# ISSUES THAT STUDENTS SHOULD BE WARY OF AS THEY USE THE DIGITAL SPACE

## 1. PASSWORD MANAGEMENT

Use strong, unique passwords, and consider password managers. Combine uppercase and lowercase letters, numbers, and special characters.

**Avoid:**

i. **Weak passwords**: Avoid using easily guessable passwords.
ii. **Password sharing:** Never share passwords with others.
iii. **Infrequent password updates:** Regularly update passwords, especially for sensitive accounts.

## 2. PHISHING AND SOCIAL ENGINEERING

Phishing and social engineering are significant threats in the cyber security world.
Phishing involves tricking people into revealing sensitive info like passwords, credit card numbers, or personal data (Fraudulent attempts). Be cautious with emails, links, and attachments from unknown sources. Don't give away sensitive information.

**Social engineering tactics:**

i. **Pretexting:** Attackers create a fake scenario to gain trust.
ii. **Baiting:** Leaving malware-infected devices or storage media for victims to find.
iii. **Quid pro quo:** Offering services or benefits in exchange for sensitive information.

**How to protect yourself:**

i. **Verify sender info:** Check email addresses and phone numbers.
ii. **Be cautious with links and attachments:** Avoid suspicious links and attachments.
iii. **Watch for spelling and grammar:** Legit organizations usually have professional communication.

**Red flags:**

i. **Urgency:** Be wary of messages creating a sense of urgency.
ii. **Suspicious requests:** Be cautious of requests for sensitive info.
iii. **Poor grammar and spelling:** Legit organizations usually have professional communication.

What can you do if you think you've been phished?

i. **Change passwords:** Immediately change passwords for compromised accounts.
ii. **Notify the organization:** Inform the organization that sent the phishing attempt.
iii. **Monitor accounts:** Keep an eye on your accounts for suspicious activity.

## 3. NETWORK SECURITY

**Key issues in network security involve;**

i. **Protecting network infrastructure:** Safeguarding routers, switches, firewalls, and servers.
ii. **Preventing unauthorized access:** Blocking malicious traffic and access attempts.

## 4. STAYING UPDATED

Regularly update your OS, software, and apps to patch vulnerabilities.