IN 2017 YOUR BUSINESS WEBSITE SHOULD WEAR AN "S"

By Dean Coclin

The number of cyber-attacks organizations come under every day is staggering - and growing every year. Attackers are always evolving and becoming more sophisticated. Yet they still rely on many of the same tactics they've been using for years to trick people into visiting fake web sites, or slip past companies' security systems. The

Certificate Authority Security Council (CASC), an advocacy group committed to the advancement of web security, is leading the effort to protect both your customers and your brand reputation by requiring visitors to your web site to add an "s" to the "http" in their browsers' address bars. Sounds simple, but behind that letter "s" are advanced security technologies and best practices that ensure your customers' interactions with you are secure.

The Threat Landscape

As we head into the busy holiday shopping and travel season, protecting your customers' information has never been more challenging in the face of the sheer number of attacks on organizations of all sizes and across all industries.

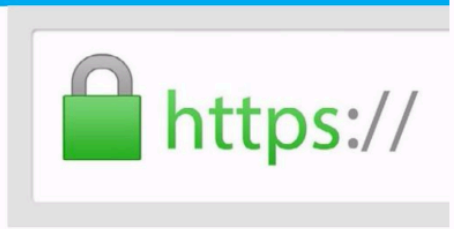
Successful attacks against large multinational enterprises and government agencies make news headlines. But small businesses are prime targets too.

71 percent of cyber-attacks are aimed at businesses with fewer than 100 employees, according to a report by the U.S. House Select Committee for Small Businesses. That's why the Committee recently advanced the Improving Small Business Cyber Security Act of 2016, which now awaits the Senate's consideration. The bill amends the Small Business Act to authorize the Small Business Administration (SBA) to make grants to small business development centers (SBDCs) to help businesses harden their security postures.

The SBA's Top 10 Cybersecurity Tips for small businesses includes recommending that businesses protect all pages on their public-facing websites, not just the checkout and sign-up pages. It's great advice for any size organization, and it's why CASC advocates for the adoption of digital certificate best practices and the proper issuance and use of digital certificates by Certificate Authorities (CAs), browsers (i.e., Firefox, Google Chrome, Microsoft Edge), and other interested parties.

Add the "S"

The four letters, "http", are known to technical and non-technical users alike as the beginning of any web address. That's about to change, and soon you won't be able to go to many popular web sites without using "https". This indicates that a web page uses the security protocol



known as TLS (formerly known as SSL) to indicate that encryption is in place between the server and the user's browser.

The adoption effort is well underway. Some of the biggest names on the Internet have already adopted HTTPS, including Facebook, Twitter and Netflix. Google announced more than a year ago that its adoption of what it calls "HTTPS Everywhere" will have a positive impact on search rankings. There are other business benefits. Google encourages site owners and their website managers to adopt https to gain a competitive advantage in search engine rankings.

As a small business owner, you and your website manager – whether that person is on-staff or you partner with a third party - should be aware of the six key ways this will affect your customers' experiences and interactions with your site:

1. Clear, visible warnings: Web browsers will use visual cues to alert users of non-https connections. For example, Google Chrome will highlight insecure pages with red X in the address bar. They will also warn if an insecure page asks for a password or credit card by showing the words "Not Secure". Firefox plans a similar warning for sites requesting passwords. In the future, both will transition from an information warning to a red triangle which is more noticeable.

2. Access to powerful features: Chrome will only be available over https. Services like Geolocation, Device Motion/Orientation, Full screen mode, DRM and more are strictly limited to https connections. Websites that need these features will have to implement SSL/TLS to utilize them.

3. Better, stronger, faster: http2 will replace the long-time standard http. It's much faster, which enables a more enjoyable and efficient user experience, while also strengthening the user's and company's security postures. This is supported by Chrome, Firefox, Internet Explorer, Safari and Opera, and http2 will require https. So as websites migrate to the speedier http2, they must use SSL/TLS.

4. Leveraging referrer data: Website managers strive to draw visitors from other sites via referrals. Moving forward, seeking referrer data from other sites will require the use of https. Without https, the destination sites won't know who is coming to their site.

5. New-look Gmail: Users of Google's popular email client will immediately know if a new message is secure or not. If the intermediary email servers do not all use SSL/TLS encryption, that message will include the image of an open padlock. Alternately, a message that does use SSL/TLS will include the details of the types of encryption that all of servers it originated from and passed through use.

6. Everywhere you look: Many sites have already made the transition to https, including Google's BlogSpot and Analytics, Reddit, Flickr, Wikimedia, WordPress, Bitly and Shopify. The U.S. Government requires all sites under the .gov domain must be https by the end of this year.

HTTPS is one of many recent advances in both the strength and adoption of SSL/TLS certificates. The major browsers are also changing their security indicators the colors and symbols used in the address bar to indicate to visitors how safe a site is to make it clear when an SSL/TLS-secured web page includes unsecured content that is vulnerable to man-in-the-middle tampering. In other words, this will make it clearer when a site fails to achieve always-on encryption and the danger this poses. This is just one example of the drive to offer added reassurance to websites visitors and online shoppers.

What Can You Do?

You also play a critical role in thwarting cyber-attacks and protecting your customers' sensitive information. Symantec reports that cybercriminals continue to take advantage of vulnerabilities in legitimate websites to infect users, because website administrators fail to secure their websites. More than 75 percent of all legitimate websites have unpatched vulnerabilities. Fifteen percent of legitimate websites have vulnerabilities deemed "critical," which means it takes trivial effort for cybercriminals to gain access and manipulate these sites for their own purposes.

You can also work to advance the education on effective website security to all parties involved –software vendors, web server administrators, even your customers. They can all contribute by getting developing an understanding of the threats and how to thwart them, and work together to place a high priority on security. That's why the CASC works actively with browsers, relying parties and other stakeholders to enhance internet security through practical, thoughtful measures and collaborative research.

About the Author

Dean Coclin is Senior Director, Business Development, at Symantec and a member of the CA Security Council.

February 7-9, 2017

Future Stores Miami

Future Stores Miami brings together retail executives to discuss in-store experience design, innovation and technology with the idea that reimagining physical stores is the key to growth and continued success in today's competitive, omni-channel environment.

February 14-16, 2017

Merchant Payments Ecosystem

MPE is the leading European event on merchant payments. One big expo with 3 parallel conferences!

February 27 - March 2, 2017

eTail West

Born in 1999, eTail is where the top minds at America's most successful retailers meet and learn. eTail is a global series with major events serving the United States, Europe and Asia throughout the year.

March 19-22, 2017

Shoptalk

Shoptalk is the new blockbuster retail and ecommerce event with 5,000+ attendees, 250+ speakers and 500+ CEOs expected at its 2017 event. An unprecedented gathering of individuals and companies reshaping how consumers discover, shop and buy.

Want to add a trade show?
Click here to contact us.