केनरा बैंक Canara Bank
सिंडिकेट Syndicate

CYBER SECURITY INITIATIVE

What is Rooted Android device?

Rooting is the process of allowing users of the Android Mobile operating system to gain Root access i.e. 'administrator' or 'super user' access over Android OS & various subsystems which are otherwise not accessible to a normal Android user.

Goal of Rooting is to overcome security restrictions put in place by device manufacturers and mobile carrier service providers to prevent users from altering or replacing system applications and settings, run specialized apps that require administrator-level permissions.

Why Rooted devices are harmful and What are the security risks!!

- May bypass inbuilt security features of Android OS
- May override prevention techniques of installing Malicious apps
- Untrusted Apps can be installed from unknown sources
- Phone becomes more vulnerable to malwares and hacking
- Malwares can gain root access to perform malicious actions
- Hackers may use malicious apps to steal sensitive personal data like login details, passwords, OTP, PIN, Card details and even payment details
- Might become unable to take future Android updates
- Might even grant complete access to hackers of the phone and data stored
- Might lose access to high security apps
- Device and OS warranty might be void

Issued in the public interest of all customers

By Technology Operations Wing, Head Office, Canara Bank

केनरा बैंक Canara Bank
सिंडिकेट Syndicate

CYBER SECURITY INITIATIVE

What is Jailbroken iPhone device?

Jailbroken is the process of freeing your device from the limitations that are imposed by Apple. Since Apple iOS is one of the most stable and secure operating systems around, it becomes too restrictive due to Apple's "closed" mantra.

Goal of Jailbroken is to empower users to super user access to read, write and even change some default setting on the iOS operating system.

The iOS's closed nature enables its design to be one of the most secure mobile operating systems available to protect personal information and the system itself.

Why Jailbroken devices are harmful and What are the security risks!!

- May bypass inbuilt security features of iPhone
- Changing the default root password means inviting a bigger risk of being prone to malware threats
- May override prevention techniques of installing Malicious apps
- Untrusted Apps can be installed from unknown sources
- Phone becomes more vulnerable to malwares and hacking
- Malwares can gain root access to perform malicious actions
- Hackers may use malicious apps to steal sensitive personal data like login details, passwords, OTP, PIN, Card details and even payment details
- Hackers may damage the device, attack network, or introduce malware, spyware or viruses.
- Might become unable to take future iOS updates
- Might even grant complete access of the phone to hackers and data stored
- Might lose access to high security apps
- Device and OS warranty might be void

Issued in the public interest of all customers

By Technology Operations Wing, Head Office, Canara Bank