Cybersecurity Best Practices

(Cyber-awareness library: https://go.gwu.edu/cyberawarelibrary)

1. Password Protection:
   - Use strong, unique passwords for all accounts. A strong password contains a combination of upper and lowercase letters, numbers, & special characters.
   - Avoid using personal information or common words as passwords.
   - Never share your passwords with anyone or write them down in easily accessible places.
   - Enable multi-factor authentication (MFA) wherever possible to provide an extra layer of security.

2. Phishing Awareness:

Phishing attacks are a huge part of modern-day cyberattacks – some are highly personalized and may contain references to your coworkers, family members, hobbies, and more. The best way to mitigate this is awareness, use the SLAM method to help identify phishing attacks:

- **S**ender: Check the sender's email address
- **L**inks: Hover your mouse and check any links before clicking
- **A**ttachments: Don't open attachments from someone you don't know or were not expecting
- **M**essage: Check the content of the message for bad grammar/misspellings

Report any suspected phishing attempts to:
LawIT@law.gwu.edu & Abuse@gwu.edu

3. Physical Security:
   - Keep your office, computer, and storage areas physically secure. Lock your office door when unattended.
   - Lock your workstation or use a screensaver password when you step away from your desk.

4. Data Storage:
   - Use secure and encrypted cloud storage services (Box or Google Drive) provided by the institution.
   - Do not store documents locally on your device in case of hardware failures or other incidents.
   - Avoid storing sensitive or regulated data on personal devices or cloud services not approved by the institution.

5. Reporting Security Incidents:
   - Promptly report any suspected or actual security incidents to the IT department at lawIT@law.gwu.edu or 202-994-5335. Include all available details and evidence related to the incident to facilitate investigation and response.