



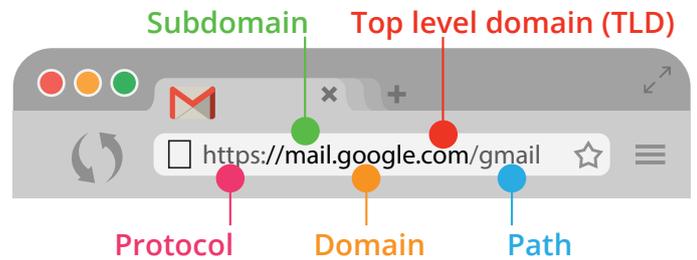
SPOOFED SITES

Phishing websites also referred to as spoofed sites, are a tactic cybercriminals use in order to extract information from unsuspecting victims.

Spoofed sites often resemble legitimate sites, and it is only by looking out for these key identifiers that you will avoid being scammed.

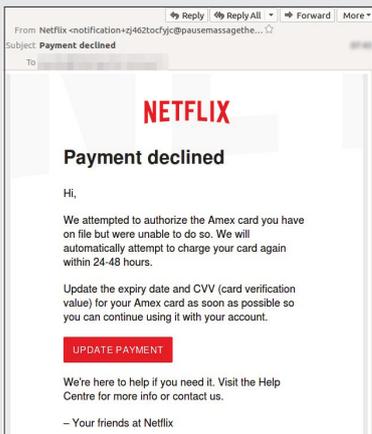
To identify a spoofed site, start by checking the URL:

- Is the structure legitimate?
- Is the domain spelled correctly?
- Are there strange characters or numbers?



It is also important to be aware of how the spoofed sites may reach you. Here are some ways criminals try to get you to fall for their scams:

Phishing mail



Phishing advert



Social media links



Accessing a fake login page



Ensure that you do not fall victim to a spoofed site scam:

- Do not click on links directly, rather type in the URL yourself.
- If you feel a link is suspicious, rather copy and paste it into another tab to check it.
- Right click to view links before clicking on them directly.
- Do not let curiosity get the better of you if you were not expecting it do not click, and if it seems too good to be true it probably is.
- Keep your browser version up to date.

By being aware of the threats we face online you are already applying the best mitigation tactic of all. Once you start to become aware of the malicious online activities taking place, you're immediately working much safer.