WARNING:

PHISHING AHEAD

Today, more than 150 million emails will hit mailboxes worldwide in an effort to steal usernames, passwords and credit card details. The emails are phishing—a malicious attempt to gain access to sensitive information. The messages will appear to come from a trusted source, but will be from criminals.

Here are things you should look for to stay safe:

- Be wary of requests for confidential information. Do not share usernames, passwords or account details.
- Question 'scare tactic' messages. Threats about account closures, account sizes exceeding limits and loss of access are fraudulent warnings.
- Recognize generic communication. General greetings such as 'Dear User,' "Dear Gmu Student/Faculty,' or 'Email user' are for mass mailings. Those greetings are not signs of personal or business relationships.
- Do not click on active links without verifying the link. Links in fraudulent emails can hide actual addresses.
- Keep software up-to-date. Software updates often contain patches that will block malicious programs.
- Delete emails from unknown address. Or verify directly by phone or by typing the URL in your browser to confirm the sender's information.

Report phishing to the ITS Support Center
at support@gmu.edu or call the Support Center at (703) 993-8870

GEORGE MASON UNIVERSITY | Information Technology Services