**Do you know what really happens when you share your RACF / VUNet-ID and e-password with another person?**

- You give that person the ability to access your personal HR data:
  - Salary
  - Date of Birth
  - Home address and phone number
  - Name of your bank and checking account# (if you have direct deposit)

- You give that person the ability to access systems with confidential information that you have access to which they may not be authorized to access, thus jeopardizing the integrity and confidentiality of the information.

- You violate the requirements set forth in the VUMC Confidentiality Agreement that you signed.

- You commit a security violation which will result in disciplinary/corrective action.

**Developing Strong Passwords:**
The following guidelines can help you create passwords that increase the level of difficulty and the time needed for someone to determine your password

**Always**
- Use a minimum of 7-8 characters
- Include numbers, letters (both upper and lower case), and special characters (when applicable)

**Avoid**
- Any word in any language spelled either forward or backward
- Numbers that reference dates, phone numbers, Social Security numbers, etc.
- Made up words or nicknames someone might associate with you
- Repeating characters

You can give your assistant or someone else permission to read and/or create e-mail messages on your behalf **without sharing your user-id password.**

You can set up a shared drive where you can share files and databases with others **without sharing your password.**

**IM 10-30.28** – Authentication to Electronic Systems and Applications
**IM 10-30.12** – Sanctions for Privacy and Information Security Violations