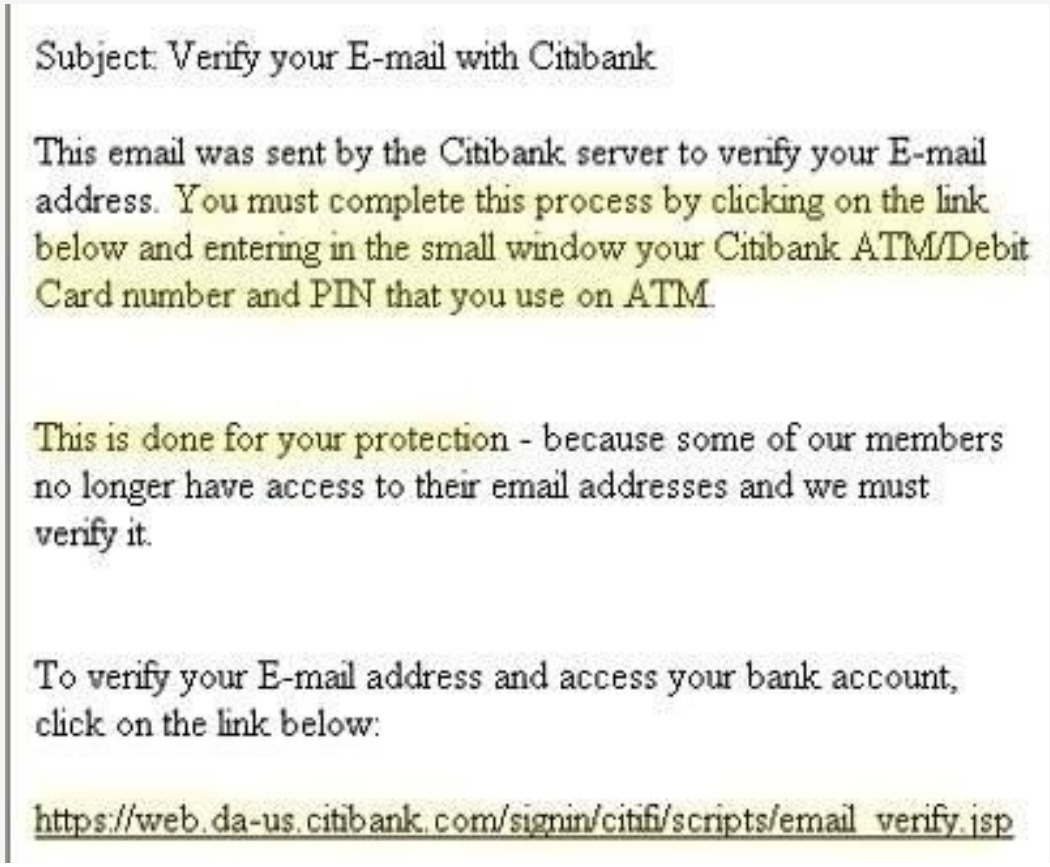
ORLEANS POLICE DEPARTMENT

90 SOUTH ORLEANS RD
ORLEANS MASSACHUSETTS 02653-3307

CHIEF JEFFREY J. ROY

TEL. 508-255-0117
FAX. 508-240-1374

4) Phishing emails and phony web pages



Subject: Verify your E-mail with Citibank

This email was sent by the Citibank server to verify your E-mail address. You must complete this process by clicking on the link below and entering in the small window your Citibank ATM/Debit Card number and PIN that you use on ATM.

This is done for your protection - because some of our members no longer have access to their email addresses and we must verify it.

To verify your E-mail address and access your bank account, click on the link below:

https://web.da-us.citibank.com/signin/citifi/scripts/email_verify.jsp

This is the most widespread Internet and email scam today. It is the modern day "sting" con game. "Phishing" is where digital thieves lure you into divulging your password info through convincing emails and web pages. These phishing emails and web pages resemble legitimate credit authorities like Citibank, eBay, or PayPal. They frighten or entice you into visiting a phony web page and entering your ID and password. Commonly, the guise is an urgent need to "confirm your identity". They will even offer you a story of how your account has been attacked by hackers to lure you into entering your confidential information.

The email message will require you to click on a link. But instead of leading you to the real login https: site, the link will secretly redirect you to a fake website. You then innocently enter your ID and password. This information is intercepted by the scammers, who later access your account and fleece you for several hundred dollars.

This phishing con, like all cons, depends on people believing the legitimacy of their emails and web pages. Because it was born out of hacking techniques, “fishing” is stylistically spelled "phishing" by hackers.

Tip: the beginning of the link address should have https://. Phishing fakes will just have http:// (no “s”). If still in doubt, make a phone call to the financial institution to verify if the email is legit. In the meantime, if an email seems suspicious to you, do not trust it. Being skeptical could save you hundreds of lost dollars.