Mohammad Sulaiman

Professor Teresa Duvall

CYSE 201S

03/06/2024

<div align="center">Journal Entry 6: Real and Fake Website Comparison</div>

Spotting fake websites involves identifying key differences from legitimate ones. Fake sites often use URLs resembling well-known brands with slight alterations. Their design may lack professionalism, featuring inconsistent layouts and excessive ads. Legitimate sites maintain clean designs with intuitive navigation. Additionally, fake sites often lack clear contact information, HTTPS encryption, and security seals. They may offer unrealistic discounts and have grammar errors in their content. In contrast, real websites prioritize user security, provide valid contact details, and offer competitive pricing with proper grammar. These distinctions help users avoid falling victim to scams online.

Now, let's compare three fake websites with three real ones:

Fake Websites:

1. "discount-apple-store.com" - Offers heavily discounted Apple products with poor website design and spelling errors.

2. "freevirusdownloads.com" - Claims to offer free antivirus software but lacks HTTPS encryption and contact information.

3. "yourbankonline-login.net" - Mimics a bank's login page but has a suspicious URL and lacks security features like HTTPS encryption.

Real Websites:

1. "apple.com" - Features a professional design, HTTPS encryption, clear contact information, and realistic product pricing.

2. "norton.com" - Provides antivirus software with HTTPS encryption, trust seals, and clear contact options for customer support.

3. "chase.com" - A bank website with a secure login portal, HTTPS encryption, and verified contact information for customer inquiries.

By comparing these examples, it's evident that fake websites often exhibit characteristics like suspicious URLs, poor design, lack of security features, unrealistic deals, and errors in content, while real websites prioritize user trust, security, and professionalism.