



**National Forensic
Sciences University**
Knowledge | Wisdom | Fulfilment
An Institution of National Importance
(Ministry of Home Affairs, Government of India)



गृह मंत्रालय
**MINISTRY OF
HOME AFFAIRS**

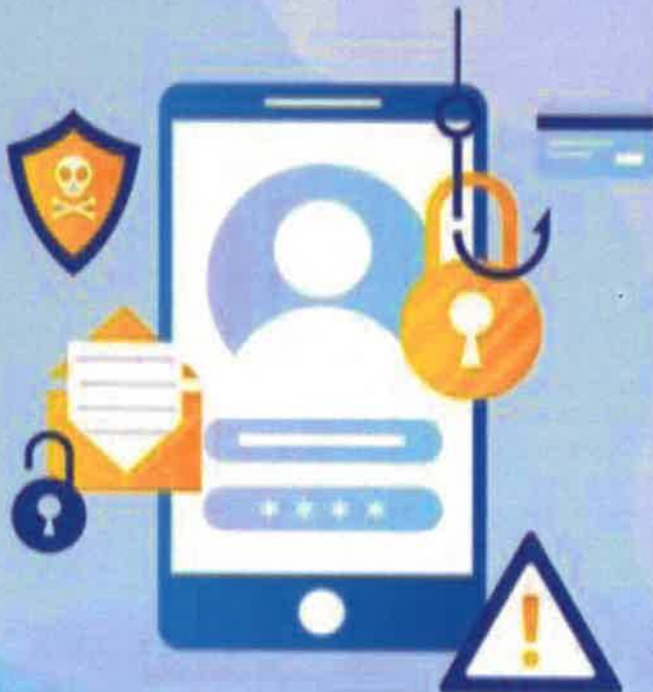
Advance Cyber Kiosk Machine



विद्यया अमृतं अश्नुते

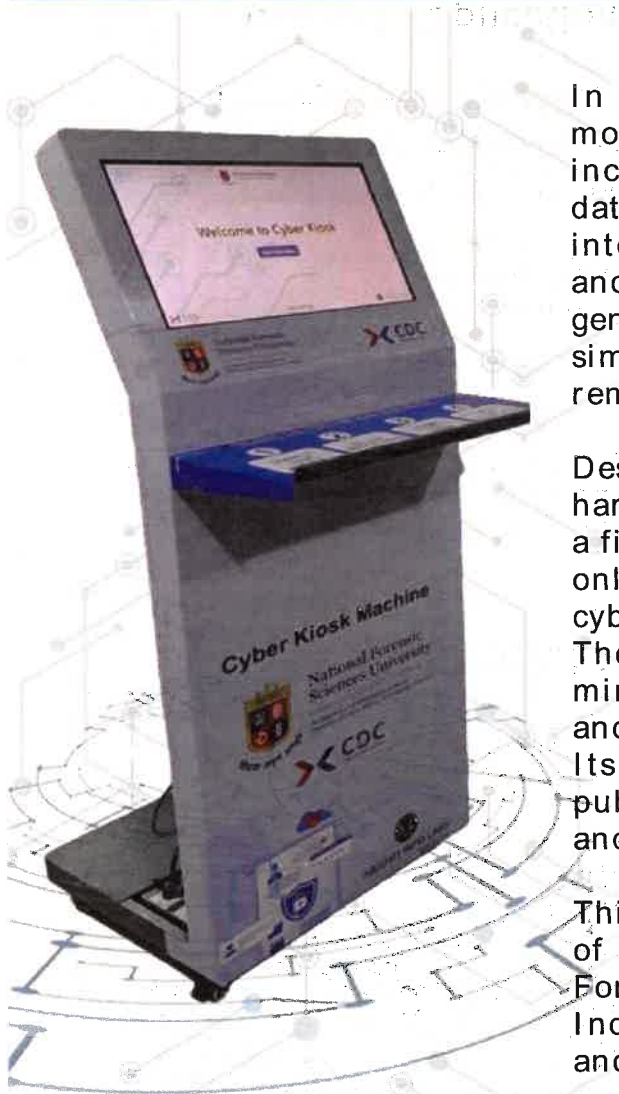
राष्ट्रीय न्यायालयिक विज्ञान विश्वविद्यालय

(राष्ट्रीय महत्व का संस्थान, गृह मंत्रालय, भारत सरकार)



CoE-CS
Cyber Defence Center
An ISO 27001/2015 Certified Lab

ADVANCE CYBER KIOSK



In today's digital world, users rely heavily on mobile and computing devices, making them increasingly vulnerable to malware, malicious apps, data theft, and cyber fraud. Cyber Kiosk offers an intelligent and automated security scan for mobile and storage devices, detecting threats and generating instant diagnostic reports. Through a simple and interactive interface, users can easily remove infections and secure their devices.

Designed to identify unknown, suspicious, or harmful files and applications, Cyber Kiosk acts as a first-line defense for citizens' digital safety. It not only enhances device hygiene but also promotes cyber awareness and safer digital practices.

The system operates with high accuracy and minimal user intervention, ensuring fast, reliable, and convenient cyber-health checks for the public. Its modular design makes it deployable across public institutions, campuses, government offices, and community spaces.

This indigenous solution is developed by the Center of Excellence in Cyber Security (CoE-CS), National Forensic Sciences University (NFSU), reinforcing India's commitment to advanced cyber protection and digital forensics innovation.

Why Security Check Required ?



1. Malicious Mobile Application.

Malicious mobile Application and backdoor are installed without the knowledge of the user.



2. Malicious File Download.

Malicious file were downloaded many times without the user knowledge and store in mobile internal storage.



3. Connect to Public Wi-Fi.

Mobile Phone can be easily connected to public Wi-Fi and other public networks. This exposes the devices to threats and makes it vulnerable to infections.



4. Banned Application.

Mobile Phone user download the banned application from the apotheosized app store.

Hardware and Performance Comparison

	Advance Cyber Kiosk (Android)	Mini Advance Cyber Kiosk (Android)	Advance Cyber Kiosk (Android + iOS)	Portable Advance Cyber Kiosk (Android + iOS)
	CK-1	CK-2	CK-3	CK-4
			 	 

Hardware

Memory	8 GB Intel	4 GB Intel	8 GB Intel	8 GB Intel
CPU	Core i5	Core i3	Core i5	Core i5
Storage	500 GB	250 GB	500 GB	500 GB
Display	21.5 Inch Touch Display	21.5 Inch Touch Display	21.5 Inch Touch Display	15.6 Inch Touch Display
Wi-Fi	Yes	No	Yes	Yes
Weigh	43 kg	34 kg	43 kg	13-16 kg
t USB	2x3.0, 1x2.0, SD Cd, Micro SD Card	2x3.0, 1x2.0, SD Cd, Micro SD Card	2x3.0, 1x2.0, SD Cd, Micro SD Card	2x3.0, 1x2.0, SD Cd, Micro SD Card
LAN	1Gbps	1Gbps	1Gbps	1Gbps

Performance

Mode	Online + Offline	Offline	Online + Offline	Online + Offline
Report Email	Yes	No	Yes	Yes
Report	Local + Cloud Storage	Local Storage	Local + Cloud Storage	Local + Cloud Storage
Kiosk Update	Auto Update	Manually Update	Auto Update	Auto Update
Signature Update	Every 24 Hours	Manually Update	Every 24 Hours	Every 24 Hours

Approx. Scanning Time (*Mobile Storage 4GB RAM, 64GB ROM)

Quick Scan	Approx. 10 to 12 Min	Approx. 15 to 20 Min	Approx. 10 to 12 Min	Approx. 10 to 12 Min
Deep Scan	Approx. 20 to 25 Min	Approx. 30 to 35 Min	Approx. 20 to 25 Min	Approx. 20 to 25 Min

Features of Advance Cyber Kiosk

- Malware/ Virus/ Backdoor detection from Mobile Phones and External storage Devices.
- Detect the Banned Application by India Government.
- Provides the location of malware file.
- It also performs Android, iOS and windows Application Scanning and identifies malicious and infected apps.
- It provides a consolidated report of the scanned device to the user.
- It also provides a dashboard feature to the administrator.
- It can also work in server-client model and a repository of the malware can be built for further research.

How Does Works Advance Cyber Kiosk Machine



STEP 1: User can connect to a handheld device on the kiosk and proceed as further instruction flashed on the screen.



STEP 2: The User will get alert about the malware if the scanned phone is infected.



STEP 3: The user can remove the detected malware file from Kiosk It self.



STEP 4: A detailed report will also be generated for the user's reference and it will also be forwarded on their Email ID.

Contact Us



www.nfsu.ac.in



cyber.kiosk@nfsu.ac.in



+91 909-995-5023



**National Forensic
Sciences University**

Knowledge | Wisdom | Fulfilment
An Institution of National Importance
(Ministry of Home Affairs, Government of India)



Center of Excellence-CS, NFSU
Police Bhavan Road,
Sector 9, Gandhinagar
Gujarat-382007