Najee Shelton

2/27/2024

Week 6 Journal Entry

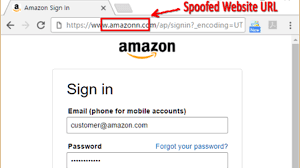
After going online to find good examples of fraudulent websites I found three which I believe to be very simi.ar to their original counterpart but can still be pointed out as a fake. The following pictures below show online resources that are counterfeit and will have a description for why users online believe they are real, and how one can know it’s fake.

Photo 1



The first photo shown was a photo that was provided from google via an article about fraudulent websites the link will be provided below. This website appears to be very similar to Facebooks home page but, the major thing to note is that the URL doesn’t reflect the website the user is currently using, whenever a user visits a website, and the URL doesn’t match there is a very real possibility that the website is fake and used to trick people into giving up important information.

Photo 2

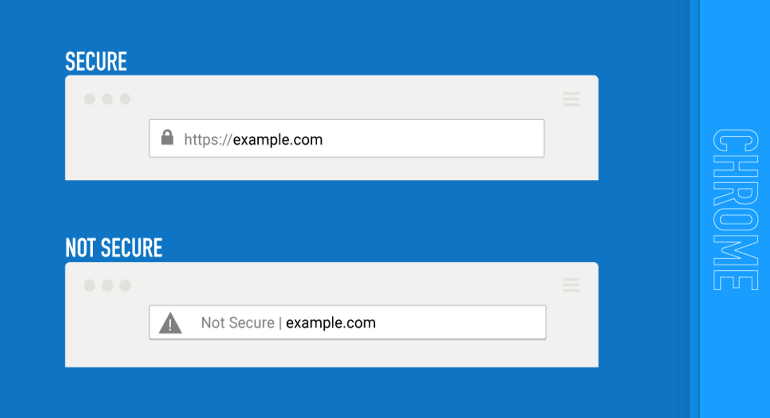


This next photo shares a similar error as the first, but this time the name of the website is spelt incorrectly, whether it be because the original website name is already taken or if the user didn’t pau close enough attention before they clicked the link. It’s very important for users to pay attention to the things they click they should always look out for small errors, the example provided in class was a great example.

* **Websiteo**
* **Website0**

Both names seem similar but one is clearly different if paying close attention users commonly don’t catch on to these things because they are so similar.

Photo 3



The final photo I chose was two example websites with one key difference one has a lock indicated its secure while the author doesn’t which means it isn’t secure. More often than not if you are familiar with a website and notice that it isn’t secure when you visit it it’s most likely fake, granted not all legitimate websites are secured but most are, having IDPS and security features enabled can greatly help mitigate this risk.