HubSpot Academy

Transcript: Implementing Website Security Best Practices

Video 1: The Importance of Website Security

How important is website security really? Well, 85% of people will not continue browsing if a site is not secure. Think about that — 85%. Imagine the traffic, leads, and revenue that you would lose as a result. Would you visit a website after seeing a security warning like this telling you that your connection is not private?

Web security is good for website visitors, customer data, and your business' reputation. In fact, 56% of all internet traffic is from an automated source such as hacking tools, scrapers and spammers, impersonators, and bots. This means having a secure website has never been more important for protecting your data.

Think about some major global businesses who have seen data breaches in the past few years. Equifax, Target, and Sony come to mind. These cases resulted in the exposure of hundreds of millions of online user information. Not to mention the fact that it cost the businesses millions of dollars to resolve in court settlement.

But big businesses are not the only ones who are susceptible to data breaches. Small-to-medium sized businesses, or SMBs, and Ecommerce Businesses are at risk online. Organizations providing online services, like ecommerce companies, contributed to the largest number of compromised credentials at over 2 billion. And small to medium-sized businesses are especially at risk.

You might see corporations in the headlines as top data breach victims, but it's actually SMBs that hackers prefer to target. SMBs have more digital assets that are more valuable than an individual online, but less security than a larger enterprise-level company. Security breaches are frustrating and frightening for both businesses and consumers. Studies show that, after a company data breach, many people take a break from shopping at that business — and some people quit shopping there altogether. But cybersecurity is about more than just avoiding a PR nightmare. Investing in cybersecurity builds trust with your customers. It encourages transparency and reduces friction as customers become advocates for your brand.

Video 2: Using HTTPS and Removing Security Vulnerabilities

Have you ever noticed that some URLs start with "http" and others with "https"? Perhaps you noticed that extra "s" when you were browsing websites that require giving over sensitive information, like when you were paying bills online. To put it simply, the extra "s" stands for secure. This means that your connection to that website is secure and encrypted. Any data you enter is safely shared with that website. The technology that powers that little "s" is one of two technologies: SSL or TLS.

SSL, or Secure Sockets Layer, is the standard security technology for establishing an encrypted link between a web server and a browser. TLS is a newer technology that also authenticates websites. TLS, or Transport Layer Security, is a protocol that provides authentication, privacy, and data integrity between computer applications. I won't go into detail about the technical differences between SSL and TLS. But just know that in many ways, TLS has superseded SSL. TLS is newer and arguably more secure. But don't worry, the certificates you used to implement the TLS and SSL protocols are often interchangeable. So from here on out, we'll look

at solutions for SSL and TLS together since they're often one-in-the-same. Both of these technologies make sure that all data passed between the web server and browser are private.

When you fill out a form on an unsecured website and hit "submit," the information you just entered can be intercepted by a hacker. This information could be anything from details on a bank transaction to high-level information you enter to register for an offer. In hacker language, this "interception" is often referred to as a "man-in-the-middle attack." The actual attack can happen in a number of ways, but one of the most common is this: A hacker places a small, undetected listening program on the server hosting a website. That program waits in the background until a visitor starts typing information on the website. It will activate to start capturing the user's information, like an account login and password, and then send it back to the hacker.

When you visit a website that's encrypted, your browser will form a connection with the web server, look at the certificate, and then bind together your browser and the server. This binding connection is secure. That means no one besides you and the website you're submitting the information to can see or access what you type into your browser. This connection happens instantly, and in fact, many suggest it is now faster than connecting to an unsecured website. You simply have to visit a website with a certificate, and voila: your connection will automatically be secured.

There are a few ways to know if your website has a certificate. Use HubSpot's Website Grader. The URL says "https" and not "http". You see a little padlock icon in the URL bar. Or the certificate is valid. In your web browser, you'll be able to tell if a site is secure because it will say "https" and you'll see a little padlock icon in the URL bar. It'll show up either on the left- or right-hand side of the URL bar, depending on your browser. You can click on the padlock icon to read more information about the website and the company that provided the certificate. Even if a website has the "https" and a padlock icon, the certificate could still be expired — meaning your connection wouldn't be secure. In most cases, a site that displays as https will be secure, but if you encounter a site that asks for a lot of personal information, it may be worth double-checking to be sure the certificate is valid.

To find out whether your certificate is still valid in Chrome, go to View > Developer Tools. From there, you will need to navigate to the Security tab and you can see if the SSL certificate is valid or expired. If you click the "View certificate" button, you will be able to see more information about the SSL certificate and the specific date it's valid through. So how can you get a certificate on your website? The first step is to determine what type of certificate you need. For example, if you host content in multiple platforms, on separate domains or subdomains, it may mean that you need different certificates. For most, a standard certificate will cover your content, but for companies in a regulated industry — such as finance and insurance — it may be worth talking with your IT team because there are specific requirements within your industry that specify the type of SSL certificate you need.

The cost of certificates vary. You can get a free certificate or pay a few hundred dollars per month to obtain a custom certificate. Let's Encrypt offers certificates at no cost, but the setup is technical. Work with a web expert to get set up. These certificates expire regularly, so you'll need to make sure they stay up to date. Many other domain providers will sell certificates that generally range from $50 to obtain a certificate for one domain, up to a few hundred dollars for multiple domains. This process will be easier than using Let's Encrypt, but does have a cost associated with the certificate. One of the other key considerations is the validity period

of a certification. Most standard certificates that you purchase are available for one to two years by default, but if you're looking for longer-term options, then look into more advanced certificates that offer longer time periods.

If you're using HubSpot, all files hosted with the HubSpot File Manager are automatically encrypted with SSL. With the HubSpot CMS Hub, you can direct all visitors to the secure version of your site, no plugins required. If you're using WordPress, there are many plugins that can help you install your certificate. Really Simple SSL, Insecure Content Finder, and WordPress Force SLL can be used to install your certificate, encrypt files, and direct traffic to the secure version of your site. Websites currently not on https will need to migrate their website from http to https. Depending on the CMS that you're using, this may be as easy as clicking a button to download a certificate and redirect your pages. For others, you might have to manually set up redirects to your new https URLs. Check out the resources for some helpful guides or work with your web team to set up a migration plan. Beyond SSL, there are other ways you can keep your visitors safe online.

There are front-end JavaScript libraries with known security vulnerabilities that you should avoid at all costs. A front-end JavaScript library is a library of prewritten JavaScript which allows for easier development of JavaScript-based applications. But not all libraries are created equally, and intruders know this. Intruders have crawlers that scan your site for known security vulnerabilities. When the web crawler detects a vulnerability, it alerts the intruder. From there, the intruder just needs to figure out how to exploit the vulnerability on your site. Scan your website in HubSpot's Website Grader to identify if your page is using any JavaScript libraries with known vulnerabilities. To fix JavaScript library vulnerabilities, you should stop using vulnerable JavaScript libraries immediately, upgrade your libraries to their newest version and continue using if it fixes the vulnerability, or use a different library without known vulnerabilities. To find which JavaScript libraries are causing you trouble, we recommend following Google's resource. I've linked to it in the resources. You may need to work with a developer to help you find which JavaScript libraries are causing you trouble. Security is practically a requirement today online.

Today, search engines will call your webpage out for not having an SSL certificate. Search engines are taking their user's cybersecurity into top consideration. With an SSL certificate and by removing vulnerabilities in your JavaScript, you will keep your visitors' best interest at the forefront of your website.