101domain.com Corporate Brand Services

SSL Certificates

Encryption is Coming. Is Your Business Prepared?

You've built your business and your brand. Now how do you secure and protect it?

CONTENTS

> SSL is a digital certificate that encrypts data in motion and authenticates connections online.

WHAT IS SSL?

Many people recognize “HTTP and HTTPS” as the beginning element in a website address. However, not everyone knows the function of the Hyper Text Transfer Protocol (HTTP). In HTTP, data is sent between your browser and the website you are on. HTTP websites are not generally considered encrypted or secure.

If HTTPS – the S for Secure, displays in the website address this means there is a secure connection via Secure Sockets Layer (SSL). SSL is the technology for encrypting this link between a web server and a browser.

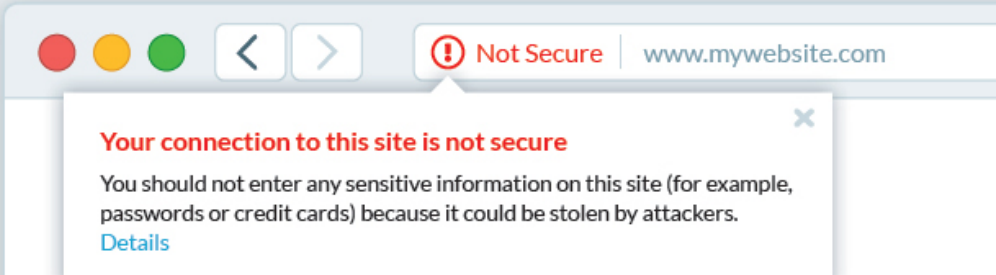
WHAT IS SSL *REALLY*, THOUGH?

When you add an SSL certificate to your website, you are encrypting sensitive information passed along your site. With an SSL certificate, you safeguard your business and your customers’ data by making sure that any data transferred between remains impossible to read for hackers.

SSL protects your customers from cybercriminals and builds brand trust with visual cues, such as a lock icon or a green bar. Creating the foundation of trust with a secure connection is essential for your success.

What type of sensitive information does an SSL Certificate protect?

- **Transaction and bank information**
- **Credit card information**
- **Usernames and passwords**
- **Contact information**
- **Search bar history**



WHAT ARE THE BENEFITS OF SSL?

The bottom line is people do business with brands they trust. Trust is the foundation of the Internet economy. To ensure that trust, you need end-to-end security with SSL.

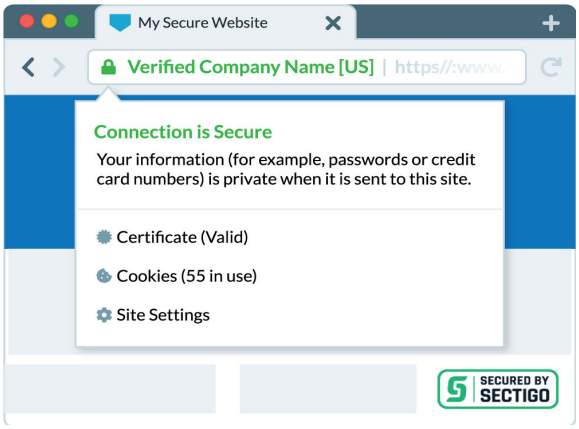
Websites without SSL are leaving one of their most valuable digital assets vulnerable. Hackers can target customers through email phishing campaigns or intercept private information passed along through a site. All it takes is a single breach to devastate a business.

- Inspire **trust/confidence**
- Boost **SEO** Rankings
- Increase **Conversions**
- Protect **Brand Reputation**
- **Future-Proof** Website

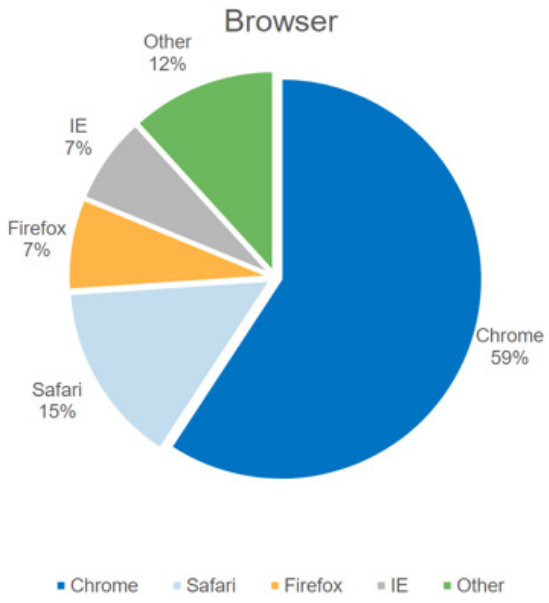
HOW WILL A VISITOR KNOW THE CONNECTION IS SECURED?

There are a few visual indicators that indicate a secure website. No matter which web browser you use, all browsers will display trusted visuals cues.

- HTTPS
- Padlock
- Company Name
- Trusted Site Seal



> *Over 50% of users choose Google Chrome as their preferred browser*



WHY IS SSL IMPORTANT?

As of now, having SSL is no longer an option, it's a requirement if you don't want to be left behind with the industry-wide shifts happening.

Online attacks are becoming more frequent and increasingly easy to execute. Organizations around the world are under increasing scrutiny to ensure online transactions involving confidential data are secure.

BROWSER MARKET SHARE

The internet is dark and full of terrors. Over the past few years, Google has taken steps to shed light on this issue and keep everyone on the web safe. Visual security indicators are more apparent now than ever to equip consumers with information to decide what companies they trust with their business.

In 2015, Google began to use HTTPS as a lightweight ranking signal in the search algorithm. Over time they have started placing more importance on implementing industry-leading security with SSL encryption, to encourage all website owners to make the switch.

Google's large browser market share means they have a significant influence on how the Internet operates and where it's going in the future. Google holds a substantial stake in SSL and favors sites that implement HTTPS across its entire site.

Since changes in treatment of HTTP went into effect

>78%

of page loads in Chrome over https

>68%

of page loads in Android over https

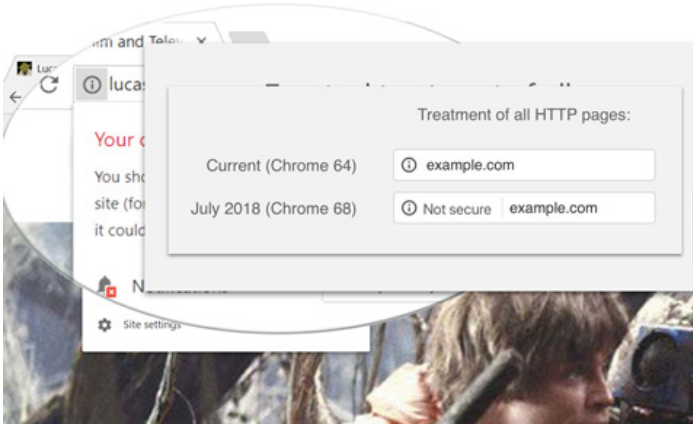
AVOID NON SECURE BROWSER WARNINGS

Many browsers trigger security warnings when a user attempts to enter a site with an unsecured connection. Google Chrome flags all non-encrypted websites as unsafe and even displays a Non Secure warning to deter customers from visiting them.

The Non Secure browser warning is the equivalent of someone standing outside the front doors of your business with a sign telling people not to go in.

The goal is to have your website served to as many people as possible and to give customers a great experience as intended. Companies who are serious about protecting customers and their business reputation should implement SSL across their digital properties.

Chrome Security Indicators



COMMON BROWSER ERRORS IN 2019

HTTP = Not secure | www.ufl.edu

HTTP + Contact Form = Not secure | www.ufl.edu/#

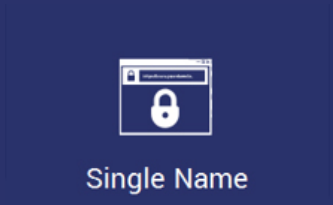
Invalid Cert Name = Not secure | ~~https~~://wrong.host.badssl.com

Expired SSL = Not secure | ~~https~~://expired.badssl.com

Self-sign SSL = Not secure | ~~https~~://self-signed.badssl.com

SSL certificates can be complex. To make things easier, we broke them down into 2 main differences:

- ✓ Types of Certificates
- ✓ Level of Validation



WHAT TYPES OF SSL CERTIFICATES ARE THERE?

There are a variety of SSL brands that range in type, price, and level of validation. Any SSL certificate will prevent browser warnings from driving traffic away from their sites, however, a website that deals with sensitive information, especially e-commerce sites, requires an SSL certificate that reflects a higher security standard with visual SSL indicators.

Single name – one certificate will cover one domain name. www and non-www versions are included for free.

Multi-domain – one certificate will cover multiple domain names and is ideal for specific server environments such as Microsoft Exchange and United Communication (UCC). Can include non-www versions for free for common name only, but not for multiple domain names.

Wildcard – one certificate will cover an unlimited number of sub-domains at a specific level – denoted with an asterisk symbol. The asterisk symbol can only secure one level, for example:

- **.domain.com* or **.secure.domain.com*
- but not **.*.domain.com*

Multi-domain wildcard – one certificate that covers multiple domain names and wildcard entries. Includes a common name and numerous domain names that can contain a mixture of regular and wildcard domain entries. One of the best SSL types on the market due to its complexity.

CHOOSTING THE RIGHT VALIDATION METHOD FOR YOUR BUSINESS

There are three levels of validation when it comes to SSL. Learn what each validation process entails so you can select the proper validation method for your business.

DOMAIN VALIDATION (DV)

DV certificates are a great introduction to SSL. With domain validation you are required to prove domain ownership in one of three easy ways:

1. **Email** Based Authentication
2. **File** Based Authentication
3. **CNAME/DNS** Based Authentication

A QUICK LOOK AT DV

BENEFITS OF DV

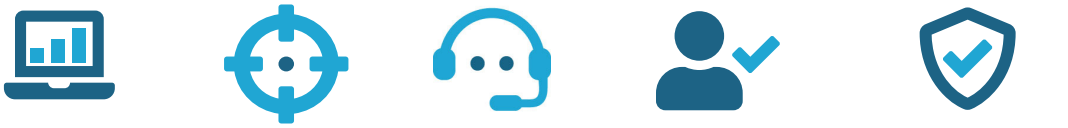
- Satisfies browser requirements
- Cost-effective
- Entry level encryption solution

WHO IS IT SUITABLE FOR?

- Non-registered businesses
- Low-traffic websites
- Short-term projects

ORGANIZATION VALIDATION (OV)

OV requires a light vetting process to prove your organization is a legitimate legal entity.
OV certificates are a nice middle ground SSL solution, as they aren't as expensive as EV options but still offer more SSL and trust indications than DV. There are **five requirements** involved in getting an OV.



Organization Authentication | Locality Presence | Telephone Verification | Domain Verification | Final Verification Call

EXTENDED VALIDATION (EV)

EV is the most premium type of validation method available. The most trusted sites in the world use EV. These certificates can be identified on websites primarily by the green address bar, the most universally recognized symbol of trust on the web. There are **seven requirements** involved in getting an EV.

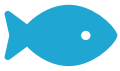
Organization Authentication | Enrollment Form | Operational Existence | Physical Address | Telephone Verification | Domain Authentication | Final Verification Call

DV VS. EV

DV certificates serve the purpose of satisfying browser requirements, but it's not the solution for everyone. Since the industry-wide rise in encryption standards, free and cost-effective solutions like DVs are commonly associated with phishing and fraudulent activity.

Select options like OV and EV require business level validation that helps overcome some of the dangers with DV. Business validated certificates also offer more control and better security indicators to assure customers you mean business.

Increase Site Transactions



Combat Phishing

Stay Compliant

Show Customers You Care

BENEFITS OF EV

EV certificates reassure customers of your website's value and security. The green address bar visually makes customers feel more confident in a website operator's identity, encouraging your users they are safe to proceed on your website. The enhanced validation process for EV certificates provides extra security against phishing and other criminal attacks involving fake impersonation sites.

Many standards and regulations such as **PCI-DSS, HIPAA, HITECH, SOC2 and GDPR** require that online businesses take measures to combat theft of confidential information online. EV is the most reliable protection an SSL certificate can offer.

"EV certificates maximize site transactions, including an increase in sales, web form completions, new user sign-ups, and engagements."

CAPITAL INVESTMENT

EV is an investment in web security that improves customer confidence and trust.

57.8%

uplift in feeling a site is trustworthy when using EV.

RISK MANAGEMENT

EV certificates reduce the risk of impact and probability of occurrence.

67.9%

uplift in feeling safe doing business online when using EV.

PREPARE YOUR DIGITAL ASSETS

Every website needs an SSL certificate. SSL is a single element in a holistic strategy to protect your brand, intellectual property, and domain portfolio.

Free and cost-effective solutions satisfy the bare minimum requirements, but do you want your company to rise above the basic industry standards and stand for more? More security for your website, more confidence in your brand, and more trust established with your customers.

Prepare your most important digital asset for the future and further your business objectives with SSL.

www.101domain.com
corporate@101domain.com
877.983.6624