CAP6135: Manually send a spam email (Spring 2016)

University of Central Florida
Cliff C. Zou

In this simple assignment, you will need to first log in Eustis (or Eustis2) machine, then use telnet to manually send a spam (faked) email to a special-created gmail account: "ucf.cap6135@gmail.com". From this experiment, you will understand why there are so many untrusted email around and how easy for attackers to send out spam or phishing email.

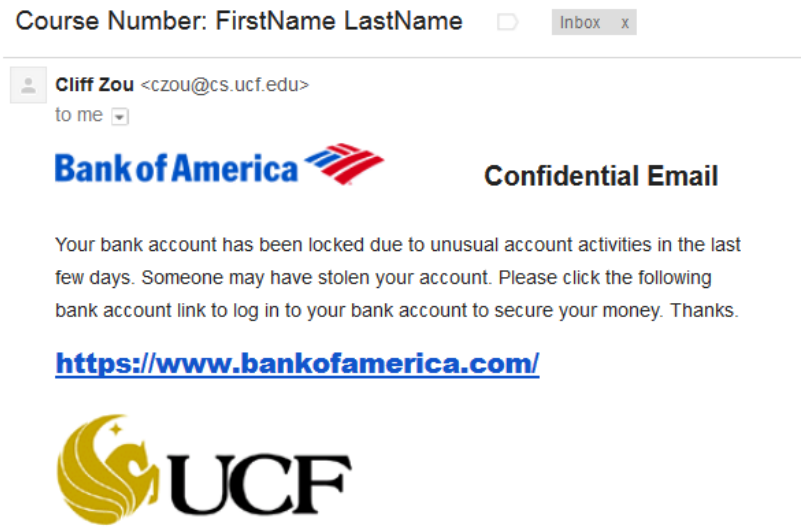
Please follow the in-class illustration (lecture 10) to send this faked email inside Eustis or Eustis2 machine. In order to make these assignment email not be treated as the other spam email, you must follow the following specifications:

1. The email must have a subject line as "CAP6135: firstname lastname". Put your name in the subject line so that you can be credited. Otherwise I cannot tell who send this email!

3. The email must have a "from: ..." and the "to: ...." field that will be shown by recipient email agent. These two fields are displayed by email software when the recipient reads an email. You MUST put the following "from:.." and "to:..." field in this email: "from: IT-support@bankofamerica.com", "to: spamHW@CNT5410". (HINT: they are typed in the "DATA" command section, not in the “mail from:” command! You can put whatever you like in the commands of “helo ….” and “mail from:…..” as long as your input can pass the email server’s checking)

4. You can type in two "rcpt to:" to include your own email address for verification in one of the "rcpt to" commands. Because CS email server now only support relay with a few local LAN IPs including Eustis, so you can only use Eustis (or Eustis2) server to manually send email to an arbitrary email address.

5. The email should have two images and one faked URL link. Please use the techniques explained in class to generate a spam email in the similar format like the following screenshot:



You don't need to generate the exact same email. But your spam email must have the above two images, and one faked URL link specified below:

1. The first "Bank of America" logo file should be included in the email (you can download the image from: http://www.cs.ucf.edu/~czou/ftp/).
2. The second "UCF" logo should be included as an image URL in the email. The image URL is: http://www.cs.ucf.edu/~czou/images/smallUCF.gif.
3. The fake URL will actually direct a user who clicks it to the URL: http://www.cs.ucf.edu/

Note:

Due to strict email spam detection systems deployed by our CS email server, and the Gmail server, your manual spam email is possibly to be treated as a spam by one or both of these email servers, however, the recipient can still receive the email. If the email is treated as spam by CS server, the email will contain SpamAssasin scores on why it is treated as spam and appears in Gmail Inbox. If the email is treated as spam by Gmail server, it will be put in the "Spam" system folder under the Gmail account, and thus the TA can still recover and grade it.

Submission:

1. You need to send this spam email AND submit your report via WebCourse before the due date/time.
2. Submit a brief report showing (1). your telnet interaction steps. (2). How you generate this image-based spam email using a mail agent. You MUST copy the SCREENSHOT IMAGE in your report showing the interaction steps when you create this spam (only the beginning part of your telnet showing the interaction and the initial pasted few lines). A simple text showing the interaction is not good enough.