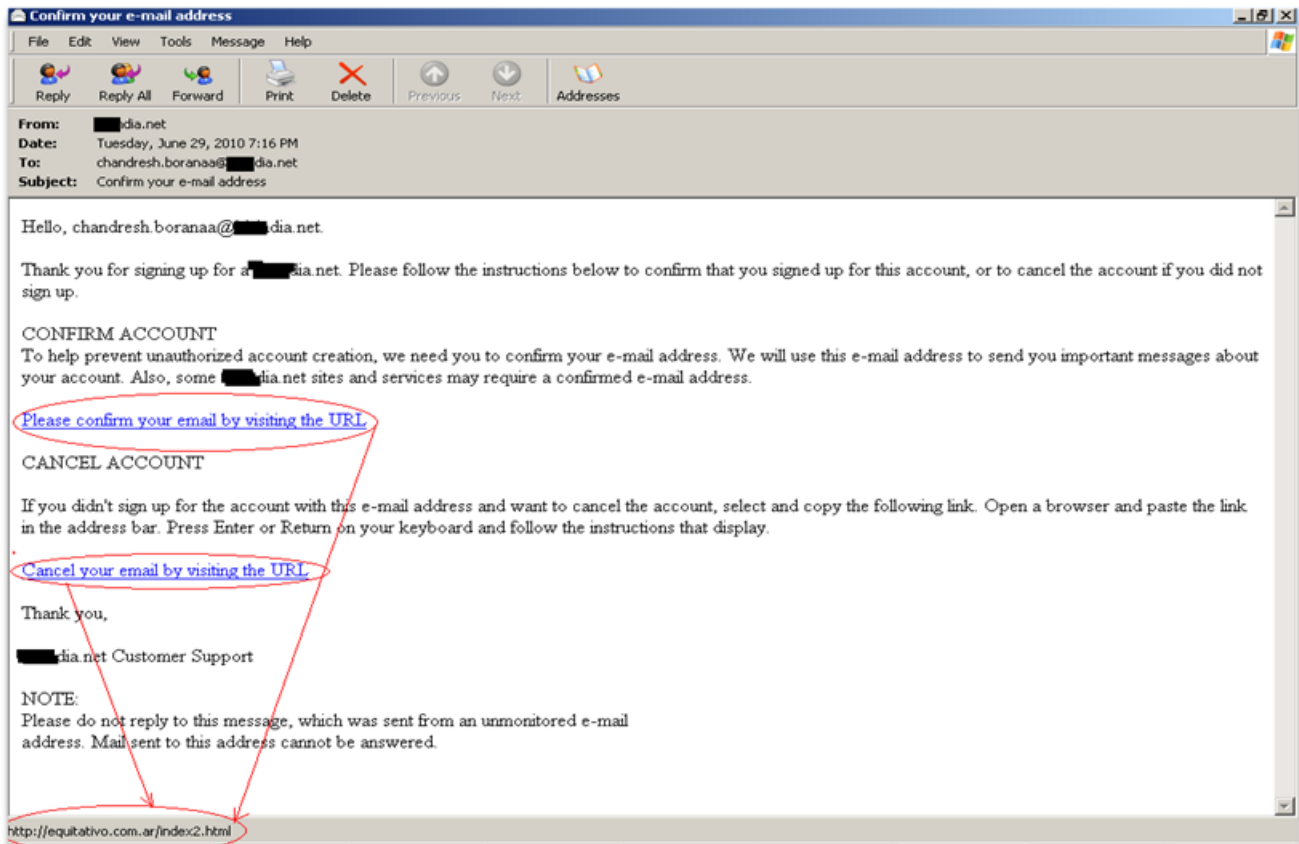


Phishing

Phishing is an attempt to induce a user to provide sensitive information or open a link or attachment, which will then harvest personal information or infect the user's device. Spear Phishing targets a specific individual or company using more tailored techniques. Spear Phishing is the most successful attack utilized today, used in over 90% of attacks.



This email is a targeted attempt at Spear Phishing – either link will lead the user to a malicious site designed to infect their computer or harvest credentials. Most trusted financial institutions will never ask you to click on a link and enter information. If they have a problem with your account, they will generally call you.

What to do?

-If you suspect that this could be a phishing attempt, look at the address from which the email was sent. If it looks strange (random numbers and letters; from a weird email server), this could be a sign that this is a phishing attack.

-Never click on the link. If you would like to check the status of your account, open up the website using secure browsing in a different window or contact the company and ask if they sent the email.

-Hold cursor over the link. Does this match what it says it is? If not, call the institution.