# Encryption is Coming

## Simply having an SSL Certificate is not enough, you also need employ Always-On SSL

The internet is dark and full of terrors. Almost no one is safe. According to Symantec, just 3% of websites across the internet are currently encrypted. But that's all about to change. Encryption is coming! In reality, the current initiative to encrypt the entire internet has been in the works for a while. In fact, the browser community is already aggressively pushing for it in a number of ways:

- Browsers will soon start marking sites without HTTPS as non-secure
- Google is giving a search rankings boost to sites with SSL/TLS
- Browsers are mandating that HTTP/2 be deployed with Encryption
- Gmail is flagging messages that originate from non-secure servers
- Popular Mobile features are only available with Encryption
- Mozilla is only making new features available to HTTPS sites

As of now, having SSL/TLS is no longer an option, it's a requirement if you don't want to be left behind following these industry-wide shifts. And simply having an SSL Certificate is no longer enough, either. You need to serve your entire site over HTTPS. You need to configure your server for Always-On SSL.

## What is Always-On SSL?

Always-On SSL is a cost-effective security measure for websites that helps protect the entire user experience from online threats. It delivers authentication of the identity of the website and encrypts all information shared between the website and a user (including any cookies exchanged), protecting the data from unauthorized viewing, tampering, or use.

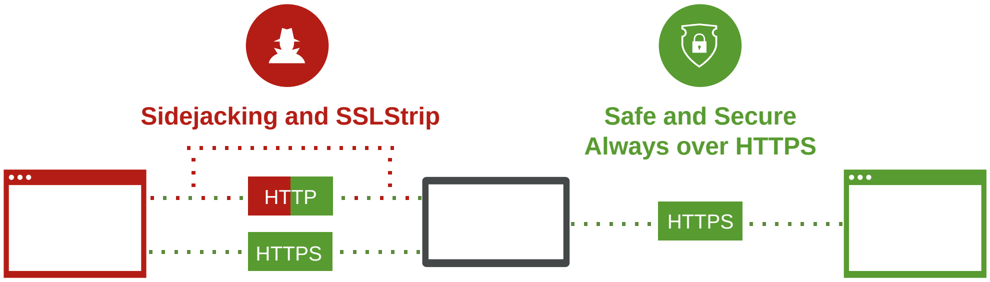
## The growing threat of data breaches

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. Take your organization's security to the next level with Always-On SSL.

## Why intermittent SSL is no longer enough

- **Intermittent SSL** – securing only the log-in and transaction pages. New threats such as Sidejacking and SSLStrip endanger consumer trust and compromise sensitive data

- **Always-On SSL** – securing the entire user session from start to finish. The entire session is secured and users are safe and secure from Sidejacking and SSLStrip



### What makes Always-On SSL different?

Intermittent use of SSL protects only certain pages, such as a website's login and transaction pages, leaving the rest of a user's session unsecured and open to attack.

Safe from start to finish - Always-On SSL delivers the same high level of SSL protection throughout the entire site, securing the visitor's complete session. Visitors will be safe with the reassuring HTTPS at the beginning of the browser address bar throughout their entire stay on your website, making it safer to search, share, and shop online.

### Why should I care?

Trust is the foundation of the Internet economy. To ensure that trust, you need end-to-end security to help protect every webpage your users visit, not just the login pages and shopping carts.

Companies who are serious about protecting customers and their business reputation should implement Always-On SSL with SSL certificates from a trusted Certificate Authority.

Google now favors websites that implement HTTPS across their entire site. Keep your visitors safe with Always-On SSL and Google will reward you with an SEO ranking boost.

Additionally, many browsers now trigger security warnings when a user is hopping between secured and unsecured connections. Ensure your customers experience your website as intended with Always-On SSL.

### What are the top 3 tips for moving to Always-On SSL?

1. Always speak with the Certificate Authority issuing your SSL Certificate as they will be able to provide you with guidance for proper implementation for Always-On SSL.

2. Un-encrypted gaps in your site will negatively impact your search ranking and website performance. If different parts of your website run on different servers, you may need to purchase additional certificates to implement Always-On SSL successfully.

3. When you switch to Always-On SSL, you are effectively moving your entire website to HTTPS, which is similar to moving to a new domain name. You need to be sure to redirect all the pages of your website to their new HTTPS counterparts and update your Google Webmaster tools.

### What SSL certificate should I use?

To reassure customers of a website’s value and security, it may be best to use an Extended Validation (EV) SSL certificate. The green address bar visually makes customers feel more confident in a website operator's identity, reassuring your users they are safe to proceed on your website.

### Conclusion

- Intermittent use of SSL encryption is no longer sufficient to protect your website visitors or safeguard against data compromise.
- Implementing Always-On SSL on your website secures the user and your organization’s data on every page – from start to finish.
- Always-On SSL is easy to implement for your website and requires no extra hardware.
- Boost your Google SEO ranking with Always-On SSL, a boost likely to increase in the future.
- Strengthen your brand and reputation by showcasing your commitment to online security.
- Increased user trust leads to lower bounce rates and shopping cart abandonments. The benefits: increasing online transactions and conversion rates.
- Use Extended Validation SSL for the highest visible display of online trust.

For more information:<br>
Phone: +1 (727) 388-4240

**The SSL Store™**
146 2nd St. N. #201
St. Petersburg, FL 33701 US
www.theSSLstore.com