

ITS SECURITY TOPICS

Operations Security Branch
Infrastructure Operations Division
International Technology Services



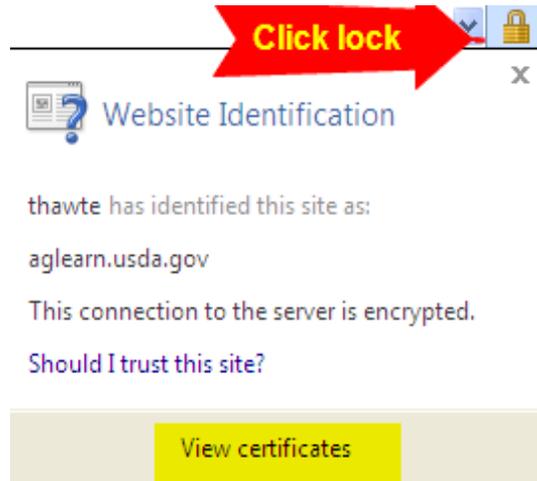
Verify the Legitimacy of a Website

A malware infested website may appear as realistic as an authentic website. Therefore, consider these specific strategies to verify the legitimacy of a website.

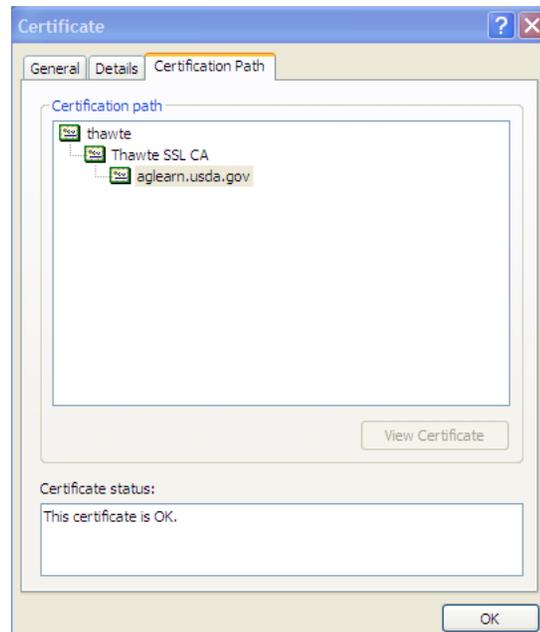
1. How did you obtain the URL for this website?
 - a. Did it come in an email? If so, question the legitimacy of it. Did someone you know send the email? If so, compose a new email or call that person to confirm that he or she sent it to you.
 - b. Did you find it via an online search? If so, do not automatically assume that the URL is authentic.
 - c. Focus on the URL. Many attackers will substitute letters and numbers to fool users. For example, they may use www.bankOfamerica.com instead of www.bankofamerica.com.
2. While appearances can be deceiving, it is still a good practice to examine the layout of the website. Does it look official? Does the website use appropriate grammar and punctuation?
3. What action is the website requesting of you? Is it asking for personal information such as your social security number and birth date? Are those reasonable requests for the context of the website?

4. Does the site begin with https? If so, this signals that there is a secure connection between your computer and the website. Data sent through the secured connection is encrypted in both directions. The encryption protects financial and sensitive transactions.

a. To check for encryption, click the padlock or site identity button in the browser bar to view the SSL certificate.



b. Click [View Certificates] to check the certification path.



c. The primary SSL certificate providers are Verisign, Entrust, Thawte, InstantSSL, Baltimore and Geotrust.