We are in an era where online transactions and interactions are very popular. A comparison of three hypothetical fake websites with three legitimate counterparts reveals distinct features that highlight their fraudulent nature. For instance, a fake online store might use a URL resembling "www.shop-fantastic-deals.com," while a real website such as Amazon operates under "www.amazon.com." Fake sites often use misspelled URLs or slight variations in domain names to mislead users (Coclin, 2021). Furthermore, these counterfeit platforms may lack essential site seals that verify security and authenticity. Another characteristic of fraudulent websites is their presentation of unbelievable offers, which can be enticing but should raise red flags for consumers. A phishing site mimicking a bank's login page may promise extraordinary interest rates compared to the real bank's official site. This tactic exploits psychological vulnerabilities by appealing to greed (Toohil, 2023). Additionally, while legitimate sites utilize TLS/SSL encryption indicated by a padlock symbol in the browser address bar, many fake sites either lack this feature or misrepresent it through deceptive graphics. Moreover, the absence of professional design elements can further distinguish fake websites from authentic ones. Legitimate platforms typically exhibit polished layouts and comprehensive contact information. In contrast, fraudulent sites may present poorly designed interfaces with excessive pop-ups or ads intended to install malware (Alkhalil, 2021). Overall, recognizing these distinguishing characteristics is crucial for navigating the digital landscape safely.