SAROJINI NAIDU VANITA PHARMACY MAHA VIDYALAYA
(Sponsored by the Exhibition Society), Tarnaka, Secunderabad
Affiliated to Osmania University, Approved by AICTE & PCI
ISO 9001: 2015 Certified Institution, NBA Accredited B. Pharmacy Course

REPORT ON CYBER SECURITY AWARENESS SESSION

1. Event Overview

Detail	Description
Event Name	Cyber Security Awareness Session
Date	Friday, 24th October 2025
Time	10:30 AM – 11:30 AM
Duration	60 Minutes
Mode	Hybrid (Online via Webex), Attended in AuditoriumSarojini Naidu Vanitha Pharmacy Maha Vidyalaya (SNVPMV), Tarnaka, Hyderabad,
Webex Link	https://ugchq.webex.com/ugchq/j.php?MTID=mfba11a74165800c50a1f9d8d1c1a1553
Attendance	Participants attended in a centralized Auditorium setting while connecting to the online Webex session.

2. Objective of the Session

The primary objective of the session was to educate and sensitize participants on proactive personal cyber hygiene, common cyber threats, and methods to prevent falling victim to digital fraud and social engineering tactics.

2. Organizing Body and Attendance

The program was successfully conducted by the **Social Media Co-ordinators**: Dr. Shiva Rama Krishna, Dr.T. Swetha, and J. Swathi.

The session was graced by the presence of key institutional dignitaries, lending significance to the awareness initiative:

- **Director:** Dr. N. Srinivas
- **Principal:** Dr. T. Mamatha
- **Vice Principal:** Dr. B. Harika

The session saw a strong turnout, with **approximately 200 students** attending the program in the Auditorium.

3. Session Highlights and Key Takeaways

The hour-long session focused intensely on practical, daily habits for digital safety. The discussion covered nineteen critical points, which can be grouped into three major categories: **Financial Vigilance, Device and Connectivity Security, and Digital Threat Awareness.**

3.1. Financial and Identity Security

This segment emphasized safeguarding financial data and personal identity proofs:

- **Verified Payments:** Exercise extreme caution regarding online challans, ensuring payments are only made via verified, official government or institutional websites.
- **Card Security:** Never save credit card or debit card details (especially the CVV number) on any online app or website. If a photograph of a card is taken, the CVV must be digitally removed.
- **UPI Caution:** Be highly careful with UPI transactions, specifically understanding that a PIN is *only* required to send money, not to receive it.
- **Aadhaar Usage:** Always utilize the **Masked Aadhaar** for submission to third parties to protect identity details.

3.2. Device and Connectivity Management

The session stressed the physical security and connectivity protocols for mobile devices:

- **Phone Access:** Restrict giving one's phone to any individual, and if necessary, use screen-pinning features.
- **Locking Protocol:** Ensure the phone is locked immediately after use, even when navigating routine applications like Google Maps.
- **Safe Charging:** Avoid using public or borrowed charging cables and ports to prevent 'Juice Jacking' (data theft via charging ports).

- **Wi-Fi Networks:** Strictly avoid using free, unsecured public Wi-Fi networks for sensitive transactions.
- **Data Erasure:** If selling or disposing of an old phone, a complete and verifiable factory data wipe must be performed.
- **Digital Habits:** Always manually type website names for sensitive services instead of relying on links, and disable auto-download features for files and updates.

3.3. Digital Threat Awareness and Vigilance

This section focused on recognizing and avoiding manipulative scams and malicious files:

- **Link and Attachment Protocol:** Never click on suspicious links from unknown sources, and absolutely refrain from opening email attachments from unsolicited senders.
- **APK Files:** Avoid direct installation of **APK files** (Android application packages) unless sourced directly from trusted, official app stores.
- **Social Engineering:** Do not respond to online messages that demand immediate action, create emotional pressure, or rely on urgency. Scammers frequently use emotional appeals or a sense of rush to compromise judgment.
- **General Response:** The core rule is to **always pause and verify**; never act in a rush, or if there is any element of doubt.

4. Conclusion

The Cyber Security Awareness Session successfully delivered a comprehensive checklist of practical safety measures to the attendees. The content was highly relevant for mitigating daily digital risks.

A final, crucial point emphasized was the responsibility of every individual to **disseminate this awareness among family and friends**, ensuring collective digital safety within the community.


GPS Map Camera
Hyderabad, Telangana, India
12-5-32, Vijayapuri Colony, Mettuguda,
Hyderabad, Telangana 500017, India
Lat 17.430265° Long 78.532395°
24/10/25 10:50 AM GMT +05:30
Google


GPS Map Camera
Secunderabad, Telangana, India
12-5-28, Vijayapuri Colony, Tarnaka, Secunderabad,
Telangana 500017, India
Lat 17.430211° Long 78.532359°
24/10/25 10:50 AM GMT +05:30
Google