staying safe on social media

• **Check your privacy settings often.**
  - Social media sites are constantly changing and updating their privacy settings. Make sure you are always up-to-date.

• **Never use your social media user IDs and passwords for other sites.**
  - Also called “chain-linking,” this method is a safety concern. If your social media profile is compromised, then the attacker has instant access to all your accounts.

• **Do not accept friend requests from people you don’t know.**
  - Accepting friend requests from strangers allows them to gather personal information on you and your friends, leaving you vulnerable to attacks.

• **Do not post your plans, cell phone numbers, current location, and other personal information.**
  - This information can easily be used in social engineering attacks; physical attacks; and also reveals most security question answers for other sites.

• **THINK BEFORE YOU POST.**
  - This is the most crucial part of staying safe on social media sites. It’s the Internet, nothing is truly private and everything is permanent.

For questions about social media, please contact:
IT Security Office • 703-993-2906 • itsoinfo@gmu.edu