

Go to



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:

Birthday:

Why do I need to provide this?

[Create a Page](#) for a celebrity, band or business.

## Security indicators

- S1. Does the URL in the location bar begin with https?
- S2. Is the domain name of the URL in the location bar correct?
- S3. Is the lock icon displayed somewhere in the browser chrome?
- S4. Are there indicators present for an extended validation certificate?

# Do people use security indicators?

# Use of security indicators: Whalen and Inkpen<sup>2</sup>

Methodology: eye-tracking, subject interviews.

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

---

<sup>2</sup>Whalen, Inkpen. Gathering evidence: use of visual security cues in web browsers. *Graphics Interface*, 112:137-144 (2005)

## Use of security indicators: Schechter et al.<sup>3</sup>

**Absence of security indicators:** Examined user behaviour when logging in to financial websites. All 67 subjects continued logging in even when no security indicators were present.

**Site authentication images:** Users were more willing to ignore browser warnings and security indicators when site-authentication images were used.

---

<sup>3</sup>Schechter, Damija, Ozment, Fischer. The emperor's new security indicators: An evaluation of website authentication and the effect of role playing on usability studies. *Proc. IEEE S&P 2007*, 51-65.

## Use of security indicators: Sobey et al.<sup>4</sup>

Methodology: eye-tracking

- ▶ Eye-tracking data showed that extended validation interface was not originally noticed by users.
- ▶ Once trained, users show a willingness to adopt these features.

---

<sup>4</sup>Sobey, Biddle, van Oorschot, Patrick. Exploring user reactions to new browser cues for extended validation certificates. *Proc. ESORICS 2008*, LNCS 5283, 411–427.

# Why do people ignore security indicators?

---

<sup>5</sup>Whitten, Tygar. Why Johnny can't encrypt: A usability evaluation of PGP 5.0 *Proc. USENIX 1999*.

<sup>6</sup>Dhamija, Tygar, Hearst. Why phishing works. *Proc. CHI 2006*.

## Why do people ignore security indicators?

1. “the unmotivated user property”<sup>5</sup>
2. lack of knowledge of security and security indicators
3. lack of attention to security indicators
4. lack of attention to **absence** of security indicators<sup>6</sup>

---

<sup>5</sup>Whitten, Tygar. Why Johnny can't encrypt: A usability evaluation of PGP 5.0 *Proc. USENIX 1999*.

<sup>6</sup>Dhamija, Tygar, Hearst. Why phishing works. *Proc. CHI 2006*.

## Why do people ignore security indicators?

1. “the unmotivated user property” <sup>5</sup>
2. lack of knowledge of security and security indicators
3. lack of attention to security indicators
4. lack of attention to **absence** of security indicators <sup>6</sup>

Our hypothesis: users are habituated to ignoring security indicators because many websites don't use them properly.

---

<sup>5</sup>Whitten, Tygar. Why Johnny can't encrypt: A usability evaluation of PGP 5.0 *Proc. USENIX 1999*.

<sup>6</sup>Dhamija, Tygar, Hearst. Why phishing works. *Proc. CHI 2006*.

## **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.

## Misuse of security indicators

- ▶ HTTP login page with HTTPS form submission
- ▶ Lock icon on page or as favicon
- ▶ Hidden location bar
- ▶ Mismatched domain name
- ▶ Very complicated URL

# Misused indicator: login protocol vs. form protocol



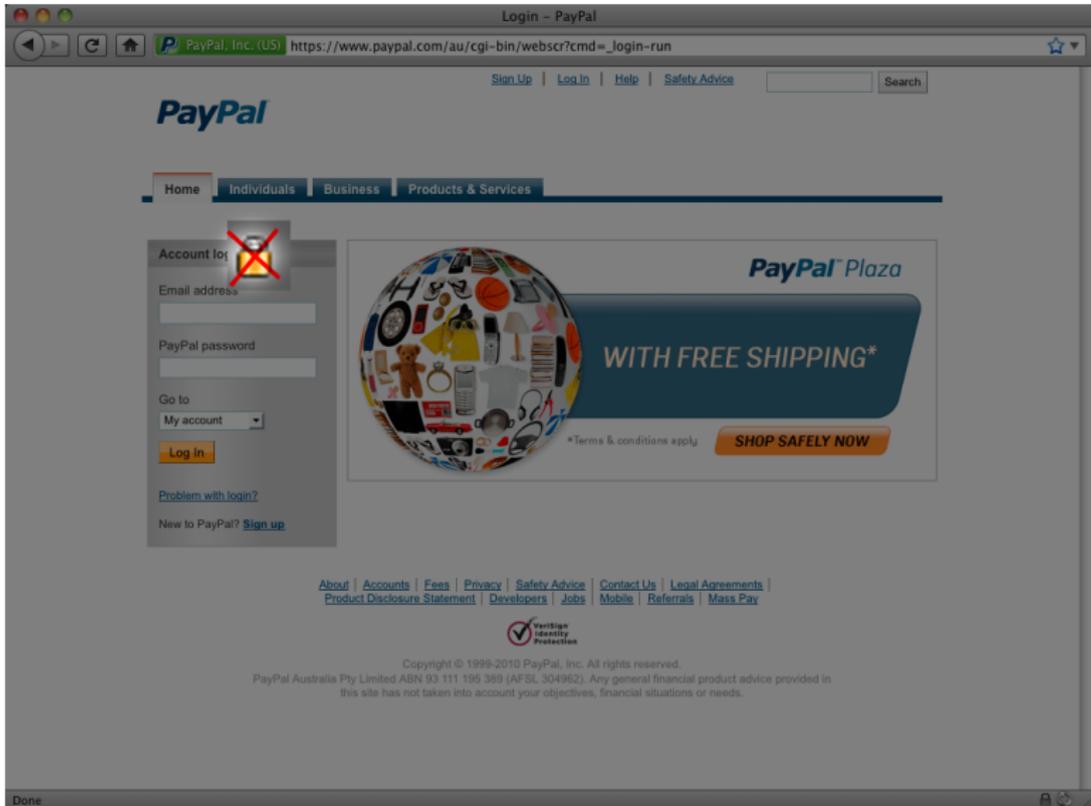


# Misused indicator: login protocol vs. form protocol

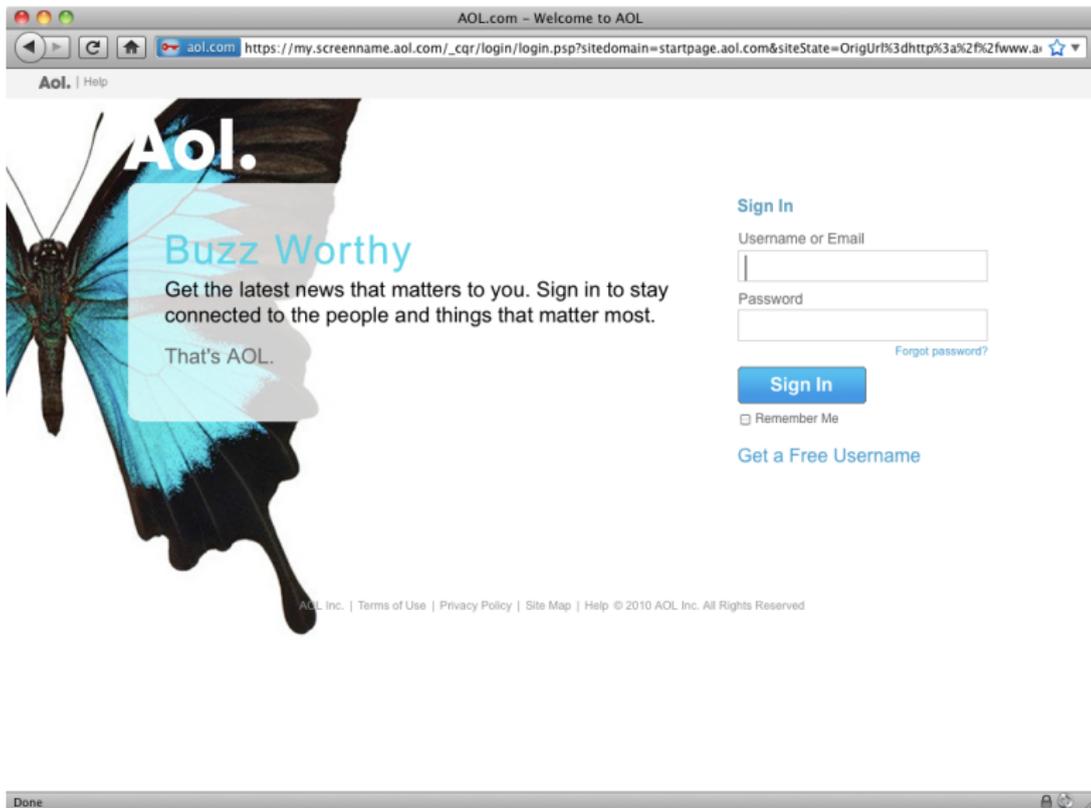
Login page	Form submission		
	HTTP	45%	*
HTTP	HTTPS	10%	×
	HTTPS w/EV cert.	5%	×
HTTPS	HTTPS	32%	✓
HTTPS w/EV cert.	HTTPS w/EV cert.	8%	✓

\* HTTP form submission provides no protection whatsoever for usernames or passwords.

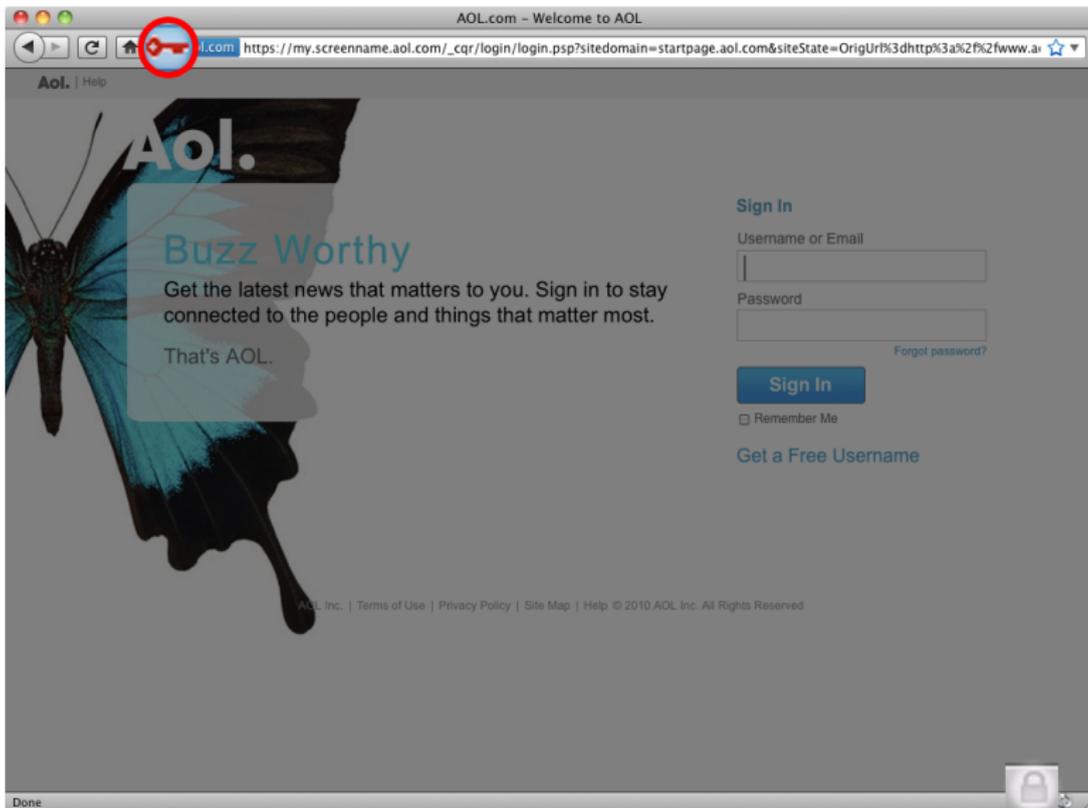
# Misused indicator: lock icon on page or as favicon



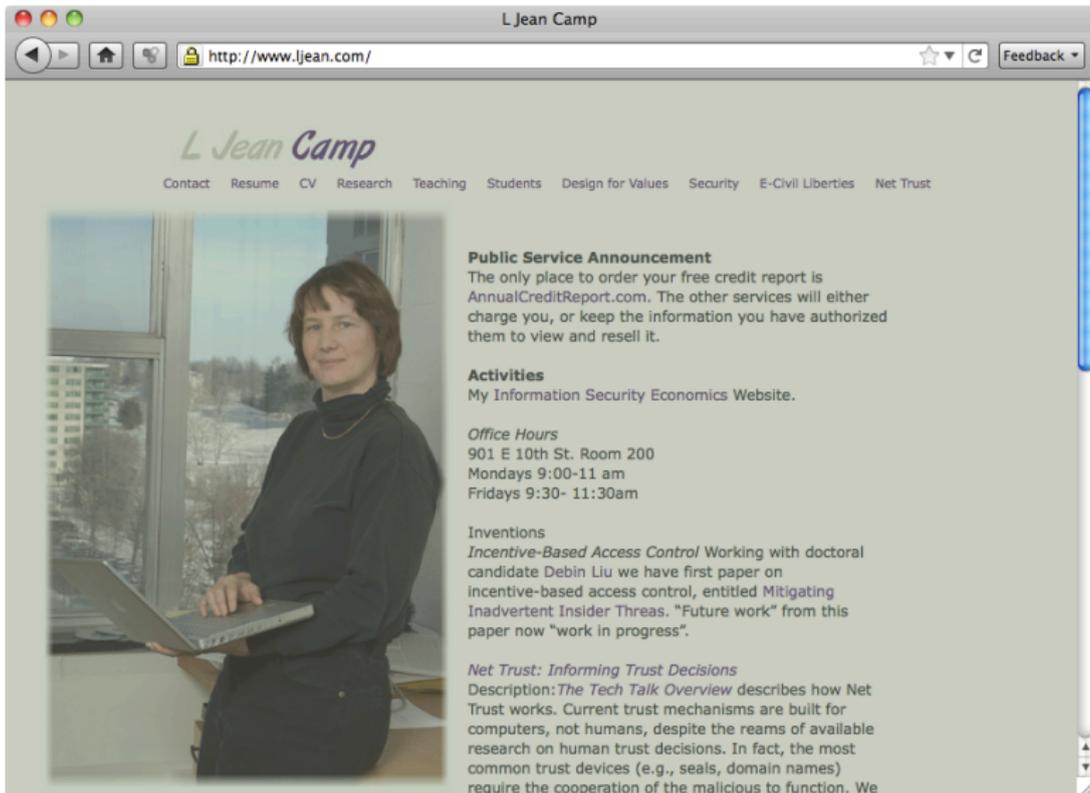
# Misused indicator: lock icon on page or as favicon



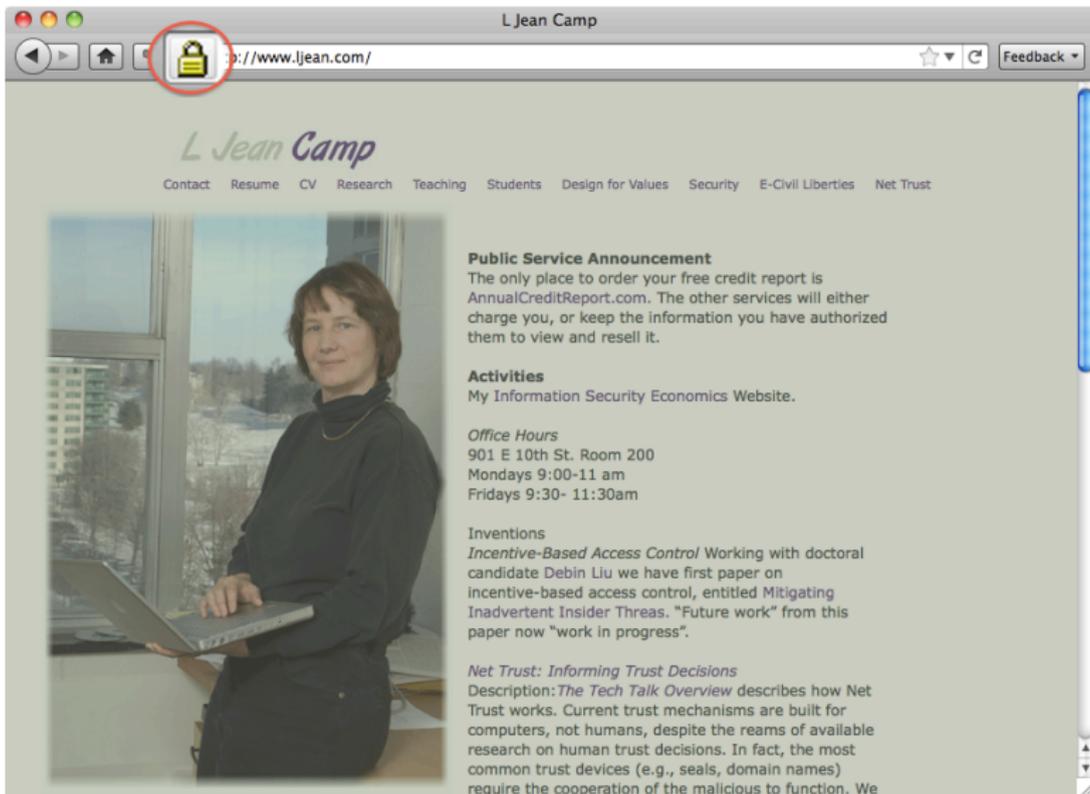
# Misused indicator: lock icon on page or as favicon



# Misused indicator: lock icon on page or as favicon



# Misused indicator: lock icon on page or as favicon



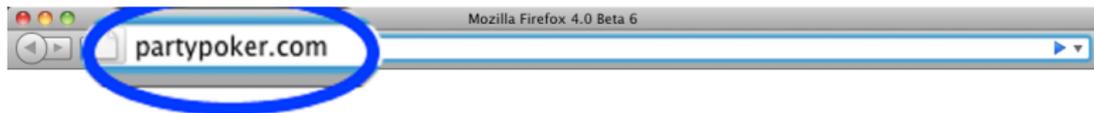
## Misused indicator: lock icon on page or as favicon

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%	××

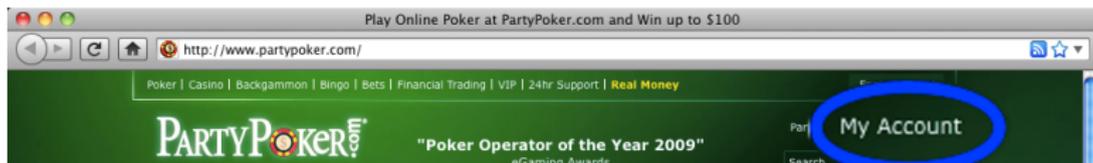
# Misused indicator: hidden location bar – 2%

The screenshot shows a Mozilla Firefox browser window with the address bar hidden. The page is the ANZ Internet Banking homepage. At the top, the ANZ logo and "Internet Banking" are displayed in a blue header bar, with a "back to ANZ" link on the right. Below the header, there is a family photo on the left and a list of services on the right: "View account statements online with eStatements" and "Start investing in minutes with the ANZ Online Investment Account". A link to "view the ANZ Internet Banking demo" is also present. A prominent yellow warning icon is followed by the text "Security alert - September 2009" and a link to "Read current security alert". Below this is a blue bar with the text "Log on to Internet Banking". The login section includes fields for "Customer Registration Number:" and "Password:", a "log on" button, and a "Trouble logging on? Help" link. To the right of the login fields is a list of links: "Tips on how to Protect your banking.", "Find out more about Internet Banking.", "Register for Internet Banking.", "Check your software settings.", and "View Terms and Conditions.". At the bottom of the page, there is a copyright notice: "© Copyright Australia and New Zealand Banking Group Limited ABN 11 005 357 522, 1996-2009. ANZ's colour blue is a trade mark of ANZ." followed by links for "Web Site Terms of Use", "ANZ Web Site Security and Privacy Statement", "Site Map", and "Jobs at ANZ". The browser's status bar at the very bottom shows the word "Done" on the left and a lock icon on the right.

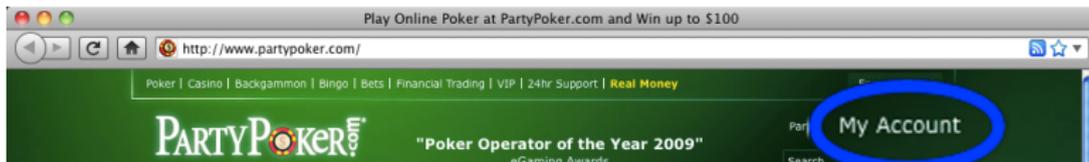
# Misused indicator: mismatched domain name



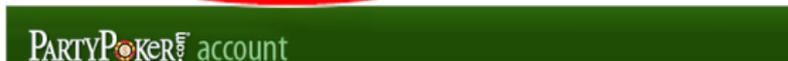
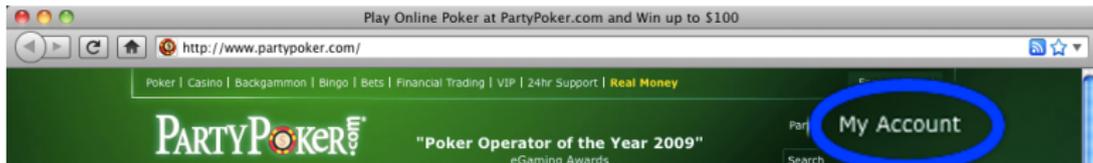
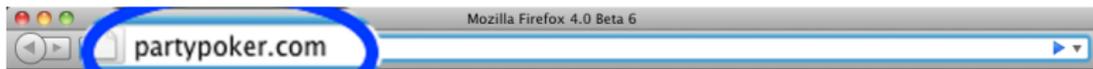
# Misused indicator: mismatched domain name



# Misused indicator: mismatched domain name



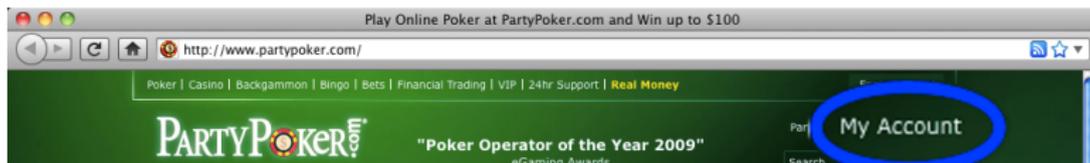
# Misused indicator: mismatched domain name



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

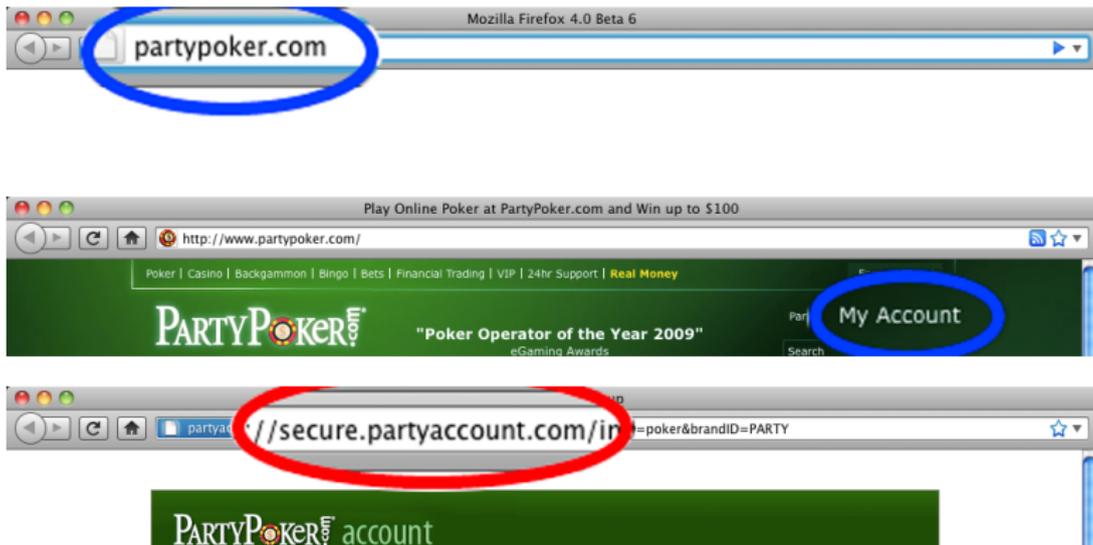
- ▶ Apparently, yes.

# Misused indicator: mismatched domain name



What about partypoker-account.com?

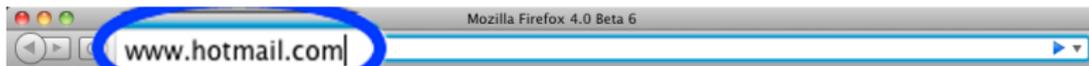
# Misused indicator: mismatched domain name



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

Match?	Example typed domain → login domain		
Exact match	google.com → www.google.com	57%	✓
Close match	yahoo.com → login.yahoo.com	30%	
No match	hotmail.com → login.live.com	13%	✗

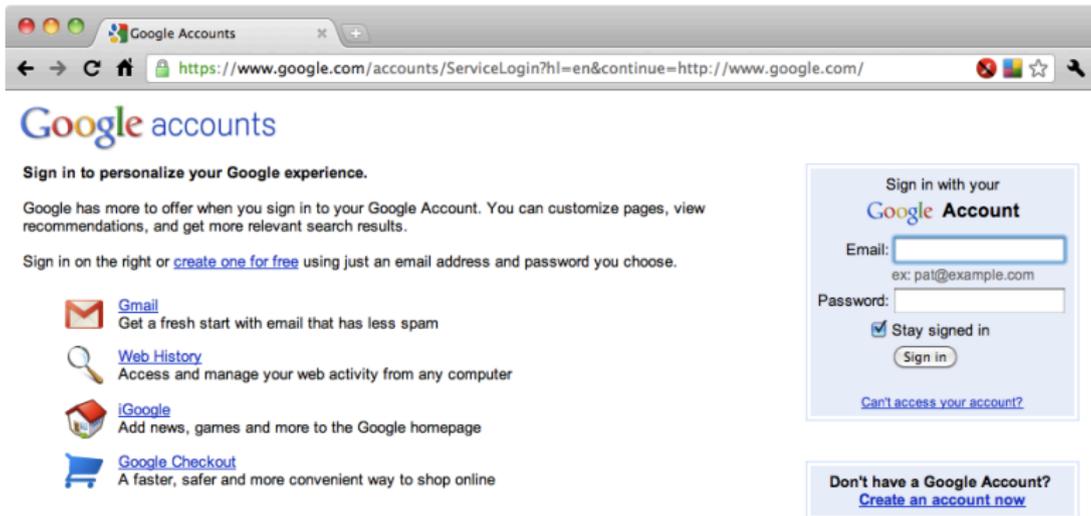
## Misused indicator: complicated URL

- ▶ Complicated URL makes checking domain name harder
- ▶ “URL as UI”<sup>7</sup>

Complexity	Example	Avg. Len.		
Domain only	<a href="https://www.chase.com/">https://www.chase.com/</a>	21.9	40%	✓
One path	<a href="https://www.blogger.com/start">https://www.blogger.com/start</a>	32.9	17%	
More than one path component	<a href="https://www.google.com/accounts/ServiceLogin?uilel=3&amp;service=youtube&amp;passive=true&amp;continue=http%3A%2F%2Fwww.youtube.com%2Fsignin%3Faction_handle_signin%3Dtrue%26nomobiletemp%3D1%26hl%3Den_US%26next%3D%252F&amp;hl=en_US&amp;ltmpl=sso">https://www.google.com/accounts/ServiceLogin?uilel=3&amp;service=youtube&amp;passive=true&amp;continue=http%3A%2F%2Fwww.youtube.com%2Fsignin%3Faction_handle_signin%3Dtrue%26nomobiletemp%3D1%26hl%3Den_US%26next%3D%252F&amp;hl=en_US&amp;ltmpl=sso</a>	110.1	42%	✗

<sup>7</sup>Jakob Nielsen. URL as UI, March 1999. <http://www.useit.com/alertbox/990321.html>

# Improved UI design for URL as UI: Google Chrome



The screenshot shows a browser window with the address bar containing the URL `https://www.google.com/accounts/ServiceLogin?hl=en&continue=http://www.google.com/`. The page title is "Google Accounts". The main heading is "Google accounts".

**Sign in to personalize your Google experience.**

Google has more to offer when you sign in to your Google Account. You can customize pages, view recommendations, and get more relevant search results.

Sign in on the right or [create one for free](#) using just an email address and password you choose.

-  [Gmail](#)  
Get a fresh start with email that has less spam
-  [Web History](#)  
Access and manage your web activity from any computer
-  [iGoogle](#)  
Add news, games and more to the Google homepage
-  [Google Checkout](#)  
A faster, safer and more convenient way to shop online

**Sign in with your Google Account**

Email:

Password:

Stay signed in

[Can't access your account?](#)

**Don't have a Google Account?**  
[Create an account now](#)

©2011 Google - [Google Home](#) - [Terms of Service](#) - [Privacy Policy](#) - [Help](#)



## Summary of results

### Misused security indicators

---

HTTP login page with HTTPS form submission	15%
Lock icon on page or as favicon	23%
Hidden location bar	2%
Mismatched domain name	13%
Very complicated URL	42%

“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.

## 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.
  - ▶ Design with usable security in mind.

## Open questions

- ▶ Dataset of most-frequently-logged-in-to sites, not most-frequently-used sites.
- ▶ Usability study of single sign-on systems, such as Facebook Connect and Twitter OAuth: how does users understand flow and security of single sign-on systems?

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

Douglas Stebila  
stebila@qut.edu.au



## Misused security indicators

---

HTTP login page with HTTPS form submission	15%
Lock icon on page or as favicon	23%
Hidden location bar	2%
Mismatched domain name	13%
Very complicated URL	42%

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.