The picture contains a message from the web browser's "Not Secure" warning, which usually means the website you are visiting does not have a secure connection. The notice is frequently seen in your browser's address bar beside the website's URL. It means the website does not have advanced SLS/TLS certificates, which allows us to establish encryption during the data communication.

If you visit such a site, you should take the following precautionary measures.

* Avoid providing any sensitive information on such websites.
* Use a VPN to add an extra security layer to encrypt your connection.
* Verify whether the website is legit or not and scrutinize the website before providing any information.
* Install some privacy extension which safeguards your data during such website visits.

The trusted to the browser symbol indicates that this browser contains a valid SSL/TLS certificate from an established Certificate Authority. It guarantees safe data transfer and boosts users' trust in the website's security.

There are multiple ways through which phishing is detected, and a few of them are listed below.

* By closely examining the URL, we can check whether the website is legit, as significant scam websites contain misspelt domains and unusual characters in their domains.
* Check whether the website has valid SLS/TLS certificates, as scam websites generally do not have these certificates.
* Scam websites have a poor design pattern and inconsistent layouts and patterns.
* Scam websites generally have very low-quality content, generally full of grammatical errors.
* Such websites can be identified using online tools and browser plugins like Google Safe Browsing and PhishTank.
* Check that it has contact information, as scam websites lack a contact page or provide vague information that may be considered suspicious.
* Anti-phishing software can offer real-time defence against known phishing sites, including browser extensions and security suites.

Typo squatting is a type of cyber-attack when criminals register domain names identical to those of trustworthy websites to deceive users who make typing errors. Victims may be taken to fictitious websites for phishing, spreading malware, or earning money through advertisements. Use bookmarks, double-check URLs, and use caution when clicking email links to protect yourself, as these types of websites do not contain any SLS/TLS certificates, and a non-secure warning always pops up with them.

UDRP stands for Uniform Domain-Name Dispute-Resolution Policy, in which Domain name disputes are handled through the UDRP. Allowing trademark owners to contest confusingly similar domain names helps prevent typo squatting. The disputed domain may be transferred or cancelled if the complainant successfully establishes their claim, deterring typo squatting. As they have an effortless and straightforward procedure and the actual owner must follow some common steps and establish the ground of his ownership, all the domains used for typo squatting are terminated in a single go as the legal channel is quite complex, expensive and time-consuming.

**ouspg.org**

* opsg.org
* oupg.org
* ouspg.live
* ouspg.net
* uspg.org

**bank.ouspg.org**

* banks.ouspg.org
* bank.oupsgs.org
* bank.oupg.org
* bank.oupsg.net
* bank.ospg.org