SINDHI COLLEGE
#33/2B, Kempapura, Hebbal, Bengaluru - 560024
Permanently Affiliated to Bengaluru City University
Approved by AICTE, NAAC Re-accredited
Ph.no: 080-23637544 E-mail: mail@sindhicollege.com

Cyber security

- Promote Two-Factor Authentication (2FA): Encourage students to activate 2FA for their online accounts to add an extra layer of security to their personal data.
- Cyber security Information Flyers and Posters: Display posters and distribute flyers in high-traffic areas on campus to inform students about safe online practices and the risks of cybercrime.

Steps to an effective approach to cyber security

1. Risk Management Plan

- Identify potential risks to your organization's information and systems and create a plan to manage them.
- Make sure the plan has the full support of senior leaders and the Board.
- Ensure that all employees, contractors, and suppliers understand the plan and know what risks they should avoid.

2. Secure Configuration

- Establish a clear approach to identify standard technology setups and processes for managing system configurations, which helps enhance security.
- Create a strategy to remove or disable any unnecessary features from systems and promptly address known vulnerabilities, often through patching.
- Failing to do this can significantly increase the risk of system and data breaches.

3. Network Security

- Connections to the internet or other networks can put your systems at risk of attacks.
- Use basic policies and tools like firewalls (e.g., Windows Firewall) to protect your systems.
- Your network may spread across multiple sites, with mobile or remote workers, and cloud services, so it's important to think about where your data is stored and where attackers could try to access it, not just physical connections.

4. Managing User Privileges

- Giving users more access than they need increases the risk of misuse or security breaches.
- Users should only be given the minimum level of access necessary for their role.
- Higher-level access privileges should be carefully controlled and monitored.
- This practice is known as the principle of **"least privilege."**

5. User Education and Awareness

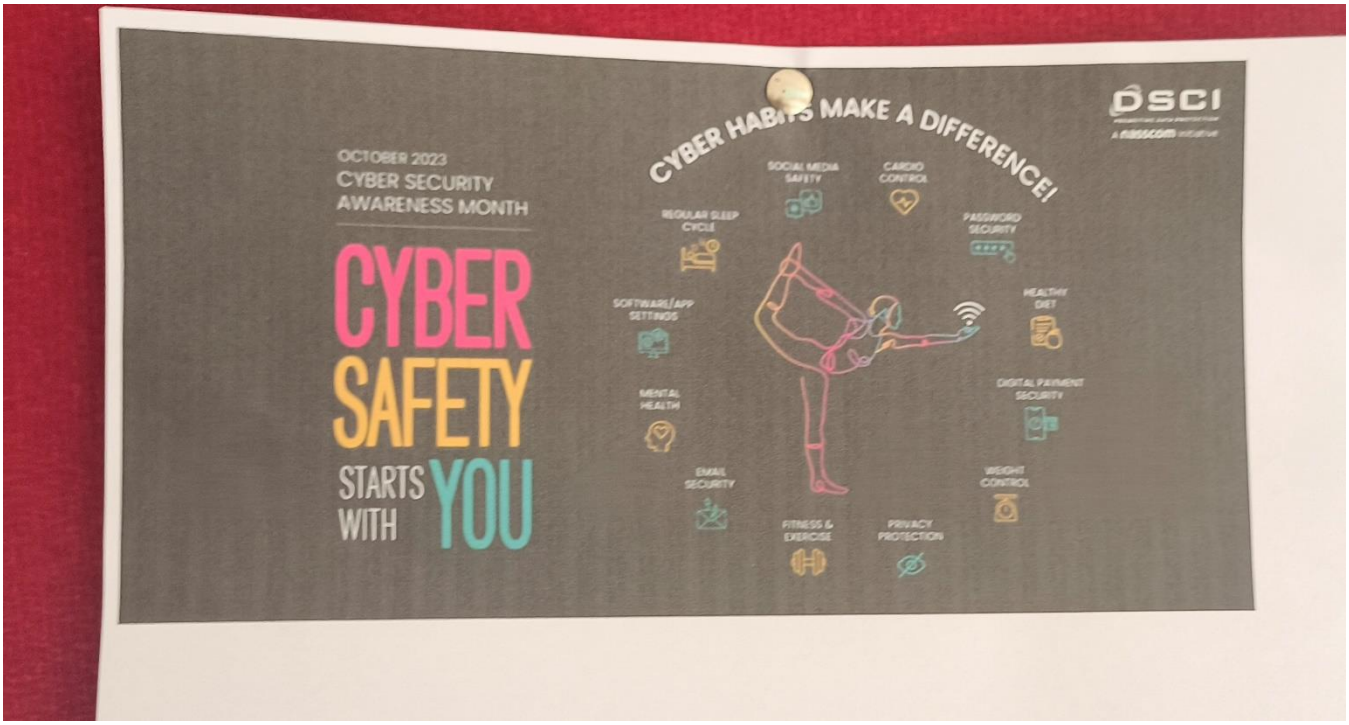
- Users play a key role in keeping the organization secure.
- It's important to educate staff about potential cyber risks so they can do their jobs safely and also help protect the organization from threats.

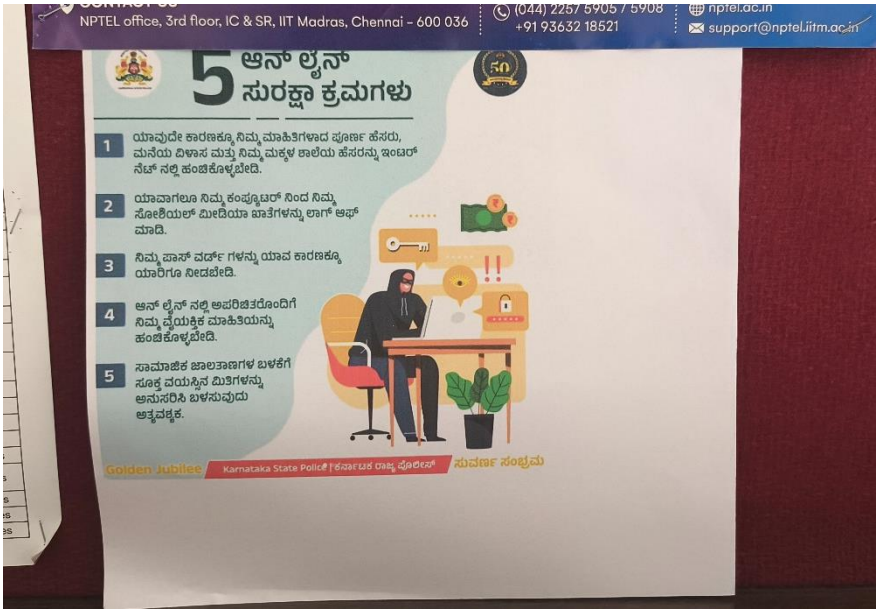
6. Malware Prevention

- Malware is harmful software that can damage or disrupt your systems.
- Anytime information is exchanged, there's a risk of malware being introduced, which can seriously impact your systems.
- To reduce this risk, use **Windows Defender** to protect your systems from malware and ensure it is always up-to-date and running.

7. Monitoring

- System monitoring helps detect attacks or attempts to compromise your systems and services.
- It's important for responding quickly to any security threats.
- Monitoring also ensures that systems are used correctly, following your organization's policies.
- It's often required to meet legal or regulatory standards.


OCTOBER 2023
CYBER SECURITY AWARENESS MONTH
CYBER SAFETY STARTS WITH YOU
CYBER HABITS MAKE A DIFFERENCE!
DSCI
SOCIAL MEDIA SAFETY
CARDIO CONTROL
REGULAR SLEEP CYCLE
PASSWORD SECURITY
SOFTWARE/APP SETTINGS
HEALTHY DIET
MENTAL HEALTH
DIGITAL PAYMENT SECURITY
EMAIL SECURITY
WEIGHT CONTROL
FITNESS & EXERCISE
PRIVACY PROTECTION


NPTEL office, 3rd floor, IC & SR, IIT Madras, Chennai - 600 036
(044) 2257 5905 / 5908
+91 93632 18521
nptel.ac.in
support@nptel.iitm.ac.in
5 ಆನ್ ಲೈನ್ ಸುರಕ್ಷಾ ಕ್ರಮಗಳು
1 ಯಾವುದೇ ಕಾರಣಕ್ಕೂ ನಿಮ್ಮ ಮಾಹಿತಿಗಳಾದ ಪೂರ್ಣ ಹೆಸರು, ಮನೆಯ ವಿಳಾಸ ಮತ್ತು ನಿಮ್ಮ ಮಕ್ಕಳ ಶಾಲೆಯ ಹೆಸರನ್ನು ಇಂಟರ್ ನೆಟ್ ನಲ್ಲಿ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.
2 ಯಾವಾಗಲೂ ನಿಮ್ಮ ಕಂಪ್ಯೂಟರ್ ನಿಂದ ನಿಮ್ಮ ಸೋಶಿಯಲ್ ಮೀಡಿಯಾ ಖಾತೆಗಳನ್ನು ಲಾಗ್ ಆಫ್ ಮಾಡಿ.
3 ನಿಮ್ಮ ಪಾಸ್ ವರ್ಡ್ ಗಳನ್ನು ಯಾವ ಕಾರಣಕ್ಕೂ ಯಾರಿಗೂ ನೀಡಬೇಡಿ.
4 ಆನ್ ಲೈನ್ ನಲ್ಲಿ ಅಪರಿಚಿತರೊಂದಿಗೆ ನಿಮ್ಮ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.
5 ಸಾಮಾಜಿಕ ಜಾಲತಾಣಗಳ ಬಳಕೆಗೆ ಸೂಕ್ತ ವಯಸ್ಸಿನ ಮಿತಿಗಳನ್ನು ಅನುಸರಿಸಿ ಬಳಸುವುದು ಅತ್ಯವಶ್ಯಕ.
Golden Jubilee
Karnataka State Police ಕರ್ನಾಟಕ ರಾಜ್ಯ ಪೊಲೀಸ್
ಸುವರ್ಣ ಸಂಭ್ರಮ