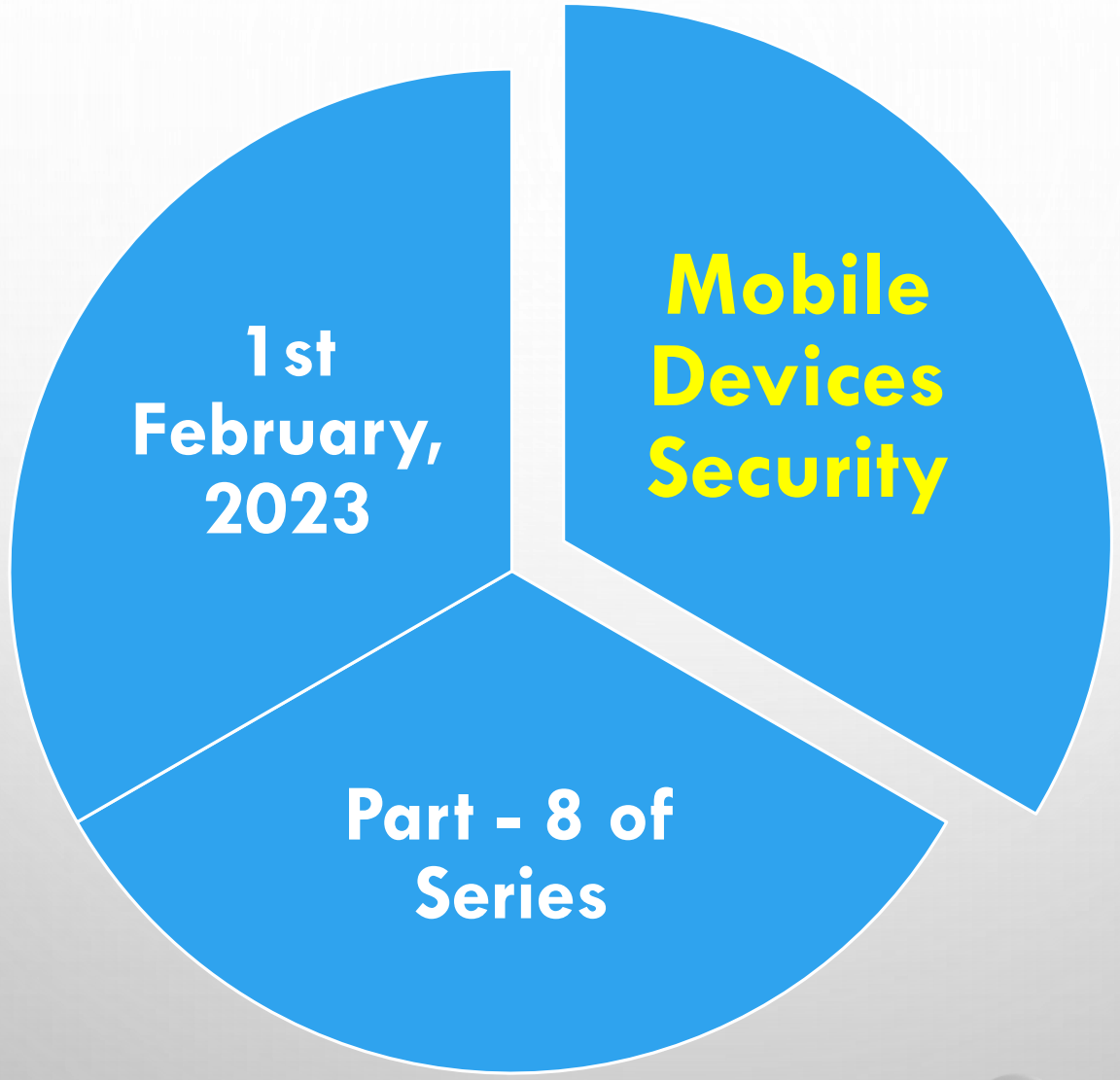
CELEBRATION OF CYBER JAAGROOKTA (AWARENESS) DIWAS (CJD)

(ON THE **FIRST WEDNESDAY OF EVERY MONTH**

COMMENCING APRIL,2022 ONWARDS)

Central Mine Planning & Design Institute Ltd.
RANCHI


1st February, 2023
Mobile Devices Security
Part - 8 of Series

Mobile devices are slowly but surely replacing Desktop Computers for quite a few activities like:

- Accessing e-mails
- Using Social Media applications
- Internet use
- Doing online transactions including online shopping (quite a few websites now use compatible web design technologies for the same)

- ***More than 60% of all web traffic these days come through Mobile Devices.***
- ***More than 90% of social media users use mobile devices to access social networks.***
- ***More than 50% of all online sales come from Mobile Devices.***

Therefore……

Lots of mobile applications are getting developed and getting installed as well, resulting in increased data consumption using mobile devices.

But, unfortunately, this trend is visible to hackers too, who are interested in grabbing personal information to use in malicious ways against unsuspecting users.

Conventional viruses are not as threatening to smartphones as they are to PCs.

Threats that exists because of lost/stolen devices or accidental/intentional malicious misuse by end users do not exist in case of PCs.

PCs are mostly monitored in organised ways.

Mobile devices are rarely controlled through some centrally managed processes and hence more difficult to manage in terms of security.

The most **common mobile device threats** include the following:

- Data thievery
- Malware attacks
- Phishing and Pharming
- Man in the Middle attacks (**An attacker intercepts or manipulates mobile device communications between the app/device and its backend service to gain access to information)**
- Misuse of lost/stolen devices
- Risky user behaviour **(Too trusting, too lazy, unprofessional etc.)**

Mobile Security Best Practices

There are quite a few recommended guidelines and safeguards for mobile devices.

However, nothing ensures absolute security as OS vulnerabilities mixed with risky user behaviour makes the threat landscape complicated.

User authentication through passwords, PINs etc.
(A strong authentication is the first and the most effective way of securing a device.)

Updating mobile operating systems with security patches.
(The security patches are published based on the vulnerabilities found in the OS. Updating OS, therefore, is very important.)

Taking Back up on a regular basis.
(Frequency of back up should depend on the criticality of the data that is there on the device.)

Using encryption whenever possible.

Avoiding insecure Wi-Fi spots.
(Public Wi-Fi spots are usually not safe.)

Disabling Bluetooth and Wi-Fi when not needed.

Getting sensitized on social engineering techniques.

(Nothing comes for free. Therefore, it's important not to fall into the traps of fraudsters.)

Avoiding or not indulging in jailbreaking of mobile devices.

(Mobile devices like other devices are best to use when factory-fitted. Tampering the devices in any way invites threat.)

Watching application behaviour and not granting unnecessary permissions to applications.
(The permissions need to be given on need-to-use basis.)

Installing mobile security and antivirus applications.

As has been indicated earlier too, following best practices doesn't ensure absolute mobile device security

However, following best practices shall surely increase security level and reduce overall susceptibility to threats.

The journey continues.....