Clifford Osei

CYSE 201

February 27, 2024

Journal Entry 6

One of my favorite websites to shop on is Nike, but this fake website was commonly used to sell counterfeit items, particularly from the world’s favorite brands, and more so during popular events. In 2023, various [fake websites impersonated Nike’s site](https://www.soleretriever.com/news/articles/nike-sues-100-fake-sneaker-sellers-june-2024) during the FIFA World Cup. These sites offered “exclusive” deals on Nike products, such as Air Jordans, at significantly lower prices, pressuring Nike customers to make quick purchasing decisions to avoid losing the deal. Like in the other scenarios previously discussed, the URL was very similar to that of the legitimate site. Another fake website is PayPal at one moment, In late 2023, a series of [fake websites replicating PayPal’s](https://www.aura.com/learn/paypal-scams) login page tricked customers into entering their account details. Hackers created these fake websites with URLs like PayPal’s, such as “paypaysecurity.com” or “paypa1.com,” and complemented this with a website layout identical to the originals. Hackers used phishing techniques, such as email notifications about an alleged account issue, to prompt users to log into their ‘PayPal accounts.’ However, these were fake websites designed to look like the legitimate PayPal site. Once, users submitted their details, hackers could steal their credentials, take over their accounts, drain their balances—or carry out a combination of these actions. This attack affected thousands of users and resulted in millions of dollars in estimated losses. While the exact number wasn’t divulged, just a few years earlier, in 2020, Action Fraud determined victims lost [$8 million](https://www.cityoflondon.police.uk/news/city-of-london/news/2020/november/fraud/fake-paypal-emails-lead-to-nearly-8-million-in-losses-this-year/) in PayPal scams during that year. Lastly, apple. There are fake iPhones, Macbooks, iPods, and even… [fake Apple customer service websites](https://9to5mac.com/2022/05/20/apple-support-scam/). Over the last few years, fake websites impersonating Apple support have targeted users seeking help solving Apple device malfunctions. These fake websites used [SEO poisoning](https://www.memcyco.com/home/what-is-seo-poisoning/) techniques to appear on top of Google results pages for keywords like “iPhone not charging,” leading Apple customers to click on the link without much thought. The hackers aimed to persuade frustrated Apple customers to call a fake support number and thousands of customers did. During the call, they were lured into buying other items or services.

 In all , Fake websites for Apple, PayPal, and Nike often mimic real ones but have key differences. Fake sites typically have misspelled URLs (e.g., apple-shop.com, paypal-verification.com, or nike-outlet.shop), poor design, and low-quality images. They often lack HTTPS encryption, display urgent warnings (especially PayPal scams), or offer unrealistic discounts (common in fake Nike stores). In contrast, real websites have official domains (apple.com, paypal.com, nike.com), high-quality branding, secure payment options, and strong encryption. To spot a fake, always check the URL, security certificate, and deal legitimacy, as scammers rely on deception to steal login credentials and financial information.