Task 1A

1. Not Secure Warning: When I see this, it simply means the website does not use encryption over HTTPS; thus, any data exchanged with the site could be intercepted. The risks are that my personal information, such as passwords or any payment details, might be stolen, or that my device will be exposed to malware.

2. Trusted site : That the site has come up as trusted means that it has a valid SSL/TLS certificate, which assures encryption of data transmission between my browser and the site and probably follows higher security standards.

3. Phishing/Scam Sites Detection: I look for strange URLs, spelling errors, suspicious or generic content, and inconsistent branding to find phishing or scam sites. I would refer to whether the website uses HTTPS and how it presents the security certificate.

4. Online Tools: I will be able to verify with online tools if a site is malicious or not, using something like VirusTotal, PhishTank, or Google Safe Browsing. Browser extensions may also help with anti-phishing filters.

5. Typosquating: This cyber-squatting involves the registration of a domain name similar to an already legitimate domain, anticipating that I will make a mistake while typing the URL into my browser . It is a trick often used to obtain my personal information.

6. UDRP: Uniform Domain-Name Dispute-Resolution Policy gives a channel for a trademark owner to object and recover the domain name confusingly similar to the trademark and could be useful in battling typosquating.

7. Phishing domain monitoring: Suppose I owned ouspg.org and did a crypto banking app at bank.ouspg.org; I'd monitor domains such as bankouspg.org, ouspgbank.org, or other variants, which would represent misspellings like bank.osupg.org to keep a tab on phishing attempts .