What are web site certificates?

If an organization wants to have a secure web site that uses encryption, it needs to obtain a site, or host, certificate. There are two elements that indicate that a site uses encryption:

- a closed padlock, which, depending on your browser, may be located in the status bar at the bottom of your browser window or at the top of the browser window between the address and search fields
- a URL that begins with "https:" rather than "http:"

By making sure a web site encrypts your information and has a valid certificate, you can help protect yourself against attackers who create malicious sites to gather your information. You want to make sure you know where your information is going before you submit anything.

If a web site has a valid certificate, it means that a certificate authority has taken steps to verify that the web address actually belongs to that organization. When you type a URL or follow a link to a secure web site, your browser will check the certificate for the following characteristics:

1. the web site address matches the address on the certificate
2. the certificate is signed by a certificate authority that the browser recognizes as a "trusted" authority

If the browser senses a problem, it may present you with a dialog box that claims that there is an error with the site certificate. This may happen if the name the certificate is registered to does not match the site name, if you have chosen not to trust the company who issued the certificate, or if the certificate has expired. You will usually be presented with the option to examine the certificate, after which you can accept the certificate forever, accept it only for that particular visit, or choose not to accept it. The confusion is sometimes easy to resolve (perhaps the certificate was issued to a particular department within the organization rather than the name on file). If you are unsure whether the certificate is valid or question the security of the site, do not submit personal information. Even if the information is encrypted, make sure to read the organization's privacy policy first so that you know what is being done with that information.

Can you trust a certificate?

The level of trust you put in a certificate is connected to how much you trust the organization and the certificate authority. If the web address matches the address on the certificate, the certificate is signed by a trusted certificate authority, and the date is valid, you can be more confident that the site you want to visit is actually the site that you are visiting. However, unless you personally verify that certificate's unique fingerprint by calling the organization directly, there is no way to be absolutely sure.

When you trust a certificate, you are essentially trusting the certificate authority to verify the organization's identity for you. However, it is important to realize that certificate authorities vary in how strict they are about validating all of the information in the requests and about making sure that their data is secure. By default, your browser contains a list of more than 100 trusted certificate authorities. That means that, by extension, you are trusting all of those certificate authorities to properly verify and validate the information. Before submitting any personal information, you may want to look at the certificate.

How do you check a certificate?

There are two ways to verify a web site's certificate in Internet Explorer or Firefox. One option is to click on the padlock icon. However, your browser settings may not be configured to display the status bar that contains the icon. Also, attackers may be able to create malicious web sites that fake a padlock icon and display a false dialog window if you click that icon. A more secure way to find information about the certificate is to look for the certificate feature in the menu options. This information may be under the file properties or the security option within the page information. You will get a dialog box with information about the certificate, including the following:

- who issued the certificate - You should make sure that the issuer is a legitimate, trusted certificate authority (you may see names like VeriSign, thawte, or Entrust). Some organizations also have their own certificate authorities that they use to issue certificates to internal sites such as intranets.
- who the certificate is issued to - The certificate should be issued to the organization who owns the web site. Do not trust the certificate if the name on the certificate does not match the name of the organization or person you expect.
- expiration date - Most certificates are issued for one or two years. One exception is the certificate for the certificate authority itself, which, because of the amount of involvement necessary to distribute the information to all of the organizations who hold its certificates, may be ten years. Be wary of organizations with certificates that are valid for longer than two years or with certificates that have expired.

Authors

Mindi McDowell and Matt Lytle