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

InfoSec
Newsletter
Jan-Feb, 2020

InfoSec
Concept 3 page

KNOW ABOUT YOUR DIGITAL FOOTPRINT

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

सी डैक
CDAC
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 - 501510Telangana(India)
Nalanda Building, No. 1 Shivabagh Satyam Theatre Road, Ameerpet, Hyderabad - 500016, Telangana (India)

InfoSec Newsletter

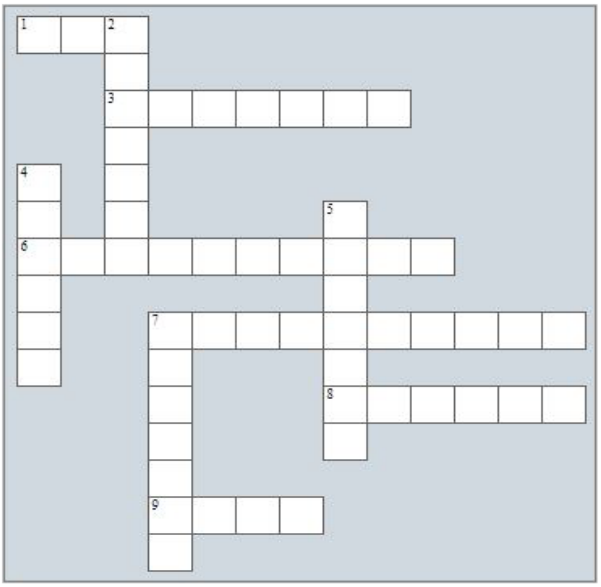
JAN-FEB 2020

CREDITS

InfoSec CONTEST

1. Digital footprints should be a significant_____concern for Internet users
   a) Privacy b) Security
   c) Identity d) None the above
2. Data are the facts or details from which_____is derived.
   a) Identity b) Information
   c) Footprint d) None the above
3. _____ can be something simple and seemingly random and useless until it is organized.
   a) Data b) Information
   c) Both d) None of the above
4. _____digital footprint is collected without our knowledge and is used to target you through advertisements, build customer profiles and more.
   a)Passive b)Active
   c) None of the above d) Both
5. How many kinds of digital foot print are there?
   a) One b) Three
   c) Two d) Four

InfoSec CROSSWORD



Across

1. Avoid usage of _____ and other external devices on office systems.
3. Agreeing to install _____ on your devices when prompted by the browser is an example for active digital foot print.
6. Carefully Managing your foot print helps you to protect your _____
7. Active digital footprint is the _____traceable information that you share online, like social media profile information, updates, posts, photos and videos shared.
8. Filling out online forms, such as when signing up to receive emails or texts is an example of _____ foot print
9. Have a _____ limit on the time spend on social media.

Down

2. Every organisation needs to ensure that they have an strong data _____ and recovery plan
4. Enforce _____ password usage in organisations
5. The _____ record that you leave behind is capable of being misused by social media service providers.
7. Keep your passwords and personal details _____

Know about your DIGITAL FOOTPRINT

There is a subtle difference between data and information.Data are the facts or details from which information is derived. Individual pieces of data are rarely useful alone. For data to become information, data needs to be put into context. In simple words, For any individual, his/her name, address, bank account details etc., are his/her personal data. when you use this personal data to get meaningful information i.e Raj got 80 % in 10th std exam is an information about Raj.

Comparison of Data & Information

Data	Information
Data is raw, unorganized facts that need to be processed. Data can be something simple and seemingly random and useless until it is organized.	When data is processed, organized, structured or presented in a given context so as to make it useful, it is called information.
Each student's exam score is one piece of data.	The average score of a class or of the entire school is information that can be derived from the given data.

Examples of Data and Information

- The temperature readings of a sick person for two days is data. If this data is organized and analyzed to find that the patient is affected with particular disease, then that is information.
- The number of visitors to a website is an example of data. Finding out how many people accessed website from a particular region is meaningful information.

Whenever you go online you leave behind some information about yourself like sending an email to someone, posting a picture on your social networks, commenting on a post or a news story, video calls, apps that you use, or even a simple Google search. So, it is extremely important that you know what kind of trail you are leaving, and what can be the possible effects it can bring in your life. Your digital footprint is all that you leave behind as you use the Internet. It is actually a part of your online history and can potentially be seen by other people, or tracked in a database by service providers. For example, the negative review you gave for a service team that could not fix your problem is available for anyone to read, forever. A picture of yours sent to your friend will be there in some server and can be used by anyone. All of these digital activities can create a much larger picture of who you are and where you have been, what you have done and how you respond to certain situations. There are two kinds of digital footprint: 'passive' and 'active'.

Passive digital footprint

Passive digital footprint is collected without our knowledge and is used to target you through advertisements, build customer profiles and more. This includes information like individual browsing data, IP addresses, purchasing habits and many more.

Here are a few examples of passive digital footprints.

- Websites that install cookies in your device without disclosing it to you
- Apps and websites that use geolocation to pinpoint your location
- Social media news channels and advertisers that use your likes, shares, and comments to profile you and to serve up advertisements based on your interests

Active digital footprint

Active digital footprint is the publicly-traceable information that you share online, like social media profile information, updates, posts, photos and videos shared.

Here are a few examples of active digital footprints.

- Posting on Facebook, Instagram, Snapchat, Twitter, and other social media platforms
- Filling out online forms, such as when signing up to receive emails or texts
- Agreeing to install cookies on your devices when prompted by the browser

Why to manage digital foot print

Digital footprints should be a significant privacy concern for Internet users, because they can be used to track user actions and are a strong basis for "profiling" by online service providers and others. The digital record that you leave behind is capable of being misused by social media service providers. Service providers and other third parties exchange data about customer profiles and online transaction statistics. Many a time third party vendors may use the data without service provider's knowledge.

Every time an individual uses Internet, the digital footprint that they leave behind is small, but when linked with previous data, it is possible to construct a complete profile about an individual. This data is mainly collected from web sites you have visited, the products you have bought or searched for, your address, and any other information you have given to any web site like age, sex, health, marital status, employment, financial information etc.., the list is as long as everything you have ever shared on the Internet.

The need to manage foot print is for

- Protecting your reputation
- Maintaining your ability to decide where and how your personal information is shared
- Preventing financial loss
- Preserving your freedom to make choices and preferences

How to carefully secure your Personal information and leave a positive digital footprint

- Use only your first name. If possible, use your nick names. Try to avoid abundance of personal information in social media profiles when you create an account. But make sure you provide only true and relevant information.
- Keep your passwords and personal details private.
- Keep evidence if you are being bullied and do not bully back; it is always better to seek help from parents/ guardians.
- Make sure the information you shared in social media is true.
- Make sure you have a check on access rights of your data by any new website or Application.
- Think about who will read the information you have shared online. Can anyone misunderstand what you have shared?
- Have a time limit on the time spend on social media.
- Try to know about the current cyber crime issues and also develop good digital hygiene habits.
- Find and use privacy enhancing tools.
- Very often, the default settings for browsers, devices and apps are set to disclose your personal data, rather than secure. It is worth taking time to investigate those settings and make sure you are comfortable with them, just like it is worth checking whether you latched the windows before you left the house.
- Think before you accept 'permission to send push notifications and access location data', by any application.
- Your camera and smart-phone usually record the time and location in each photo you take, and when you share those photos, you may be publishing that data unless you specifically block it.

Data / Information Protection Tips for organizations:

With new threats emerging, it is inevitable for organizations including all employees to adopt certain measures to protect personally identifiable information (PII).

- **Update Your Systems and Software:** Stay up to date with the latest operating system and additional software updates.
- **Encryption:** Encrypt confidential information shared by employees, partners, and customers.
- **Password Creation:** Enforce strong password usage, with a regular change in passwords every few months.
- **No External Connections:** Avoid using USBs and other external devices on your office system, which can implement the transfer of data from one device to the other. This also includes using USB portals to charge mobile phones and other electronic devices.
- **Data Backup and Recovery:** Consult your information security executives to ensure that you have a strong data backup and recovery procedure that is constantly updated.

At the same time, it also important to ensure that you actually have an online presence. Once you are in online world, he/she needs to manage their Personal information and digital identity and be aware of the permanence of their actions in a digital world". Now since most of our lives are intertwined with digital technology, the best thing we can do is to be aware and be secured.

References

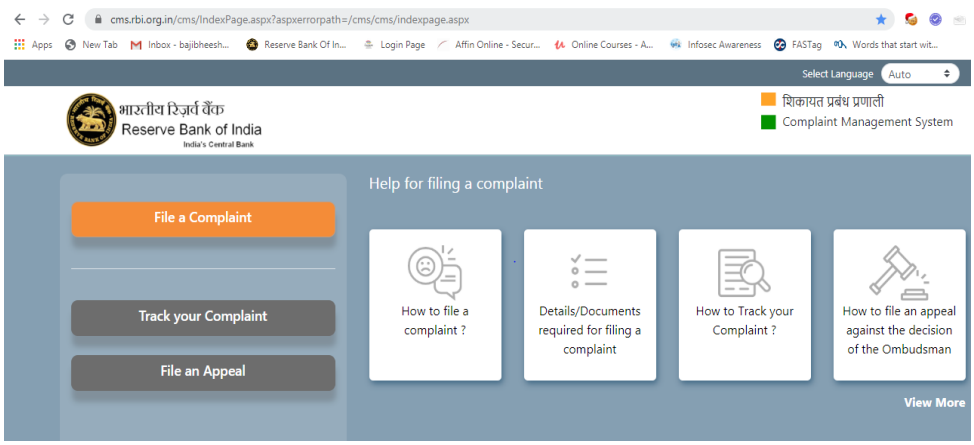
- http://www.itpro.co.uk/
- https://us.norton.com/
- https://www.internetsociety.org
- https://blogs.upm.es
- https://www.diffen.com

ISEA, Supported by MeitY, Government of India

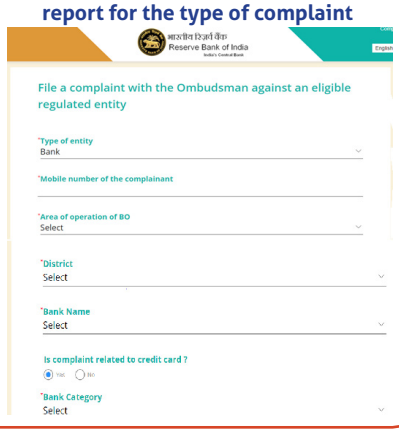
InfoSec

Newsletter updates

File a complaint to Reserve Bank of India if you are a victim of financial fraud in India.
To report click on the link
https://cms.rbi.org.in/cms/IndexPage.aspx?aspxerrorpath=/cms/cms/indexpage.aspx



Select the category Bank and report for the type of complaint



VPNs emerge as new channel for attacks as security researchers uncover multiple security issues

Virtual Private Networks (VPNs) are basically used to shield online users against web attacks and other online threats but with the emergence of new vulnerabilities, they can now be weaponized against users.

- An attacker can sniff, hijack and tamper VPN-tunneled connections by abusing a flaw in Linux, Android, macOS, and other Unix-based operating systems.
- Aviatrix VPN is also found to be impacted by multiple local privilege escalation vulnerabilities.

For more details click on the link below
https://cyware.com/news/vpns-emerge-as-new-channel-for-attacks-as-security-researchers-uncover-multiple-security-issues-a9dd4cda

Linux Bug Opens Most VPNs to Hijacking

A vulnerability in most Linux distros has been uncovered that allows a network-adjacent attacker to hijack VPN connections and inject rogue data into the secure tunnels that victims are using to communicate with remote servers.

For more information click on the link given below:
https://threatpost.com/linux-bug-vpns-hijacking/150891/

Newsletter updates

Fake Windows update installs Ransomware on PCs, Beware of emails claiming to be from Microsoft

Researchers fromTrustwave's SpiderLabsdiscovered the spam emails, which come with an 'Install Latest Microsoft Windows Update now!' or 'Critical Microsoft Windows Update!' subject line. Microsoft, of course, doesn't send out Windows updates through email.

The messages contain just one sentence, and the first word begins with two capital letters, making it appear even less legitimate. Recipients are asked to click an attachment to download the 'update.' While the file has a .jpg extension, it's actually an executable .NET downloader that delivers malware to the infected system.

Clicking on the file will download another executable, this one called bitcoingenerator.exe from a (now-removed) Github account named misterbtc2020. Like the email attachment, this is .NET compiled malware—the Cyborg ransomware.

For more information click on the link given below:
https://www.techspot.com/news/82850-fake-windows-update-installs-ransomware-pcs.html

Android Camera App Bug Lets Apps Record Video Without Permission

A new vulnerability has been found in the Camera apps for millions, if not hundreds of millions, of Android devices that could allow other apps to record video, take pictures, and extract GPS data from media without having the requiredpermissions.

This vulnerability, known as CVE-2019-2234, is known to affect the Google Camera and Samsung Camera apps if they have not been updated since before July 2019.

For more information click on the link given below:
https://www.bleepingcomputer.com/news/security/android-camera-app-bug-lets-apps-record-video-without-permission/

Officials warn about the dangers of using public USB charging stations

Travelers should use only AC charging ports, use USB no-data cable.

Travelers are advised to avoid using public USB power charging stations in airports, hotels, and other locations because they may contain dangerous malware. USB connections were designed to work as both data and power transfer mediums, with no strict barrier between the two. As smartphones became more popular in the past decade, security researchers figured out they could abuse USB connections that a user might think was only transferring electrical power to hide and deliver secret data payloads.
This type of attack received its own name, as "juice jacking."

For more information click on the link given below:
https://www.zdnet.com/article/officials-warn-about-the-dangers-of-using-public-usb-charging-stations/

Virus Alerts

CERT-In Advisory CIAD-2019-0037 StrandHogg vulnerability in Google Android

Software Affected
Android Operating System

Description
A vulnerability which has been named "StrandHogg" has been reported to be present in the Android operating system. The vulnerability allows a malicious application tomasquerade as any other app.The vulnerability exploits an Android control setting called "taskAffinity" which allows an application to assume any identity in the multitasking system.

When users tap on a legitimate app, a malicious code is triggered in place of the original one. The attacker can then access sensitive information and fetch user's login credentials and gain access to security-sensitive apps.

References
https://promon.co/security-news/strandhogg/
https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/strandhogg-android-vulnerability-allows-malware-to-hijack-legitimate-apps
https://threatpost.com/strandhogg-vulnerability-allows-malware-to-pose-as-legitimate-android-apps/150750/

CERT-In Vulnerability Note CIVN-2020-0001 Denial of Service Vulnerability in Linux Kernel

Software Affected
Linux kernel version 5.0.0-rc7

Overview
A vulnerability has been reported in Linux kernel which could allow a local attacker to cause denial of service conditions on a targeted system.

Description
This vulnerability exists in ttm_put_pages() function of the file drivers/gpu/drm/ttm/ttm_page_alloc.c of Linux kernel. A local attacker can exploit this vulnerability by mounting a specially crafted f2fs file system image to cause an out-of¿bounds memory read operation.

Solution
Apply appropriate patches as mentioned in the following links:
https://github.com/torvalds/linux/commit/ac1e516d5a4c56bf0cb4a3dfc0672f689131cfd4

https://github.com/torvalds/linux/commit/a66477b0efe511d98dde3e4aaeb189790e6f0a39

https://github.com/torvalds/linux/commit/453393369dc9806d2455151e329c599684762428

For more details visit:
https://cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES01&VLCODE=CIVN-2020-0001

CERT-In Vulnerability Note CIVN-2020-0002 Remote Code Execution Vulnerability in Citrix Products

Component Affected
- Citrix Application Delivery Controller(ADC) and Citrix Gateway version 13.0
- Citrix Application Delivery Controller(ADC) and NetScaler Gateway version 12.1

Overview
A vulnerability has been reported in Citrix Application Delivery Controller and Citrix Gateway which could allow a remote attacker to execute arbitrary code on a targeted system.

Description
The vulnerability exists in Citrix ADC and Citrix Gateway due to improper handling of HTTP based VPN requests. A remote attacker may exploit this vulnerability by sending a crafted web request to the affected systems. Successful exploitation of the vulnerability could allow the attacker to execute arbitrary code on the targeted system.

Solution
Apply appropriate mitigation steps as mentioned in the following link:
https://support.citrix.com/article/CTX267027

CERT-In Vulnerability Note CIVN-2020-0003 Remote Code Execution and Other Vulnerabilities in Ruckus Wi-Fi routers

Component Affected
- Ruckus ZoneDirector9.10.x
- Ruckus ZoneDirector9.12.x
- Ruckus ZoneDirector9.13.x
- Ruckus ZoneDirector10.0.x
- Ruckus ZoneDirector10.1.x

Overview
Multiple vulnerabilities have been reported in Ruckus Wi-Fi routers which could allow an attacker to gain unauthenticated access to ZoneDirector and Unleashed APs.

Description
Multiple Vulnerabilities exist on the ZoneDirector and Unleashed product lines due to insufficient input validation. These vulnerabilities allow an attacker to perform the following actions:

- Unauthenticated, remote code executions and gain command line interface (CLI) and shell access
- Command injections

For more details visit:
https://cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES01&VLCODE=CIVN-2020-0003

Workshops


@Medak

@Chennai


@Erode


@Ramagundam


@NCR Region


@Delhi


@Delhi


@Bhubaneshwar


@Bhubaneshwar

Request for workshop
https://isea-pmu.in/requestForWorkshop/

MeitY's Information Security Education Awareness (ISEA) Project, being implemented by C-DAC Hyderabad along with other C-DAC centres, won NASSCOM-DSCI Excellence Awards 2019 (Special Jury Recognition) for its concerted efforts in Raising Information Security Awareness through direct workshops for Academic, Government, General Users and creating extraordinary mass outreach through Print and Electronic Media (Newsletters/Annual Magazine, Handbooks, Short Videos etc.,), Awareness Week, Master Trainer's program etc.

Shri Ajay Sawhney, IAS, Secretary, Ministry of Electronics & Information Technology (MeitY) Government of India presented the Award to ISEA, C-DAC Team.

Release of ISEA New Year Calendar 2020, by Shri Sanjay Dhotre, Hon'ble Minister of States, MHRD & MeitY at ISEA Stall during National ICT Awards, 2019 at New Delhi

ISEA,Supported by MeitY,Government of India

Short Story on Identity Theft

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**

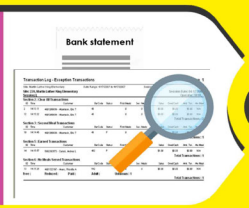
Best practices to avoid Financial Frauds

Never handover your device to strangers

Avoid using open Wi-Fi for making payments

Disclose your banking details only in secure payment websites

Keep a watch on transaction logs and alerts



Always verify and install authentic e-wallet Apps

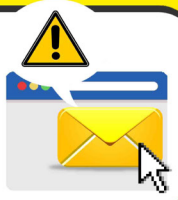
Immediately block your SIM if your device gets lost or stolen

Report promptly the theft or loss of your card on the toll free numbers

Ensure that you securely dispose your payment receipts & bank statements

Use strong passwords and change frequently

Refrain from clicking suspicious links received in SMS or email



For more details / queries on Cyber Security visit or call us to our Toll free number

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

www.InfoSecawareness.in

1800 425 6235

For Virus Alerts, Incident & Vulnerability Reporting
certin Handling Computer Security Incidents
http://cert-in.org.in/

www.cyberswachhtakendra.gov.in

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 and Information Technology (MeitY)
Government of India

सी डैक
CDAC
www.cdac.in

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,
Pahadi Shareef Via Keshavagiri (Post), Hyderabad - 501510, Telangana(India)