RUTGERS
Office of Information Technology | Newark

Rutgers will never ask you for your personal information in email.

Never respond to emails asking for your password or Social Security Number.

Never share your password with anyone.

Avoid becoming a victim of Internet fraud.

Phishing is the attempt to solicit your personal information such as your username, password or Social Security Number by an untrustworthy entity. Your Rutgers and personal email accounts may be targeted. You should never reply to these requests. Instead you should delete the message and all future phishing messages.

If you responded to a phishing email with your Rutgers password, you should change your password as soon as possible at:

http://netid.rutgers.edu

If you responded to a phishing email with your personal password, you should change your personal password as soon as possible.

You can learn more about Phishing at:

http://rusecure.rutgers.edu/students/topics/phishing

Internet fraud refers to the use of Internet services to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme.

Internet fraud can occur in email, chat rooms, message boards, or on websites.

Here are some tips you can use to avoid becoming a victim of cyber fraud:

- Do not respond to unsolicited (spam) e-mail.
- Do not click on links contained within an unsolicited e-mail.
- Be cautious of e-mail claiming to contain pictures in attached files, as the files may contain viruses. Only open attachments from known senders. Scan the attachments for viruses if possible.
- Avoid filling out forms contained in e-mail messages that ask for personal information.
- If you are asked to act quickly, or there is an emergency, it may be a scam. Fraudsters create a sense of urgency to get you to act quickly.

- Always compare the link in the e-mail with the link to which you are directed and determine if they match and will lead you to a legitimate site.

- Log directly onto the official website for the business identified in the e-mail, instead of "linking" to it from an unsolicited e-mail. If the e-mail appears to be from your bank, credit card issuer, or other company you deal with frequently, your statements or official correspondence from the business will provide the proper contact information.

- Contact the actual business that supposedly sent the e-mail to verify if the e-mail is genuine.

- Verify any requests for personal information from any business or financial institution by contacting them using the main contact information.

- Remember if it looks too good to be true, it probably is.

For more information contact the Newark Computing Services Help Desk.

Location Hill Hall - Room 109
Phone: 973-353-5083
Email: help@newark.rutgers.edu