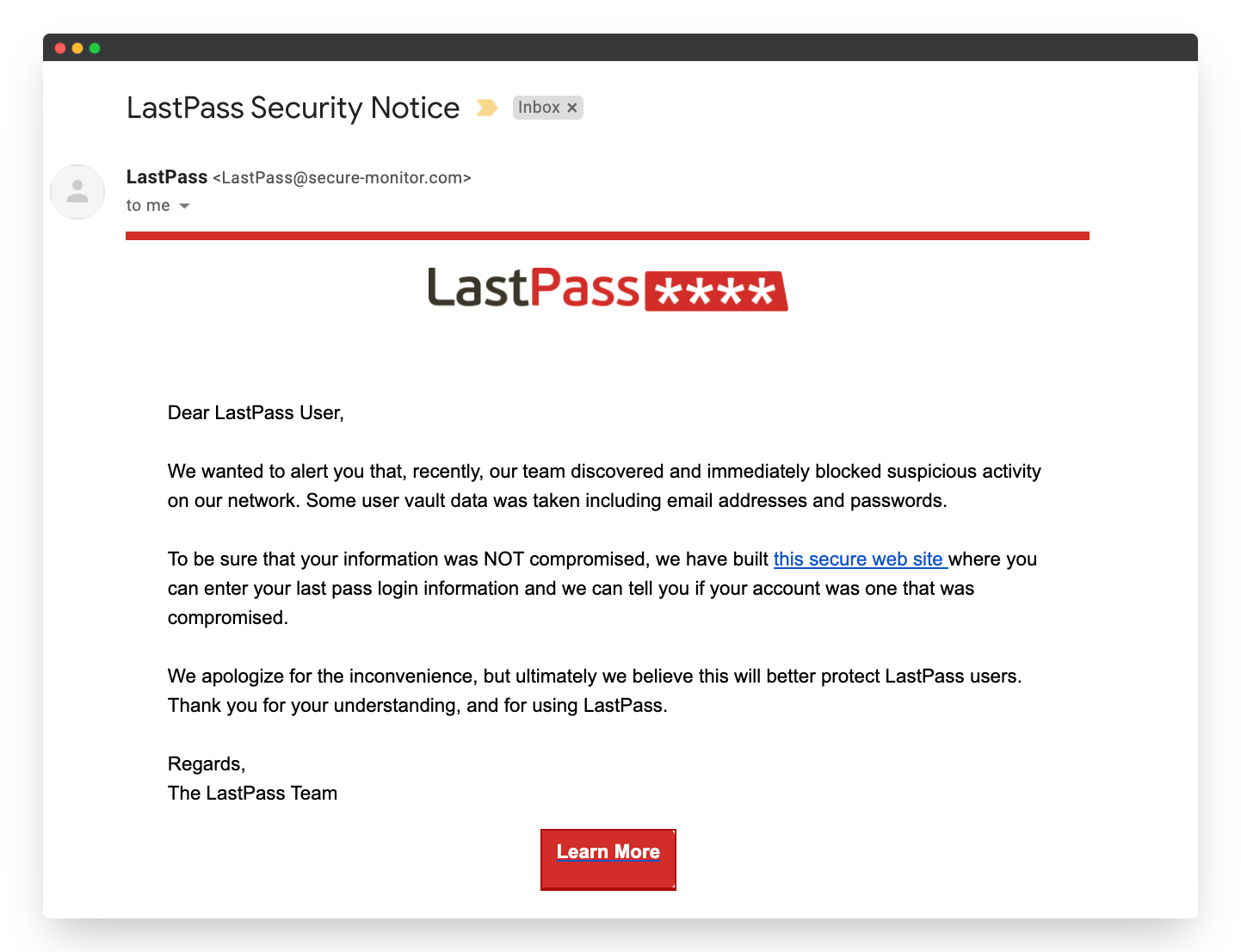
**Phishing** is one of the methods used by hackers to acquire credentials or sensitive data by sending a mail to the targeted individual from a well reputed company with a spoofed email to make it look like the company's email. To trick people, usually these emails contain links which redirect you to a login page which is actually fabricated by the attacker into acquiring your data.

Email is just an example that there are other methods to like SMS from where malicious links can be sent to the user and their credentials can be taken away.

**Several signs to lookout for if you are being phished-**

* Check the email address sent by the attacker as these people usually use look-alike domains to not bring much suspicion.
* Urgency is the key here if there is an urgency like “Verify within 24 hours” that can give away the possibility of a phishing attack.
* LINKS look out for them here things can go south as these usually open up fake login pages setup by the attacker to steal your credentials. Hover on them to see if it is secure or unsecure or login from the original site or app instead of the link given.
* Look out for Generic Greeting. These are a big give away of phishing mails like “Dear Valued Customer” these greetings are not used by the companies because they use your name to greet you “Dear John”.
* Grammatical Errors or the informality of tones in the mail itself.
* Not using HTTPS but HTTP is a huge giveaway, as big companies use HTTPS for a safe connection transfer.

**Let’s analyze this mail from LastPass-**

****

**Let’s lookout for some red flags-**

* As we can see the person is not greeted by name, whereas these big corporations use our names to greet us.
* Secondly we can see they have linked a website which they say is “Very Secure”.
* Then let’s look at the domain of the email which gives away that this is a phishing email.
* The informal tone in the mail does speak volumes for this is a phishing mail

