Determining the Legitimacy and Security of a Website

Overview

This article provides general tips to determine if a website is legitimate or secure.

Is the Website Legitimate?

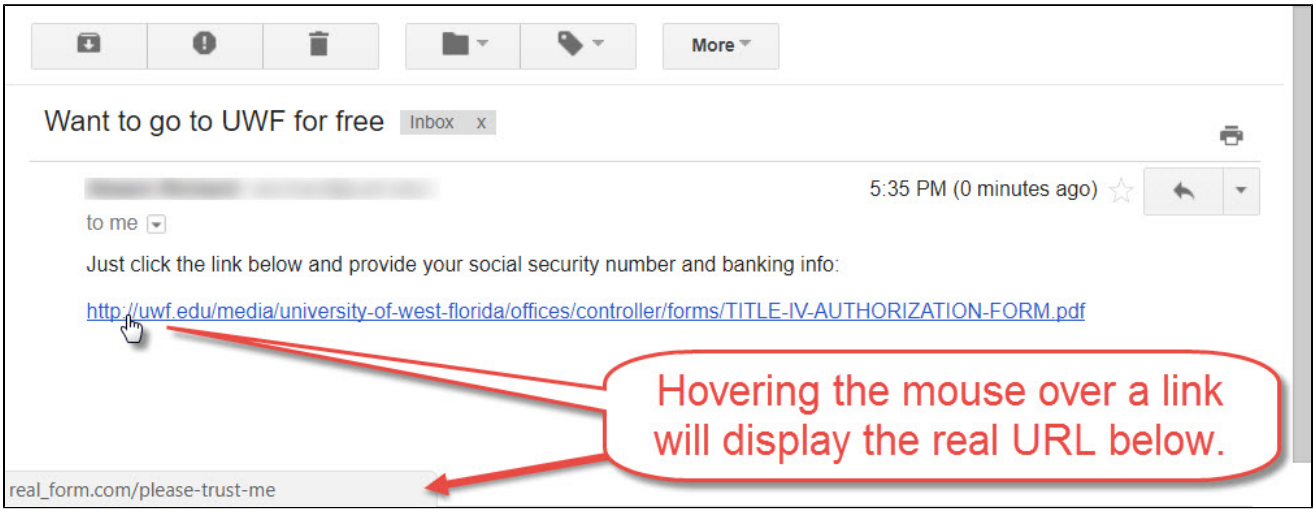
A **domain name** is the name of a website. For example, **uwf.edu** is a domain name.

It's very difficult for scammers to create fake websites with **https://uwf.edu** as the domain name. But scammers can create websites that have URLs similar to the official address. Users must pay close attention:

- ✅ https://uwf.edu/helpdesk (many UWF websites will have **uwf.edu/** at the beginning of the URL)
- ✅ https://learnmore.uwf.edu/ (this URL has **uwf.edu/** nearly at the beginning, but this URL is still valid because a period separates **learnmore** and **uwf**)
- ❌ https://learnmore-uwf.edu/ (even though **uwf.edu/** comes nearly at the beginning, this URL isn't valid because a hyphen separates **learnmore** and **uwf**, not a period)
- ❌ https://university_west_florida.com/ (this URL doesn't have **uwf.edu/**)
- ❌ https://financial-forms.com/uwf.edu/forms (this URL goes to **financial-forms.com/**)
- ❌ https://uwf.edu.free_money.com/ (this URL actually goes to **free_money.com/**)

By checking the address bar, you can verify that the site you accessed did not "redirect" you to a different site. Some attackers will use a "redirect" method to gather data. When redirected, you may click or access a link for a known site and may be sent to another. For example, accessing Amazon should bring you to a website with the web address of "amazon.com." If the address bar shows a different website, the website may not be legitimate. Please see the FAQ for further information about web addresses.

Also note you can hover over links on webpages and emails to see what their actual URLs are. See screenshot below for an example.



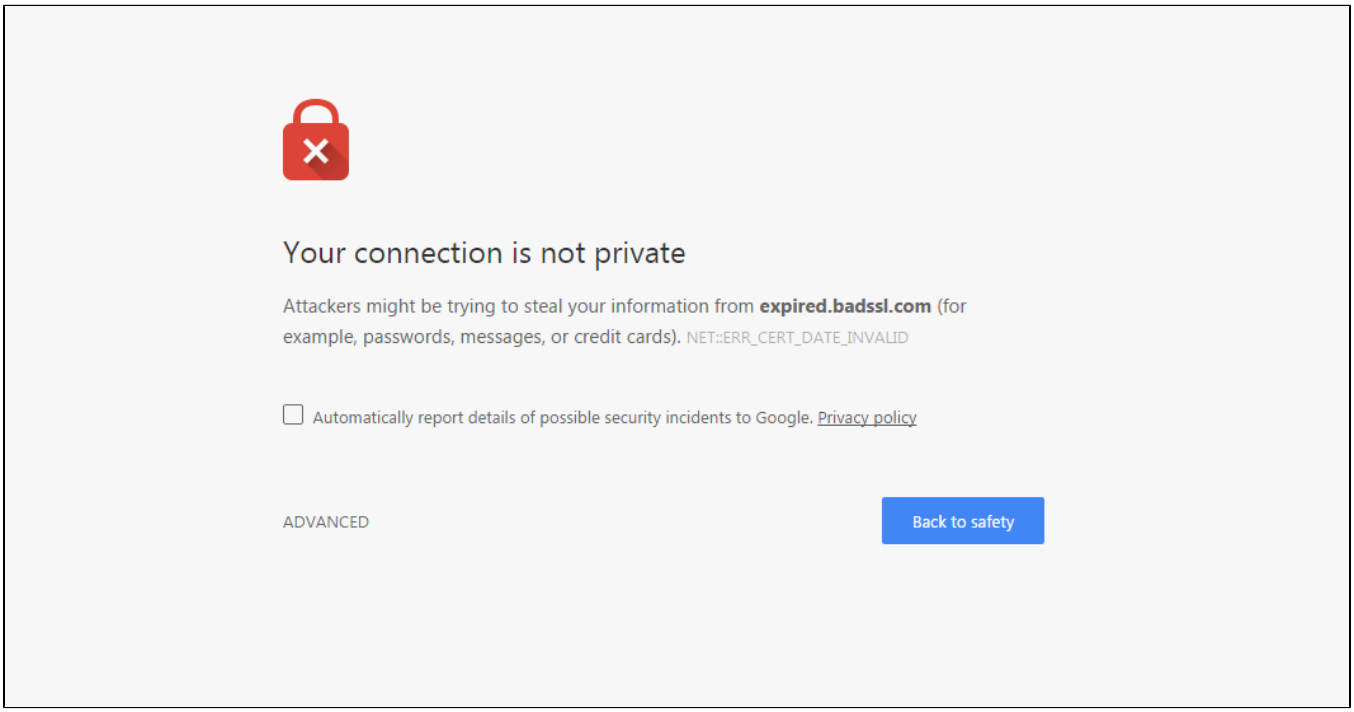
Many scammers realize that users accidentally mistype URLs. For example, some users will type **gmial.com** when trying to access Gmail. Scammers could then simply purchase the **gmial.com** domain for their website, and imitate Gmail's login screen. So when people go to **gmial.com**, see something that looks like Gmail, and provide their login credentials, now the scammers have compromised these users Gmail accounts.

Simply put, always ensure that the URLs you visit are accurate.
Users may choose to shorten their links, for example, to fit into a 240-character Twitter post. However, in most other instances, tiny links should be avoided, as character limits are usually not an issue, and you won't know where that tiny link leads until after you click it.

Please note one major exception – tiny links to Confluence pages. This is an exception because users can tell where the link comes from; a tiny link from Confluence still begins with **confluence.uwf.edu**. But with most other tiny links, users can't tell where the original link came from (e.g., https://bit.ly/32uPBBt this link is safe).
Check the website itself before conducting business with the website. Usually, at bottom of a website, there is an option called "Contact Us." If you do not trust a website, contact the company using the contact information listed. If you do not receive a response (or you notice the phone number is out of service), the site may not be legitimate.

Please know that malicious websites may have contact info as well. So don't assume a website is good simply because it has this info listed on its website. Legitimate businesses try to keep their websites professional in appearance and behavior. Check the website for things such as spelling errors, major grammatical errors, or readability ("Does the text make sense?"). Sites with these sorts of errors may not be legitimate. Trust your instincts. If the page does not look right, it may not be.
A common method of investigating the legitimacy of a site is to use a major search engine (such as Google). Feel free to refer to VirusTotal's tool to check for possible vulnerabilities (use the "URL" tab to scan the site).

When trying to connect to an illegitimate website, your web browser may prompt you with an error message. If you receive a message like the one below, the website may not be legitimate.



Is the Website Secure?

If there is a lock symbol located before the address in the address bar, you are using a private connection. If a website has private connections, it usually is a secure website.

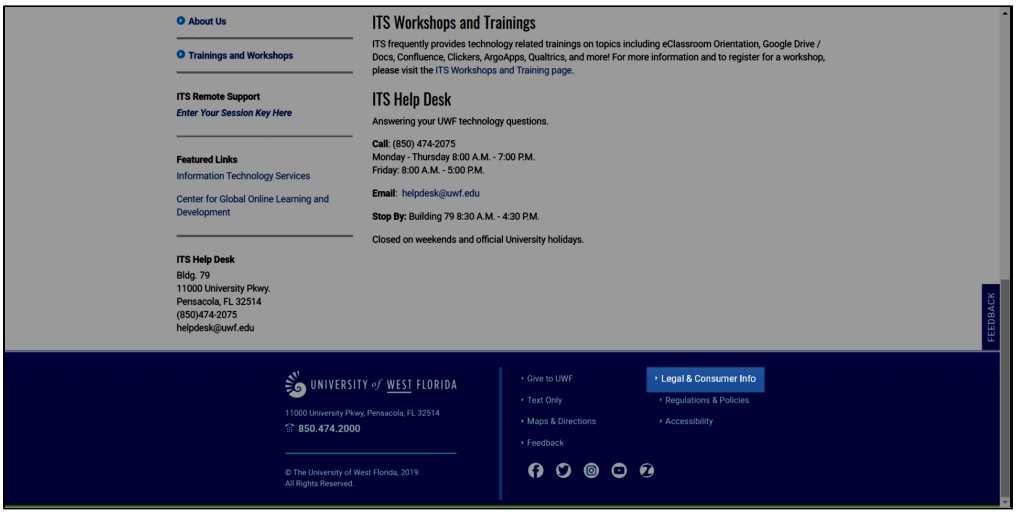
"http" stands for "**h**yper**t**ext **t**ransfer **p**rotocol"; the **s** in "https" stands for "secure." All websites used to begin with "http," but recently, with all the security breaches and advances in technology, more and more websites are moving to "https."

"https" helps to ensure that the website you're visiting is actually the site you intended to visit.

Please know that there are still many legitimate websites using the old "http." Not all legitimate sites use or need to use a secure connection. This does not mean that you cannot trust a legitimate website, but you should exercise caution when using the site.

Also know that a site isn't automatically safe because it begins with "https". This only helps to ensure scammers aren't impersonating sites they don't own. However, scammers could simply purchase the "https" security certifications for their illegitimate websites.
A website's privacy policy will state how data is collected on the company's website. If you're concerned about the data the website may be gathering, refer to their privacy policy. If you're unable to easily locate the website's privacy policy, the site may not be secure.

Below is an example of what appears at the bottom of most uwf.edu webpages:



Before continuing to the tips below, please ensure that the website is legitimate by following the tips listed in the "Is the Website Legitimate?" section of this article.

- Do not log into a website unless you trust it.
- If you do not feel comfortable logging into the website, do not log in.
- If you logged into a site, be sure to log out as soon as you're finished using it.

ITS Help Desk

(**850) 474-2075**
helpdesk@uwf.edu