September - October-2010 www.infosecawareness.in

Information Security Awareness

Program by
Information Security Education and Awareness (ISEA)
Department of Information Technology
Ministry of Communications and Information Technology
Government of India

InfoSec Tip

If you are a victim of identity theft, report it immediately

- If it is your credit card, immediately alert to your bank to stop the credit card activity.
- In case of any other financial frauds such as lottery mails, money offer, report to nearest Cyber Crime Cell.
- Always remember to document all conversions so you know whom you spoke to and when.
- Don't put your Social Security number on anything, unless it is legally required.
- Don't have it printed on your cheques. For those of you with driving licenses that routinely use your Social Security number, check with your DMV to see if they offer another option.
- Check your bank statement once or twice a year to make sure it doesn't have accounts you don't know about.

Some More Tips

- Shred or burn papers with credit card or bank account numbers, Social Security numbers, etc.
- The next time you order cheques, have only your initials (instead of first name) and last name put on them. If someone takes your chequebook, they will not know if you sign your cheques with just your initials or your first name. Your bank will know.
- Do not sign behind your credit cards. Instead put "PHOTO ID REQUIRED".
- When you are writing cheques to pay on your credit card accounts, DO NOT put the complete account number on the "For" line. Instead, just put the last four numbers.
- Don't list any telephone number. You can always write it on the cheque at the time of the transaction. If you have a PO Box, use that instead of your home address or your work address.

InfoSec Quote

"People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems." — Bruce Schneier

InfoSec Cartoon

TAKE CARE ABOUT SHOULDER SURFING

Executed by :
Centre for Development of Advanced Computing
Hyderabad

InfoSec Quiz

1.) What is the other name for crackers or malicious hackers who infiltrate secure systems in order to steal information or cause damage?
   a.) Black hats
   b.) Pirates
   c.) Digital rogue
   d.) None of the above

2.) What is vishing ?
   a.) A technique used to collect the personal information through e-mails
   b.) A criminal practise or act done through telephone
   c.) It is one type of the social engineering
   d.) Both b and c

3.) Software used to access the World Wide Web is called
   a.) Computer
   b.) MS Office
   c.) Web Browser
   d.) Adobe Photoshop

4.) What is a hash? In terms of computer security
   a.) Decryption key
   b.) Algorithm
   c.) Encrypted value
   d.) None of the above

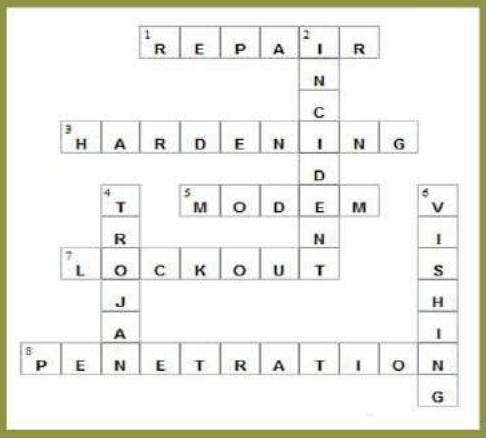
5.) Skimming is terminology given to
   a.) Theft of Internet banking information
   b.) Theft of Credit card information
   c.) It is one type of Social Engineering
   d.) Both b & c

June-July 2010 Contest Answers

InfoSec Quiz

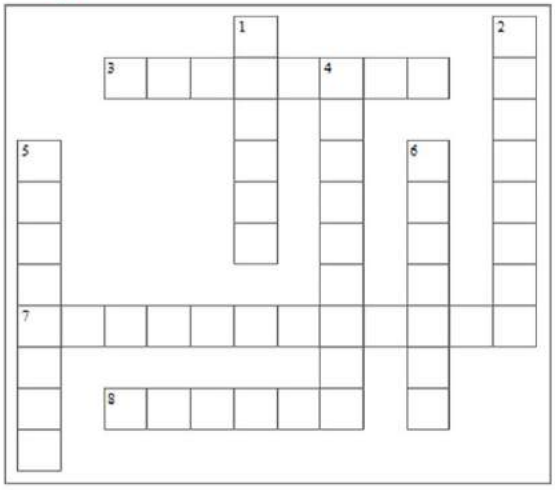
1) C 2) D 3) D 4) B 5) B

InfoSec Crossword



Log on to www.infosecawareness.in to participate in the

InfoSec Crossword



ACROSS

3.The interception, alteration, and retransmission of data to fool the recipient.

7._____is ensuring that information systems and the necessary data are available for use when they are needed.

8.is malware that appears to perform a desirable function for the user prior to run or install but instead facilitates unauthorized access of the user's computer system

DOWN

1.A mechanical device used by software developers to prevent unlicenced use of their product.

2.The process of recreating files which have disappeared, or become corrupted, from backup copies.

4.An uninvited and unwelcome entry into a system by an unauthorised source.

5._____ is a private network which uses the Internet protocols and extends beyond an organisation's premises, typically to allow access by clients, suppliers.

6.is the criminal practice of using social engineering over the telephone system.

Congratulations

LAST EDITION CONTEST WINNERS

InfoSec Crossword

Madhumathi Andrews
Bangalore

InfoSec Quiz

K.Priya

Browser Control Bar

Downloads for parental control bar

Download Parental Control bar tool from

http://www.parentalcontrolbar.org/

Add-ons for the Internet Explore

http://www.ieaddons.com/en/details/Security/ParentalControl_Bar/

Add-ons for Mozila Firefox

https://addons.mozilla.org/en-US/firefox/search?q=parental+control&cat=all

https://addons.mozilla.org/enUS/firefox/addon/160759/

InfoSec Tools

Browser Control Bars -> K9 Web Protection
-> Parental Control Bar

K9 Web Protection

The K9 web protection is a Free, enterprise-class security software designed for home computers.
To protect your home computer from online threats of all kinds, you need a robust security solution that's updated in real time.

With Blue Coat K9 Web Protection, you don't have to wait for the latest security patch or upgrade, which can leave your computer vulnerable to new and evolving Web threats. K9 delivers the comprehensive protection you need automatically. With K9, you get the same advanced Web filtering technology used by enterprise and government institutions worldwide — all with a user-friendly interface that allows you to control Internet use in your home.

For more details:
http://www1.k9webprotection.com/

Guess the tip which suits the below cartoon picture & win prizes

LOGON TO
www.infosecawareness.in
TO SEND THE TIP

InfoSec Concept

ClickJacking

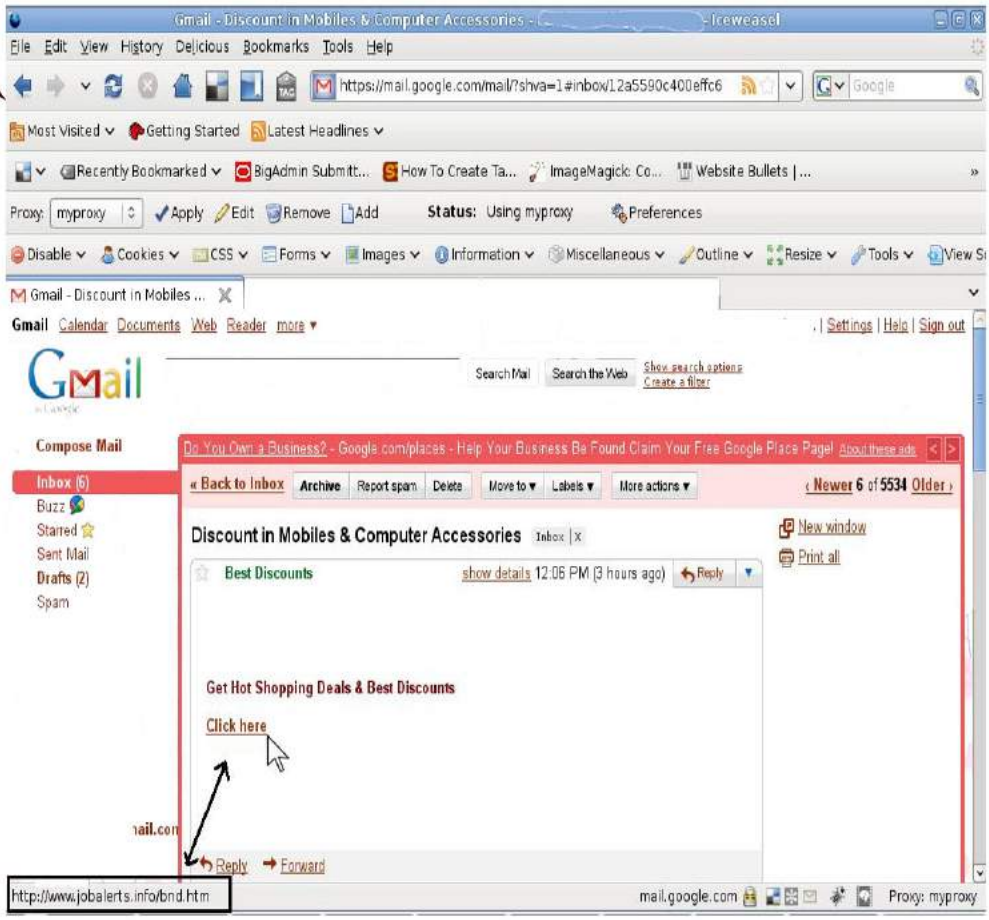
Clickjacking is a malicious technique of tricking Web users into revealing confidential information or taking control of their computer while clicking on seemingly innocuous Web pages. A vulnerability across a variety of browsers and platforms, a clickjacking takes the form of embedded code or script that can execute without the user's knowledge, such as clicking on a button that appears to perform another function.

Clickjacking is possible because seemingly harmless features of HTML Web pages can be employed to perform unexpected actions.

A clickjacked page tricks a user into performing undesired actions by clicking on a concealed link. On a clickjacked page, the attackers show a set of dummy buttons, then load another page over it in a transparent layer. The users think that they are clicking the visible buttons, while they are actually performing actions on the hidden page. The hidden page may be an authentic page, and therefore the attackers can trick users into performing actions which the users never intended to do and there is no way of tracing such actions later, as the user was genuinely authenticated on the other page.

TIPS

- Never click on the links received from the unknown users.
- Always type URL in browser
- If necessary cross check the target of the link by placing mouse at the given link and check the details at bottom left corner of the browser before clicking.
- Take the help of the picture below to understand.



Don't Click the Links

Some of the ISSUES

CLICKJACKING

InfoSec Concept

ISSUE 1 : Clickjacking allows attackers to subvert clicks and send the victim's clicks to web-pages that allow themselves to be framed with or without JavaScript. One-click submission buttons or links are the most vulnerable. It has been known since at least 2002 and has seen at least three different PoC exploits (Google Desktop MITM attack, Google Gadgets auto-add and click fraud). All major browsers appear to be affected.

ISSUE 2 : JavaScript is not required to initiate the attack as CSS can place invisible iframes over any known target (EG: the only link on the red herring page). Turning off JavaScript also neuters one of the only practical web based defenses against the attack which is the use of frame busting code.

ISSUE 3 : ActiveX controls are potentially susceptible to clickjacking if they don't use traditional modal dialogs, but rather rely on on-page prompting. This requires no cross domain access, necessarily, which means iframes/frames are not a prerequisite on an attacker controlled page.

ISSUE 4 : Flash security settings manager is also particularly vulnerable, allowing the attacker to turn off the security of Flash completely. This includes camera/microphone access as well as cross domain access. Resolved using frame busting code, bug #4 below notwithstanding. However, as pointed out elsewhere, it is possible to directly frame the SWF file example here and here.

ISSUE 5 : All prior versions of Flash on Firefox on MacOS are particularly vulnerable to camera and microphone monitoring due to security issues allowing the object to be turned opaque or covered up. This fix relies on all users upgrading, and since Flash users are notoriously slow at upgrading, this exploit is expected to persist. Turning off microphone access in the BIOS and unplugging/removing controls to the camera are an alternative.

ISSUE 6 : "Unlikely" XSS vulnerabilities that require onmouseover or onmousedown events on other parts of pages on other domains are suddenly more likely. For example if a webpage has a XSS vulnerability where the only successful attacks are things like onmouseover or onmousedown, etc... on unlikely parts of the page, an attacker can promote those exploits by framing them and placing the mouse cursor directly above the target XSS area. Therefore, otherwise typically uninteresting or unlikely XSS exploits can be made more dangerous.

For more details:
http://ha.ckers.org/blog/20081007/clickjacking-details/

InfoSec News

Firefox 4.0 beta download scam on Twitter

A Twitter update hash-tagged "Firefox" spotted by Sunbelt offers a unique opportunity: follow the offered shortened link to download a cracked Mozilla Firefox 4.0 or a key generator for it.

For those who are unaware of the fact, Firefox 4.0 is currently in beta testing, and can be downloaded for free from the official Mozilla web site, so this is an offer that can't stand even a casual check.

Fortunately for the malware peddlers behind this scheme, there are always those who don't bother to check things before downloading - and this time, the malicious file masquerading as the cracked version or as the key generator is a downloader Trojan

An additional threat comes from trying to download Firefox 4.0 from the site, since the pressing the button redirects the victim to another site that offers other Trojans and viruses masquerading as legitimate programs.

For more details:
http://www.net-security.org/malware_news.php?id=1422

Email promising job a fake, say firm

The cyber crime investigation cell (CCIC) of the city crime branch is probing a case against a person who, posing as an employee of a Godrej company, sent emails to several job seekers, asking them to deposit Rs 6,850 in an account for a job at a new Godrej plant, with salaries ranging from Rs 30,000 to Rs three lakh per month.

P B Rao, assistant general manager (Industrial Relation) of Godrej and Boyce Manufacturing Company Ltd, filed a complaint stating that someone was trying to dupe people using their company's name. The email states, "Your bio-data has been selected for our new plant (manufacturing of refrigerators, air conditioners and washing machines). The company offers you the post of an executive/manager in your respective department.

The sender further stated that the recruitments are being done for new plants across the country. Candidates were asked to deposit Rs 6,850, to be refunded after the interview, in an account at Hyderabad Bank of India.

Godrej stated that their recruitment office was flooded with calls after the fraud. "The mails asking candidates to deposit money in an account against their so-called selection in the so-called 'Godrej Electronics India Ltd' are fake, they said. Police say they will initiate action once they get the details about the mail's origin from the server.

For more details:

http://infosecawareness.in/wiki/index.php/Email_promising_job_a_fake,_say_firm_officials

InfoSec News

FACEBOOK POPULARITY GROWING BUT PRIVACY STILL A WORRY: EXPERTS

More and more Indians might be hooked to social networking site Facebook, but experts feel that privacy issues still remain a concern since users face the vulnerability of their personal data getting hacked. According to experts and publicly available information, users' privacy is not fully protected while using many of the applications available on Facebook.

Facebook applications have potential privacy issues and when a user signs up for an application, they are in essence allowing the developer to access all of their information and their friends' information, they said.

Rahul Chaudhry, partner at intellectual property law firm Lall Lahiri & Salhotra said that although Facebook is a great way of being connected, the site also brings several potential privacy issues which the user must be aware of. "Your basic information, pictures, notes, local hard drive, the posts that one likes are vulnerable of becoming public. "A users' profile pictures would be available on websites liked by clicking Facebook 'like' application. The pictures can also be downloaded by the person one is allowing to view them. Your local drive/information becomes accessible to third parties," he noted.

For more details:
http://economictimes.indiatimes.com/infotech/internet/Facebook-popularity-growing-but-privac

Scammers hit Twitter, Facebook, send free iPad spam
Robert McMillan

Facebook and Twitter users are complaining about their accounts being compromised and then being used to spam friends with suspicious "free iPad offers."

Twitter warned users of the scam, Wednesday, saying that it was resetting passwords of affected users. "If you've received a message promising you a new iPad, not only is there no iPad, but also your friends have been hacked," Twitter said

The scam is also hitting Facebook users too, according to company spokesman Simon Axten. "It's affecting an extremely small percentage of people on Facebook, but we take all threats seriously," he said via email.

Online marketing programs pay cash for Web traffic, and hackers have found that by phishing victims and then using that information to break into legitimate Twitter and Facebook accounts, they can earn money. This type of spam is particularly effective, because the messages appear to come from a trusted source.

Source:
http://www.pcworld.in/news/scammers-hit-twitter-facebooksendfree-ipad-spam-33472010

InfoSec Virus Alert

Stuxnet Rootkit

It has been observed that a multi-component family of rootkit-enabled backdoor Trojan named Stuxnet is spreading in the wild.

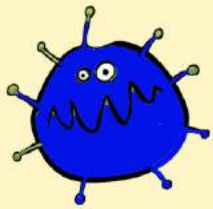
The rootkit uses a specially crafted shortcut files (. LNK) that infects the operating system when viewed by an icon rendering file explorer such as Windows Explorer or Total Commander by leveraging a recently reported zero day vulnerability in Microsoft windows shell (CVE-2010-2568 , CIVN-20210-169).

Once successful, drops a back door(Worm:Win32/Stuxnet.A) which in turn drops two malicious drivers with rootkit capabilities and adds as system services.

Countermeasures

- Delete files and the registry entries made by the Stuxnet rootkit mentioned above
- Install and maintain updated anti-virus software at gateway and desktop level
- Apply appropriate patches as mentioned in CERT-In vulnerability note (CIVN-2010-169)
- Use caution when opening attachments and accepting file transfers.
- Use caution when clicking on links to web pages.

For more details:
http://www.cert-in.org.in/virus/Stuxnet_Rootkit.htm



Large Zeus botnet used for financial fraud

Trusteer announced that it has uncovered a large Zeus version 2 botnet being used to conduct financial fraud in the UK which is operated and controlled from Eastern Europe.

The botnet appears to be controlling more than 100,000 infected computers, 98% of which are UK Internet users. The criminals have been harvesting all manner of potentially lucrative and revenue-producing credentials - including online account IDs plus login information to banks, credit and debit card numbers, account types plus balances, bank statements, browser cookies, client side certificates, login information for email accounts and social networks and even FTP passwords.

Trusteer discovered the extent of the botnet after they gained access to the botnet's drop servers and command and control center which contained the stolen information including hundreds of thousands of stolen credentials. Trusteer are sharing the information with UK law enforcement agencies.

"What is especially worrying is that this botnet doesn't just stop at user IDs and passwords. By harvesting client side certificates and cookies, the cybercriminals can extract a lot of extra information on the user that can be used to augment their illegal access to those users' online accounts."

For more details:
http://www.netsecurity.org/malware_news.php?id=1418&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29

InfoSec Virus Alert

Worm Win32/Vobfus.U

It has been observed that a highly obfuscated visual basic (VB) compiled network aware worm family dubbed Vobfus(Visual Basic Obfus cated) is spreading

The propagate through removable and shared dries by dropping traditional autorun.inf files and crafted shortcut files(.LNK files) pointing to the dropped worm copy. It is also reported that the dropped LNK files are exploiting the recently disclosed zero day vulnerability(CVE-2010-2568 , CIVN-20210-169) wherein Windows which fails to handle short cut files.

Once successfully installed, the worm pulls further malware(Hiloti, Alutreon, Renos, Virut) on to the victim system.

Countermeasures:

- Delete files and the registry entries made by the Vobfus worm mentioned above
- Install and maintain updated anti-virus software at gateway and desktop level
- Apply appropriate patches as mentioned in CERT-In vulnerability note (CIVN-2010-169)
- Disable autoplay
- Exercise caution while using USB devices.
- Use caution when opening attachments and accepting file transfers.

For more details:
http://www.cert-in.org.in/virus/Win32_Vobfus.htm

Propagation of Zeus bot through spam campaign

It has been observed that unsolicited spam mails carrying information stealer trojan " Zeus" is surging. The mail disguised as a birthday invitation, photos, or resume with a ZIP attachment arguably the latest Zbot variants. Detailed description of Zbot can be seen here .

Some of the subject lines of this spam are:

- Beauty and the Geek 2
- fill this Passport Form
- First Birthday Invitation
- In USA on August 15 and 16
- Picture sizes
- Resume & Coverletter - Feedback
- Status
- Employee Orientation
- Your reservation is confirmed - Ref: 00338/058758
- Garages
- Picture sizes
- Another candidate brought to you
- Sales Dept

Source: http://www.cert-in.org.in/currentacts/currentact.htm#MSIA

Participants Comments

According to me the session was very useful which helped me toknow more about security whihc i will use it properly.

By:Jaishree
Jyothi Kendriya Vidyalaya
Bangalore

I was really wondered about the harms and affects of internet and also computing but this program enabled me to do my computing or interneting safely here after.Thanks a lot for your guidance.

By:M.Abharna
ITI Vidya Mandir
Bangalore

This workshop is all about taking precautions like we should not reveal our idenity while we are chatting .This kind of workshops are very rare and should be conducted to who are more unaware of using internet properly.

By : RajLaxmi Varma
XI KV,Hyderabad

InfoSec Workshops

@ Naval Children School, Mumbai

@ Kendriya Vidyalaya No.1, Port Blair

Information Security Awareness workshop
covered School Children- 20938,
College Students -1443
Teachers, Govt. Employees- 5656
till August 31 2010

@ Government Polytechnic College , Solan, HP

@ Garden City College, Bangalore

Interested to organize InfoSec Workshop at Your Place ?
for more details visit ....
http://infosecawareness.in/isea-pi or mail us at isea@cdac.in

InfoSec Workshops

Information Security Awareness to Others (Teachers,Air Force, Govt. Employees)

Participants Comments

This is a very necessary and good step taken by the Indian Government as this workshop awares us alot about Internet security and the faculty of CDAC provides this knowlegde in a very good manner.

By: Deepaknandal
Govt. employee from Himachal Police
Mohali

An Informative lecture gave an insight on to many things and internet ethcis, some of which were over-looked during daily usage of the " World wide web"

Flt tt Karan
College of Air Warfare
Secunderbad

I found this workshop is very useful to know many things like i never know that pop-ups can corrupt computer and there are many things i learnt today,from now i will enable pop-up blocker for all the sites I visit like google, yahoo, orkut, facebook.

By: Anish,IX D
AMS P Obul Reddy Public School, Hyderabad

@ CDAC ,Mohali

@ITI Bassi Pathana, Fatehgarh Sahib, Punjab

@ College of Air Warfare, Secunderabad

@Naval Children School, Kochi

@Central Power Research Institute, Bangalore

Users Views on the Cartoon – Guess Tip Contest

KEEP YOUR PC IN CLEAN PLACE.

- Karan

PHYSICAL ACCESS PREVENTION SECURITY.

- Shashi Shekhar

COVER THE PLACE WITH SMALL WIRE MESH SO THAT RAT AND CAT DON'T ENTER INSIDE.

- Akash Ganga

KEEP THE COMPUTER ENVIRONMENT CLEAN AND NEAT.

- Amol

Feedback on infosecawareness portal

Your efforts towards a aware and secure cyber user is commendable. the information posted on the site is very useful and people in India as they can relate to it easily. Also the language used is well suited for the indian cyber citizen. I would like to bring to your attention one small detail that user's frequenting you site encounter. The content posted is not downloadable. I hope you would look into the issue at the earliest. But for the rest keep up the good job. **By: Amit Setty**

Our Sincere Thanks to Action Group Members for Guiding us

Shri G.V.Raghunathan, Senior Director and HoD, DIT
Dr.N.Sarat Chandra Babu, Executive Director, CDAC Bangalore
Shri Sitaram Chamarthy, Principal Consultant, TCS
Dr.Dhiren R Patel, Professor of Computer Science Department, IIT ,Gandhinagar

Centre for Development of Advanced Computing (C-DAC), a Scientific Society of Department of 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

For Information Security Awareness Workshops at your place contact:

Editorial Committee :
D.K .Jain Director
C-DAC Hyderabad
S.K.Vyas Joint Director
Department of Information Technology
Ch.A S Murty &
Indraveni.K
C-DAC Hyderabad

Comments & Feedback
mail us at isea@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
JNT University Campus, Kukatpally, Hyderabad - 500 085. Tel: 040-2315 0115
Fax: 040-2315 0117.
www.cdac.in