T2025_24 Beware of Typosquatting and Homograph Attacks (September 30, 2025)

Cybercriminals often register domains that mimic legitimate websites using typosquatting (e.g., “amaz0n.com” instead of “amazon.com”) or homograph attacks with look-alike characters from different alphabets, making these fake sites nearly indistinguishable from the real ones, especially on mobile devices where full URLs are hidden. These sites are used to steal credentials, spread malware, or trick victims into fraudulent transactions. To stay safe, always inspect URLs carefully for misspellings, unusual characters, or suspicious domain extensions, use bookmarks for frequently visited financial or business sites, avoid clicking links in emails, and enable browser security features or extensions that detect phishing and homograph attacks.

References

- MetaCompliance. (2024, June 3). The Dangers of Typosquatting: Harmless Mistakes, Serious Risks. MetaCompliance. Retrieved from MetaCompliance. https://www.metacompliance.com/blog/security-awareness-training/typosquatting

- Dörrie, H. (2017, April 20). Cybersquatting: Beware of homograph attacks! Retrieved from IPTalk. https://iptalk.com/2019/04/01/cybersquatting-beware-of-homograph-attacks/?lang=en