The fake websites I have chosen use typosquatting to take advantage of victims. Simple changes to the real website's URL can trick users into believing they are clicking on a safe link when, in reality, the websites are trying to steal your information. For example, “goggle.com,” “twiter.com,” and “micr0soft.com” have clear, minute changes to the legitimate URL but take the user to an entirely different website. These sites contain fake, authentic-looking pages that may prompt the user to enter their private account details, or unwanted, malicious files can be downloaded to your computer through a drive-by download. This simple exploit has been used for many years and will continue to be an effective method due to the carelessness of users.

Real Websites

https://www.google.com/

https://twitter.com/ or x.com

https://www.microsoft.com/en-us/