Think About These…Phishing Things!

Phishing is a type of Internet fraud where the scammer sends email messages that try to trick recipients into giving up private information (i.e., username, password, account number, etc.).

Employees are the first line of defense against phishing. So, ask yourself…

1) Do I know the person identified in the FROM field?
   Red Flag – if you do not know the person.

2) Is the *email address* displayed FROM someone that I recognize for this person?
   Big Red Flag – if the email address is not one you recognize for this person.

   Note: FROM email addresses are easily forged. Just because it displays a known person's email address, it does not mean that person really sent the message.

3) Is it reasonable that I should be receiving an email message from this person?
   Red Flag – if it seems odd to be getting an email from this person.

4) Does the message have an attachment?
   Big Red Flag – be super-cautious about all attachments.

5) Does the attachment file name end with .exe, .vbs, .bat?
   Really Big Red Flag – **Just Hit Delete (JHD!)** Get rid of the entire message.

6) Does the attachment file name end with .zip or .7z?
   Red Flag – there are legitimate reasons for sending attachments as archive files (.zip, .7z). You should only open an archive file if you were expecting to receive one from the sender. Contact them to confirm they sent it and the reason they sent it before opening it. Otherwise, JHD!

7) Does the message say that something is wrong with your Florida Poly account or username?

Really Big Red Flag – Florida Poly **never** uses email to ask you to login to a web page to fix a problem with your account nor requests your username/password. FPU will send email reminders to change your password during the month before it expires. This reminder will include instructions on how to change your password **but will not contain links to a web address.** If you receive a "password reset email" containing links to a web address, JHD no matter how persuasive, legitimate or compelling the email may seem to be.

8) Does the message contain minimal information but urges you to "check this out" or "get something amazing here" or something otherwise playing to your curiosity?

Big Red Flag – curb your curiosity! JHD! As a general security check, always verify the link before clicking and check with Helpdesk for any questions.

9) Does the message seem very legitimate but has a clickable link that does not visibly show the entire website address?

Red Flag – depending on your email client you may be able to hover over or right-click the link to display or copy the full URL. If you can only copy it, do so, paste it into a blank text document, and examine it carefully.

10) Does the message contain a link that has part of a familiar web address but has additional text that follows domain segment of the link?

Red Flag – Website addresses (URLs) are essential to getting you to the website you want. Just because they are long, does not mean they are dangerous. Be on the lookout for URLs that contain information that is almost identical to real organizations (i.e. paaypal.com instead of paypal.com). Pay special attention to the domain segment of the URL (the last .aaa notation between the :// and next / symbols). This part of the URL is the address where the web server "lives" and if it does not end with the familiar .edu, .com, .org, .info, etc., be careful—particularly if the domain is an ".aa" country code that you wouldn't expect for the kind of URL you are examining.

Remember: JHD! Just Hit Delete!

It is better to delete suspicious email messages than it is to let your curiosity override your judgment and common sense. If you delete something that is was not dangerous and the sender wanted or needed you to read it—if it really is that important—they will send a follow up message.