Keep criminals from getting their hands on your sensitive personal and financial data.

Never send user names, passwords, SSNs, or account information in response to an e-mail request.

The results of a phishing attack can range from account closures to financial ruin, and in the worst cases, identity theft.

**Protect yourself!**

**IT Security Warns:**

1. **Be wary of requests for confidential information.**
   Passwords, user names, or accounts should never be shared.

2. **Question the “scare tactic” message.**
   Account closures and loss of access are common fraudulent threats.

3. **Be alert to the generic communication.**
   “Dear Gmu Student/Faculty” signals a mass mailing, not a business relationship.

4. **Avoid clicking active links without verifying.**
   Links in fraudulent e-mails can hide actual addresses.

5. **Keep software up-to-date and perform regular scans.**
   Anti-virus, spyware, firewall and anti-spam help protect against threats.

6. **Delete e-mails from unknown addresses.**
   Or verify directly by phone or by typing the URL in your browser.

*Mason will never ask for your personal information over e-mail.*