



Information Security Education & Awareness

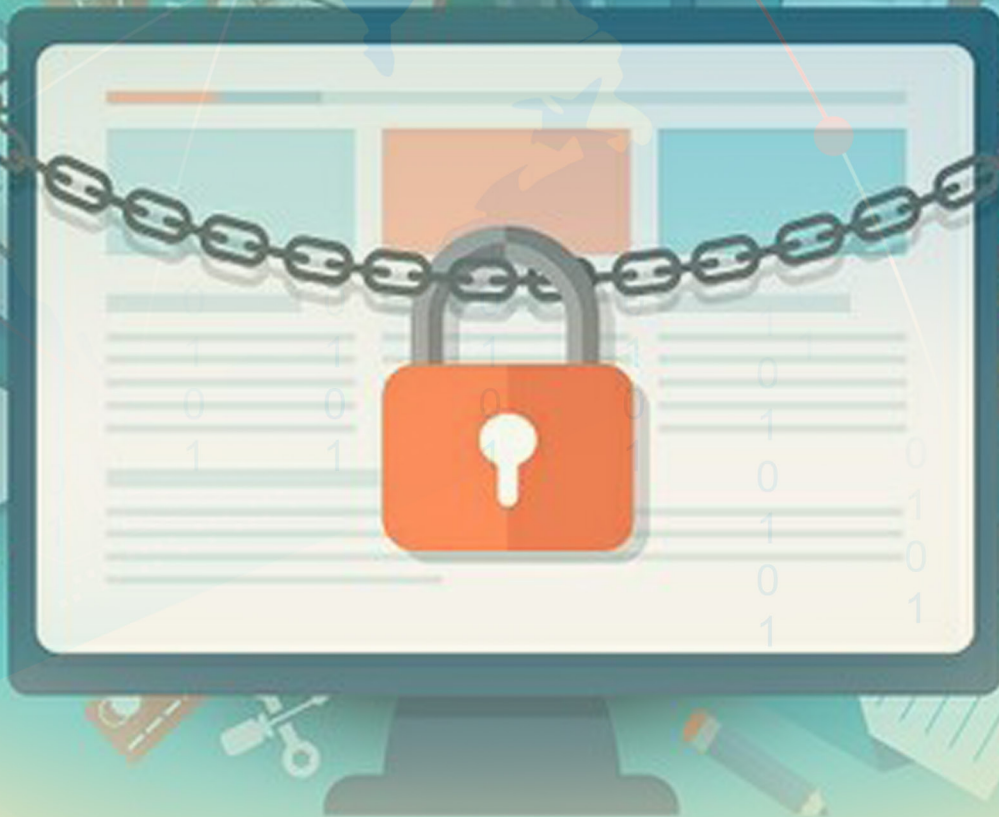
Department of Electronics and Information Technology
Ministry of Communications and Information Technology
Government of India

सी डैक
CDAC

InfoSec Newsletter July-August 2016

Concept 3
Alerts 9
Tools 10
News 11

Data privacy



For Virus Alerts, Incident & Vulnerability Reporting

certin
Handling Computer Security Incidents

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, Srisailem Highway, Pahadi Shareef Via Keshavagiri (Post)
Hyderabad - 500005, Telangana (India)

Newsletter July - August 2016

Credits

Prof. N Balakrishnan
(IISc, Bangalore)
Prof. Sukumar Nandi
(IIT, Guwahati)
Prof. V Kamakoti (IIT, Madras)
Prof. M S Gaur (SVNIT, Jaipur)

Design & Technical Team

Ch A S Murty
I L Narasimha Rao
K Indra Veni
K Indra Keerthi
P S S Bharadwaj

Action Group Members

HoD (HRD), DeitY
Shri.Sitaram Chamarthi (TCS)
Prof. M S Gaur (MNIT, Jaipur)
Prof. Dr.Dhiren R Patel
(NIT Surat)
Representative of Chairman
(CBSE)
CEO, DSCI (NASSCOM)
Representative of Prasar Bharati,
Member of I & B
Shri U Rama Mohan Rao
(SP, Cyber Crimes, CID,
Hyderabad, Andhra Pradesh)
Shri S K Vyas, DietY

Compiled by

G V Raghunathan

From C-DAC

E Magesh, Director

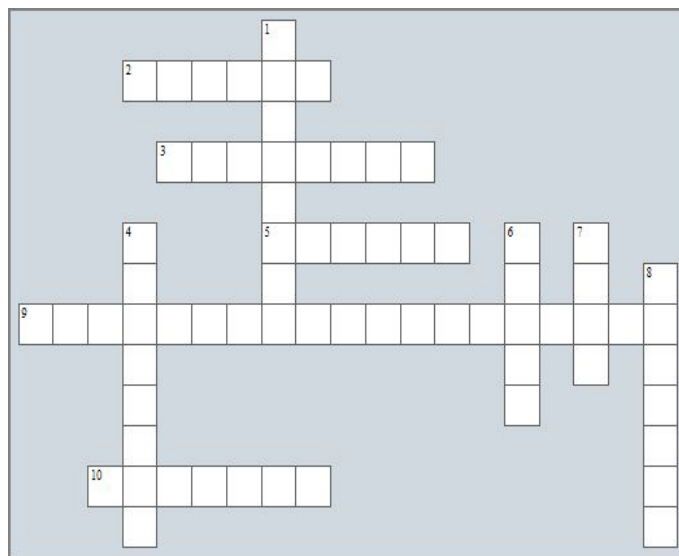
Acknowledgement

HRD Division
Department of Electronics &
Information Technology
Ministry of Communications &
Information Technology
&

For Virus Alerts, Incident & Vulnerability Reporting

certin
Handling Computer Security Incidents

1. The statement, "Information systems should be configured to require strong passwords," is an example of a/an:
A) Security requirement B) Security policy
2. What term describes software that allows a hacker to remotely take control of a computer while avoiding detection?
A) Linux B) Rootkit
3. When you sign in to the online store to do online shopping you get notification that their password database has been hacked and that you reset your password. What's the best password to choose?
A) B@n@na\$ B) CB@n@n@\$
4. Only Click the web links in your e-mail for updating your personal details as and when the bank will ask you to update the accounts through online(Required)
A) True B) False
5. Junk e-mail, as in mass mailings, is annoying but harmless
A) True B) False



login to
**www.
InfoSec
awareness.in
/contest**
to participate in
Infosec Contest and
WIN PRIZES

**InfoSec
Crossword**

Across

2. A _____ is the small amount of information that a website copies to the hard drive, which helps that website identify you the next time you visit. Of course, it is also a small flat sweet cake.
3. Use this tool to dispose of documents that contain personal or financial information.
5. _____ is software that displays ads on your computer while you are using it, often in the form of popups. It is almost always installed without your authorization or hidden with another program you installed
9. _____ is any information that can personally identify you, such as your name, address, phone numbers, Social Security number, bank account number, credit card number etc.,
10. The front line of defense in Information Security

Down

1. A _____ is hardware or software that helps keep hackers from using your computer to send out your personal information without your permission. It watches for outside attempts to access your system and blocks communications to and from sources you don't permit.
4. Never share your _____ with another person
6. To protect personal information, avoid sending it via _____.
7. _____ is a term for spam messages sent to instant message addresses.
8. A _____ is a program and/or device that monitors data traveling over a network. These programs/devices can be used both for legitimate network management and for stealing information off a network.



Data Privacy

Information privacy, or data privacy (or data protection), is the privacy of personal information and usually relates to personal data stored on computer systems.

The need to maintain information privacy is applicable to collected personal information, such as medical records, financial data, criminal records, political records, business related information or website data.

The Privacy exist wherever personally identifiable information or any other sensitive information is collected, stored, used, deleted or destroyed in digital form or otherwise.

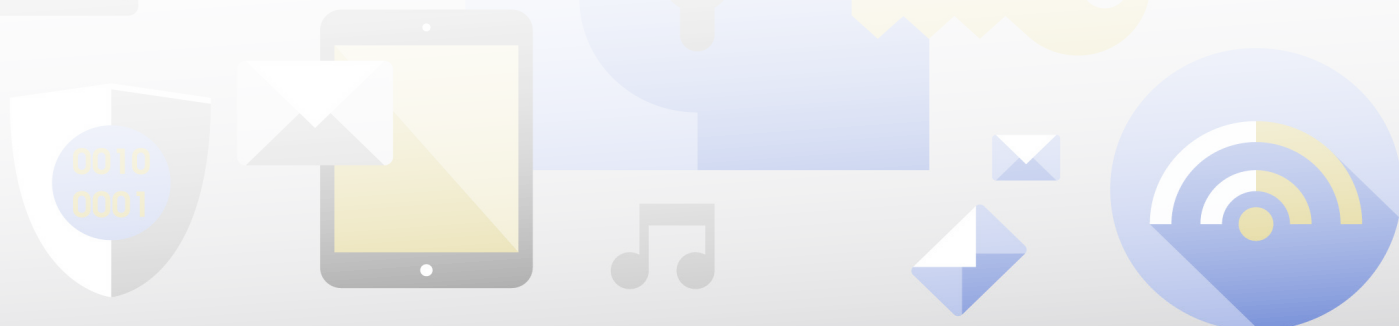
Improper or non-existent disclosure control can be the root cause for privacy issues. Data privacy issues can arise in response to information from a wide range of sources, such as financial, health care transactions etc.,

The challenge of data privacy is to utilize data while protecting individual's privacy preferences and their personally identifiable information. While designing the data/Information Systems, Security Systems -- software, hardware, the aspects of data privacy are taken into account. As the laws and regulations related to Privacy and Data Protection are constantly changing, it is important to keep abreast with any changes in the law and continually reassess compliance with data privacy and security regulations.

Information privacy relates to different data types, including:

Internet privacy (online privacy): All personal data shared over the Internet is subject to privacy issues. Most websites publish a privacy policy that details the website's intended use of collected online and/or offline collected data.

Financial privacy: Financial information is particularly sensitive, as it may easily be used to commit online and/or offline fraud.



Security Vs Privacy

Privacy is not security and security is not privacy, even if these words are erroneously interchanged all the time.

Privacy is concerned with the collection and use of personal data. Security is concerned with protection of that personal data from unwanted intruders

Privacy is personal. It is the understanding between a customer and a company about what information will be collected and how it will be used. In general, the users may give up their personal data in exchange for services what they want. For example, if we want to buy a book online, we have to provide the vendor our name, address, and credit card information so that we can receive that book. We entrust our personal information with the understanding that the bookseller will not use our information for any other purpose. It will maintain the privacy of our personal data.

Security is impersonal. Security is not concerned with what is collected or how it is used. Rather, security guards the personal data that we provide to a vendor from those who shouldn't see it and ensures that when that data needs to be seen, it's in the right format and is accessible. More simply, security is a wall around the castle, and just as there can be many different walls around a castle, there can also be many different walls of security around our personal data. Security walls can include network protection, encryption, and authentication, to name a few; and companies spend a lot of money to create and maintain these walls.

Even though security and privacy are not the same, they are interdependent on each other. You can't have one without the other. It just doesn't make sense. If

a company doesn't have security in place to protect our data, then its privacy policies will be meaningless because it won't be able to prevent the unauthorized access and usage of an individual's personal data. Conversely, if a company doesn't have a clear understanding of what data it collects and how it will use it, then it will be impossible to provide real security.

Why We Care about Privacy:

Privacy is important for a number of reasons as people can be harmed or debilitated if there is no restriction on the public's access to and use of personal information. Other reasons are more fundamental, touching the essence of human personhood. There are many ways a person can be harmed by the revelation of sensitive personal information. Medical records, psychological tests and interviews, court records, financial records--whether from banks, credit companies, sites visited on the Internet and a variety of other sources hold many intimate details of a person's life. The revelation of such information can make the subjects vulnerable to many abuses. Therefore, even though the privacy does not get mentioned in the list of Fundamental rights, it is necessary to protect like other Fundamental rights.

Do You Agree? For Security Vs Privacy

The most important job of government is to "secure the general welfare" of its citizens. Security is a common good that is promised to all citizens, and it must outweigh any personal concerns about privacy. The word "privacy" is not found in the Constitution so it cannot be claimed as a fundamental right (Yes/NO)

Surveillance is the secret watching of suspects' private activities. In the past this usually involved following people, or going through their trash. These days it is mostly electronic, with the police and intelligence



*Guess the Tip
which best suits the
cartoon by
logging in to*

www.
InfoSec
awareness.in



agencies listening into private phone conversations or reading emails (wiretapping). Surveillance can also involve looking at bank account details to see where money comes and goes. All these are vital tools for tracking the actions of terrorists when they are planning attacks. The government cannot stand by and wait until criminal acts are carried out: it must stop attacks before they happen. (Yes/No)

Any idea that increases the power of government agencies should be rejected. In the past, government agencies (for example, the tax authorities) have misused their power over citizens. More power means a greater potential for abuse. (Yes/No)

Tighter security controls at airports and borders will help prevent attacks and loss of life. Such measures could include more intrusive scanning, body searches, watch lists, etc. In addition to their deterrence effect, they will enable officials to stop attacks as they are happening. (Yes/No)

Tips for Online Privacy

Do not reveal personal information inadvertently

You may be “shedding” personal details, including e-mail addresses and other contact information, without even knowing it unless you properly

configure your Web browser.

In your browser’s “Setup”-“Options” or “Preferences” menus, you may wish to use a pseudonym instead of your real name, and not enter an e-mail address, nor provide other personally identifiable information that you don’t wish to share.

Give your Information only in trusted websites and only if it is mandatory.

Children may have an additional “security problem” - “have you set clear rules for your kids, so that they know that they should not reveal personal Information unless you give consent on a site-to-site basis?”

Turn on cookie notices in your Web browser, and/or use cookie management software

“Cookies” are tidbits of information that Web sites store on your computer, temporarily or more-or-less permanently.

In many cases cookies are useful and innocuous. They may be passwords and user IDs, so that you do not have to keep retyping them every time you load a new page at the site that issued the cookie. Other cookies however, can be used for “data mining” purposes, to track your motions through a

Web site, the time you spend there, what links you click on and other details that the company wants to record, usually for marketing purposes. Most cookies can only be read by the party that created them. However, some companies that manage online banner advertising are, in essence, cookie sharing rings. They can track which pages you load, which ads you click on, etc., and share this information with all of their client Web sites (who may number in the hundreds, even thousands).

Always enable cookie management to know about your browser cookies to control your sensitive information

Keep a “clean” e-mail address.

When mailing to unknown parties; posting to newsgroups, mailing lists, chat rooms and other

public spaces on the Net; or publishing a Web page that mentions your e-mail address, it is best to do this from a “side” account, some pseudonymous or simply alternate address, and to use your main or preferred address only on small, members-only lists and with known, trusted individuals.

Addresses that are posted (even as part of message headers) in public spaces can be easily discovered by spammers (online junk mailers) and added to their list of targets. If your public “throw away” address gets spammed enough to become annoying, you can simply kill it off, and start a new one. Your friends, boss, etc., will still know your “real” address.

You can use a free (advertising-supported) e-mail service provider like Yahoo Mail or Hotmail for such “side” accounts. It is best to use a “real” Internet service provider for your main account,

InfoSec Tip

Read all disclosures for online shopping

Guidelines for online shopping

- Ensure that your operating system and web browser (Internet Explorer, Firefox, etc) are fully patched and up to date before surfing the web.
- Install and run a personal firewall as well as anti-virus software with the latest virus signatures.
- Check the terms and disclaimers of any e-shopping site before using their services, e.g. check personal privacy statements, etc.
- Choose well-known or trustworthy e-shopping sites.
- Keep notice of key measures on providing information or making a purchase on a website:
- Informed consent on personal information
- Whether Seals of Approval applied (e.g. TRUSTe or WebTrust)
- Apply for a Digital Certificate for electronic transactions.
- Consider using Encryption to protect sensitive data transmitted over public networks and the Internet.
- Be alert to the latest news on sites that are notorious for suspicious activities, or labeled as “bad sites”.
- Remember to logoff at the end of a session.
- Use different sets of logins and passwords for different web applications and services.
- Change your passwords used in critical web applications regularly if a one-time password is not supported.
- Report abnormal behaviour to your service provider or ISP immediately.



and to examine their privacy policies and terms of service, as some “free mail” services may have poor privacy track records.

You may find it works best to use an e-mail package that allows multiple user IDs and addresses (a.k.a. “personalities”, “aliases”) so that you do not have to switch between multiple programs to manage and use more than one e-mail address (though you may have to use a Web browser rather than an e-mail program to read your mail in your “throw away” accounts - many freemail providers do not allow POP or IMAP connections).

If you are “required” to give an e-mail address to use a site (but will not be required to check your mail for some kind of access code they send you), you can use “someuser@example.com” (example.com is a non-existent site, set up by the Internet standards to be used as an example that will never accidentally coincide with anyone’s real e-mail address, which is always a danger if you just make up one off the top of your head.)

Don’t reveal personal details to strangers or just-met “friends”

The speed of Internet communication is often mirrored in rapid online acquaintanceships and friendships. But it is important to realize that you don’t really know who these people are or what they are like in real life. Also avoid face-to-face meetings as If you and your new e-friend wish to meet in person, do it in a public place. Bringing a friend along can also be a good idea. One needn’t be paranoid, but one should not be an easy mark, either.



Never give system or network information to strangers

Take care of shoulder surfing



Some personal information you might wish to withhold until you know someone much better would include your full name, place of employment, phone number, and street address (among more obvious things like credit card numbers, etc.) Needless to say, such information should not be put on personal home pages. (If you have a work home page, it may well have work contact information on it, but you needn’t reveal this page to everyone you meet in a chat room.)

For this and other reasons, many people maintain two personal home pages, a work-related one, and an “off duty” version. In the commercial sector, too, beware “fast-met friends”. A common “social engineering” form of industrial espionage is to befriend someone online just long enough to get them to reveal insider information.

Beware of sites that offer some sort of reward or prize in exchange for your contact information or other personal details

There’s a very high probability that they are gathering your information for direct marketing purposes. In many cases your name and address are worth much more to them because they can

sell it to other marketers (who can do the same in turn...). Be especially wary of sweepstakes and contests. You probably won't win, but the marketer sure will if you give them your information.

Remember that YOU decide what information about yourself to reveal, when, why, and to whom

Don't give out personally-identifiable information too easily. Just as you might think twice about giving some clerk at the mall your home address and phone number, keep in mind that simply because a site asks for or demands personal information from you does not mean you have to give it.

You donot have to give accurate billing information if you are buying something, of course, but if you are registering with a free site that is a little too intrusive for you, there is no law (in most places) against providing them with pseudonymous information. (However, it would probably be polite to use obviously fake addresses, such as "123 No Such Street, Nowhere, Delhi 110001". If they are generating mailings based on this information - presumably in accordance with the terms of their privacy policy - they can probably weed such addresses out and not waste the postage on them. **Definitely do NOT use someone else's real address!**

However, if you are required to agree to terms of service before using the free service, be sure those terms do not include a requirement that you provide correct information, unless the penalty is simply not being allowed to use the service any more, and you're willing to pay that price if they figure out you are not providing them with your actual personally-identifiable information



***Never Respond to
Unknown Persons
in Internet***

CERT-In Vulnerability Note CIVN-2016-0166

Microsoft Windows Search Component Denial of Service Vulnerability

Software Affected

- Windows 7 for 32-bit and x64-based Systems Service Pack 1
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows Server 2008 R2 for Itanium-based Systems Service Pack 1
- Windows 8.1 for 32-bit and x64-based Systems
- Windows Server 2012 and R2
- Windows RT 8.1
- Windows 10 for 32-bit Systems
- Windows 10 for x64-based Systems
- Windows 10 Version 1511 for 32-bit Systems
- Windows 10 Version 1511 for x64-based Systems
- Windows Server 2008 R2 for x64-based Systems Service Pack1(Service Core installation)
- Windows Server 2012 and R2 (Server Core installation)

Overview

A vulnerability has been reported in Windows Structured Query Component could allow a local attacker to cause a denial of Service (DoS) condition.

Description

The vulnerability exists due to improper sanitization of user-supplied data in requests by Windows Structured Query Component. A local attacker could exploit this vulnerability by running a program

designed to send malicious request to the affected component.

Successful exploitation of this vulnerability could allow an attacker to degrade servers performance and cause a denial of service condition.

Solution

Apply appropriate patches as mentioned in Microsoft Security Bulletin MS16-082

Vendor Information

Microsoft

<https://technet.microsoft.com/library/security/MS16-082>

References

Cisco

<http://tools.cisco.com/security/center/viewAlert.x?alertId=46551>

Symantec

https://www.symantec.com/security_response/vulnerability.jsp?bid=91113

CVE Name

CVE-2016-3230

For more details visit

<http://www.cert.org.in/>

CERT-In Vulnerability Note CIVN-2016-0164

Multiple Vulnerabilities in Microsoft Windows PDF

Software Affected

- Microsoft Edge
- Windows 8.1 for 32-bit and x64-based Systems
- Windows 10 for 32-bit and x64-based Systems
- Windows 10 Version 1511 for 32-bit and x64-based Systems
- Windows Server 2012 and Windows Server 2012 R2

Overview

Multiple vulnerabilities have been reported in Microsoft Windows Edge which could be exploited by a remote attacker to execute arbitrary code, bypass security controls and obtain potentially sensitive information on the target users system.

Description

1. Information Disclosure Vulnerabilities (CVE-2016-3201 CVE-2016-3215)

These vulnerabilities exist due to improper parsing of pdf files by the affected software. A remote attacker could successfully exploit these vulnerabilities by persuading the target user to open a crafted pdf file which triggers an exploit thereby allowing the attacker to obtain access potentially sensitive information which could be used to conduct further attacks.

2. Arbitrary Code Execution Vulnerability (CVE-2016-3202)

This vulnerability exists due to improper parsing of pdf files

MS EDGE. A remote attacker could successfully exploit this vulnerability by persuading the target user to open a crafted pdf file which triggers an exploit thereby allowing the attacker execute arbitrary codewith the privileges of the target user leading to complete system compromise.

Solution

Apply appropriate patches as mentioned in MS16-080

Vendor Information

Microsoft

<https://technet.microsoft.com/en-us/library/security/ms16-080.aspx>

References

Cisco

<https://tools.cisco.com/security/center/viewAlert.x?alertId=46527>

<https://tools.cisco.com/security/center/viewAlert.x?alertId=46528>

<https://tools.cisco.com/security/center/viewAlert.x?alertId=46530>

CVE Name

CVE-2016-3201

CVE-2016-3202

CVE-2016-3215

Application & Device Control (ADC)

ADC is a centralized management console to manage client components in Windows Active Directory Domain Network. It enforces the Application Whitelisting, USB mass storage device control and Secure browser add-on to protect from HTML & Javascript based attacks at the client.

Features

- SSL enabled Web based management console
- Remote Deployment of client components – requires domain administrator privileges
- Supports Batch Installation of remote clients
- Centralized Logging – using MSMQ (Microsoft Message Queuing)
- Graphical Log Analysis
- Supports verifying application hashes with VirusTotal
- Analysis of applications during scanning with binary heuristic application analyser
- Supports Import/Export of whitelists
- Remote registration of USB mass storage devices
- Supports USB printers and scanners

Some of the screenshots of ADC software are shown below

☒ Application Control	☐ Device Control	☐ BrowserJSGuard	INSTALL
Managed Clients	Application Control Installation Status		
☐ WIN7_32_VM	Absent		
SANDEEP-PC	Installed 		
WIN7_TEST	Installed 		

Figure 1. ADC's Client Management

Select Unmanaged System to Install ADC Agent				INSTALL ADC AGENT
Domain Systems	System Status	Application Control Status	Device Control Status	
☐ ASHU-PC12345678	Unmanaged	N.A	N.A	
ASHUTOSH-PC	Managed	Present	Present	

For more details visit : http://cdac.in/index.aspx?id=dl_free_eps_solutions

Mobile Device Security Solution (M-Kavach)

M-Kavach is a comprehensive mobile device security solution for Android devices addressing threats related to mobile phones. It can be customized for the needs of various user groups and addresses threats related to malware that steal personal data & credentials, misuse of resources viz WiFi, Bluetooth, Camera and Mobile Data, lost or stolen mobile device, SMS Filter and unwanted/unsolicited incoming calls.

The web based enterprise variant consists of device management features viz lock & wipe, factory reset and backup & restore. In personal edition also, users can remotely manage their mobile devices using SMS

Features

- Protects the critical information stored on mobile device
- Prevents the usage of mobile device by unauthorized personnel by changing the SIM
- Allows easy backup & restore of data
- Enables to have remote control on the device such as remote lock & wipe

- Protects access to resources like Bluetooth, WiFi, Camera and Mobile Data
- Blocks unwanted Calls/SMS
- Application Securelisting
- Secure Browsing
- Web based interface for managing mobile devices
- Three variants to cater the needs of Personal, Enterprise and Critical User Groups

Some of the screenshots of M-Kavach software are shown below



Google Play Store : <https://play.google.com/store/apps/details?id=org.cdac.mkavach>

M-Gov App Store : <https://apps.mgov.gov.in/descp.do?appid=958>

C-DAC Website : http://cdac.in/index.aspx?id=dl_free_eps_solutions



PRESENTING SPONSOR

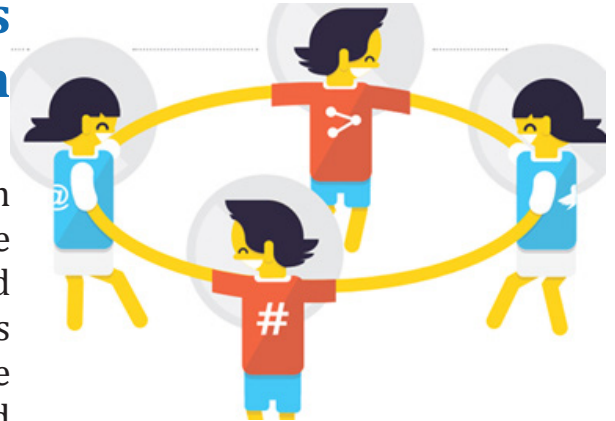


Search...



Stop Cyberbullying: Indian teens face biggest risk among Asian countries

India ranks highest among a few Asian countries in cyber bullying with 53 percent currently utilizing the internet between the ages of 8 to 17 and have faced some form of online bullying more than once. This is in contrast to a sizeable 49 percent children who face cyber bullying in Bangladesh, 33 percent in Thailand and only one in 4 children in Malaysia, according to the Norton Cyber security Insights Report by Norton by Symantec.



Cyberbullying refers to electronic communication used for the purpose of bullying.

In the latter half of 2015, Intel Security released its Teens, Tweens and Technology Study 2015, which revealed that 81 percent of Indian children between the age of 8 and 16 were active on social media networks and of these 22 percent reported being bullied online. This was the highest when compared to Australia, USA and Singapore being part of the survey.

<http://www.firstpost.com/business/stop-cyberbullying-indian-teens-face-biggest-risk-among-asian-countries-2840552.html>

2

HOWSTUFFWORKS

MONEY

FOLLOW US



SEARCH



5 Ways to Spot a Hacked ATM

When you arrive at an ATM, look for any off-color plastic near the top of the machine. Anything there? Even an innocent-looking object that appears part of the ATM could be housing a tiny camera recording your keypad input [source: Walters]. Because they're better camouflaged than objects sitting in broad daylight, molded pieces can be designed to blend in with a specific ATM and hide a spy cam.

Even if it may blend in at first glance, take a second to study anything placed above the ATM. Does the color look a little off? Does it simply look out of place? Most telling would be a pinhole positioned above the keypad. Believe it or not, a tiny hole is enough for a camera to peek through and record dozens -- or hundreds -- of people every day entering their PINs. As we previously mentioned, remember to cover the pad as you input your PIN.

Unfortunately, cameras aren't the only tools at the ATM skimmer's disposal -- fake keypads can be used to record PIN inputs, too.

<http://money.howstuffworks.com/personal-finance/banking/5-ways-to-spot-hacked-atm3.htm>

BOINGBOING / DAMIEN ZAMMIT / 5 AM WED, JUN 15 2016

Intel x86s hide another CPU that can take over your machine (you can't audit it)

Recent Intel x86 processors implement a secret, powerful control mechanism that runs on a separate chip that no one is allowed to audit or examine. When these are eventually compromised, they'll expose all affected systems to nearly unkillable, undetectable rootkit attacks. I've made it my mission to open up this system and make free, open replacements, before it's too late. attack were CCTV boxes that were connected to more than 25,500 different IP addresses. The IP addresses were located in no fewer than 105 countries around the world.

The Intel Management Engine (ME) is a subsystem composed of a special 32-bit ARC microprocessor that's physically located inside the chipset. It is an extra general purpose computer running a firmware blob that is sold as a management system for big enterprise deployments.

<http://boingboing.net/2016/06/15/intel-x86-processors-ship-with.html>

[Register](#) [Log in](#)[HOME](#) [MAIN MENU](#) [MY STORIES: 24](#)

Large botnet of CCTV devices knock the snot out of jewelry website

Researchers have encountered a denial-of-service botnet that's made up of more than 25,000 Internet-connected closed circuit TV devices.

The researchers with Security firm Sucuri came across the malicious network while defending a small brick-and-mortar jewelry shop against a distributed denial-of-service attack. The unnamed site was choking on an assault that delivered almost 35,000 HTTP requests per second, making it unreachable to legitimate users. When Sucuri used a network addressing and routing system known as Anycast to neutralize the attack, the assailants increased the number of HTTP requests to 50,000 per second.

The DDoS attack continued for days, causing the Sucuri researchers to become curious about the origins of the attack. They soon discovered the individual devices carrying out the attack were CCTV boxes that were connected to more than 25,500 different IP addresses. The IP addresses were located in no fewer than 105 countries around the world.

<http://arstechnica.com/security/2016/06/large-botnet-of-cctv-devices-knock-the-snot-out-of-jewelry-website/>

Comunity Workshop (Cyber Sunday) at Hyderabad & Rangareddy District



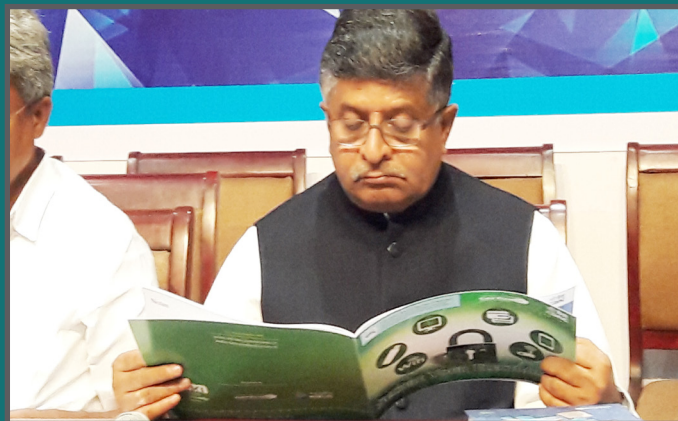
Awareness Workshop at Chennai



Awareness Workshop at Noida



Briefing about Information Security Education and Awareness Project and
Information Security Awareness material to
Shri Ravi Shankar Prasad, Hon'ble Minister for Communications and Information
Technology, Government of India,
Shri Sudarshan Bhagat, Hon'ble Minister of State for Rural Development,
Prof. V.S.S. Kumar, Hon'ble Vice Chancellor, JNTUK Kakinada
and Dr. G.V.R. Prasada Raju, Registrar, JNTUK Kakinada



To Share Tips / Latest News, mail us to
isea@cdac.in

For more details visit

www.
InfoSec
awareness.in

To conduct Information Security Awareness Workshop
at your Institution, please submit
“Request for Workshop in the website www.isea.gov.in

For any queries on Information Security
Call us on Tollfree No.

1800 425 6235

Between 10 AM to 6 PM or give us a missed call, We will call back within 24hrs

ISEA Whataspp Number for Incident Reporting

+91 9490771800

Between 9.00 AM to 5.30 PM



Subscribe us on **You Tube**

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

Follow us on **twitter**

<https://twitter.com/InfoSecAwa>

Like us on

facebook

<https://www.facebook.com/infosecawareness>

Centre for Development of Advanced Computing (C-DAC), a Scientific Society of Department of Electronics and Information Technology, Ministry of Communications & Information Technology, Government of India, is primarily an R&D institution involved in design, development and deployment of Advanced Electronics and Information Technology Solutions, including the celebrated PARAM series of Supercomputers. The C-DAC, Hyderabad is working in R&D with a focus on system level programming, web technologies and embedded programming in the application domains of Network Security, e-learning, Ubiquitous Computing, India Development Gateway (www.indg.in), Supply Chain Management and Wireless Sensor Networks.



Department of Electronics & Information Technology,
Ministry of Communications & Information Technology,
Government of India



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, Srisaillam Highway, Pahadi Shareef Via Keshavagiri (Post)
Hyderabad - 500005, Telangana(India)

BOOK POST

From :

**C-DAC, Plot No. 6 & 7, Hardware Park, Sy No. 1/1,
Srisaillam Highway, Pahadi Shareef Via Keshavagiri
(Post) Hyderabad - 500005, Telangana(India)**