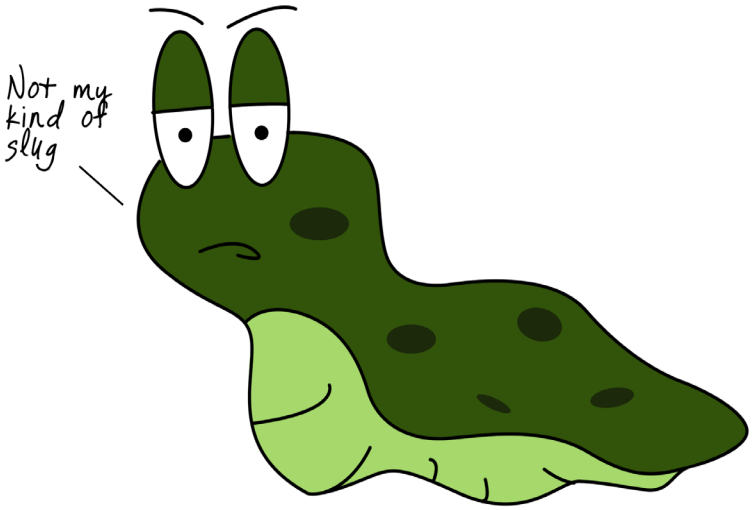
Is Your SSL Security Truly Secure?

What is a (SHA) SSL Certificate and what does it do?

As you venture out into the vast planes of the Internet, you'll notice that there are websites that show up with an HTTPS heading instead of HTTP or just WWW inside the address bar.

Further, you'll see these websites with a lock symbol or even a green bar. This is to show you that you've entered a website that has a secure and encrypted connection, using a Secure Socket Layer (SSL) Certificate from a trusted vendor (known as Certificate Authorities, or CA). It also provides the user knowledge that the website has been verified by the CA as the true website, and not a reproduction.

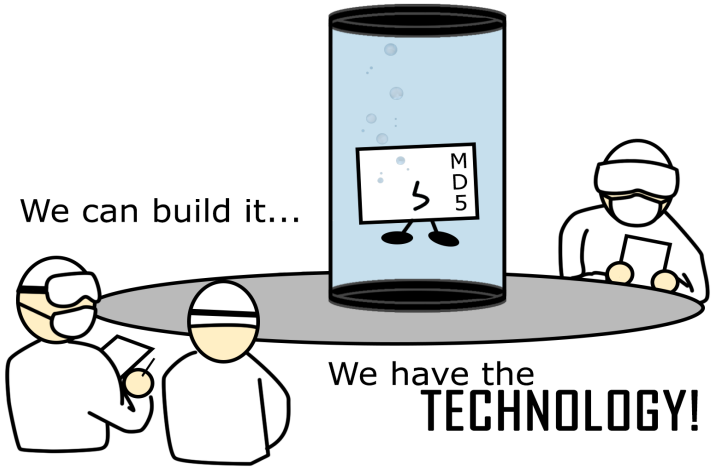
How does it work?



Like any encryption, it uses a complex math based algorithm that generates a unique signature or "slug". This is then compared to the cryptographic signature that the CA issued certificate has and your browser then verifies whether or not it's the real deal. One-way algorithms like SHA-1 are designed to produce unique, irreversible slugs. You should not be able to take a slug and work backwards to produce the encrypted data. As importantly, no other file should produce that same slug — even changing one little period should cause the SHA-1 result to change so drastically as to be unrelated.

Why the new push for SHA-2?

With the evolution of technology, computers being faster than ever before, eventually encryptions will have to be updated to keep secure. As we have learned with the past history of the SHA predecessor known as MD5, Google, Microsoft, among others, have been pushing for the updates to happen much sooner than later.



So what happened with the MD5 encryption? Well, it was proven in the mid 90's that it was a pretty weak encryption pattern, but it went ignored for well over a decade. In 2003, a group of researches successfully engineered a completely authentic looking fake MD5 certificate. Of course this has now been completely blacklisted off of every internet browser available, but the point was made that it was time to upgrade the encryption patterns to more suitable standards.

In 2005, cryptographers made a startling discovery that the SHA-1 encryption, following Moore's Law of Computing, was roughly 2,000 times easier to break than previously estimated. Despite being a much better standard of encryption that MD5, it is becoming more affordable to engineer a fake certificate to pass it as authentic. Estimates for engineering are as follows: $2M in 2012, $700K in 2015, $173K in 2018, and $43K in 2021. This means that it could be practical for a large crime syndicate to launch their own certificate in 2018 to steal data from unsuspecting users.

What are internet browsers doing?

Google Chrome, Opera, and Firefox are going to start showing in different levels how secure the encryption is on the website. Chrome, for example, inside the Address Bar you'll notice a Padlock with different symbols, and sometimes a green bar.

Browsers showing SHA-1 certificates that expire on or after January 1, 2017 "secure with minor errors" (Padlock with yellow triangle).

Sites with SHA-1 certificates that expire between June 1, 2016 and December 31, 2016 will show "secure with minor errors". Sites with certificates that expire on are after January 1, 2017 will be treated as "neutral, lacking security".

A red strike through HTTPS will be more prominently featured if the SHA-1 certificate expires AFTER January 1st, 2017. This won't show until mid-2015 on browsers.

Why the long timeline if this is urgent?

As fast as technology grows and becomes more secure, there are those that don't necessarily update their systems/browsers.

With this in mind, there needs to be a larger timeframe that's urgent enough to make the push, but doesn't force those with older software to make the upgrade immediately.

SHA-2 encryption does not work on systems using Windows XP SP2 and older, and can be a problem with Windows XP SP3 and Vista SP1. Browsers themselves will also need to be updated. For a full listing of what's compatible, check out: https://support.globalsign.com/customer/portal/articles/1499561.

What can I do about it?

To see if you have your SSL certificate already modernized, you can easily check your domain and test it via SSL Labs (https://www.ssllabs.com/ssltest/index.html) and/or SHAAAAAAAA (https://shaaaaaaaaaaaa.com/). If you notice that the results are giving you SHA-1 results, talk to your local IT team, or contact E-Tech and we can

help you upgrade your certificates for you. This in part means that with your chosen CA, we (E-Tech) must communicate with the CA in order to get the upgrade completed which may require login credentials to be presented to us (E-Tech) at the time of the upgrade.

What are the risks of upgrading now?

As mentioned before, older browsers and/or operating systems are incompatible with the newest edition of the SHA certificate. This also includes that some older mailing systems may be affected as well. Please refer to the chart for full compatibility requirements.

E-TECH computing

www.etechcomputing.com
contact@etechcomputing.com
(647) 361-8191
250 Consumers Rd, Suite 214
North York, Ontario
M2J 4V6