



Computer Ethics

Ethics

◎ What are Ethics?

- A set of moral principles that govern an individual or a group.

◎ What are Computer Ethics?

- Computer ethics are set of moral principles that governs the usage of computers.

◎ What are Internet Ethics?

- Internet ethics means an acceptable behavior for using internet. We must be honest, respect the rights and property of others on internet.

Ethical Values

⦿ Pretending

- We must not hide our identity and fool others.

⦿ Language

- We must not use bad or rude language.

⦿ Importance of copyrights

- We must give respect and importance while downloading and we must not use the copyrighted material.



Ethical Values

- ◎ Internet is not a value-free zone
 - As World Wide Web is not a just web where we can get the information from the world but it is a place where values are considered in a broadest sense.
- ◎ Sensitivity
 - It belongs to all, there is no barrier of national and local cultures.

Example



- Mr. A stepped out from the computer lab without logging off.

Example

- Mr. B sits on Mr. A computer and still logged in as Mr. A and sends false e-mail messages to a number of students and posts similar messages on the class newsgroup.



So teach children to never misuse others computer and e-mail ID to harm others and defame them.

Do's

- ◉ Do use the internet to help your knowledge and to do a school work
- ◉ Do use the internet for communication with family and friends
- ◉ Do use the internet for listening the music, video, learning how to play instruments etc.
- ◉ Do use the internet to gain the knowledge

Don't

- ⦿ Don't use the internet to copy the information and say it is your own
- ⦿ Don't use the internet to communicate with strangers
- ⦿ Don't use the internet to make strangers as your friends
- ⦿ Don't pretend someone else and try to fool others

**We should encourage
children to use Internet**

Wisely and Safely

Importance of Copyrights

Copyrights

- Intellectual Property
- Piracy
- Duplication
- Illegal downloads
- Violating terms and conditions



Copyrights

- Copyright gives authors, artists and others the right to exclude others from using their works.
- Copyright laws protect the rights of the owner.
- Obtain the copyright owner's permission.
- Should always give the source from which you copied.
- For ex: © Copyright 2011, Centre for Development of Advance Computing, Hyderabad



Plagiarism punch knocks out IITs

Charu Sudan Kasturi, Hindustan Times

[Email Author](#)

New Delhi, October 10, 2010

First Published: 23:51 IST(10/10/2010)

Last Updated: 01:05 IST(11/10/2010)

 [email](#)  [print](#)

70 Comments

 Like

42

0

[tweet](#)

share



more ...

Independent cases of plagiarism have hit three different Indian Institutes of Technology with scientists accused of stealing credit for others' research, shocking the academic community and raising concerns about scientific ethics. IIT Kharagpur physics professor R.N.P. Choudhary has lost his position as head of department after a junior faculty member A.K. Thakur accused him of not sharing research credit with him.

A research paper jointly authored by professors of IIT Delhi, Jamia Millia Islamia and the Inter University Accelerator Centre (IUAC), published in 2009, has been retracted by editors of the journal Nuclear Methods and Instruments. The retraction notice says the "authors have plagiarized parts of a paper that had already appeared" in another journal.

Two review articles coauthored by a senior IIT Kanpur professor Ashok Kumar have also been retracted by the journal Biotechnology

[Plagiarism Software](#)

Software checks for Plagiarism Plagiarism and Anti - Plagiarism

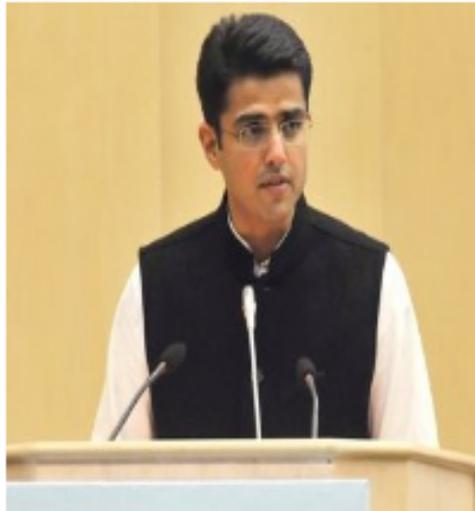
[TurnitinSafely.com/Plagiarism](#)



Ads by Google

Bengaluru, Delhi top in cyber crimes

TT Correspondent | | 29 Mar 2012



In the recent past the country has witnessed a rise in the cyber crimes with Bengaluru and national capital Delhi registering the maximum number of cases. While Bengaluru registered a total of 137 cases of cyber crimes during 2009-10, the figure in Delhi is 46. The figure in Mumbai and Chennai is slightly on lower side with 12 each during the same period.

In a written reply in the Parliament, Sachin Pilot, the minister of state of state for Communications & Information said that as per the cyber crime data

maintained by National Crime Records Bureau, a total of 217, 288, 420 and 966 Cyber Crime cases were registered under Information Technology Act, 2000 during 2007, 2008, 2009 and 2010 respectively. Also, a total of 328, 176, 276 and 356 cases were registered under Cyber Crime related Sections of Indian Penal Code (IPC) during 2007, 2008, 2009 and 2010 respectively.

He said that a total of 154, 178, 288 and 799 persons were arrested under Information Technology Act 2000 during 2007-2010. A total number of 429, 195, 263 and 294 persons were arrested under Cyber Crime related Sections of Indian Penal Code (IPC) during 2007-2010.

Usage of Public Computers

Public Computers

- Most of us use Public computers
 - Emergency
 - Unavailability of our computer
- Some risk is involved in using them:
 - Exposing personal data

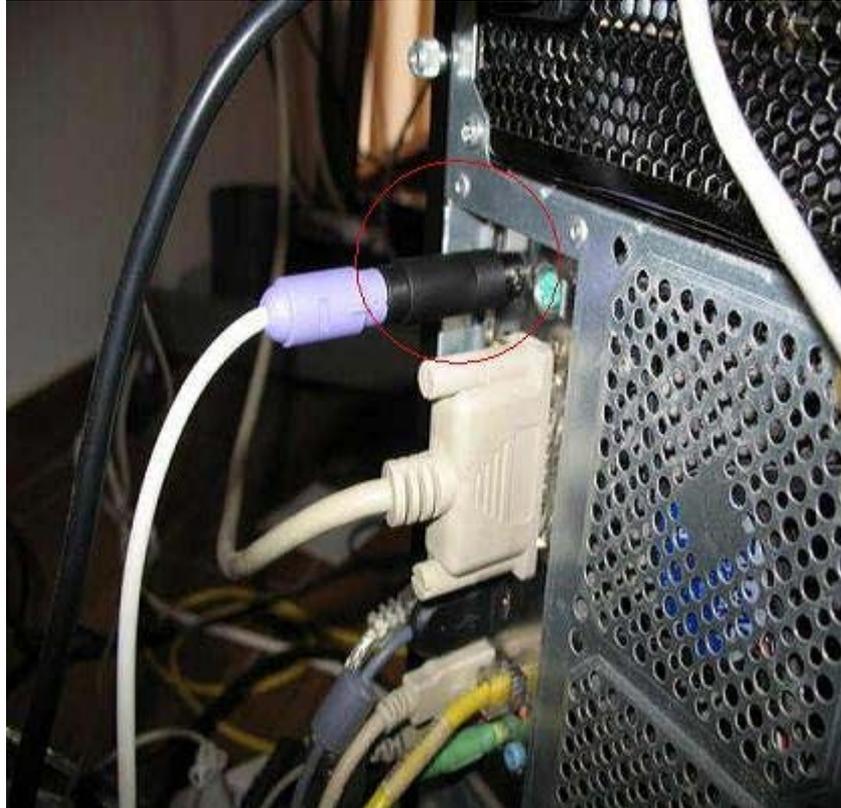
Keyloggers

- **Keystroke logging** (often called **keylogging**) is the practice of tracking(or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored.
- There are numerous keylogging methods, ranging from hardware and software-based to electromagnetic and acoustic analysis.

Types of Keyloggers

- ⦿ Software-based keyloggers
- ⦿ Hardware-based keyloggers

Hardware Key logger



How to Detect Key loggers

- Use Updated anti-spyware
- Run your antivirus checker, it's possible this will pick up the Key loggers on your system.
- Run Spybot S&D, this program checks for some known keyloggers.
- Prevent your self from keyloggers ,Use Virtual key Board

Safety tips for using a public computer

- Don't save your logon information
- Don't leave the computer unattended with sensitive information on the screen
- Disable the feature that stores passwords
- Erase your tracks
- Don't enter banking information into a public computer
- Force Cyber Cafe Owner to allocate you a computer loaded with updated antivirus software



- Prevent your self from keyloggers ,Use Virtual key Board

E-mail and its Risks

- E-mail stands for Electronic mail
- Used for
 - Exchanging messages any time, any where
 - Sending the same message to several people at the same time
 - Transmitting the files



E-mails/chat Risks

- E-mails with attachments
 - May have virus
 - Fake e-mails
 - Spam
 - Lottery mails
 - Job offers
 - Online predators
 - Cyberbullying

E-Mail Risks

- Spam mails
- Junk mails
- Phishing mails
- Chain mails
- Offer mails
- Attachments with
 - Virus files
 - Double extension files

Spam

- It is an unsolicited e-Mail
- Spam may contain
 - Malware
 - Hoaxes
 - Fill up your Inbox
 - Waste of time
 - May contain hidden attachments or links

My Spam e-mail box

Folders:

[Refresh](#) • [New Message](#) • [Empty Trash](#) • [Folder Management](#) • [Vacation Message](#) • [Spa](#)

Disk Space Used: 108.2 MB

[1 - 25 of 59]

Status	Date (▼)	From	Subject	Size
	12/08/09 22:39	AMERICAN ONLINE LOTTERY	AMERICAN ONLINE LOTTERY!! (YOU HAVE WON USD1,300,000.00)	61
	12/08/09 16:18	plolidays	Re: Invitation for air tickets booking	281
	12/07/09 22:52	DR SANUSI LAMIDO	Fund Transfer Notification usd\$7.2million	211
	12/07/09 00:49	info@whitesmokemail.com	{Disarmed} Cyber Monday re-run! 24 Hours Only	101
	12/05/09 15:27	info@whitesmokemail.com	{Disarmed} Can Cyber Monday be Beat? Check Inside...	291
	12/04/09 16:00	Suresh Ramasubramanian	{Disarmed} [India-InfoSec] Nigerian trying to catch sbi gold accounts	271
	12/04/09 11:33	Prasanthi Kothamasu	FW: WHY RATAN TATA IS RESPECTED THE MOST?	411
	12/04/09 01:30	info@whitesmokemail.com	{Disarmed} Can Cyber Monday be Beat?	241
	12/03/09 01:11	info@whitesmokemail.com	{Disarmed} Unbeatable Price Via Our Live Chat / Call Center	221
	12/01/09 17:49	Royal Bank of Scotland Group PLC	Account Notice!!!	81
	11/30/09 23:45	Parth Manna	{Disarmed} RE: [India-InfoSec] Virus attack in many rooms at a time, says IIM B director	351
	11/30/09 22:21	Sunbelt Software	{Disarmed} Uncoming Webinars from Sunbelt Software	111
	11/28/09 18:02	coca cola	YOU HAVE WON!!!	2181
	11/27/09 21:29	MINISTRY OF FINANCE	[SPF:fail] OUTSTANDING PAYMENT APPROVED	61
	11/13/09 19:03	srivalli.j.	RE: Offer from R G B C - Kerala	171
	11/12/09 14:05	Prasanthi Kothamasu	FW: REALITY OF KONKAN	51



How do spammers get your e-Mail?

- Publishing e-Mail address
- Spammers use software's
- Buy your e-Mail address
- Spyware
- Opening attachments from unknown users

How to avoid spam?

- Limit who gets your email
- Personalize the spam setting
- Use e-Mail with anti-spam software
- Disable graphics for unknown senders
- Only enable graphics from senders you trust

Phishing

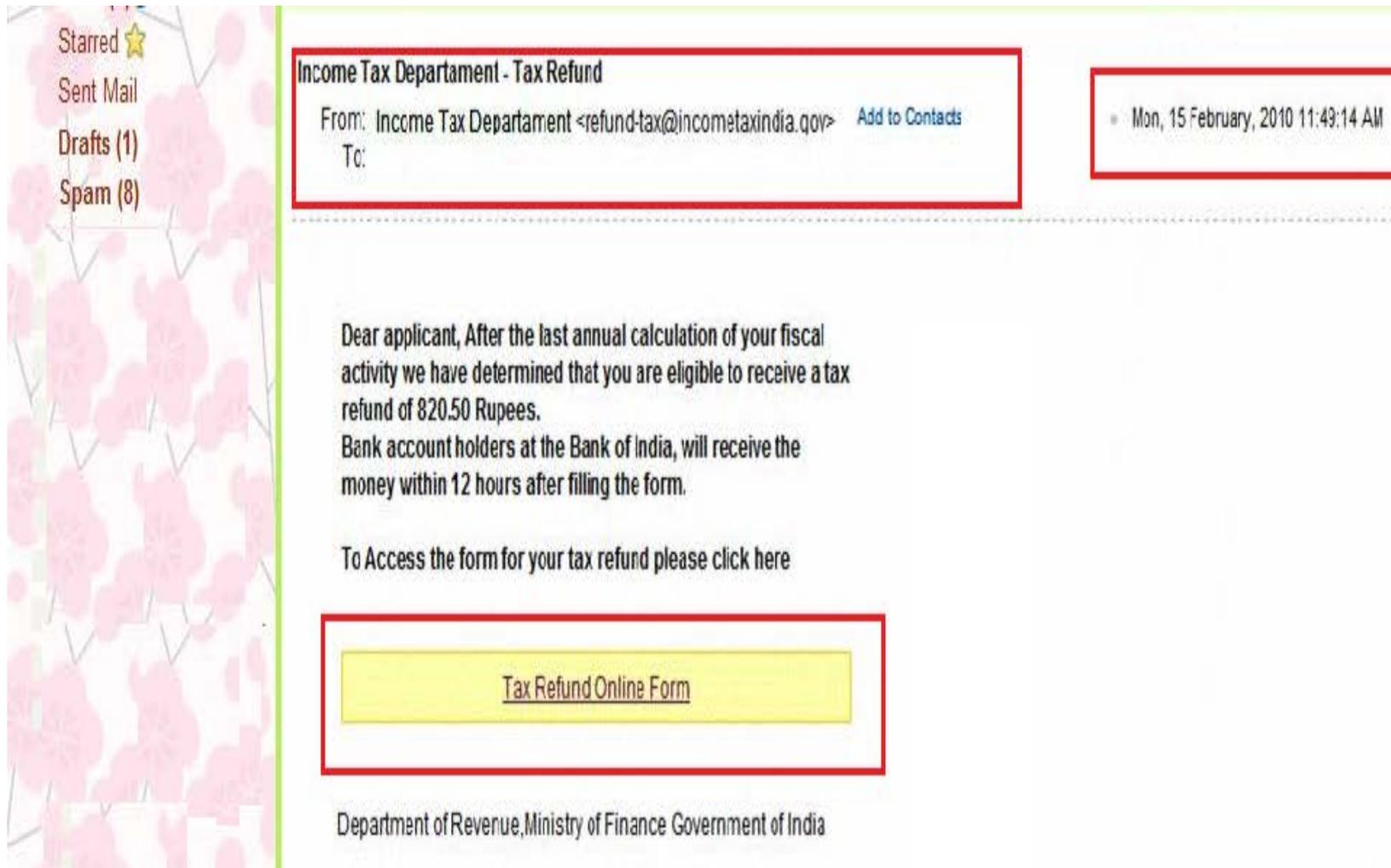
- E-mail sent by online criminals to trick you into going to fake Web sites and revealing personal information.
- In other words It is the criminally fraudulent process of attempting to acquire sensitive information such as **usernames, passwords and credit card details** by masquerading as a trustworthy entity in an electronic communication.

Example

- ⦿ www.g00gle.com
- ⦿ www.yah00.com
- ⦿ www.gmai1.com
- ⦿ www.amaz0n.com
- ⦿ www.paypa1.com

Do not click on suspicious links. In some cases, doing so may cause malicious software to be downloaded to your computer or they may tempt you to leak your personal information for misuse

Example of Phishing e-Mail



Starred ☆
Sent Mail
Drafts (1)
Spam (8)

Income Tax Department - Tax Refund

From: Income Tax Department <refund-tax@incometaxindia.gov> [Add to Contacts](#)
To:

Mon, 15 February, 2010 11:49:14 AM

Dear applicant, After the last annual calculation of your fiscal activity we have determined that you are eligible to receive a tax refund of 820.50 Rupees.
Bank account holders at the Bank of India, will receive the money within 12 hours after filling the form.

To Access the form for your tax refund please click here

[Tax Refund Online Form](#)

Department of Revenue, Ministry of Finance Government of India



Draft Direct Tax Code

PAN

TAN

eTDS

AIR

OLTAS

PAY TAXES ONLINE

VIEW YOUR TAX CREDIT

Tax-Payers Information Booklet

BPR

Foreign Remittance (Form 15CA)

Aaykar Sampark Kendra (ASK)
PAN/TAN/OLTAS & eFiling queries

0124 2428000



Where's My Refund

Dear applicant,

After the last annual calculation of your fiscal activity we have determined that you are eligible to receive a tax refund of 820.50 Rupees.

Please submit the tax refund and allow us 3-5 business days in order to process it.

If you don't receive your refund within 5 business days from the original IRS mailing date shown on Where's My Refund?, you can start a refund trace online.

To get to your personal refund information, be ready to enter your:

- Full name, Address and the Debit/Credit Card where refunds will be made.

To access the form for your tax refund, please click on the "Where's My Refund?" above image or [Tax Refund Online Form](#).

Note:

- For security reasons, we will record your ip-address and date.
- Deliberate wrong inputs are criminally pursued and indicted.



Press Release



Educational Institutions under section 10(23 C)



Industrial Parks u/s 80 IA(4)(iii)



Tax Information Network



TIN Helpdesk



Tax Calculator



Departmental News



Cadre Review and Restructuring of Income Tax Department



Tax return preparers scheme

[Draft Direct Tax Code](#)

[PAN](#)

[TAN](#)

[eTDS](#)

[AIR](#)

[OLTAS](#)

[PAY TAXES ONLINE](#)

[VIEW YOUR TAX CREDIT](#)

[Tax-Payers Information Booklet](#)

[BPR](#)

[Foreign Remittance \(Form 15CA\)](#)

Aaykar Sampark Kendra (ASK)
PAN/TAN/OLTAS & eFiling queries

Tax Refund Online Form

Please enter your information where the refund will be made.

*Cardholder Name:

*Date of Birth:

Month Day Year

*Mother Maiden Name:

*Address:

*Town/City:

*State/Province/Region:

*Postal Code:

*Phone Number:

*Bank Name:

*Card Number:

*Expiration Date:

Month Year

*Card Verification Number:

*ATM Pin:



[Press Release](#)



[Educational Institutions under section 10\(23 C\)](#)



[Industrial Parks u/s 80 IA\(4\)\(iii\)](#)



[Tax Information Network](#)



[TIN Helpdesk](#)



[Tax Calculator](#)



[Departmental News](#)



[Cadre Review and Restructuring of Income Tax Department](#)



Tax return

Original Site

Visit Field Offices:

[Select]

Visit Directorate Generals:

[Select]

 **Income Tax Return**
TDS Return
AIR Return
 **e-Pay Taxes**

- PAN
- TAN
- eTDS
- AIR
- OLTAS
- PAY TAXES ONLINE
- VIEW YOUR TAX CREDIT
- Tax-Payers Information Booklet
- BPR/ARC New
- Foreign Remittance (Form 15CA)

Clarification for deduction in respect of contribution to pension scheme under Section 80 CCD

Clarification regarding deduction under Section 80 CCD for contribution made under pension scheme in the light of Circular No-1 /2010 dated 11th Jan'2010 issued on the subject of Deduction of Tax at Source. Clarification

Notification about M/s School of Human Genetics and Population Health, Kolkata.

The Organization M/s School of Human Genetics and Population Health, Kolkata, has been approved by the Central Government for the purpose of clause (ii) of sub-section (1) of section 35 of the Income-tax Act 1961 (said Act), read with Rules 5C and 5E of the Income-tax Rules, 1962 (said Rules) from Assessment year 2008-2009 onwards in the category of 'Other Institution', partly engaged in research activities. Notification

Notification about M/s Sundar Lal Jain Charitable Eye Hospital, New Delhi.

The Organization M/s Sundar Lal Jain Charitable Eye Hospital, New Delhi, has been approved by the Central Government for the purpose of clause (ii) of sub-section (1) of section 35 of the Income-tax Act 1961 (said Act), read with Rules 5C and 5E of the Income-tax Rules, 1962 (said Rules) from Assessment year 2009-2010 onwards in the category of 'Other Institution', partly engaged in research activities. Notification

Notification about "The Indian Law Institute, New Delhi".

The Organization "The Indian Law Institute, New Delhi", has been approved by the Central Government for the purpose of clause (iii) of sub-section (1) of section 35 of the Income-tax Act 1961 (said Act), read with Rules 5C and 5E of the Income-tax Rules, 1962 (said Rules) from Assessment year 2009-2010 onwards in the category of 'Other Institution', partly engaged in research activities. Notification

Recruitment of Sportspersons to the posts of Inspector and Tax Assistants

The Chief Commissioner of Income Tax, Delhi-I, New Delhi, invites applications for the Recruitment of meritorious Sportspersons in different games, sports as listed for the posts of Inspectors and Tax Assistants. Notification in English, Notification in Hindi

Circular on FBT Released by the CBDT

Adjustment of "Advance Tax in respect of Fringe Benefits" for Assessment Year 2010-11

 Hindi Version

 Alerts

 FAQs

 Press Release

 Educational Institutions under section 10(23 C)

 Industrial Parks u/s 80 IA(4)(iii)

 Tax Information Network

 TIN Helpdesk

 Tax Calculator

 Departmental News New

How to recognize?



Fake website address

Official Website Address



Beware of phishing expedition in Hindi

By: Shashank Shekhar **Date:** 2011-05-24 **Place:** Delhi

Spam emails in Devanagari script are being circulated

Real estate executive Badal Srivastava (26) was overjoyed after receiving a mail written in Hindi, which claimed that he had won a handsome amount in a lottery scheme. But when he looked at it again with some friends, several spelling errors in the mail raised doubts. Finally, they consulted a cyber expert who told them it is part of what's popularly known as 'Nigerian spam'.



Representative pic



This Connection is Untrusted

You have asked Firefox to connect securely to **infosecawareness.in**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

▼ Technical Details

infosecawareness.in uses an invalid security certificate.

The certificate is not trusted because it is self-signed.
The certificate is only valid for www.infosecawareness.in

(Error code: sec_error_untrusted_issuer)

▼ I Understand the Risks

If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.**

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

Add Exception...

Add Security Exception

 You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location:

Certificate Status

This site attempts to identify itself with invalid information.

Wrong Site
Certificate belongs to a different site, which could indicate an identity theft.

Unknown Identity
Certificate is not trusted, because it hasn't been verified by a recognized authority.

Permanently store this exception

Certificate Viewer: "www.infosecawareness.in"

General Details

Could not verify this certificate because the issuer is not trusted.

Issued To

Common Name (CN)	www.infosecawareness.in
Organization (O)	C-DAC
Organizational Unit (OU)	Research & Development
Serial Number	00:E1:5D:25:7C:28:B8:EC:BD

Issued By

Common Name (CN)	www.infosecawareness.in
Organization (O)	C-DAC
Organizational Unit (OU)	Research & Development

Validity

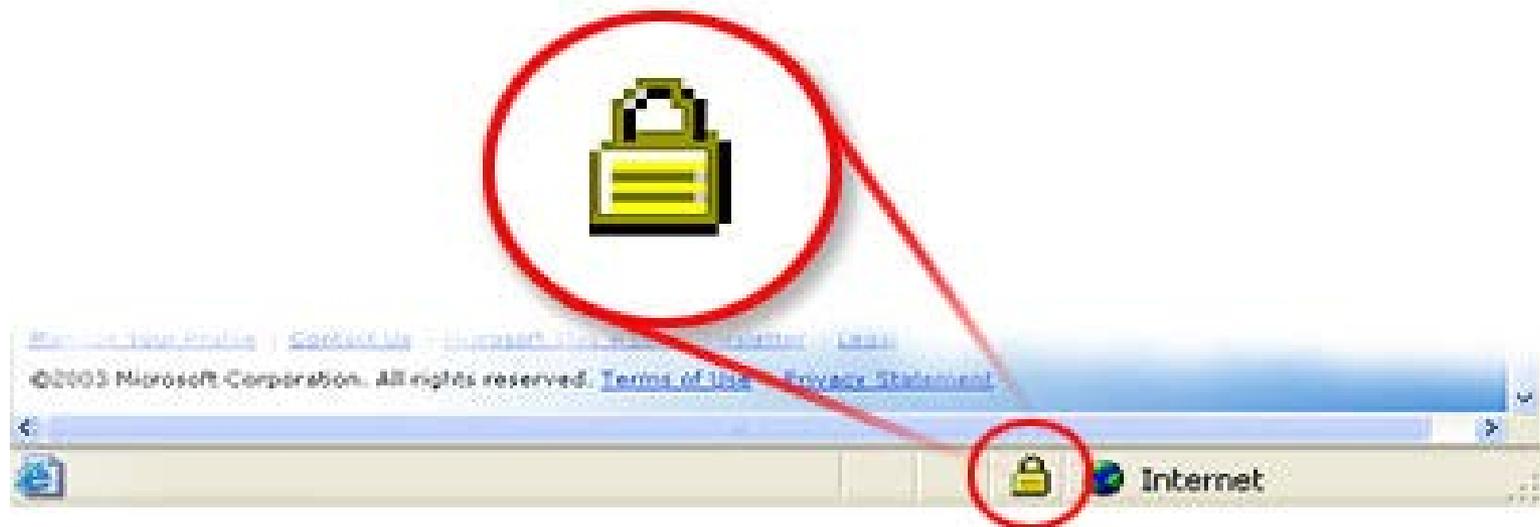
Issued On	23-10-2008
Expires On	22-10-2013

Fingerprints

SHA1 Fingerprint	E5:9D:CB:F5:92:2B:95:73:9D:0F:EE:3D:FC:BB:DA:41:E4:DF:C3:E9
MD5 Fingerprint	20:96:BD:27:93:8D:E6:E9:CE:D7:21:F1:E8:9F:C7:72

Close

- This symbol signifies that the website uses encryption to help protect any sensitive personal information—credit card number, Social Security number, payment details—that you enter



Browser address bar: https://login.yahoo.com/config/login_verify2?&.src=ym

Browser toolbar: Search web..., Favorites, PC Health, Spaces, My Yahoo!, Basketball, Games, Music, Page, Tools.

Taskbar: Windows Live Hot..., US-CERT Cyber S..., Improve the safe..., Gmail - the flight..., Gmail - Inbox ...

YAHOO! MAIL

[Yahoo! - Help](#)

Secured Browser

Phishing Filter

To access Yahoo! Mail...
Sign in to Yahoo!

Yahoo! ID:

Password:

Keep me signed in
for 2 weeks unless I sign out. *New!*
[Uncheck if on a shared computer]

[Forget your ID or password?](#) | [Help](#)

Don't have a Yahoo! ID?
Signing up is easy. [Sign Up](#)

One Yahoo! ID. So much fun!
Use your single ID for everything from checking Mail to checking out Yahoo! Music, Photos, Messenger, and more.

Taskbar: Internet, 100%

Lottery offers

- ⦿ Emails boasting enticing odds in foreign lotteries. You may even get a message claiming you've already won!
- ⦿ You just have to pay taxes or custom Duties to get your prize or collect your winnings

Lottery e-Mails

<input type="button" value="Delete"/> <input type="button" value="Mark"/> <input type="button" value="Move..."/>			
<input type="checkbox"/>	From	Subject	Date
<input type="checkbox"/>	MOTOROLA ELECTRONIC MAIL PROMO WINN	MOTOROLA ELECTRONIC MAIL PROMO WINNING NOTIFICATION	9:40 PM
<input type="checkbox"/>	OCEAN BLU LOTTERY	Congratulations	9:28 PM
<input type="checkbox"/>	Mrs.Helen Anderson	ATTN:WINNER	8:32 PM
<input type="checkbox"/>	FreeLotto Board	Claims Requirrements	8:27 PM
<input type="checkbox"/>	THE FORD FOUNDATION	Donation Grant	8:07 PM
<input type="checkbox"/>	U.K ONLINE LOTTERY INTERNATIONAL	FINAL NOTIFICATION.....	7:22 PM
<input type="checkbox"/>	Uk Claims Dept	Attn:Lucky Winner	6:52 PM
<input type="checkbox"/>	Uk Claims Dept	File For Claim	11:59 AM
<input type="checkbox"/>	ALI DANJUMA	FROM THE DESK OF DR.ALI DANJUMA	11:38 AM
<input type="checkbox"/>	THE FORD FOUNDATION	Congratulaion!!!...Ford Foundation Grant	9:44 AM
<input type="checkbox"/>	IRISH NATIONAL LOTTERY	Attention: Lucky Winner	8:16 AM
<input type="checkbox"/>	Online Co-Ordinator	Your Email Address Was Luckily Selected	7:02 AM
<input type="checkbox"/>	suzanne_y	Dearest,	6:53 AM
<input type="checkbox"/>	ABDU YOLA	FROM, THE DESK OF MR ABDU YOLA,	3:50 AM
<input type="checkbox"/>	Dell Notification Office	Claims informations:	Sun, 7/27/08
<input type="checkbox"/>	global promotion	GLOBAL LOTTERY CORPORATION	Sun, 7/27/08
<input type="checkbox"/>	Irish Lottery News Center	Confirm Your Winning Amount	Sun, 7/27/08
<input type="checkbox"/>	Wins !	2008 LUCKY WINNER !	Sun, 7/27/08
<input type="checkbox"/>	abdul sani karim	FROM:MR ABDUL SANI KARIM	Sun, 7/27/08
<input type="checkbox"/>	Wins !	2008 LUCKY WINNER !	Sun, 7/27/08

Job Offers

- Short listed information for overseas jobs and may demand for Rs 25,000 VISA fees
- Another Example
 - By giving commission Job



Subject: Fw: Your Resume is selected. Recruitment Code - A2045302

From: [simhadri jagadeesh](#)

Date: Monday 26 July 2010 10:23 AM

To: indravenik@cdac.in



Dear Candidate,

It is our good pleasure to inform you that your Resume has been short-listed online for our direct recruitment Campus. Company has short-listed 24 candidates list for **IT, Administration and Production Departments**, as well as Company offered you to join as a **Senior Executives and Managers** post in respective department. You are selected according to your resume in which Project you have worked on according to that you have been selected in Company. The Company is recruiting the candidates for new plants in **Pune and Bangalore**.

The Company is a leading Electronics manufacturing business (ISO-9001: 2000 Certified) having a turnover of 8,000 Crores. The Company is manufacturing Electronics products.

Your Appointment Process will held at Company HR - office - from **2nd August 2010**. You will be pleased to know that Company has advise you in the selection panel that your Application can be progressed to final stage. You will come to Company HR office. Your call letter with Air Ticket will be send to you by courier before date of interview. The Company can be offering you as salary with benefits for this **post 30,000/- to 3, 80,000/- P.M. + HRA + D.A + Conveyance and other Company benefits**. The designation and Job Location will be fixing by Company HRD at time of final process. You have to come with all photo-copies of your qualification documents.

Regarding your coming surety to company on time. You have to deposit an initial security amount in favor of Company HRD for the sum of **Rs.8,450/-** This is refundable interview security against your interview management by HRD. Company will pay all the expenditure to you at the time of face-to-face meeting with you In Company. The Job profile and salary offered by Company will be mention in your call latter. Your call letter and Air Ticket will dispatch very shortly after receiving your confirmation of security deposited in BANK. We wish you the best of luck for the subsequent and remaining stage.

E-Mails with Attachments

October 27, 2009 10:48 AM PDT

Fake Facebook e-mail contains Trojan

by Don Reisinger

Font size Print E-mail Share 36 comments

A new variant of the Bredolab Trojan horse is attached to a fake "Facebook Password Reset Confirmation" e-mail, security firm MX Labs is **reporting**.

391 diggs

[digg it](#)

Some users are receiving the e-mail from "The Facebook Team," according to the security firm. The sender's e-mail address displays "service@facebook.com." In reality, the address and sender were spoofed.

MX Labs found that the e-mail was accompanied by an attachment named, "Facebook_Password_4cf91.zip" and includes the file "Facebook_Password_4cf91.exe" that, the e-mail claims, contains the user's new Facebook password. The security firm said that the element between the underscore and .zip are randomly chosen letters and numbers for each recipient.



When a user downloads the file, it could wreak havoc on their computer. MX Labs said in a blog post that the Trojan horse Bredolab "executes files from the Internet, such as rogue anti-spyware. To bypass firewalls, it injects its own code into legitimate processes svchost.exe and explorer.exe. Bredolab contains anti-sandbox code (the trojan might quit itself when an external program investigates its actions)." In other words, it's nasty.

Once it makes its way to the user's PC, Bredolab creates "%AppData%\wiaservg.log" and "%Programs%\Startup\isqsys32.exe" in the user's system files. MX Labs said that it also creates two new processes, called "isqsys32.exe" and "svchost.exe."

Watch Out for Trojans Circulating in PDFs

Techtree News Staff, Apr 16, 2010 1351 hrs IST

Websense Security Labs warns of Zbot campaign; an information stealing trojan



Websense Security Labs has received several reports of a Zbot trojan campaign spreading via email that connects your PC to a malicious remote server in China. They have seen over 2,200 messages so far.

Zbot (also known as Zeus) is an information stealing trojan (infostealer) collecting confidential data from each infected computer. The main vector for spreading Zbot is a spam campaign where recipients are tricked into opening infected attachments on their computer.

This new variant uses a malicious PDF file which contains the threat as an embedded file. When recipients open the PDF, it asks to save a PDF file called Royal_Mail_Delivery_Notice.pdf. The user assumes that the file is just a PDF, and therefore safe to store on the local computer. The file, however, is really a Windows executable. The malicious PDF launches the dropped file, taking control of the computer. At the time of writing, this file has a 20 percent anti-virus detection rate (SHA1 : f1ff07104b7c6a08e06bededd57789e776098b1f).

Location of the Zbot:

The Zbot trojan creates a subdirectory under %SYSTEM32% with the name "lowsec" and drops the "local.ds" and "user.ds" files. The "local.ds" and "user.ds" are configuration files for the threat. It also drops an executable "sdra64.exe" and modifies the registry entry "%SOFTWARE%\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit" to launch itself during system startup. When it runs, it injects malicious code into the Winlogon.exe instance in memory. This Zbot variant connects

Users Received e-Mails as

October 28, 2009 1:16 PM PDT

Bank Trojan botnet targets Facebook users

by Elinor Mills

Font size Print E-mail Share 14 comments

On the heels of one fake Facebook e-mail scam, a researcher warned on Wednesday of another such campaign in which users of the popular social network are being tricked into revealing their passwords and downloading a Trojan that steals financial data.

In the latest scam being blasted to e-mail in-boxes, a legitimate-looking Facebook notice asks people to provide information to help the social network update its log-in system, said Fred Touchette, a senior security analyst at AppRiver. When the user clicks the "update" button in the e-mail, they are directed to a fake Facebook log-in screen where their user name is filled in and they are prompted to provide their password.



This is a screen shot of the message in the body of the fake Facebook e-mail.
(Credit: AppRiver)

Updatetool.exe

- By running this tool Trojan will install in PC



This is the prompt Facebook users get as part of the latest phishing scam. Downloading the "update tool" installs a Trojan.

(Credit: AppRiver)

First cyber conviction in Hyderabad

A man who was arrested in 2004 for publishing pornographic material of his ex-wife on a matrimonial site and sending obscene mails to her family, was convicted under the Information Technology Act, 2000.

This is the first case in CCPS, CID Hyderabad that has ended in conviction.

Additional Director General of Police, CID, U. Ramamohan said the accused Sanaula Faisal was arrested in 2004 after a complaint was registered against him by the family of his ex-wife. He was running a computer business, and within a year of the marriage he had allegedly started to harass his wife, and she filed for divorce.

To take revenge on his ex-wife and her family, Faisal created a profile in the name of the victim on a matrimonial site and started posting obscene comments and pictures on it. The photos were taken when they were married.

He also started sending obscene e-mails to her family members.

After the case was registered, Faisal's house was raided and his camera and computer were seized and sent for forensic examination.

An incriminating report from the forensic laboratory regarding the material seized helped the prosecution to clinch the case, and the VI Additional Chief Metropolitan Magistrate's court, Nampally, convicted the accused on February 1, 2012.

The sentence is one year's imprisonment and a fine of Rs 12,000. The accused will have to undergo additional imprisonment if the fine is not paid.

Mr U. Ramamohan said, "We have arrested 30 people for cyber crimes. We recently caught a doctor and some engineers."

Other cyber sexual harassment cases

- Dr Manohar held for posting morphed images of a woman
- Engineer held for breaking the engagement of schoolmate by sending abusive emails
- K. Deepak held for creating a false FB profile of a woman and posting her private photos
- Software professional held for sending obscene messages

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



Search Mail Search the Web

Show search options Create a filter

Compose Mail

- Inbox (6)
- Buzz
- Starred
- Sent Mail
- Drafts (2)
- Spam

Do You Own a Business? - Google.com/places - Help Your Business Be Found Claim Your Free Google Place Page! About these ads

Back to Inbox Archive Report spam Delete Move to Labels More actions

Newer 6 of 5534 Older

Discount in Mobiles & Computer Accessories

Best Discounts show details 12:06 PM (3 hours ago) Reply

Get Hot Shopping Deals & Best Discounts

Click here

Reply Forward



○ Fake emails

GHMC no action was taken.

Exhibition in Hyderabad | ...

12 Nabbed for Online Fraud

Express News Service

Hyderabad: Officials of the state Crime Investigation Department (CID) on Monday arrested 12 persons, mostly Nigerian nationals, for duping a woman to the tune of ₹3.2 lakh by sending a fake mail claiming she had won a prize from Microsoft.

The Cyber wing of CID said that the arrested include Paulinus Oti alias Victor Scott, Nwaneti Chigozie, Obumnaenne Emmanuel Ezenwaka, Solomon E Achulo, Ojimba Henry, Paulinus Emeka

Adibe, Ezennayi Emmanuel, Ekechukwou Onyebuchi Patrick and Umeokoli Nnaemeka from Nigeria and Malsawmthangi, Chatwanrenlali and Laldingliani from Aizwal in North east.

Additional superintendent of police (Cyber cell) U Ram Mohan said that on February 9, the victim received a mail informing her that she had won the Anniversary Award of Microsoft, London and asked her to collect \$1,000,000.

But they told her that she should have to share some of her details besides depositing an amount of

₹3.2 lakhs to claim the cash prize.

"The complainant believed the e-mail to be genuine and replied to the mail. She even deposited the amount demanded, citing processing charges and customs tax to claim the prize amount, into various bank accounts belonging to North Eastern States," Ram Mohan said.

On March 13, one Iswick showed up at her home, claiming to be a representative from the UN Courier Service. He took out two US currency notes which were stained with black colour. Iswick used a

chemical and cleaned the notes for her.

Meanwhile, he took out 100 more similar stained currency notes and told the victim that she needed to buy the chemical to clean the notes and demanded a payment of ₹2 lakh for it.

"Iswick subsequently left for Delhi. But the victim developed suspicion and registered a complaint at the Cyber Crime Police Station, CID," police said.

The accused was traced to New Delhi and a raid was conducted in which 12 persons were nabbed.



Four of the Nigerians arrested by Cyberabad police from Mumbai for online fraud
| EXPRESS PHOTO

Father-Son Also Duped of ₹19 Lakh

Express News Service

Hyderabad: "Congratulations! Your mobile number has won 7,50,000 pounds in the Coca Cola world promotion event" - was the SMS received by Amit Kumar, a second-year engineering student.

Enticed by the promise of easy money, he informed about it to his father, Senapathi, who recently retired from the defence services. The duo in their greed to receive the prize money of 7,50,000 pounds deposited ₹19 lakh in a bank account. It was only after

they deposited the money, they realised they had been duped.

The culprits were arrested on Monday by Cyberabad police in Mumbai, out of which five are Nigerians. Police, however, said they could recover only ₹57,000 of the stolen cash.

Police said Amit Kumar had received an SMS on February 28 which asked him to contact Sir Diplomat Brain Smith on an e-mail address to claim the prize money. He got enticed and informed his father Senapathi about the prize money. "Initially

they were asked to pay ₹15,000 as customs fee. Later, the accused asked them to pay ₹18.68 lakh for claiming the prize money. In hope of bagging the huge amount, Senapathi deposited ₹18.68 lakh in an ICICI bank account as directed by the accused," said an official of the Cyber Crime Cell.

The online fraudsters contacted the victims yet again by informing that another ₹5 lakh should be transferred for payment of the prize money.

At this point they realised they were being duped.



Collector shocked by begging email

[Page](#) [Discussion](#) [View source](#) [History](#)

Date of Publishing:05/12/2010

Location:Hyderabad

A hacker changed the password of Mr Gulzar's email and changed the settings and removed the address list before sending mails to the contacts.

Hackers broke into the email account of the district collector, Mr Natarajan Gulzar, and sent mails to all the contacts in the address book asking them to send £2,200 to him.

After breaking in and creating mischief, the hacker also changed the password of Mr Gulzar's email account in gmail.

The mail that went to the contacts in the name of Mr Gulzar said that he was in England for a seminar and had misplaced his wallet on his way to the hotel.

"I would like you to assist me with an urgent loan of £2,200 to sort out my hotel bills and get myself back home," said the mail.

"Please send the money through Western Union to Gulzar Natarajan, Address: 75, Sloane Street, London, SW1X9SC United Kingdom." The message added: "Kindly help me to make the transfer as soon as you receive this email and once you have it sent, send me the money transfer control number with details." Mr Gulzar was shocked when he started receiving calls from his friends and family members about the message.

"I was in my office at Chiragh Lane and by around 10.30 am on Friday people started calling me," he said.

"I had logged into my email at 9.30 am and kept it open while doing some office work.

Immediately, I checked my email and found a virus. I logged out and when I tried to login again I could not. My password was changed." The hacker even changed the settings and removed the address list from the email before sending mails to the contacts.

Mr Gulzar lodged a complaint with the cyber crimes police with a request to register a case, investigate into it and take necessary action .

The deputy commissioner of police (crimes), Mr J.Satyanarayana, said it will take two days for the cyber crime wing to trace out the details of the hacker. "Hacking is a punishable offence with an imprisonment of three years and fine of '1 lakh," he added.

पंजाब नैशनल बैंक  **punjab national bank**
...भरोसे का प्रतीक ! ...The name you can BANK upon!

- Retail User** ([Click here](#))
- Corporate User** ([Click here](#))
- Corporate User** ([Click here](#))
With Digital Certificates [Help](#)

Restore your Punjab National Bank account.

Complete all fields unless otherwise stated.

Card number:

Expiration date: /

ATM PIN

Customer Information

- Login Tips
- > Internet Banking for NRI
- > Precautions for NetBanking

>>> Contact us

011-23708151 / 23716659
(Mon to Fri 10:00 a.m. to 6:00 p.m.
Sat 10:00 a.m. to 4:00 p.m.)

>> VeriSign Secure Site

All information sent to this site is encrypted and protected from third parties.

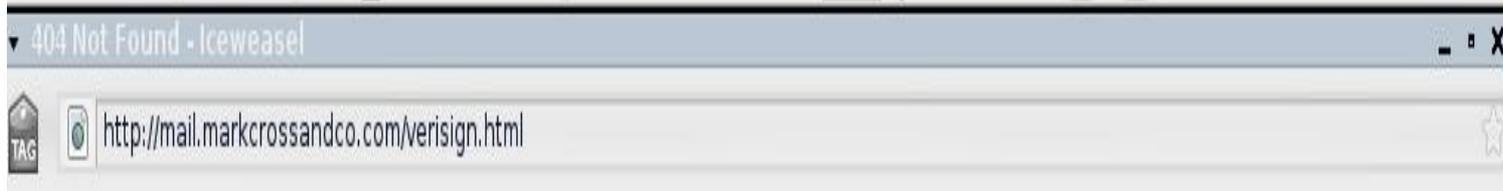


Important Message

Customer Care

Call our toll free number **1 8 0 0 1 8 0 2 2 2 2** from anywhere in India or paid number **0 1 2 4 - 2 3 4 0 0 0 0** accessible from mobile also

Information Bulletin



Not Found

The requested URL /verisign.html was not found on this server.

*Apache/2.2.4 (Win32) mod_ssl/2.2.4 OpenSSL/0.9.8e mod_fastcgi/mod_fastcgi-SNAP-0404142202 PHP/5.2.1
mod_perl/2.0.3 Perl/v5.8.8 Server at mail.markcrossandco.com Port 80*

Don'ts

- Never click on the links received from the unknown users.
- If necessary cross check the target of the link by placing mouse at the given link and check the details at bottom left corner before clicking.

Tips for e-mail



How to handle suspicious e-mail

1. If you receive a phishing e-mail message, do not respond to it.
Don't open junk mail at all
2. Approach links in e-mail messages with caution
3. Approach images in e-mail with caution
4. Approach attachments in e-mail messages with caution
5. Don't trust the sender information in an e-mail message
6. Don't trust offers that seem too good to be true
7. Report suspicious e-mail
8. Don't enter personal or financial information into pop-up windows
9. Don't forward chain e-mail messages
10. Update your computer software
11. Verify the Identity and Security of Website
12. Type addresses directly into your browser or use your personal bookmarks

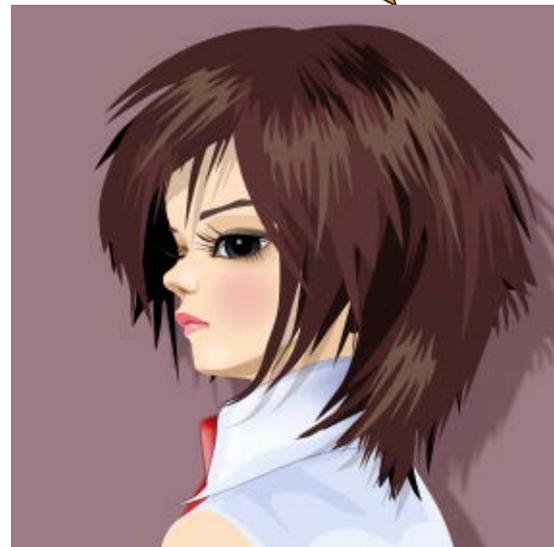
Block images in e-mail

- Pictures in e-mail messages--also called "Web beacons"-- can be adapted to secretly send a message back to the sender
- Spammers rely on information returned by these images to locate active e-mail addresses.
- Images can also contain harmful code and be used to deliver a spammer's message in spite of filters
- The best defense against Web beacons is to prevent pictures from downloading until you've had a chance to review the message
- Beware of malware disguised as holiday greetings in e-mail
- Approach links in e-mail, on social networking sites, or in IMs with caution

Instant Messaging (IM)

- Instant Messaging is a text based communication between two or more connected over internet

**What is
Instant
Messaging**



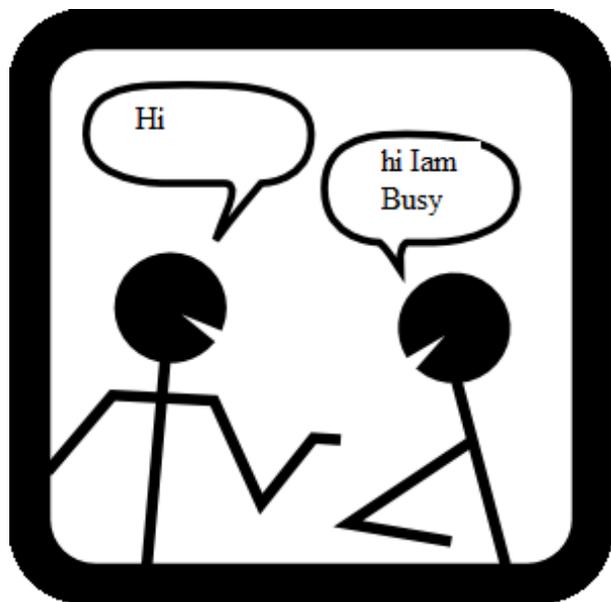
Advantages

- Faster
- Cheap
- Easy to use
- Multitasking



Risks

- Your friends can see when you are online and jump into chat with you no matter how busy you are



Risks in IM

- ◎ **Spim:** It is a short form of spam over instant messaging, it uses IM platforms to send spam messages over IM



Disadvantages

- The voice can be trapped by others
- Once message is posted cannot be deleted
- Chatting may also weaken your language because of extensive use of short forms.
- eg: because – bcoz/coz/cos/bcos
- Why – y
- You – u
- Please – plz

Cont....

- In a public chat rooms you never know with whom you are chatting with and sharing of personal information may lead to complications.
- Sometimes personal information may sent to wrong address.
- Spim (spam on IM) maybe posted every now and then by the strangers which contain advertisements or web links

Contd..

- Hackers constantly access the instant messaging to gather your information
- Hackers try to insert the malicious software by sending files



You sends your photo



Stranger may receive it



But Always remember
"Be careful"

You never know who is on other side



Online Predator

Risks: Online predators try to trap children by making friends online and then insist to meet in person.

They may also offer free gifts in which malicious information is contained

Tips: Children should be aware that they should not give out information about themselves on net.

Never open, accept or download a file in IM from strangers.



Student harassed by online lover for 6 years

Mid-Day.com, Updated: April 05, 2011 14:01 IST

Ads by Google

[Vista 90 is Here](#) – The Most Powerful Petrol Hatch in its Class.Blink it & You'll Miss it

Cars.tatamotors.com/Vista90



Pune: A 40-year-old businessman was arrested on charges of molesting and sending lewd messages to a 20-year-old medical student, with whom he allegedly had been in a relationship for the last six years. Sali Bhalchandra Nanal, who hails from Mumbai, was arrested yesterday evening for harassing the victim while she was studying in Solapur.

According to the complaint lodged, the victim was introduced to Nanal in 2005 through a social network

site.

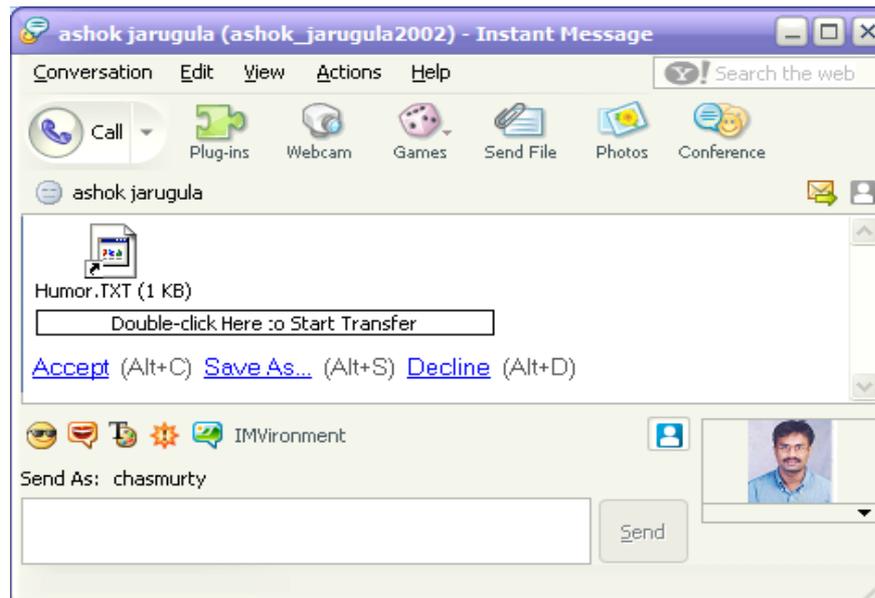
Cont....

- ⦿ In a public chat rooms you never know with whom you are chatting with and sharing of personal information may lead to complications.
- ⦿ Sometimes personal information may sent to wrong address.
- ⦿ Spim (spam on IM) maybe posted every now and then by the strangers which contain advertisements or web links



Mitigations

- Choose a nick name that doesn't give away your real name.
- Never open, accept, or download a file in IM from someone you don't know.



Cyberbullying



Introduction

- ◎ Technology gives today's kids more ways to connect, socialize and communicate than ever before, that is the good news
- ◎ The bad news is that some kids are abusing the technology.
 - Cyberbullying
- ◎ Victims:
 - Tweens and teens,
 - Troubles adults.

Definition

- The use of information and communication technologies to bully, embarrass, threaten or harass



Cyberbullies Can be...

- ◉ E-mail
- ◉ Cell phones
- ◉ Instant messaging
- ◉ Defamatory personal web sites
- ◉ Defamatory online personal polling websites
- ◉ Interactive games



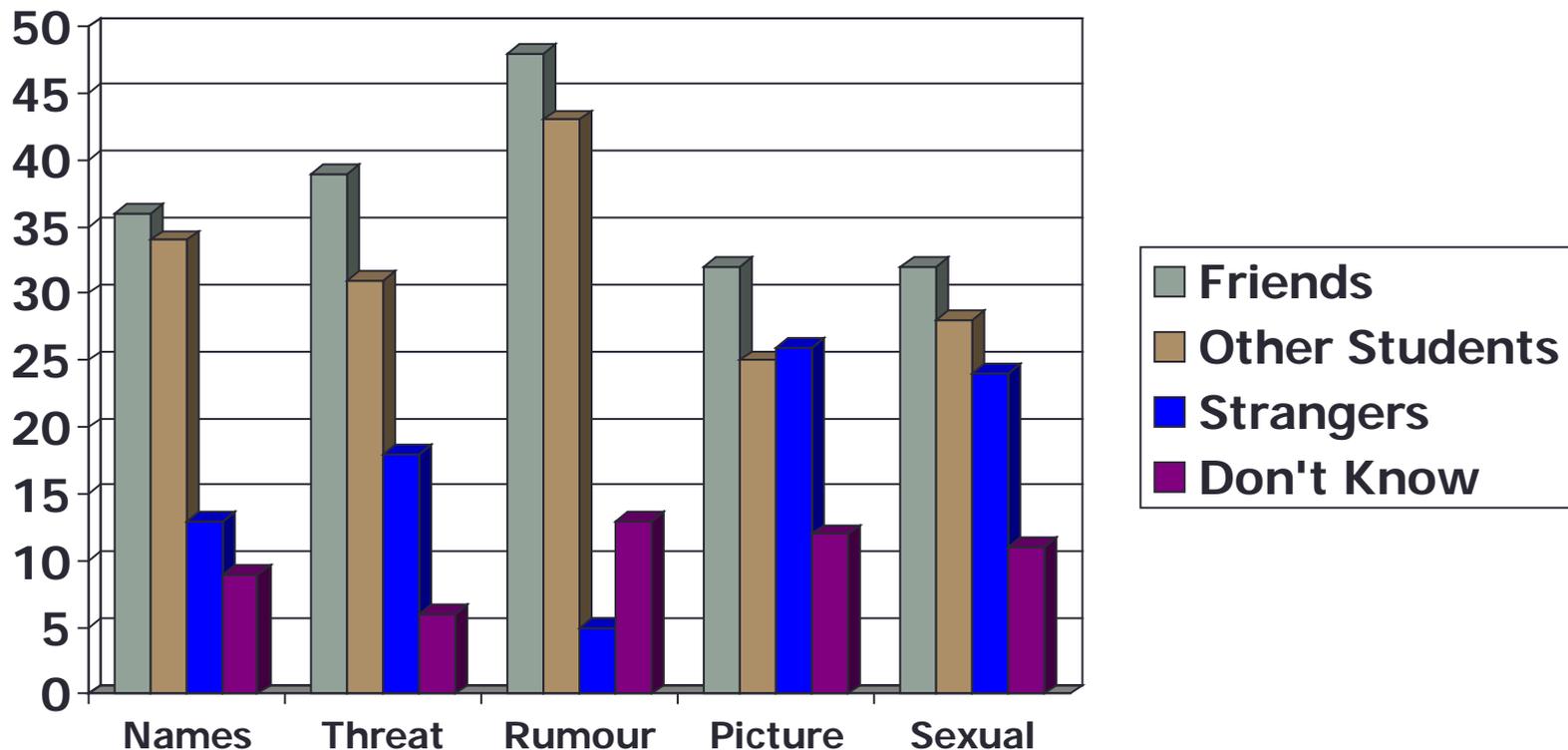
Who bullies whom?

- Student to student
- Students to student
- Student to teacher
- Students to teacher
- Students to school administrators
- Employee to employer
- Employer to employee

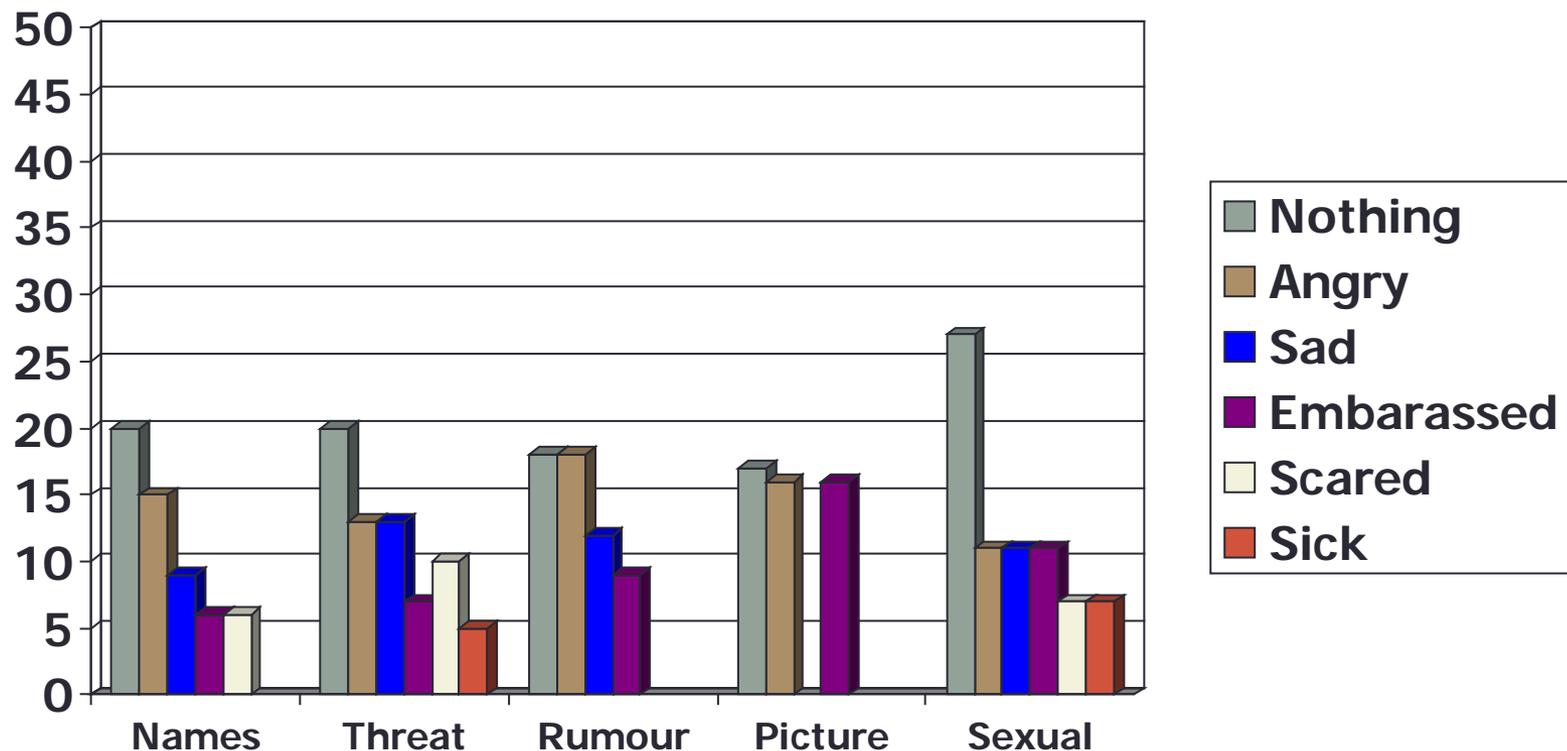
Why do they Cyberbully?

- Motivations of anger, revenge or frustration
- For entertainment or laughs
- To get a reaction after harassing and become popular on cyber world
- By accident – they reacted impulsively
- Power hungry to pain others and to boost their ego
- Mean girls do it to sustain their social standing

Who is doing the cyber-bullying?



How do students feel when they have been cyber-bullied?



Ways of Cyberbullying

Electronic or Cyberbullying

- email, cell phones and internet sites to threaten, harass



Disability bullying

- Treating them badly because of a disability

Sexual

- Spreading a sexual rumour about someone



Examples of e-mails and text messages

○ Text Messages

- Verbal abuse
 - You fat bitch
- Death threats
 - Trust me ur gonna die
- Physical violence
 - You're being knocked out after school

○ Emails

- Verbal abuse
 - Nasty things about my appearance
- Death threats
 - I will kill you
- Chain mails
 - If you don't pass this on you will die

Cont'd

⦿ Social bullying

- Damaging friendships, Spreading rumours and Setting others up to look foolish

⦿ Racial bullying

- Treating people badly because of their racial background

⦿ Religious

- Saying bad things about a religious background



Cyber-bullying 'now the most common form of bullying'

Agencies

Font size: - +

[Kohima Marriage](#)

Looking For Kohima Life Partner?
Register Free! Search, Chat & Marry



[Apply For a Personal Loan](#)

Fast and Flexible. Easy Paper work Up to
Rs 10 Lakh. Apply Online Now!

Ads by Google

London, November 23 (Agencies): Cyber-bullying is now the most common form of intimidation among students in Britain, a new research has revealed. The British government-commissioned research, conducted by the National Centre for Social Research, analysed bullying among more than 10,000 secondary school pupils in England aged 14-16. The initial findings show that 47 per cent of young people report being bullied at the age of 14. This falls to four in ten (41 per cent) among 15-year-olds and less than a third (29 per cent) among 16-year-olds. After cyberbullying – where children face taunts, threats and insults via the Internet and mobile phones – and name calling, the most common type of bullying was teenagers being threatened with violence, being excluded by their friends and facing actual violence. The study showed that girls were more likely to be bullied than boys at the age of 14 and 15. Girls were more likely to face name calling than boys, and to be excluded from friendships, whereas boys were more likely to have their money and possessions taken, and to face violence.



California Law Targets Cyberbullying

January 07, 2009 03:42 PM ET | [Jessica Calefati](#) | [Permanent Link](#) | [Print](#)

Last week, California joined the growing number of states that have passed laws against cyberbullying —harassment inflicted not by physically menacing bullies at schools but through social networking sites, instant messenger programs, and other forms of digital communication.

As of January 1, officials in California schools may suspend or expel students who harass their peers through cyberbullying, the *Washington Post* reports. Like California's law, anti-cyberbullying laws passed in other states call on school districts to develop policies regarding cyberbullying detection and punishment. Other states with cyberbullying laws include: Arkansas, Delaware, Idaho, Iowa, Michigan, Minnesota, Nebraska, New Jersey, Oklahoma, Oregon, South Carolina, and Washington.

More laws are needed because the problem is becoming increasingly widespread. According to a 2006 National Crime Prevention Council study, 40 percent of teens surveyed had experienced some form of cyberbullying in their lifetime. The study also found cyberbullying to be most common among females and adolescents who are 15 and 16 years old.

Perhaps one of the most well-known cases of cyberbullying is that of Megan Meier, a 13-year-old girl from Missouri who hanged herself after being harassed online by a middle-aged woman posing as a teenage boy on MySpace.com. After courting Meier and gaining her trust, 49-year-old Lori Drew (known to Meier as Josh) began sending insulting, hurtful messages to Meier, who had a history of depression and low self-esteem. Before her suicide, Meier told her mother of online posts including "Megan Meier is a slut" and "Megan Meier is fat," *ABC News* reports.

Guidelines

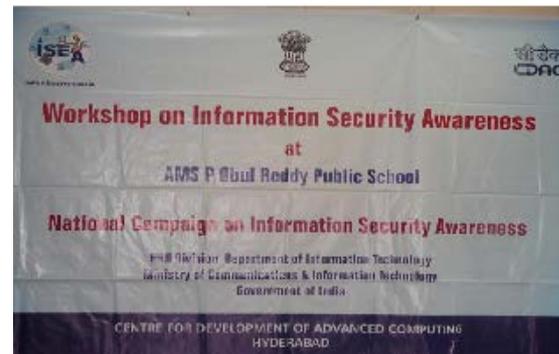
- Follow family rules
- Monitor your child activities
- Educate your children about cyber bullying
- Tracking sender's e-mail
 - E-mail Tracker



Cont'd

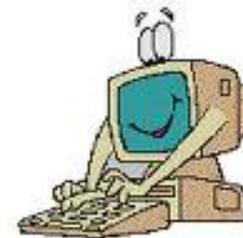
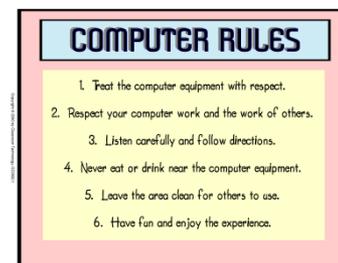
- Use filtering and blocking software
 - Parental control bars, Desktop firewalls, Browser filters to avoid

- Make your child school has internet safety education programming



Cont'd

- Form the rules of computer labs, internet labs specify clear rules
 - Policies for using internet
 - Policies for USB, CD-ROM
- Teach students the impact of the cyber bullying
- Contact the police immediately
 - In any form of cyberbullying death threats



What schools must do?

- ⦿ **Address** cyber-bullying in the curriculum
- ⦿ **Educate** everyone about the consequences of cyber-bullying
- ⦿ **Enforce** the clearly and publicly stated consequences of cyber bullying including the pressing of criminal charges
- ⦿ **Include** cyber-bullying in the school's code of behaviour
- ⦿ **Monitor** e-communications on school site
- ⦿ **Block** harmful websites to students