FORRESTER®

Forrester Opportunity Snapshot: A Custom Study Commissioned By Entrust Datacard | May 2018

Browser UI: What Does “Secure” Really Mean?

IT Decision Makers’ Perceptions And Expectations On Browser UI Security Indicators

GET STARTED ▶

Forrester Opportunity Snapshot: A Custom Study Commissioned By Entrust Datacard, May 2018

Browser UI: What Does “Secure” Really Mean?

Overview

IT decision makers are seeing a growing threat to digital business that jeopardizes the foundation of eCommerce today — consumer trust. Major banks and retail firms are completely dependent on consumer trust to conduct digital transactions, which are vital to business success. To gain trust, organizations must prove to their customers that their digital interactions are secure. SSL certificates have built trust since the late 1990s by displaying an icon in the web address bar that shows the website is using encryption, and more recently, whether or not the website owner’s identity has been confirmed. While SSL has been a vital component of transaction security, recent issues with the way SSL is being used by phishers can potentially expose customer data to criminals. Organizations must understand these challenges and block them, or risk losing customer trust and loyalty.

SSL (secure sockets layer) also known as TLS, is a security protocol for encrypting data between a server and web browser.

In March 2018, Entrust Datacard commissioned Forrester to conduct a study exploring current attitudes and challenges with SSL/TLS encryption. The study surveyed 105 IT decision makers in the US responsible for website security at large retail and financial services firms using encryption.

Company size (# of employees):

- **18%** 20,000 or more
- **33%** 5,000 to 19,999
- **49%** 1,000 to 4,999

Industry

- **49%** Financial services
- **51%** Retail

Title

- **45%** C-level executive
- **19%** Vice president
- **23%** Director
- **13%** Manager

IT job function

- **64%** CIO/CIO office/CTO
- **19%** Line of business mgmt.
- **17%** Security

Browser UI: What Does “Secure” Really Mean?

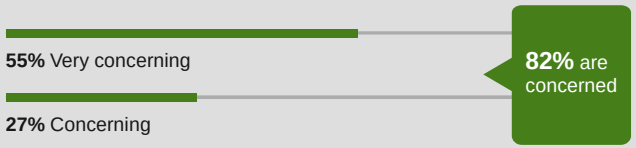
Consumer Trust Is A Valued And Threatened Commodity

Customers need to feel that their financial information and personally identifiable information (PII) are safe when interacting with firms online. This trust forms the basis of eCommerce today.

However, it’s easier than ever for phishing and malware sites with lookalike URLs to pose as your official company website. These sites can even obtain anonymous SSL/TLS certificates that grant them a misleading “secure” browser UI, making their fake website look even more authentic, threatening consumer safety and eroding customer trust. This should — and does — concern financial services and retail firms today.

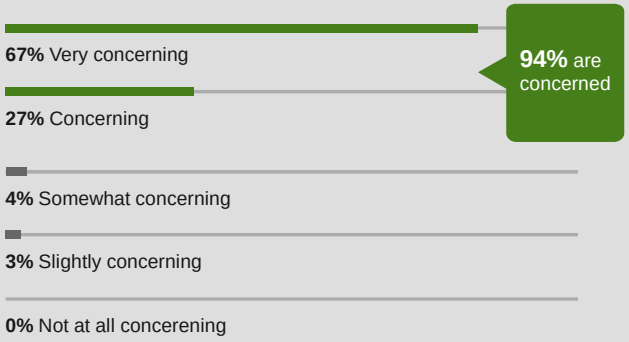
82% of firms are concerned that criminals can create fraudulent lookalike sites designed to steal their customers’ PII — and even more are concerned that their methods of doing so are becoming harder to detect.

“How concerned are you that there could be fraudulent lookalike sites that imitate your company website?”



Base: 105 IT decision makers at large retail and financial services firms in the US
Source: A commissioned study conducted by Forrester Consulting on behalf of Entrust Datacard, March 2018

“How concerning is it that fraudulent websites can obtain security certificates to make their lookalike sites appear to have the same security verification as your website?”



Base: 105 IT decision makers at large retail and financial services firms in the US
Source: A commissioned study conducted by Forrester Consulting on behalf of Entrust Datacard, March 2018

Browser UI: What Does “Secure” Really Mean?

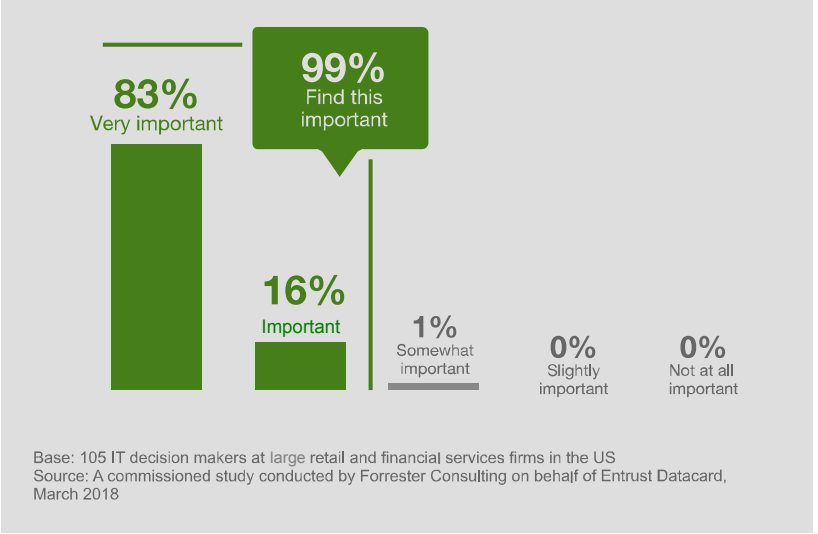
SSL Tries To Solve This Challenge, But Not All SSL Certificates Are The Same

To combat this, almost all firms today think it’s critically important that SSL certificates tell customers that a website is official **by showing confirmed organization identity** and is therefore safer to use. However, firms (and customers) should know that there are multiple types of SSL verifications and all SSL certificates are not the same. Encrypted websites may use any of three types of certificates:

- **Domain validated (DV)** certificates verify control of a website’s domain only.
- **Organization validated (OV)** certificates verify both a website’s domain and basic website owner identity.
- **Extended validation (EV)** certificates verify both a website’s domain and the website owner’s identity and organization existence.

Of these, OV and EV certificates do confirm identity. However, DV certificates do not. Unsurprisingly, almost all fraudulent sites with SSL certificates today have DV certificates.

“How important is it that your website has an SSL certificate that tells customers they are at your company's official website?”



Base: 105 IT decision makers at large retail and financial services firms in the US
Source: A commissioned study conducted by Forrester Consulting on behalf of Entrust Datacard, March 2018

Browser UI: What Does “Secure” Really Mean?

The Real Meaning Of “Secure”

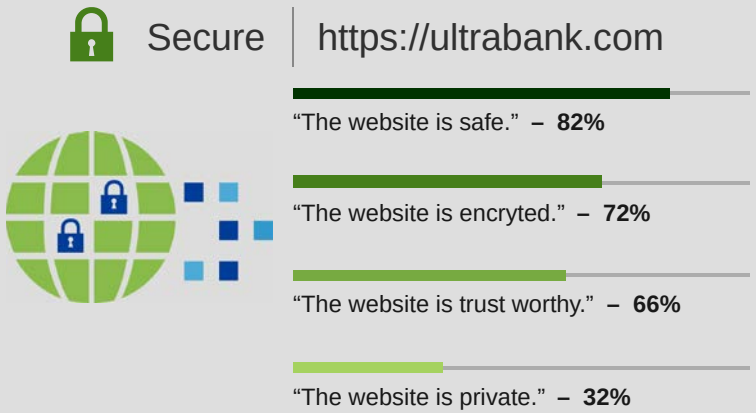
To help show the distinction between websites that have SSL certificates and websites not using encryption, browsers have designed UI indicators — typically a lock symbol and/or the word “secure.” But what that symbol conveys and what it actually means are two different things.

The lock and/or “secure” browser UI indicator only shows that the site is using encryption. This means it’s possible for fraudulent sites to obtain the same browser indicators as official sites with confirmed identities.

Even IT professionals responsible for their websites are unclear on this distinction; most feel that browser UI indicators denote “safety” which means almost certainly that consumers think the same.

Further complicating this issue is the fact that different browsers have different UI indicators, and many show different indicators for the different encryptions types (DV versus OV or EV). All of these factors add up to a system that is confusing for professionals and consumers alike; a system where safe and unsafe sites can look the same.

“Some websites receive the following browser user interface (UI) security indicator in the browser. What do you think the security indicator is intended to tell users?”



Base: 105 IT decision makers at large retail and financial services firms in the US
Source: A commissioned study conducted by Forrester Consulting on behalf of Entrust Datacard, March 2018

82% of IT professionals in our survey think the lock and/or “secure” symbol in browsers indicates security, when in reality it only denotes encryption.

Browser UI: What Does “Secure” Really Mean?

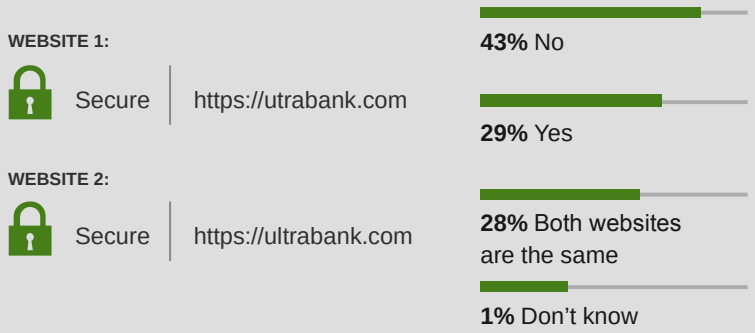
Ambiguity Leaves Consumers In Danger

If fraudulent websites can get the same lock and/or “secure” iconography in browsers, will consumers be able to tell the difference between safe and unsafe sites? IT professionals in our survey don’t think so. Forty-three percent of respondents say they don’t think their users can tell the difference between an official site with confirmed identity and a fraudulent site. And perhaps more concerning, 28% of respondents can’t tell the difference themselves.

This points to a need for better education in the market around website security, as well as a need to clearly distinguish between different the SSL types in browsers, including which ones establish website identity.

Note: Look carefully at the URLs in the two examples. Website 1 is the lookalike phishing site with the anonymous DV certificate, while Website 2 is the official site with an OV identity certificate.

“For a bank named UltraBank, Inc., with the website address as ‘ultrabank.com’ do you think most of your users can tell which website below is fraudulent?”



Base: 105 IT decision makers at large retail and financial services firms in the US
Source: A commissioned study conducted by Forrester Consulting on behalf of Entrust Datacard, March 2018

Close to half of the IT professionals surveyed don’t think customers can tell the difference between a fraudulent site and an official one, ***and 28% are unable to do so themselves!***

Browser UI: What Does “Secure” Really Mean?

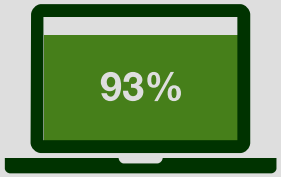
Firms Believe SSL Certificates Should Indicate Both Encryption And Ownership

To help protect consumers from fraudulent, lookalike websites, firms in our survey want a browser indicator that shows their customers are indeed at the official website. To this end, respondents strongly believe SSL should both confirm a website’s official identity and encrypt communication.

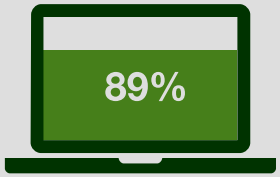
- The good news is that OV and EV encryption certificates do this today!
- More needs to be done to show the difference between different certificate types (OV and EV confirm identity and DV does not), and consumers need to be both educated on the different types and how to use them when looking for a company’s official website.

PCI security standards recommends that for eCommerce transactions, firms should use OV or EV identity verified SSL certificates

“What should SSL certificates do for your official website?”



Show confirmed organization identity to prove to customers that it is our official website



Encrypt communications between our website and our customers

Base: 105 IT decision makers at large retail and financial services firms in the US
Source: A commissioned study conducted by Forrester Consulting on behalf of Entrust Datacard, March 2018

Browser UI: What Does “Secure” Really Mean?

1 2

Browsers Have A Responsibility To Help Distinguish Website Identity

One of the best ways to show the difference between different SSL types is with distinctive browser UI indicators. Some browsers do this today. An example of a DV certificate indicator (anonymous identity) and an EV indicator (confirmed identity) are below. Website owners rely on indicators like these to show customers they are at the official company website. Because of the ambiguity of the design, firms overwhelmingly agree that browsers must have a different UI indicator to show that the identity of a website is known (and that it is the official website) versus unknown or anonymous.

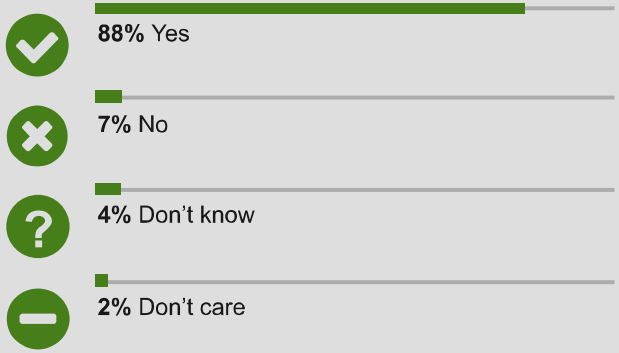
Sample DV certificate browser UI:

Secure | https:

Sample EV certificate browser UI:

Ultrabank, Inc. [US] | https:

“Imagine you are visiting a website that identifies itself by name as the company's official website. Do you think the browser's user interface (UI) security indicators should show a difference depending on whether the identity of the owner is known versus unknown/anonymous?”



Base: 105 IT decision makers at large retail and financial services firms in the US
Source: A commissioned study conducted by Forrester Consulting on behalf of Entrust Datacard, March 2018

Forrester Opportunity Snapshot: A Custom Study Commissioned By Entrust Datacard, May 2018

Browser UI: What Does “Secure” Really Mean?

To Protect Customers All Parties Must Work Together

Customer trust is both difficult for firms to earn-and very easy for them to lose. Criminals try to get one step ahead of retailers and financial services firms by creating more convincing lookalike sites with basic DV SSL encryption certificates which lack identity information, but receive the misleading “secure” and/or lock UI in browsers. To combat this, and keep customers safe, browsers, certification authorities (CAs), and website owners must work together to create and maintain distinctions between official websites, with confirmed identity information, and potentially unsafe ones, where the owner is anonymous, and educate customers on the important differences.

METHODOLOGY

› This Opportunity Snapshot was commissioned by Entrust Datacard. To create this profile, we surveyed 100 IT decision makers responsible for SSL technologies at their organization at US financial services and retail firms with 1,000 or more employees, who conduct online transactions through their website(s) and use encryption on at least some of their webpages. The custom survey was completed in March 2018. For more information on Forrester’s data panel and Tech Industry Consulting services, visit forrester.com.

Project Director
Andrew Magarie
Market Impact Senior Consultant