Information Security Education & Awareness
Ministry of Electronics and Information Technology
Government of India

InfoSec Newsletter

MAY-JUNE, 2020

Public Kiosk Safety

InfoSec Concept
Page 3

For Virus Alerts,Incident & Vulnerability Reporting
certin Handling Computer Security Incidents
www.cyberswachhtakendra.gov.in

सी डैक CDAC
www.cdac.in

प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
संचार एवं सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Communications and Information Technology, Government of India
Plot No. 6 & 7, Hardware Park, Sy No. 1/1,Srisailam Highway, Pahadi Shareef Via Keshavagiri (Post)
Hyderabad - 501510 , Telangana(India)

InfoSec Newsletter

MAY - JUNE 2020

CREDITS

For Virus Alerts,Incident & Vulnerability Reporting

certin
Handling Computer Security Incidents

InfoSec CONTEST

InfoSec QUIZ

1. Juice jacking is hacking through_____ports
   A) Mini USB B) USB C) Audio o/p Port D) None of the above

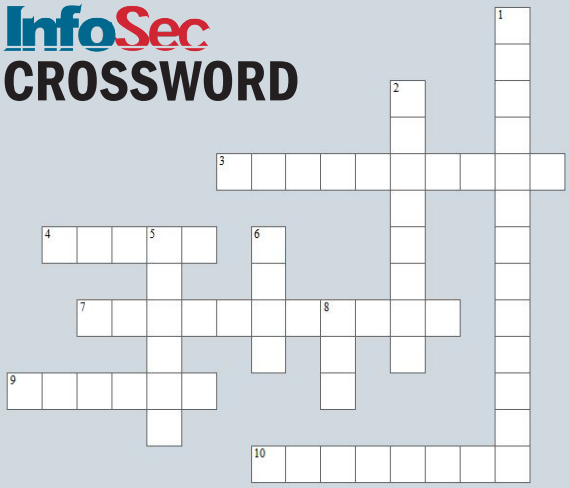
2. While charging your phone at public charging stations it is better to _____your phone to prevent Malware attack.
   A) Switch OFF B) Switch ON C) hibernate D) None of the above

3. _____ are actually devices that can be used as a buffer between your data charging cable and a public USB port.
   A)USB B) Mini USB C) USB Condoms D) None of the above

4. Keep Wi-Fi _____When You Don't Need It
   A) ON B) OFF C) Sleep D) None of the above

5. _____ involves specialized intercepting tools or software that can intercept and reassemble internet data sent between a router and a device.
   A) Wi-Fi Sniffing B) Virus attack C) karma attack D) None of the above

InfoSec CROSSWORD



Across

3. Juice jacking is not possible if a device is charged via the_____
4. _____ is a small, stand-alone booth typically placed in public utiliy places
7. Malicious hacker driving around various locations, looking for vulnerable Wi-Fi connections he can later exploit is called as _____
9. When your phone is_____ your phone should not pair with the device it is connected to.
10. Malicious hackers bypass a public Wi-Fi password by mass testing a huge amount of passwords. This type of attack is called_____attack.

Down

1. The method of leveraging the USB data/power cable to illegitimately access the phone's data and/or inject malicious code onto the device is known as _____
2. Juice jacking can install _____ programs into your smart phone
5. Consider using a privacy _____ if you must access sensitive information in public areas.
6. While using public Wi-Fi, you run the risk of a _____ travelling from another device that's connected to the network to your computer.
8. If you regularly use public Wi-Fi, it is better to use a _____.

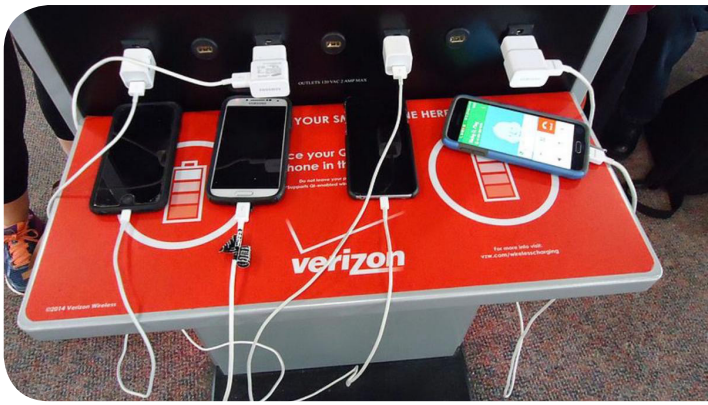
PUBLIC KIOSK SAFETY

A kiosk is a small, stand-alone booth typically placed in public utility places or high-traffic areas. It typically provides information and applications on education, commerce, entertainment, and a variety of other topics. Public kiosks are convenient and can be found in most airports, parks, hotels, and conference centers. If you have spent any time traveling through an airport, you have seen a public charging and free Wi-Fi kiosk. These public kiosks have made our life easier. But most come with unseen and unintended consequences, especially those which use USB cables to charge your device. So, before you plug your phone or login into one of these kiosks, there are some serious security issues and ramifications which needs serious discussion.

PUBLIC CHARGING KIOSK

Most of us might have been in a situation where our mobile phone is running out of battery. Nowadays no one is worried when your phone beeps with low battery as most public places are equipped with charging stations. If you are at an airport, railway station or a shopping mall, it is not that big a problem because these places often have charging stations installed that can be used to charge the battery of almost any mobile phone; and the kiosk will have a suitable charging port for your phone.

These Public kiosk with mobile charging stations are convenient but at the same time, it also has serious security risks associated with. When we think of cyber-attack methods and threats, most of us think of insecure network connections, phishing emails, and malicious websites only.



We may not think of a cyber threat through a public USB power station. Use of freely available charging station make you open to illegal hacking called 'Juice jacking' - hacking through USB ports

But what exactly is Juice Jacking ?

How does it work

The Answer is,

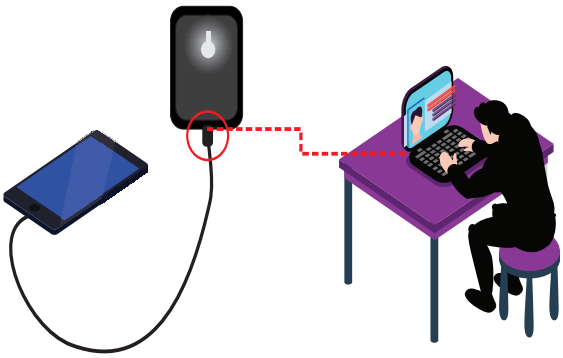
'One Cord Two Functions'

Regardless of the kind of latest smart phone you have – be it an Android device or iPhone, –there is one common feature across all phones viz., the power supply and the data stream pass through the same cable. Whether you are using the USB miniB connection or Apple's proprietary cables, it's the same situation:

The cable used to recharge the battery in your phone is the same cable you use to transfer and sync your data viz., Data/Power being on the same cable, makes it easy for a malicious user to gain access to any phone during the charging process;

This method of leveraging the USB data/power cable to illegitimately access the phone's data and/or inject malicious code onto the device is known as Juice Jacking. Essentially, cybercriminals hijack your power supply channel and use it for their own nefarious deeds.

The attack could be as simple as an invasion of privacy, wherein your phone pairs with a computer concealed within the charging kiosk and information like private photos and contact information and are transferred to the malicious device. The attack could also be as invasive as an injection of malicious code directly into your device where in it can lead to hacking of your personal and financial accounts leading to financial loss.



Cyber criminals try install malware on a victim's device and/or steal data while they use the charging ports. This process can include installing tracking programs and mirroring their screen to see (and record) any passwords and PIN codes they enter while the device is charging. Hence, sometimes juice jacking is also known as "juice filming" or "juice filming charging attacks."

Types of Juice Jacking

There are two types of juice jacking. Juice jacking is a broad enough category that it doesn't just involve the use of malicious or compromised USB wall chargers for data theft. It also includes the use of compromised smartphone charging cables.

Juice jacking attacks typically fall under one of two categories:

Data Theft: This type of juice jacking occurs when victims plug their devices into compromised or fake charging stations using their data-transmitting USB cables. This allows the hackers to steal information, including passwords and pins.

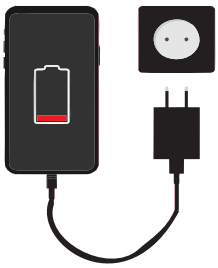
Malicious Installations: This type of juice jacking involves the victims using compromised mobile device accessories such as charging cables. Such a device looks like a regular lightning charging cable, but it's essentially a phone charger that steals your info. Hackers could potentially use these compromised cables to transmit malicious payloads from your device to a nearby device that they control that is within Wi-Fi range.

Note: The use of these charging stations can also offer malicious users a window to your device even after you are no longer in contact with the kiosk: the kiosk you just recharged your Phone can maintain a Wi-Fi to your device for continued access even after you have unplugged your phone.

How to Avoid being a victim of Juice Jacking ?

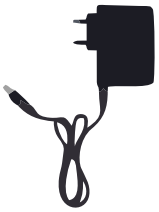
As a precautionary measure it is better to avoid charging your phone using a third-party system unless it is extremely necessary.

- **Keep Your Devices charged:** Keep your mobile device charged. Make it a habit to charge your phone at your home and office when you are not actively using it or sitting at your desk doing your work.
- **Carry your charging cable:** Chargers have become so small and lightweight that they scarcely weigh more than the actual USB cable they attach to. Throw a charger in your bag so you can charge your own phone and maintain control over the data port.



- **Carry a Power bank as Backup:** You can opt to carry an external reserve battery you can travel longer without needing to use a kiosk or wall outlet.

- **Make use of AC adapters:** Juice jacking is not possible if a device is charged via the AC adapter



- **Lock Switch off Your Phone before charging:** When your phone is locked and inaccessible without the input of a PIN or equivalent pass code, your phone should not pair with the device it is connected to.
- **Disable data sharing:** Do not accept the request to allow the cable to be used for data transfer. In case only a data cable is accessible, 'cancel' the request to transfer data, hence, disabling the data flow and allow it to only charge.
- **Switch off Your Phone before charging**: While charging your phone at public charging stations it is better to switch off your phone as it averts the possibility of Malware attack.
- **Use USB "Condoms" or Power-Only USB Cables in Public:** USB condoms are actually devices that can be used as a buffer between your data charging cable and a public USB port. Essentially, they're data blockers, it simply needs to be connected to the USB cable and which prevents data transfer when the mobile is connected to a public USB charging station.

In other words, this device simply converts your USB cable into a mere charging cable, blocking data transfer.

Power-Only USB cables are USB cables with the data wires either removed called as "power only" cables, these cables are missing the two wires necessary for data transmission and have only the two wires for power transmission remaining. By using such cables your device will usually charge more slowly than modern chargers.

According to police sources, there is steep rise in the number of victims of juice jacking. As these ports at the kiosks are not properly monitored, they can be easily tampered with. Inside that tempting cord is an extra chip that deploys hidden malware on your phone to download information without your knowledge. One must be aware that these cords are also designed to transfer data, not just power. Let us see a few examples

Example case 1:
Mr. Kumar Mishra was in Central Delhi's Connaught Place for a reunion when his iPhone vibrated in his jeans pocket. It wasn't a text. A 'low battery' caution had popped up on the screen. The 39-year-old plugged into a nearby free USB power charging station. The party was to be spoiled soon when he received a message that Rs 50,000 has been debited from his bank account, though he had not made any such transaction.

Example Case 2:
Fashion designing student Sushmita Purohit, who often visits South Delhi's Khan Market, was also shocked when objectionable content had been posted on her social media. pages - without her knowledge. She immediately reported the post in the social media and the posts were removed. When she recollected, she could recollect connecting her phone to a free charging station at Khan Market.

Note: A victim of "Juice Jacking" can move to police with a request for FIR under section 66 of Indian Information Technology Act and moreover, he can seek for claim too under section 43 of Information Technology Act.

PUBLIC WI-FI KIOSK

Recognizing internet as a critical tool for day-to-day work and facilitating increased access to it in the past few years, the Indian Government as well as Governments across the world have rolled out plans for offering public Wi-Fi. This recent explosion of free, public Wi-Fi has been an enormous boon for working professionals. This freedom comes at a price.

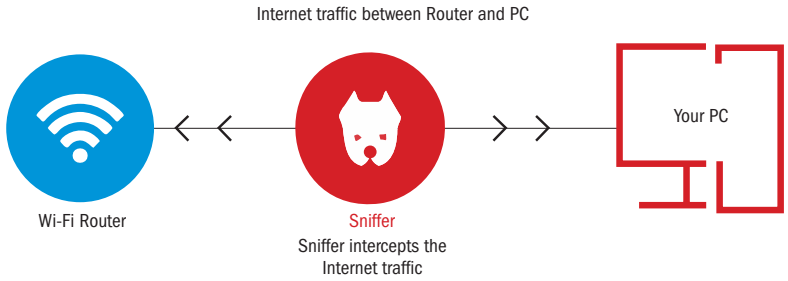
The biggest threat to free Wi-Fi security is the ability for the hacker to position himself between the user and the connection point. So instead of the hotspot, the user will send your information to the hacker.

In such a case, an attacker creates a rogue hotspot with the intent to unleash man-in-the-middle (MITM) attacks on unsuspecting victims that join their rogue network. This type of attack allows an attacker to intercept the communication between you and the servers of the websites you visit, allowing them to read, insert, and modify messages.

The hacker then has access to every piece of information the user is sending out on the Internet like important emails, credit card information and even security credentials to your business network. Just because you may need a password to log in, it does not mean your online activities are encrypted.

Methods of attack used by hackers

- **Brute force/cracking attacks:** These can be used by malicious hackers to bypass a public Wi-Fi password either by mass testing a huge amount of passwords (brute force attacks) or by using specialized software and tools to trick the router into revealing the password (cracking attack).
- **War driving:** In this method malicious hacker driving around various locations, looking for vulnerable Wi-Fi connections he can later exploit.
- **Wi-Fi Sniffing:** This process involves specialized intercepting tools or software that can intercept and reassemble internet data sent between a router and a device. From a technical perspective, it's very easy to set up a Wi-Fi sniffer since all you need is a laptop and some widely available software to add the necessary functions.



- **Karma Attacks:** To carry out this type of attack, a malicious hacker needs a specialized hardware tool which can create a clone of the target Wi-Fi, tricking connected devices into switching to the cloned network. At this stage, the malicious hacker has complete visibility of what the connected devices are doing while in the network.
- **Distribution of malware over unsecured Wi-Fi:** Hackers can also use an unsecured Wi-Fi connection to distribute malware. Having infected software on your computers and devices can be financially crippling
- **Worm attacks:** Worms act much like viruses, with one key difference. Viruses must have a program to attack in order to successfully compromise a system, while worms can wreak havoc all by themselves. When connected to a public Wi-Fi, you run the risk of a worm travelling from another device that's connected to the network to your computer.

Measures you can take to stay protected on public Wi-Fi

Generally speaking, as a precaution, you should not engage in any sort of sensitive web browsing, such as accessing your bank account or entering payment details when connected to public Wi-Fi. Consider these additional safety measures to keep your information protected:

- **Stay Protected:**
  Never use public Wi-Fi networks to access sensitive information. Casual browsing is ok with public Wi-Fi.
- **Use a VPN:**
  

  If you regularly use public Wi-Fi, it is better to use a Virtual Private Network (VPN), which creates a private network for you to shuttle information back and forth, adding an extra layer of security to your connection. Find a trusted VPN services online, but always better to choose one from a reputable security provider.
- **Keep Wi-Fi Off When You Don't Need It:**
  
  If you're just using your computer to work on a Word or Excel document, keep your Wi-Fi off. Also, configure the wireless settings on your devices to not automatically connect to available Wi-Fi hotspots. This ensures that you do not unknowingly connect to public networks. You can do this by turning off the "Connect Automatically" feature on your computers so do not auto-connect and search for known Wi-Fi networks.
- **Use SSL Connections:**
  

  Only browse websites that start with HTTPS and avoid websites that start with HTTP while on public Wi-Fi. Websites that start with HTTPS are encrypted, adding an extra layer of security and making your browsing more secure. You should also consider installing an extension like HTTPS-Everywhere to force all websites you visit to connect using HTTPS.
- **Make use of Privacy Screen:**
  Consider using a privacy screen if you must access sensitive information in public areas.

Case study:

Within 20 minutes a hacker was able to know many details of the people who used the public Wi-Fi at the coffee shop; where he was there. Personal information like name, age, birthplace, schools attended and last five things they have goggled wee easily accessible by the hacker.

All that Hacker uses is a black box with antenna and his laptop. Hacker switches on his laptop and device, launches some programs and soon the screen starts to fill with green text lines. It gradually becomes clear that hacker's device is connecting to the laptops, smart phones, and tablets of cafe visitors. The antenna of the device is intercepting the signals that are being sent from the laptops, smart phones, and tablets around. Hacker was able to see which Wi-Fi networks the devices were previously connected to; the names of the networks are composed of mostly numbers and random letters, making it hard to trace them to a definite location. The hacker could also retrieve their passwords; steal their identity, and their banking details.

Any hacker trying to hack using public wifi network will wait for everyone to connect to the fake network. Then he will scan for name, passwords and other details. Later he will try to obtain information about his employment and, hobbies.

Treat and protect your mobile devices such as smart phones and tablets with the same precautions you would do for your laptop or desktop computer when you join a Wi-Fi network.

CERT-In Vulnerability Note CIVN-2020-0054
Remote code execution vulnerability in Zoho ManageEngine Desktop Central

Software Affected
Zoho ManageEngine Desktop Central prior to 10.0.474

Overview
A vulnerability has been reported in Zoho ManageEngine Desktop Central, which could allow an unauthenticated remote attacker to execute arbitrary code on a targeted system.

Description
This vulnerability exists in ZohoManageEngine Desktop Central due to improper input validation in the FileStorage class. An unauthenticated remote attacker could exploit this vulnerability by uploading a malicious file containing a serialized payload onto an affected system and then make a subsequent request for the uploaded file to trigger an untrusted deserialization.

Successful exploitation of this vulnerability may allow the attacker to gain root-level access and execute arbitrary code on the targeted system.

For more deails visit
https://www.manageengine.com/products/desktop-central/service-packs.html

CERT-In Vulnerability Note CIVN-2020-0053
Windows Adobe Type Manager Library Remote Code Execution Vulnerabilities

Overview
Two remote code execution vulnerabilities have been reported in Microsoft Windows, which could allow a remote attacker to run malicious code on the target machine.

Description
These vulnerabilities exist in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles a specially-crafted, multi-master font - Adobe Type 1 PostScript format. A remote attacker could exploit these vulnerabilities by convincing a victim to open a specially crafted document or view it in the Windows Preview Pane. Attackers could exploit this vulnerability through WebDAV also.

Successful exploitation of these vulnerabilities allow the attacker to trigger memory corruption and executing arbitrary code on the system. This may result in complete compromise of vulnerable system.

Note: Some attackers are already exploiting them in limited, targeted attacks.

For more deails visit
https://www.cert-in.org.in/t?pageid=PUBVLNOTES01&VLCODE=CIVN-2020-0053

CERT-In Vulnerability Note CIVN-2020-0052
Multiple Vulnerabilities in Microsoft Visual Studio

Overview
Multiple vulnerabilities have been reported in Microsoft Visual Studio which could allow remote attacker to execute denial of service attack, elevation of privilege and spoofing on the targeted system.

Description
Denial of Service Vulnerability (CVE-2020-0789)This vulnerability exists in Microsoft Visual Studio due to improper handling of hard links by the Extension Installer Service. A local attacker could exploit this vulnerability by running a specially crafted application on the affected system.
Successful exploitation of this vulnerability could allow the attacker to overwrite system files and cause Denial of Services on targeted system.

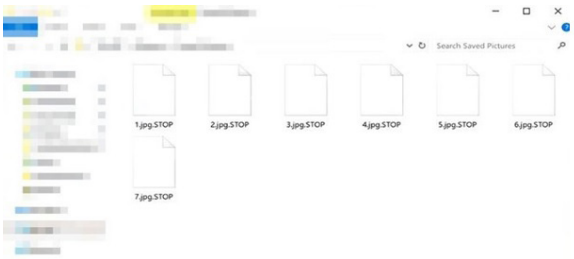
Elevation of Privilege Vulnerability (CVE-2020-0793 CVE-2020-0810)
This vulnerability exists in Microsoft Visual Studio due to improper handling of file operations by the Diagnostics Hub Standard Collector or the Visual Studio Standard Collector. An unauthenticated attacker could exploit this vulnerability by running a specially-crafted application on the affected system.
Successful exploitation of this vulnerability could allow the attacker to escalate privileges on targeted system.

Spoofing Vulnerability (CVE-2020-0884)
This vulnerability exists in Microsoft Visual Studio due to the use of reply URL that is not secured by SSL .An attacker could exploit this vulnerability by persuading a victim to open a specially-crafted content.
Successful exploitation of this vulnerability could allow a remote attacker to spoof access tokens and obtain potentially sensitive information.

For more deails visit
https://www.cert-in.org.in/t?pageid=PUBVLNOTES01&VLCODE=CIVN-2020-0052

"STOP" Ransomware

CERT-In has observed a new variant of "STOP" ransomware is spreading widely. Once the victim computer is infiltrated with STOP ransomware, all files are encrypted and an extension ".stop" is appended to the encrypted iles at the end. After encrypting all the files, ransomware will also delete the Shadow Volume Copies so that recovery is not possible.



After encrypting, STOP malware generates a ransom note file "!!! YourDataRestore !!! txt" which contains the message asking for ransom from the victim to decrypt their encrypted data. Ransom note provides an email address for communication.

The ransomware campaign uses Spear Phishing, Social Engineering, Browser Targeted Code Injection and Abuse of Application Functionality as its attack vectors. The ransomware is exploiting flowing vulnerabilities mainly belonging to Buffer overflow, Remote Code Execution and Windows Denial of Service categories (CVE-2016-10057, CVE-2016-10401, CVE-2017-0144, CVE-2017-10271, CVE-2017-12149, CVE-2018-0986, CVE-2018-1000136, CVE-2018-10115, CVE-2018-20250, CVE-2018-3639, CVE-2018-5383, CVE-2018-5391, CVE-2018-6789, CVE-2018-7602, CVE-2018-9995, CWE-119, CWE-19, CWE-20, CWE-200, CWE-22, CWE-255, CWE-284, CWE-310, CWE-347, CWE-502).

Following are some steps which can be taken to prevent further such Infections:

- Perform regular backups of all critical information to limit the Impact of data or system loss and to help expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline
- Keep the operating system third party applications (MS Office, browsers, browser Plugins) up-to-date with the latest patches.
- Maintain updated Antivirus software on all systems.
- Don't open attachments in unsolicited e-mails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited e-mail, even if the link seems benign. In cases of genuine URLs ,close out the e-mail and go to the organization's website directly through the browser.

For moredetails visit:
https://www.cyberswachhtakendra.gov.in/alerts/STOP_ransomware.html

Storyboard on Malware

Siddu and Somu were best friends in their school. Both of them loved to play PC games.

One day, both of them were playing "Battle kings" limited version game in Somu's PC

After sometime, they started searching for new game

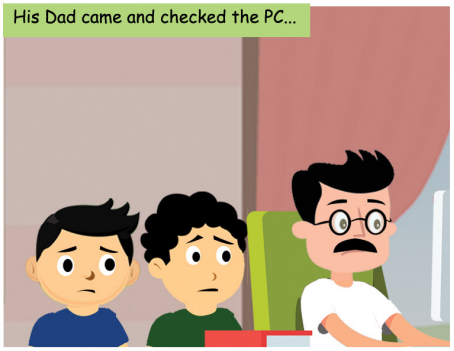
A game download link of "Battlekings" popped up in a website

Both of them were excited. They downloaded the game and started installing it

After the installation completed, the PC was affected

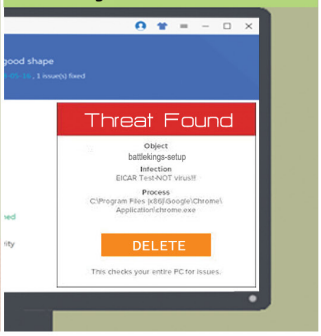
Somu got tensed and called his Dad for help...

His Dad came and checked the PC...



He installed an antivirus and scanned the PC

They came to know that this happened due to the game download



His Dad warned him not to install anything from unknown links

For queries on Information Security
Call us to Toll Free No.

1800 425 6235

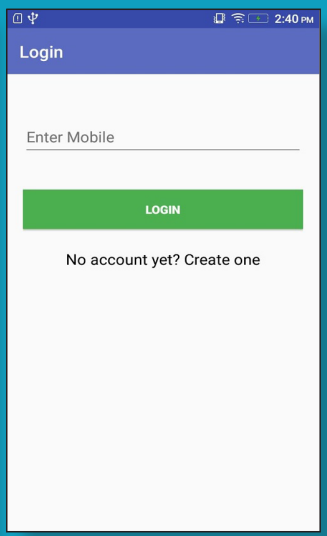
For details on
Cyber Crime Cells in India and Cyber Crime Reporting Portal
visit https://www.infosecawareness.in

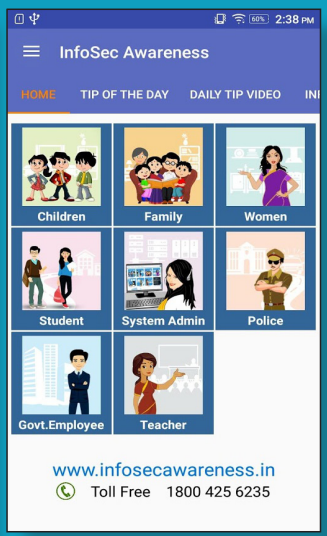
InfoSec WORKSHOPS

Tales of Cyber Security fir Children in telugu @ Hyderabad
Released by
Shri V C Sajjanar, IPS, Commissioner of Police, Cyberabad,
Smt. C Anasuya, Dy. Commissioner of Police, SHE Teams, Cyberabad,
Ch A S Murty, Associate Director, C-DAC Hyderabad and UNICEF

Request for workshop

https://isea-pmu.in/requestForWorkshop/





Download ISEA Mobile App From Google PlayStore

To Share Tips / Latest News, mail us to

isea@cdac.in

About ISEA

Looking at the growing importance for the Information Security, Ministry of Electronics & Information Technology has identified this as a critical area. Information Security Education and Awareness (ISEA) Project was formulated and launched by the Govt. of India. One of the activities under this programme is to spread Information Security Awareness among children, teachers, home users, IT and non-IT professionals throughout the country. C-DAC Hyderabad has been assigned the responsibility of executing this project by Ministry of Electronics & Information Technology, Government of India. As part of this activity C-DAC, Hyderabad has been preparing Information Security Awareness material, coordinating with Participating Institutes (PI's) in organizing the various Information Security Awareness events all over India.

About C-DAC

C-DAC established its Hyderabad Centre in the year 1999 to work in Research, Development and Training activities embracing the latest Hardware & Software Technologies. The centre is a Knowledge Centre with the components of Knowledge Creation, Knowledge Dissemination and Knowledge Application to grow in the areas of Research & Development, Training and Business respectively. The R & D areas of the centre are e-Security, Embedded Systems, Ubiquitous Computing, e-Learning and ICT for Rural Development. The centre has developed over a period of time a number of products and solutions and has established a number of labs in cutting edge technologies. In line with these R&D strengths, the centre also offers Post Graduate level diploma courses. Centre is also actively involved in organizing faculty training programs. The centre regularly conducts skill based training and information security awareness programmes. InDG portal is hosted and maintained to facilitate rural development through provision of relevant information, products and services in local languages.

BOOK POST

For queries on Information security

Call us on Toll Free No.

1800 425 6235

between 10.00 AM to 6.00 PM
or give us a missed call
we will call you back within 24 hrs

ISEA Whatsapp Number for Incident Reporting

+91 9490771800

Between 9.00 AM to 5.30 PM

Subscribe us on

https://www.youtube.com/c/InformationSecurityEducationandAwareness

Follow us on

https://twitter.com/InfoSecAwa

Connect us with

https://www.facebook.com/infosecawareness

Ministry of Electronics & Information Technology
Government of India

प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Electronics and Information Technology, Government of India

Plot No: 6&7, Hardware Park Sy. No.1/1, Srisailam Highway Raviryal (V & GP), Via Ragaanna guda, Maheshwaram (M), Ranga Reddy District, Hyderabad – 501510. Tel: 9248920201.