www.infosecawareness.in

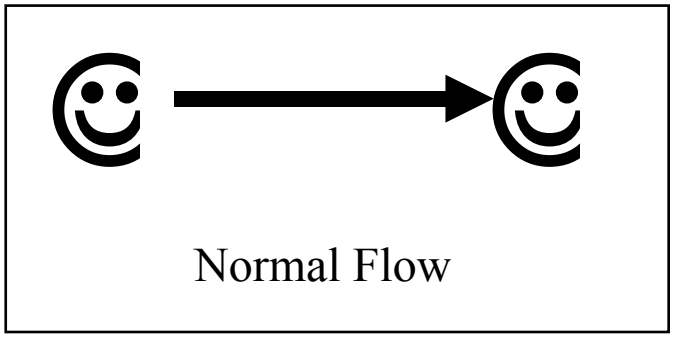
Information Security Awareness

ISEA TEAM
HYDERABAD

www.infosecawareness.in

Basic security concepts

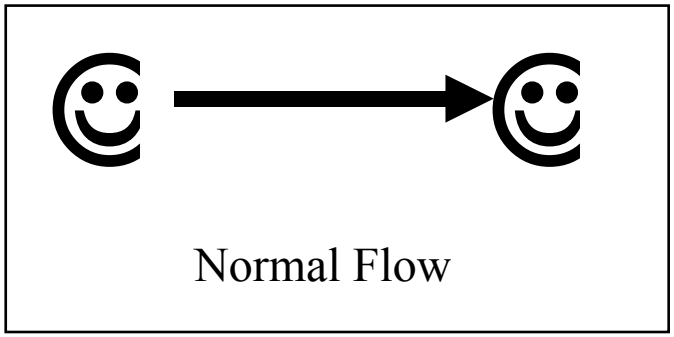
Basic security Concepts

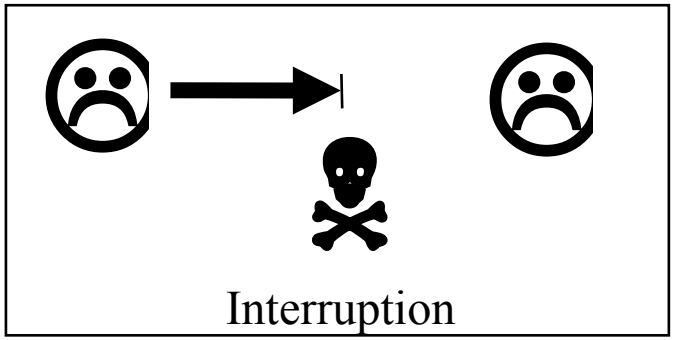


Normal Flow

www.infosecawareness.in

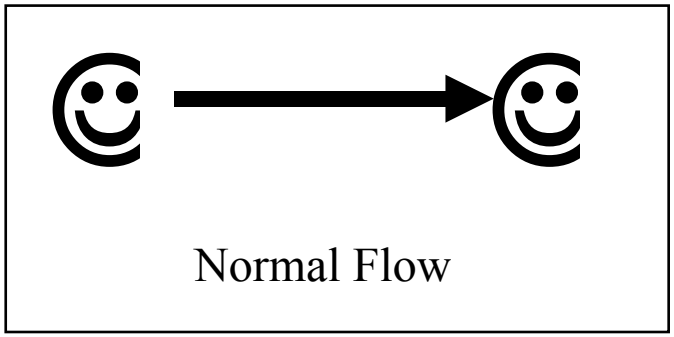
Information Processes

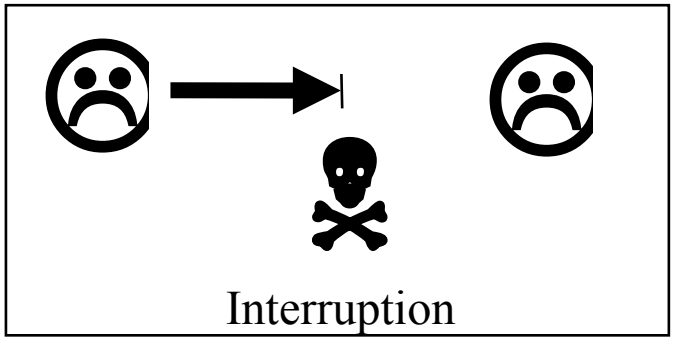


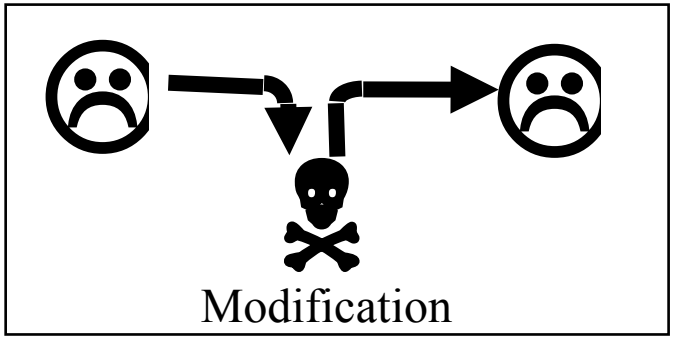


www.infosecawareness.in

Information Processes

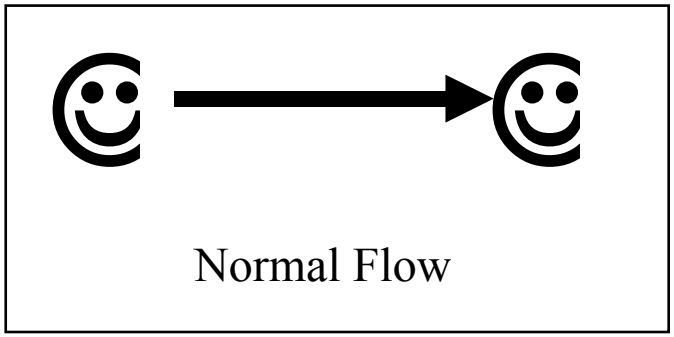


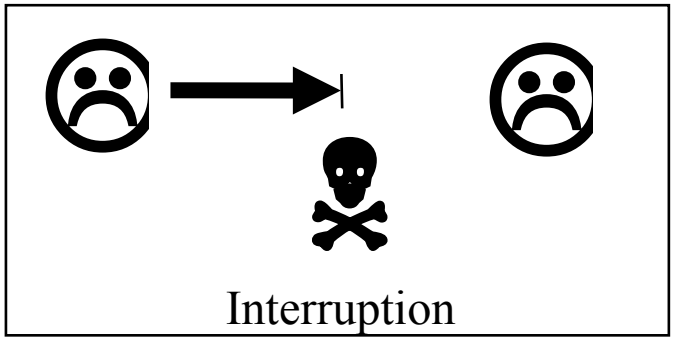


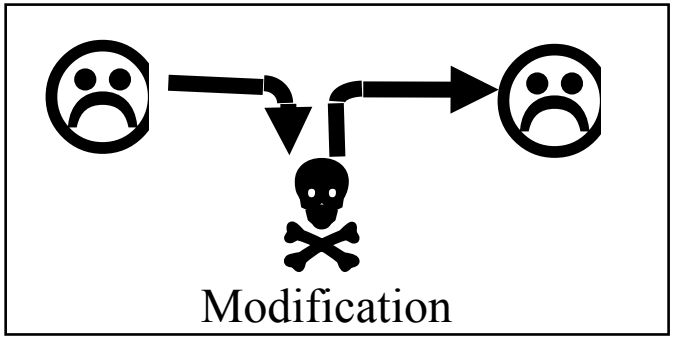


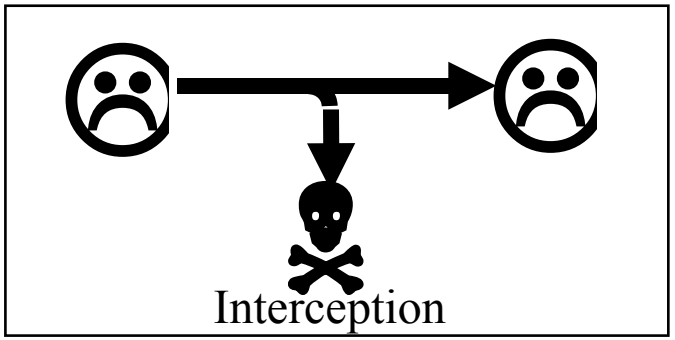
www.infosecawareness.in

Information Processes



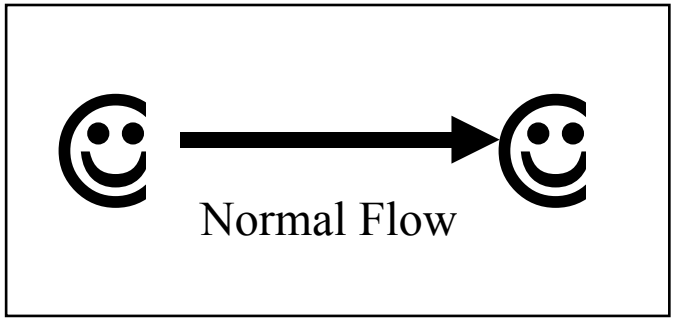


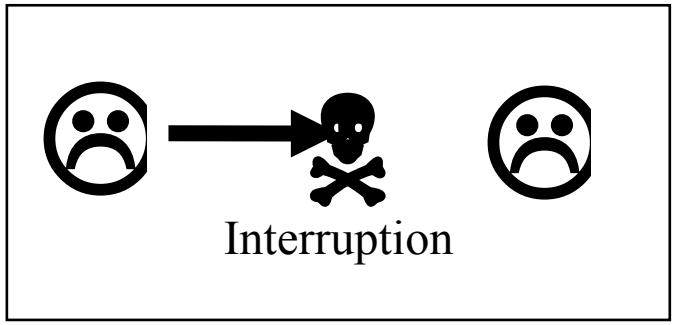


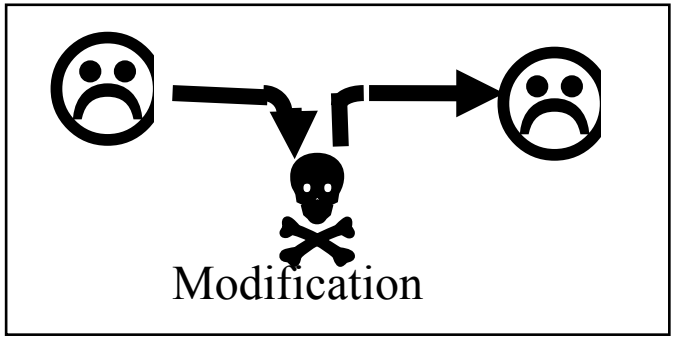


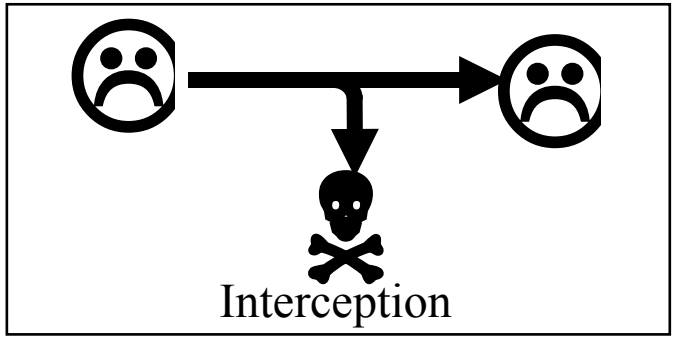
www.infosecawareness.in

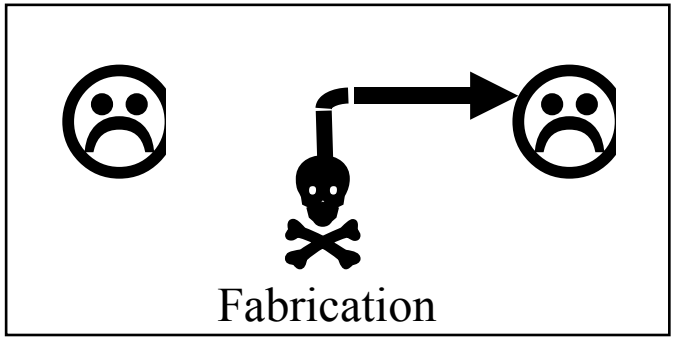
Information Processes





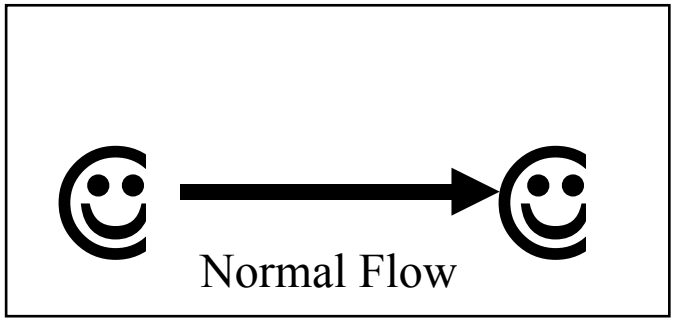


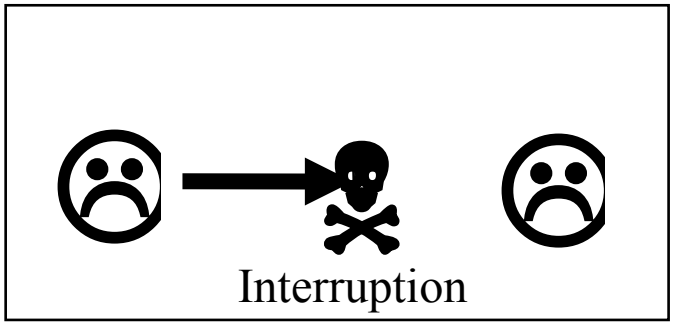


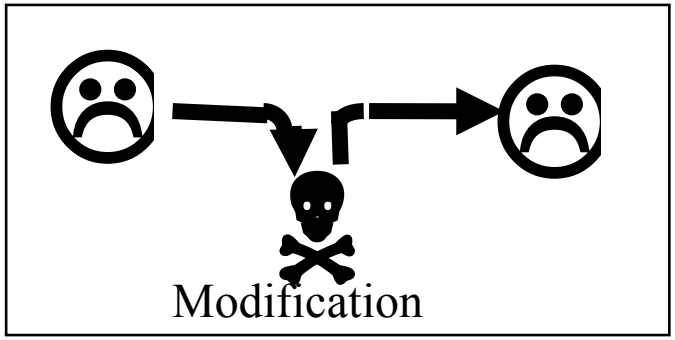


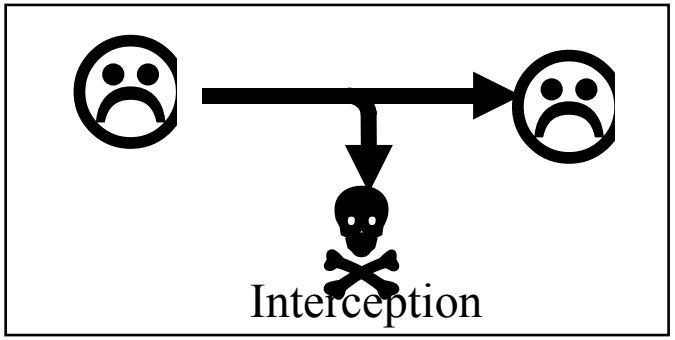
www.infosecawareness.in

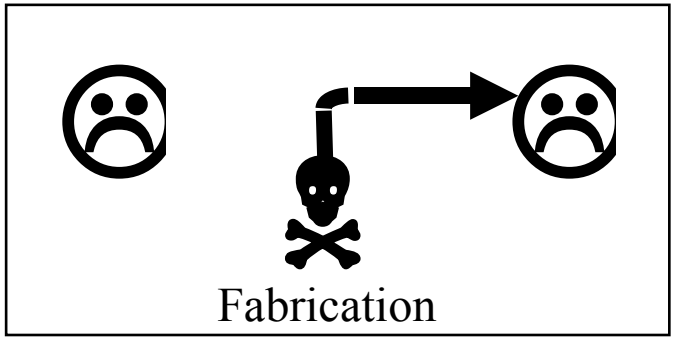
Information Processes

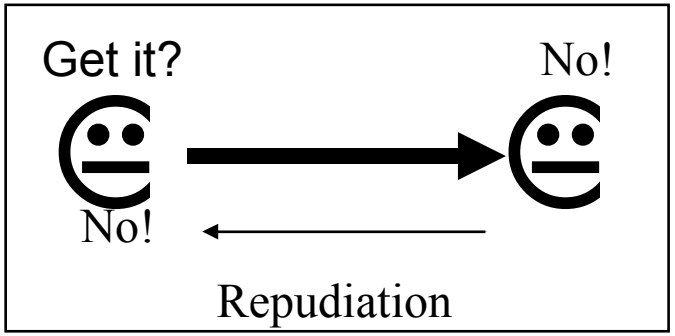






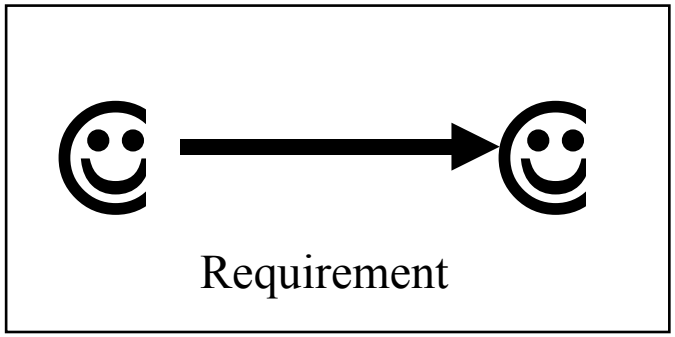




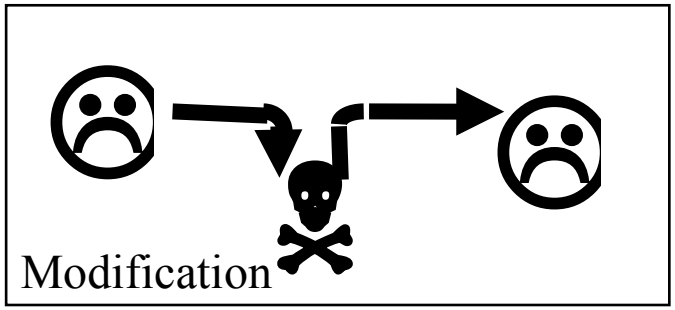


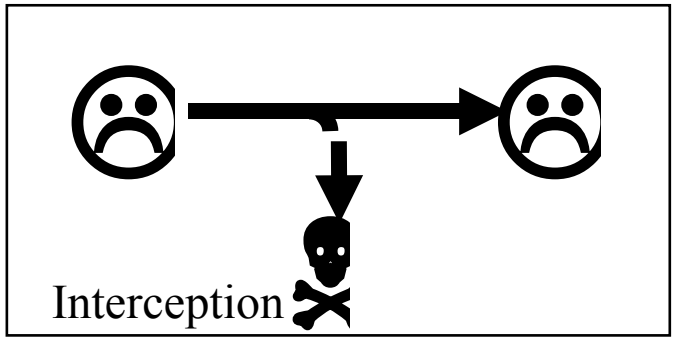
www.infosecawareness.in

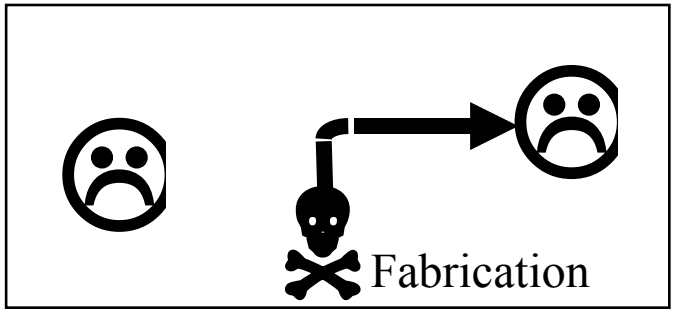
Information Assurance

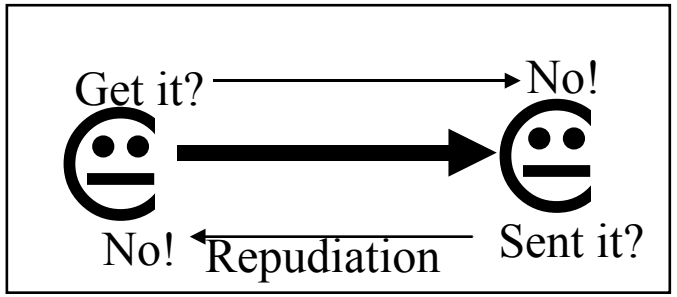


Availability



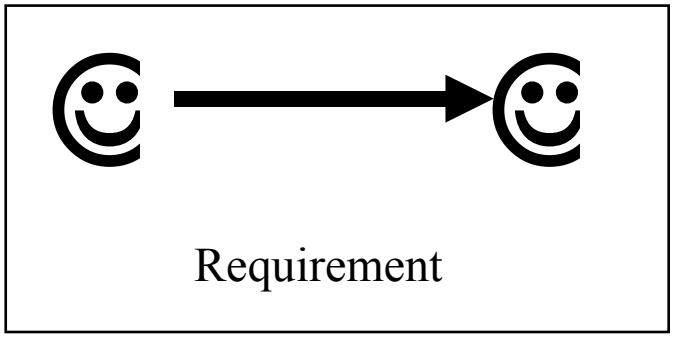






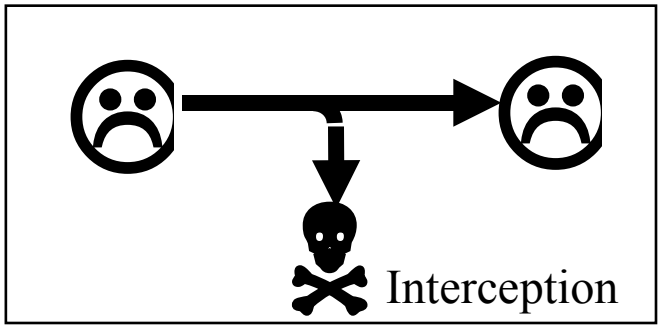
www.infosecawareness.in

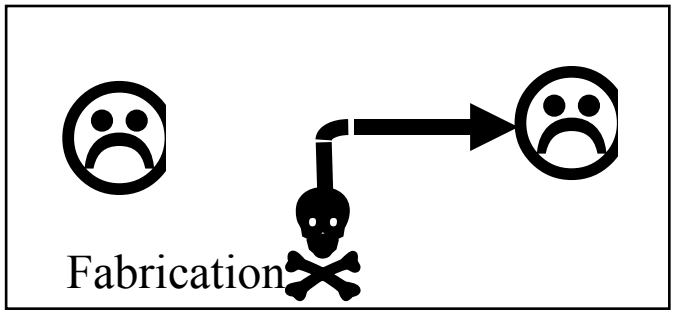
Information Assurance

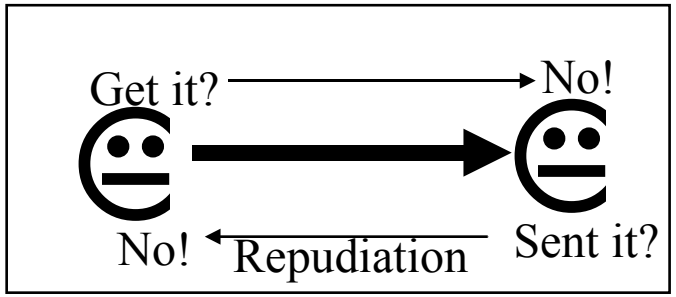


Availability

Integrity







www.infosecawareness.in

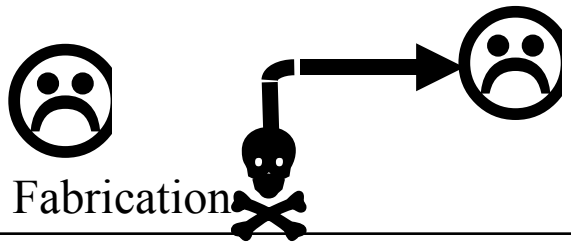
Information Assurance

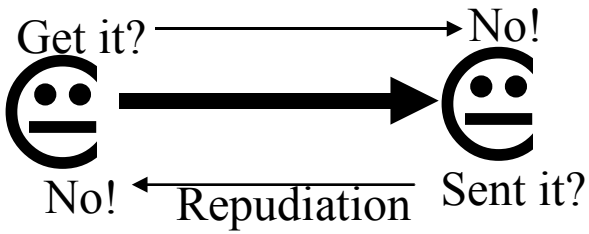
Requirement

Availability

Integrity

Confidentiality





www.infosecawareness.in

Information Assurance

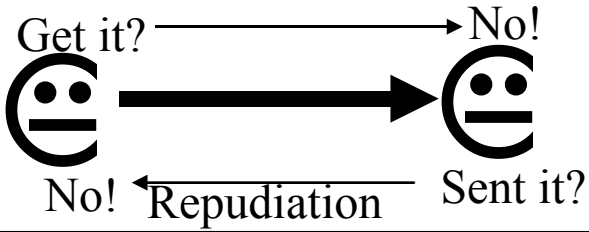
Requirement

Availability

Integrity

Confidentiality

Authenticity



www.infosecawareness.in

Information Assurance

Requirement

Availability

Integrity

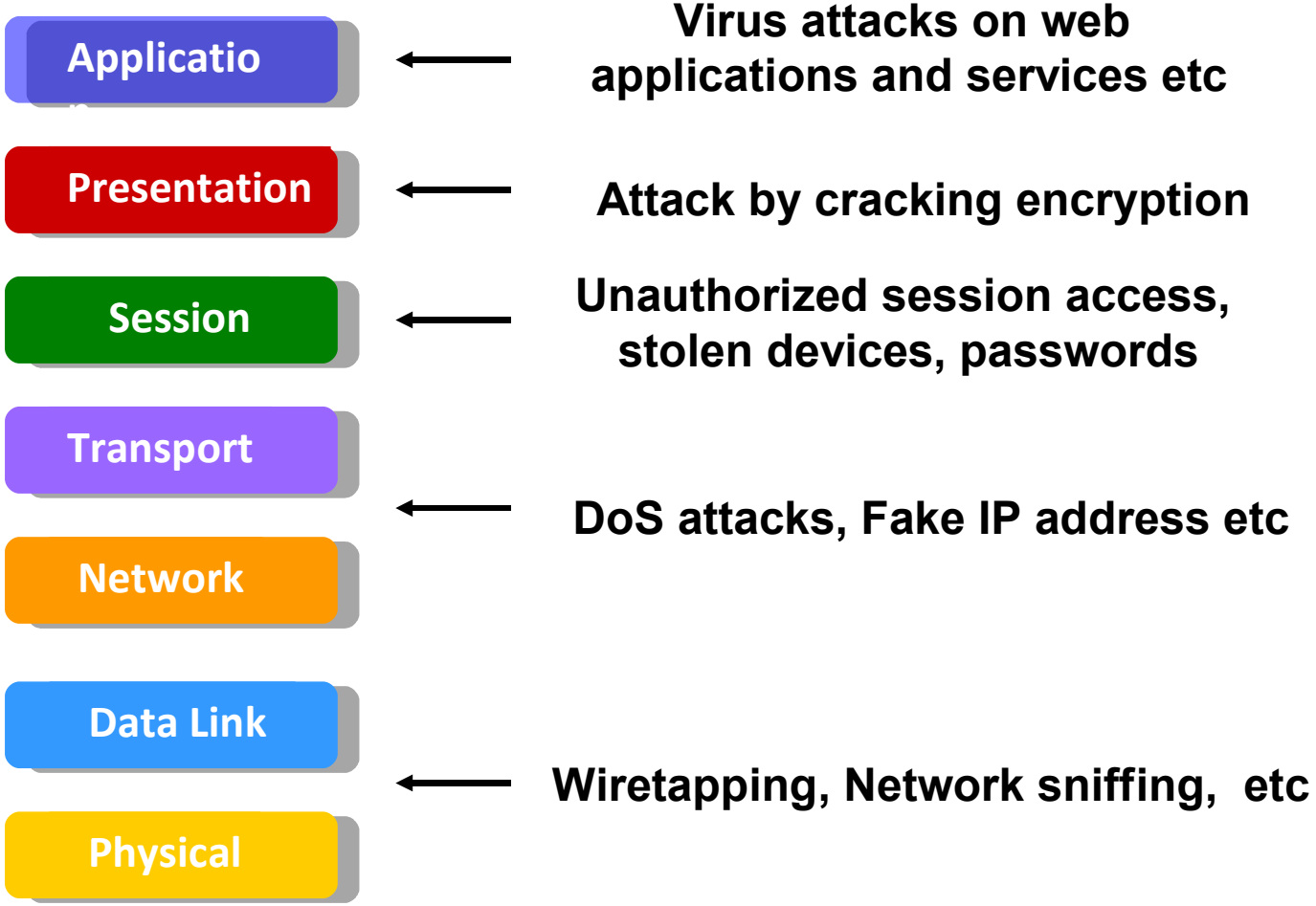
Confidentiality

Authenticity

Non Repudiation

www.infosecawareness.in

Attacks on layer wise

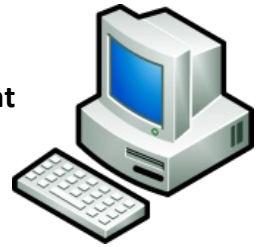


www.infosecawareness.in

Attacking Techniques

- Information Gathering
- Scanning
- Gaining Access
- Controlling Access
- Covering the Tracks

www.infosecawareness.in



Connection Establishment

Syn "I want to connect you at port 80"

Syn + Ack " Fine, I am ready for connection"

Ack "Fine"

Data Transfer

Push + Ack " Data is send from Client and the acknowledge of the same will be send from Server"

Push + Ack " Data is send from Server and the acknowledgement of the same will be send from Client"

Connection Termination

Fin " I want to close the connection"

Ack of Fin " Fine"

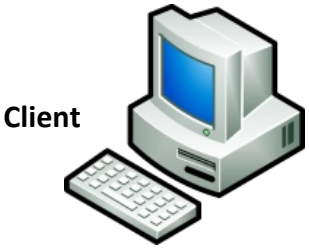
Fin " Ok I am closing the connection"

Ack of Fin "GoodBye"

In case if either side sends RST flag set, then the connection will be closed abnormally, without Fin or ack.

www.infosecawareness.in

Half open



Syn "I want to connect you at port 80"

Syn + Ack " Fine, I am ready for connection"

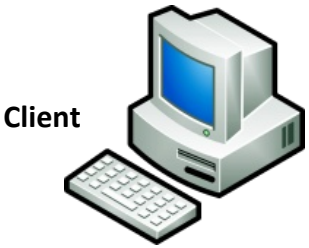
Ack "Fine"

Instead of SYN+ ACK, RST is sent by server in 2nd step – Port is closed

Instead of ACK, Client sends RST- i.e Half open

www.infosecawareness.in

XMAS/FIN



FIN/URG/PSH

No Response/RST/ACK

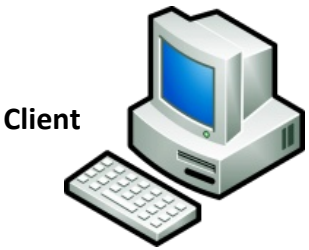
If Server responds with No Response – Port is open

If Server responds with RST/ACK – Port is closed

RFC 793

www.infosecawareness.in

Null Sacn



NO Flag Set

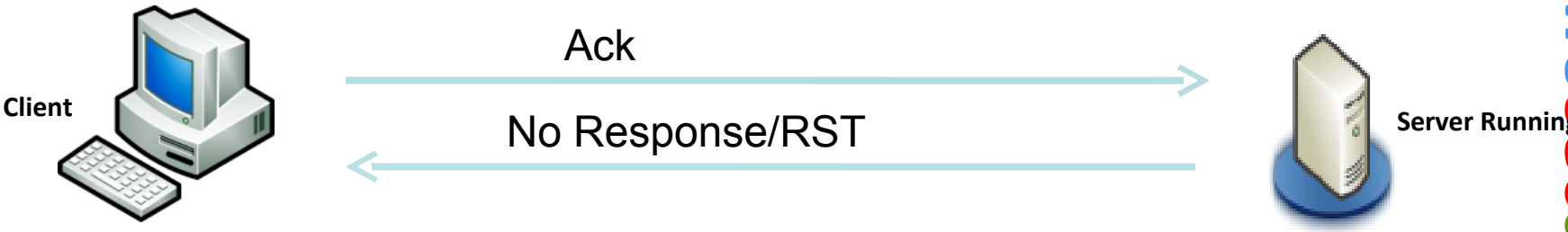
No Response/RST/ACK

If Server responds with No Response – Port is open
If Server responds with RST/ACK – Port is closed

NULL SCAN

www.infosecawareness.in

Ack Scan

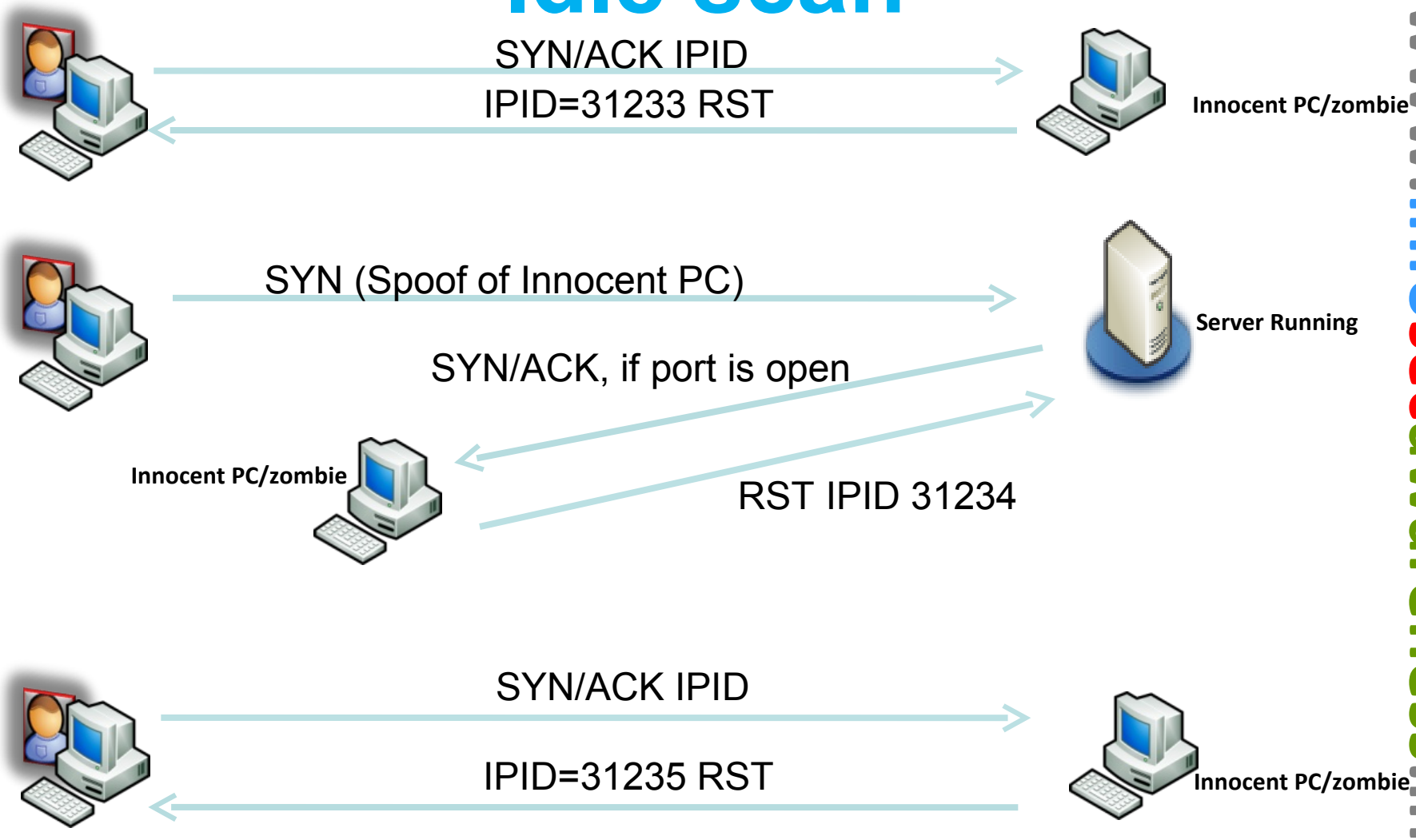


If Server responds with No Response – Port is Filtered

If Server responds with RST – Port is non filtered

www.infosecawareness.in

Idle scan



www.infosecawareness.in

Technology Implementation

- Encryption
- Firewalls
- Authentication
- Passwords

www.infosecawareness.in

Most Common Attacks

- Social Engineering
- Identity theft
- Denial of service
- Phishing

www.infosecawareness.in

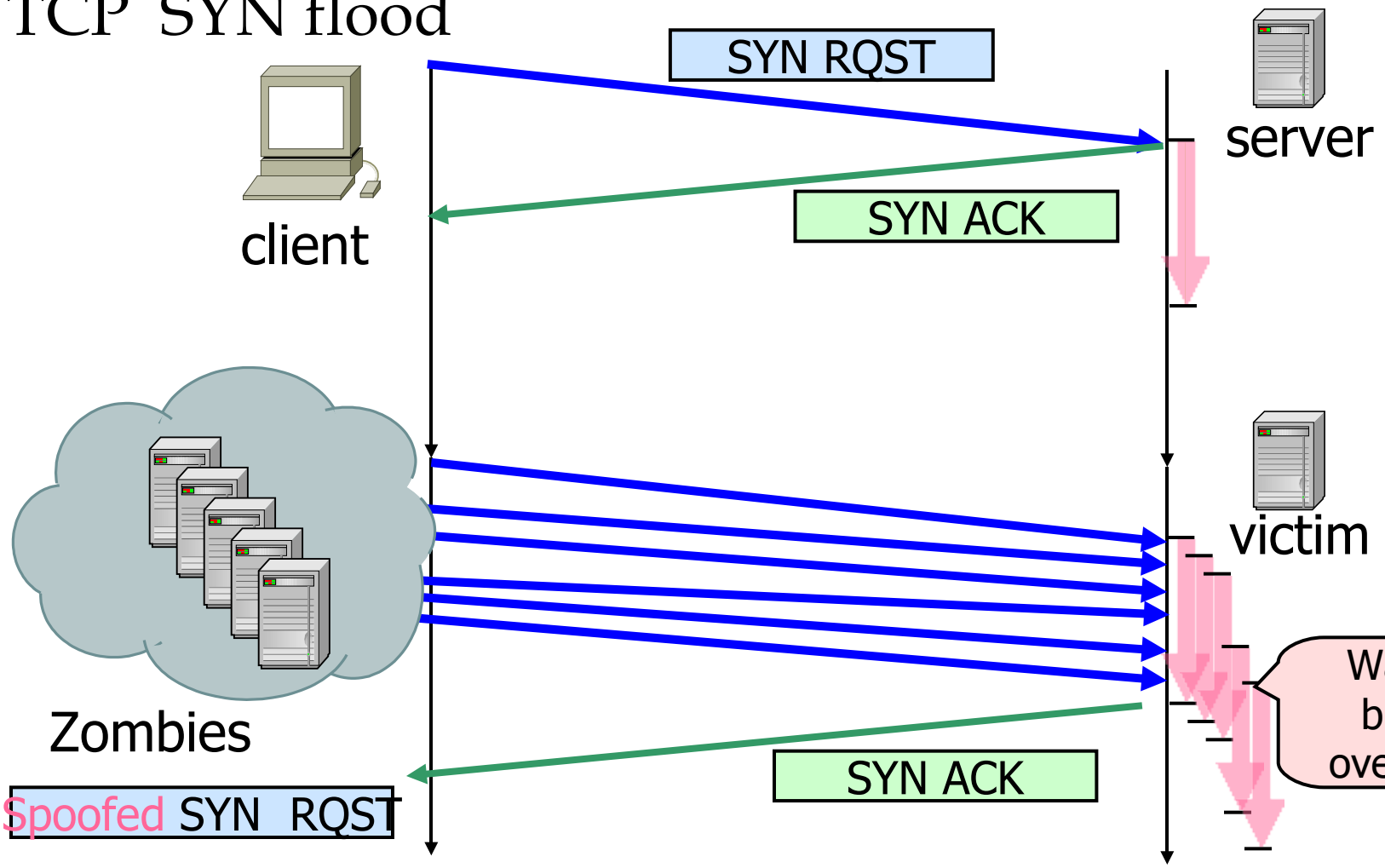
Denial of Service

- Is an attempt to make a computer unavailable to its intended users

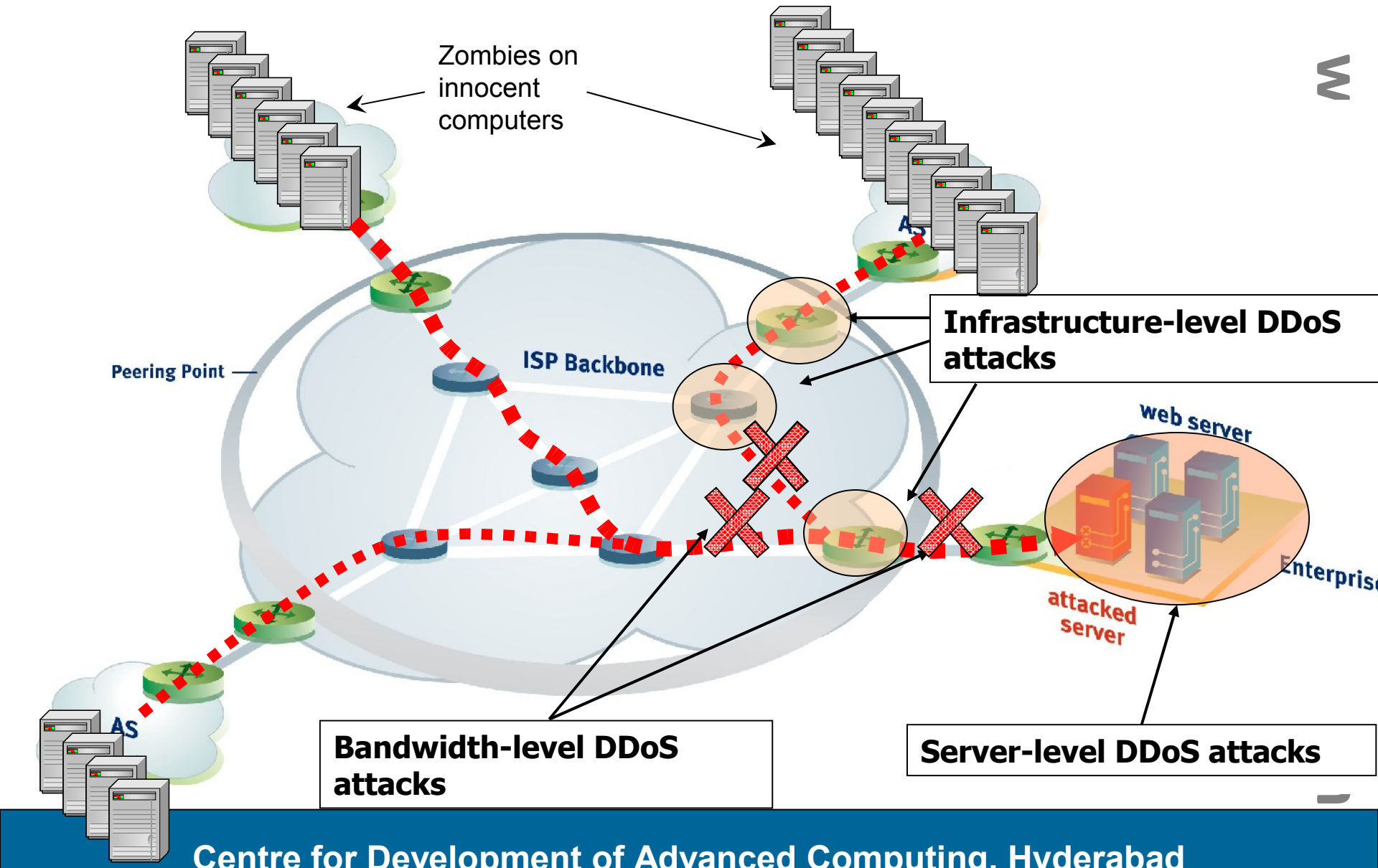
- Attackers overloads the resources by flooding the network with useless traffic

www.infosecawareness.in

TCP SYN flood



www.infosecawareness.in


Zombies on innocent computers
Peering Point
ISP Backbone
AS
AS
web server
attacked server
Infrastructure-level DDoS attacks
Bandwidth-level DDoS attacks
Server-level DDoS attacks

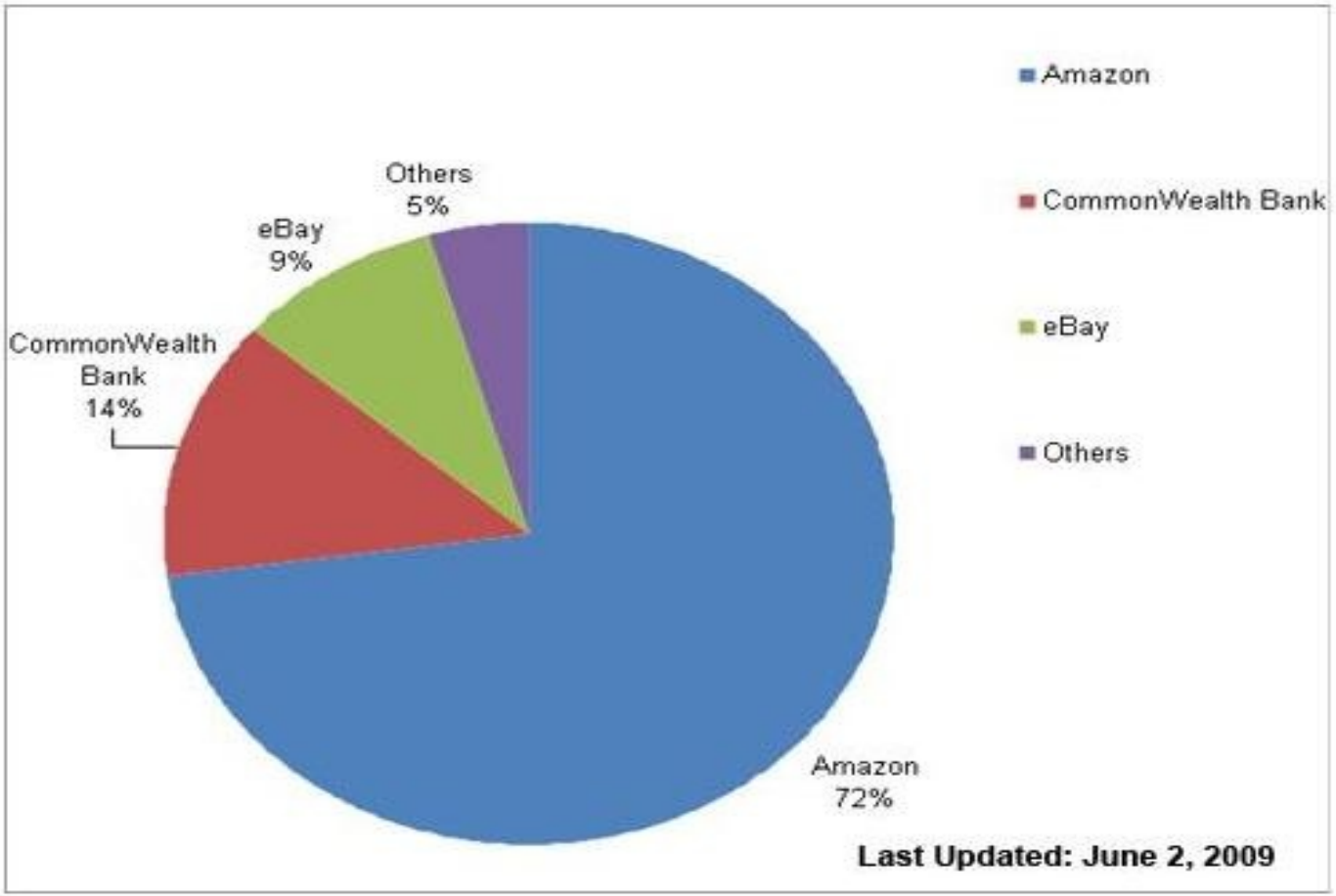
Social Engineering

- Telephone
- Dumpster Driving
- Online
- Shoulder surfing
- Reverse social engineering
- Persuasion
- Baiting
- Vishing

www.infosecawareness.in

Top Brands Exploited by Phishing Scams

The following chart shows the top brands exploited by Phishers.



www.infosecawareness.in

Beware Of Strangers On Net----tcs Gal Murder Case Story Revealed - The India Tree - The All Ind - Windows Internet Explorer
http://www.theindiatree.com/forum2/index.php?showtopic=3381
Yahoo! Search
Web Search
Bookmarks
Settings
Mail
My Yahoo!
Answers
Games
Yahoo! Anti-Spy
murder of woman orkut - Go...
Beware Of Strangers On ...
Wine Juice: The Indian Orkut...
Page
Tools

Beware Of Strangers On Net----tcs Gal Murder Case Story Revealed, A tragic love story: Flourished on Orkut, died in a bullet

Options

chetanhooli

May 25 2007, 06:45 AM

Post #1

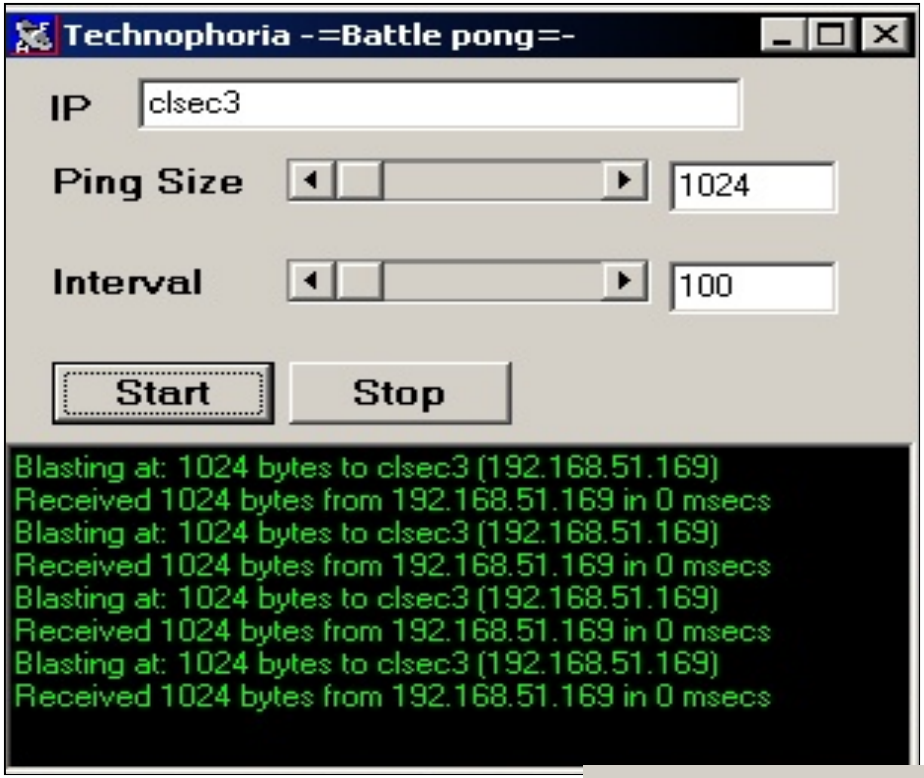
A tragic love story: Flourished on Orkut, died in a bullet

Administrator

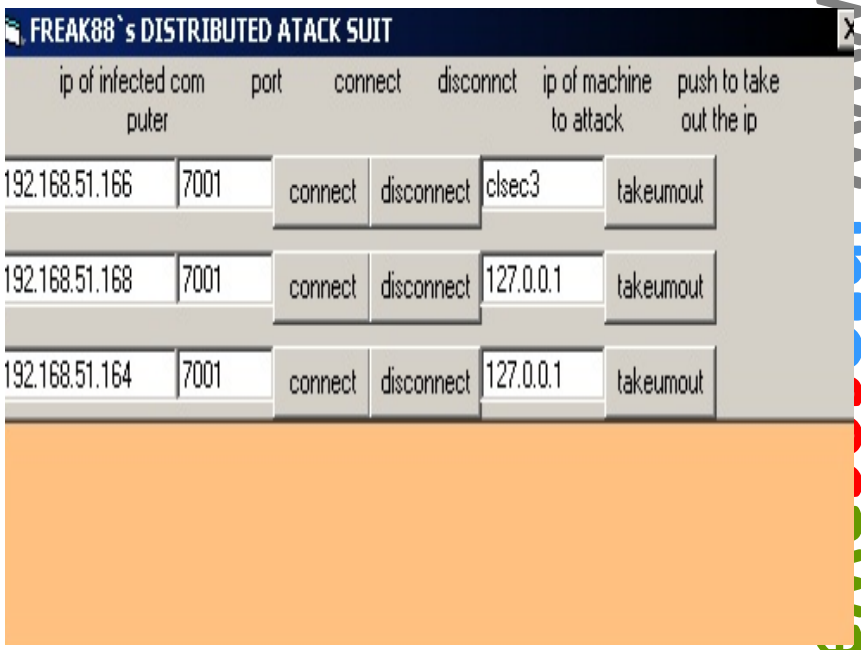
Group: Root Admin
Posts: 160
Joined: 3-May 06
From: Bangalore / Santa Clara California
Member No.: 1

(1 item remaining) Downloading picture http://www.theindiatree.com/forum2/style_images/mocha1.2/rss.png...
Unknown Zone
100%

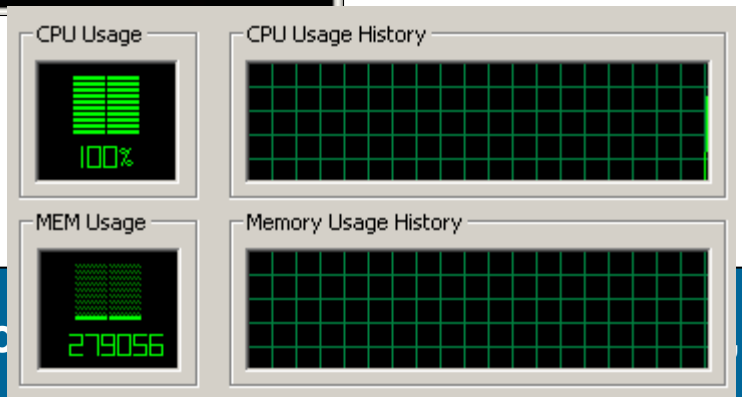
Screen Shots of DOS TOOLS



DOS Tools



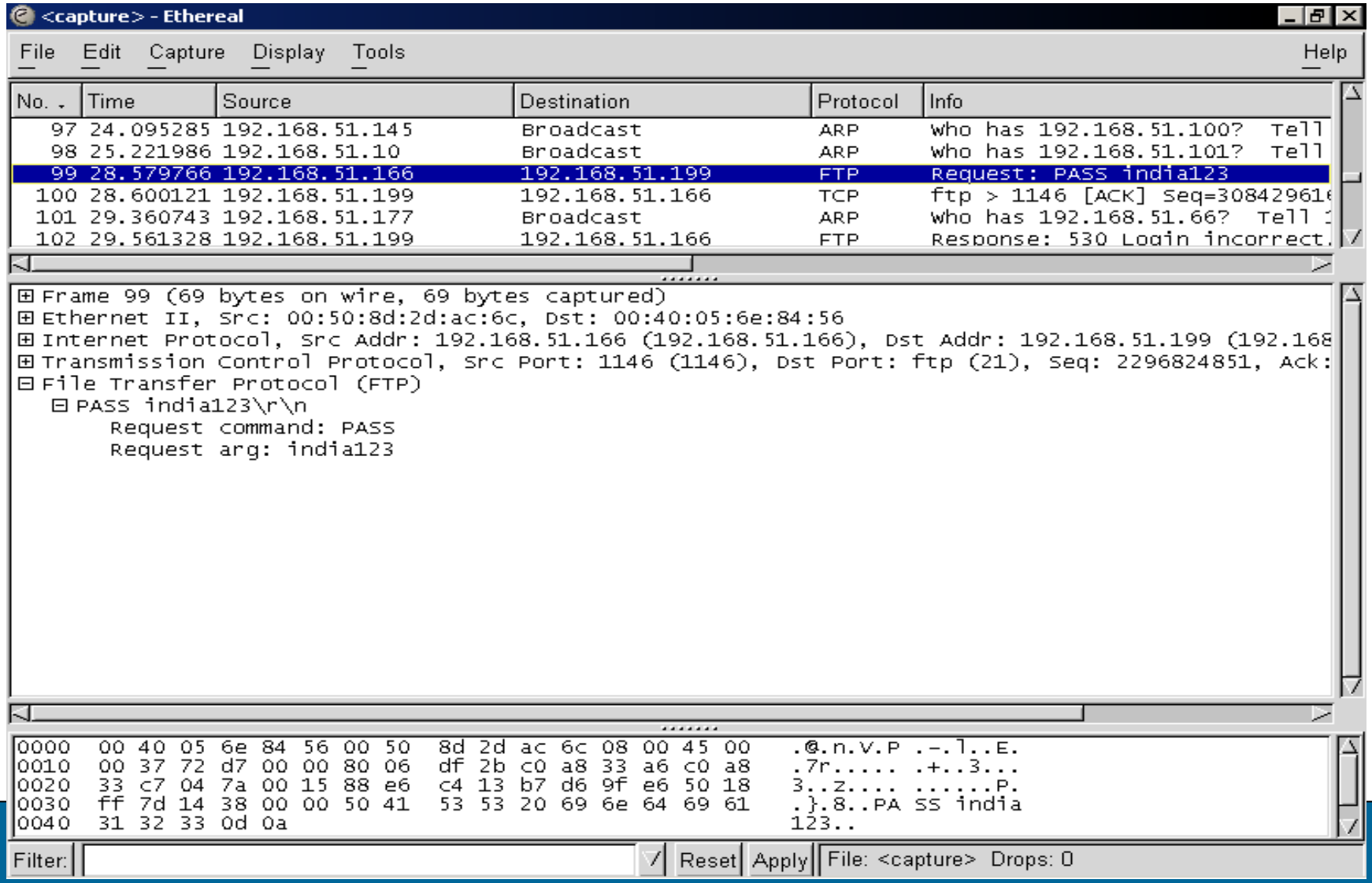
DDOS Tools



CPU Usage

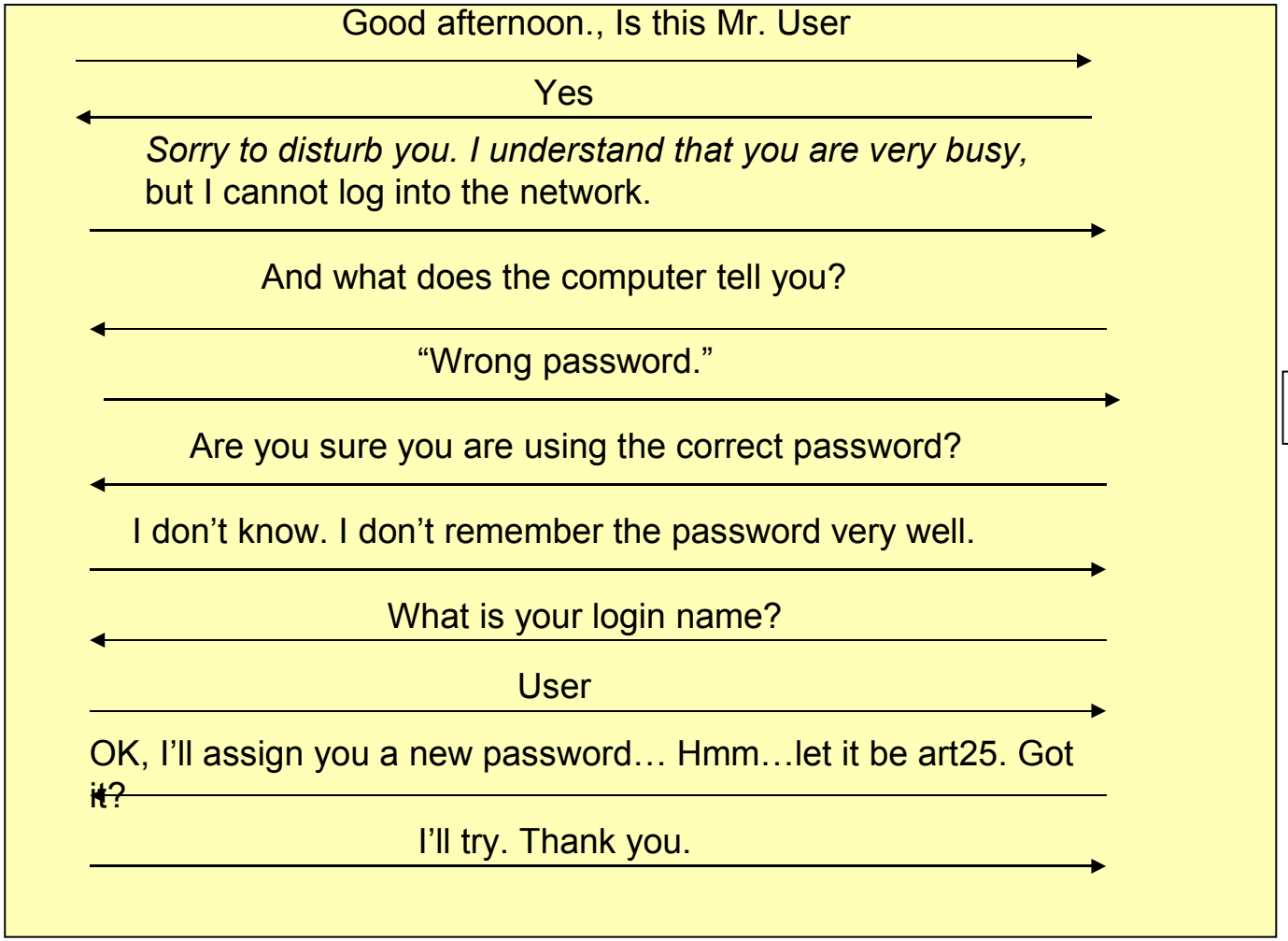
www.infosecawareness.in

Screen Shot of Password Capturing



www.infosecawareness.in

Social Engineering -Example



www.infosecawareness.in

Identity theft

- A crime where con artists get your personal information and access your cash and/or credit

www.infosecawareness.in

Hide your credit card, cyber criminals only a swipe away

Ads by Google

Replay

One million US dollar scholarship program in INDIA

Call +91 11 40574000 or email at info@innovationu.in

MAII K.K. MODI GROUP Stratford UNIVERSITY USA

Abhishek Sharan, Hindustan Times
Email Author
Noida, March 04, 2010

BUY REPRINTS Print
SHARE

First Published: 00:27 IST(4/3/2010)
Last Updated: 00:28 IST(4/3/2010)

It is a palm-sized, state-of the-art gadget and presently the subject of an alert issued to the public by the Noida police.

According to Noida police, cyber-sawy criminals are now frequently using a magnetic stripe reader and writer to fleece credit/debit card users.

It is a computer device that decodes unique identification data stored on the magnetic strip of a credit or debit card with a swipe and transfers the information to another card.

"The usage of MSRW to dupe cardholders is a new-age crime against which we have issued an alert," said Deputy Superintendent of Police R.N. Mishra.

"We have received up to a dozen complaints from local residents about the theft of their credit and debit card data. Our probe revealed this was done with the help of MSRW machines," added Mishra.

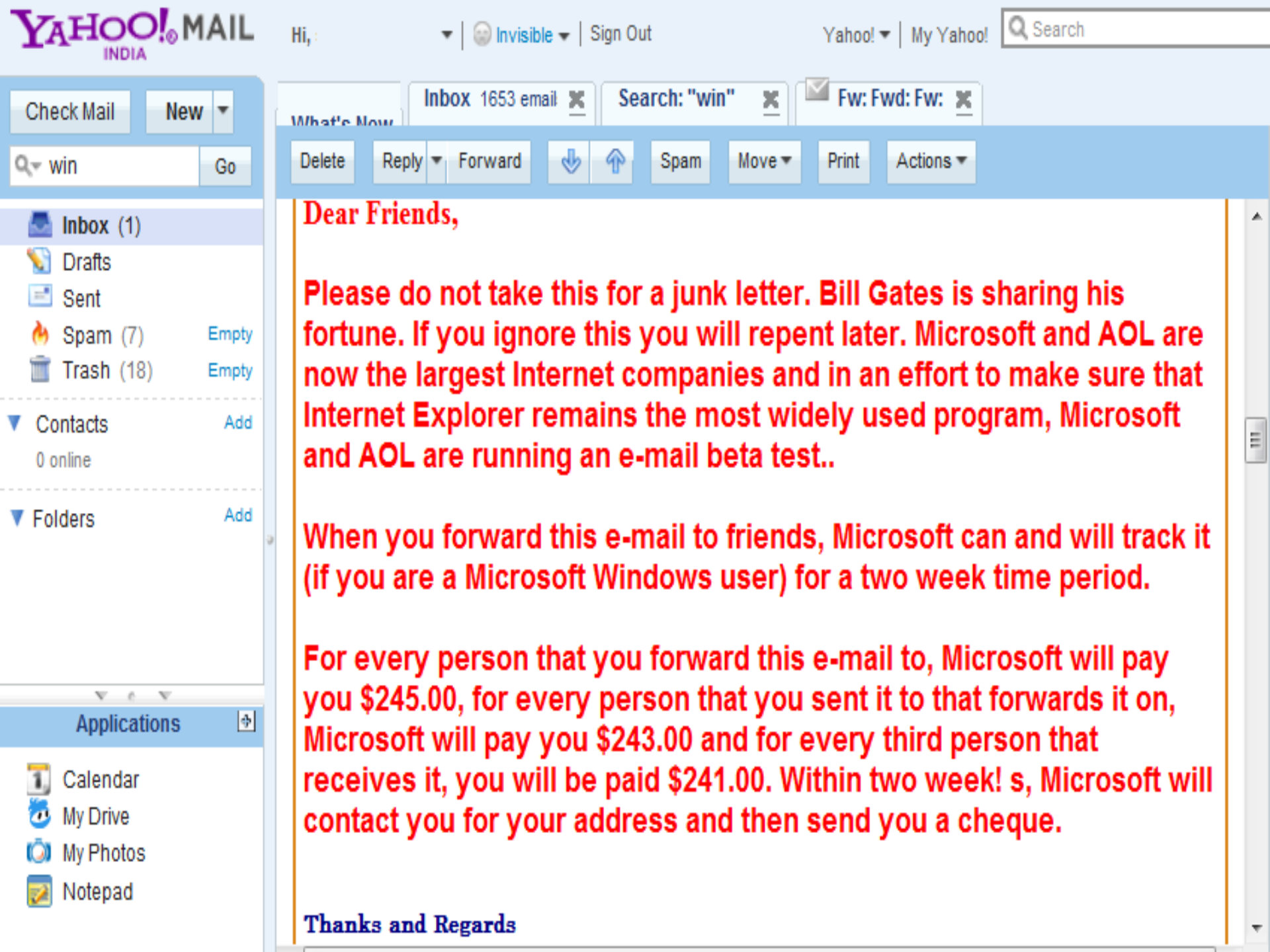
The police arrested several people for the illegal use of MSRWs to cheat cardholders.

Of them, three names — Shahnawaz Khan alias Tinku, Shabbir Khan alias Praveen and Mohammed Afaque alias Raheesh — stood out.

Hoaxes

- E-mail sent by online criminals to trick you into giving them money
  - Example
    - Email claims that Bill Gates of Microsoft is "sharing his fortune" with those who forward the email to others

www.infosecawareness.in

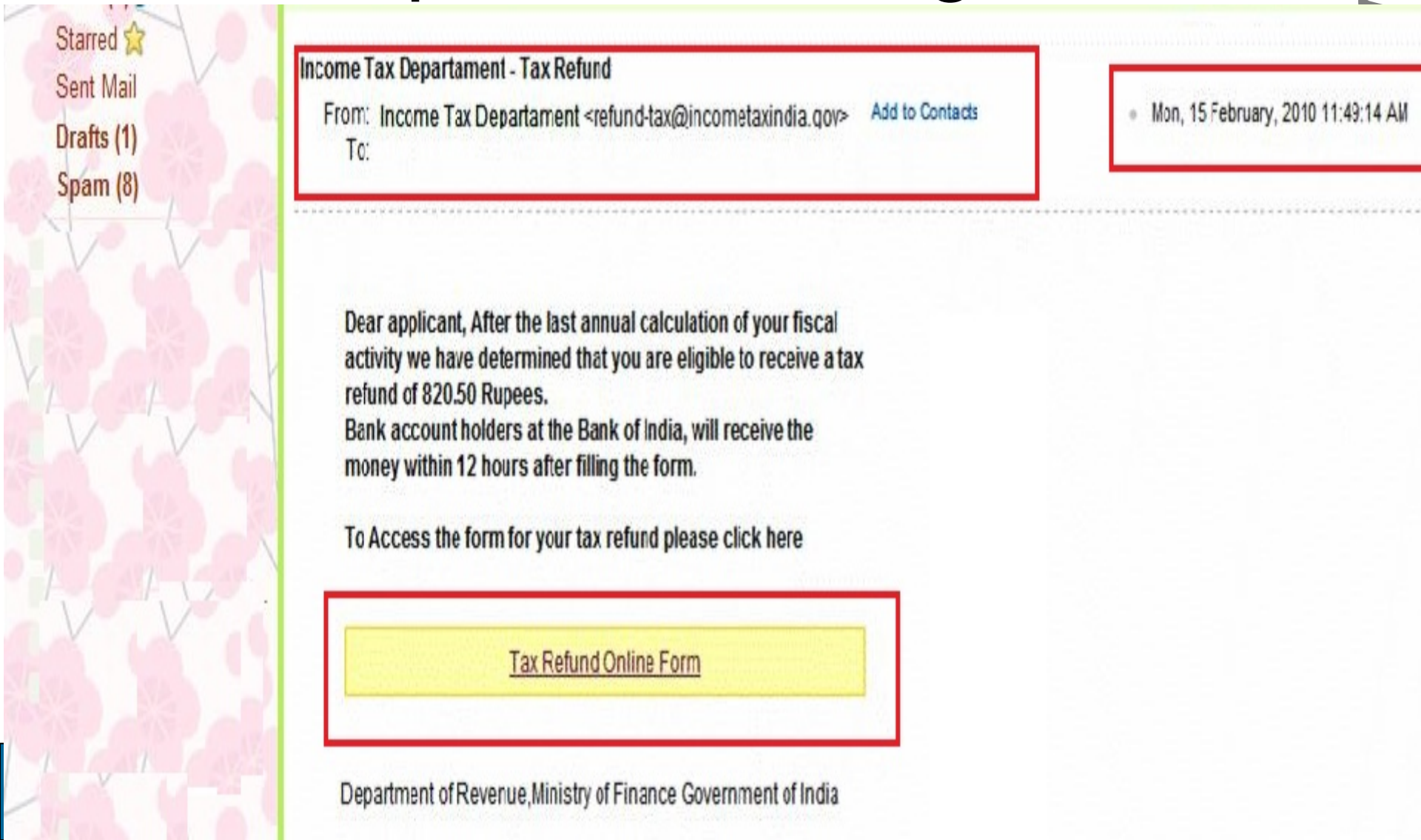

YAHOO! MAIL
INDIA
Hi,
Invisible
Sign Out
Yahoo!
My Yahoo!
Search
Check Mail
New
win
Go
Inbox (1)
Drafts
Sent
Spam (7)
Empty
Trash (18)
Empty
Contacts
Add
0 online
Folders
Add
Applications
Calendar
My Drive
My Photos
Notepad
What's Now
Inbox 1653 email
Search: "win"
Fw: Fwd: Fw:
Delete
Reply
Forward
Spam
Move
Print
Actions
Dear Friends,
Please do not take this for a junk letter. Bill Gates is sharing his fortune. If you ignore this you will repent later. Microsoft and AOL are now the largest Internet companies and in an effort to make sure that Internet Explorer remains the most widely used program, Microsoft and AOL are running an e-mail beta test..
When you forward this e-mail to friends, Microsoft can and will track it (if you are a Microsoft Windows user) for a two week time period.
For every person that you forward this e-mail to, Microsoft will pay you $245.00, for every person that you sent it to that forwards it on, Microsoft will pay you $243.00 and for every third person that receives it, you will be paid $241.00. Within two week! s, Microsoft will contact you for your address and then send you a cheque.
Thanks and Regards

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.

www.infosecawareness.in

Example of Phishing e-Mail



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

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

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

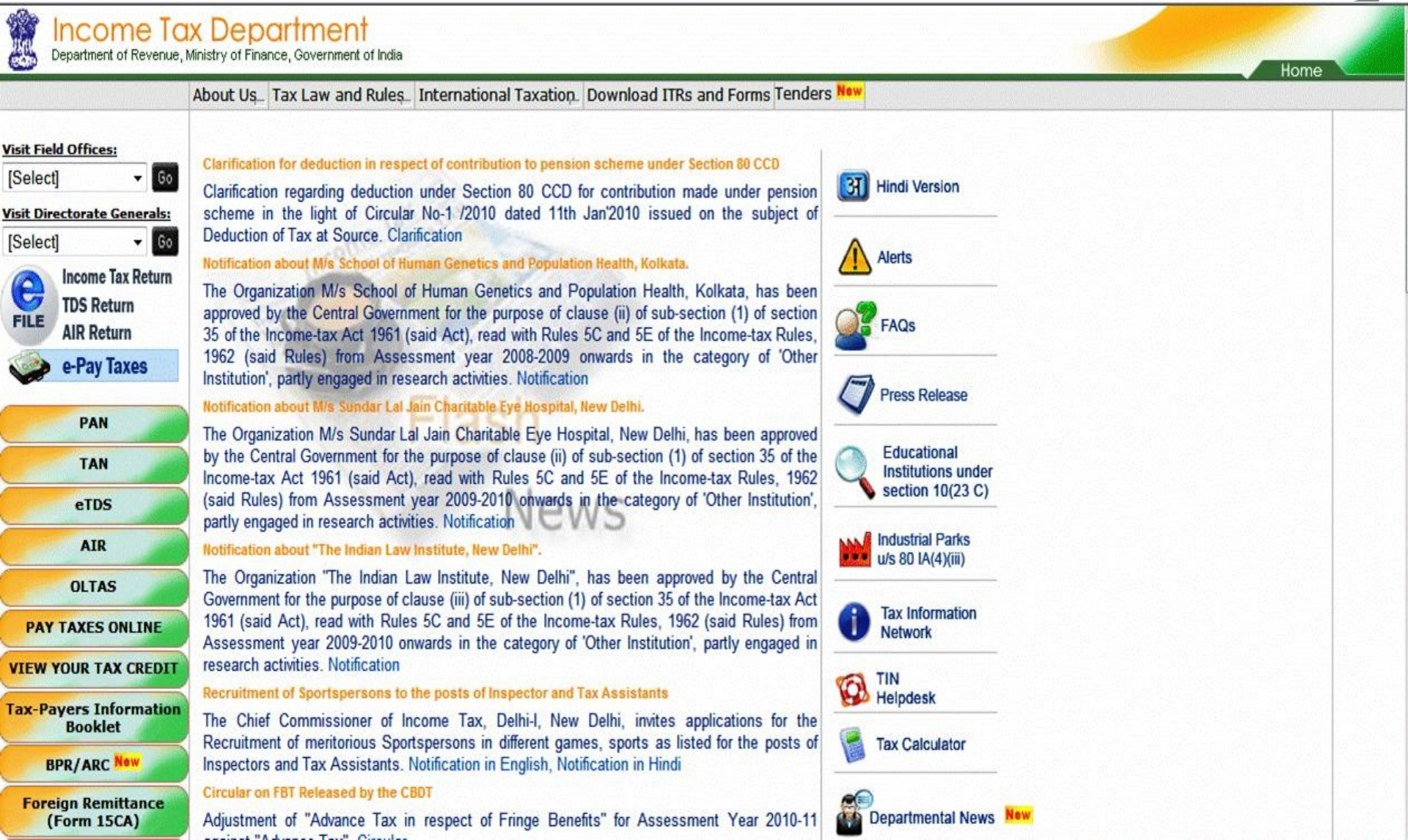
Please enter your information where the refund will be made.

*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:	

Submit

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



Income Tax Department
Department of Revenue, Ministry of Finance, Government of India

Home

About Us | Tax Law and Rules | International Taxation | Download ITRs and Forms | Tenders New

Visit Field Offices:
[Select] Go

Visit Directorate Generals:
[Select] Go

e-FILE
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?

www.infosecawareness.in

Hackers launch phishing attack on Facebook users

Thu May 14, 2009 6:50pm EDT

Email | Print | Share | Reprints | Single Page [-] Text [+]

By Jim Finkle

BOSTON (Reuters) - Hackers launched an attack on Facebook's 200 million users on Thursday, successfully gathering passwords from some of them in the latest campaign to prey on members of the popular social networking site.

Facebook spokesman Barry Schnitt said on Thursday that the site was in the process of cleaning up damage from the attack.

He said that Facebook was blocking compromised accounts.

Schnitt declined to say how many accounts had been compromised.

The hackers got passwords through what is known as a phishing attack, breaking into accounts of some Facebook members, then sending e-mails to friends and urging them to click on links to fake websites.

Those sites were designed to look like the Facebook home page. The victims were directed to log back in to the site, but actually logged into the one controlled by the hackers, unwittingly giving away their passwords.

The purpose of such attacks is generally identify theft and to spread spam.

The fake domains include www.151.im, www.121.im and www.123.im. Facebook has deleted all references to those domains.

Schnitt said that Facebook's security team believes the hackers intended to collect a large number of credentials, then use those accounts at a later time to send spam hawking fake pharmaceuticals and other goods to Facebook members.

The site fought off a similar attack two weeks ago, he said.

e-Mails contains Malware

- Attackers sends e-mail with an attachment and asks to click on the clink or download the attached file.
- Those attached file may contain may contain malicious software like
  - Trojan
  - Virus
  - Spyware
  - Key loggers

www.infosecawareness.in

October 27, 2009 10:48 AM PDT

Fake Facebook e-mail contains Trojan

by Don Reisinger

A A Font size Print E-mail Share 36 comments

391 diggs

digg it

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**.

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."

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)

www.infosecawareness.in

Updatetool.exe

- By running this tool Trojan will install in PC

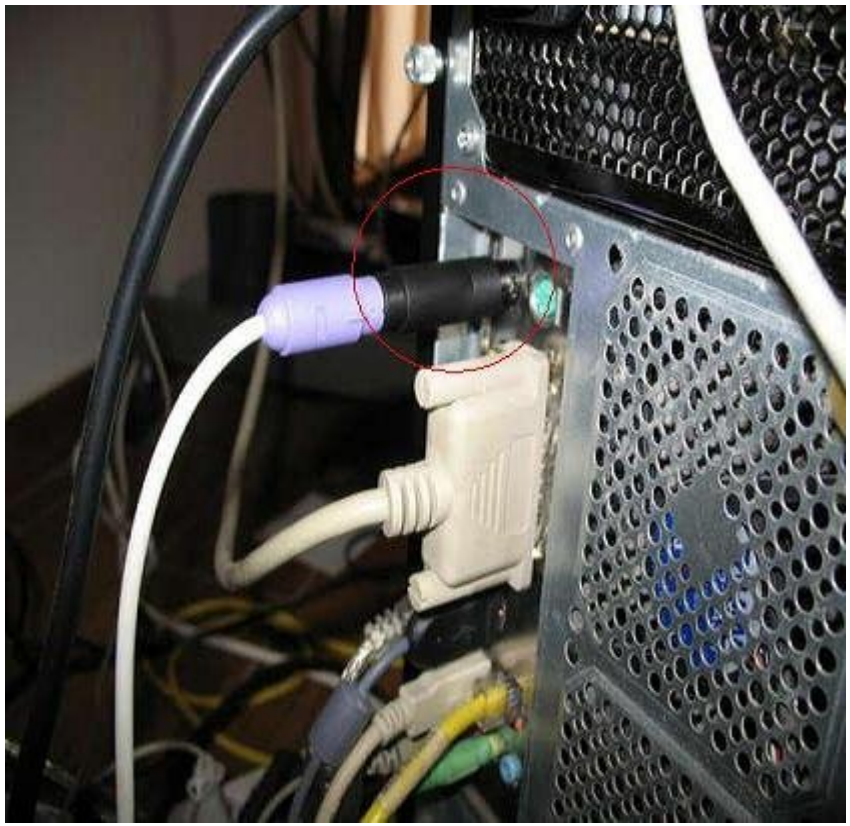
This is the prompt Facebook users get as part of the latest phishing scam. Downloading the "update tool" installs a Trojan.

(Credit: AppRiver)

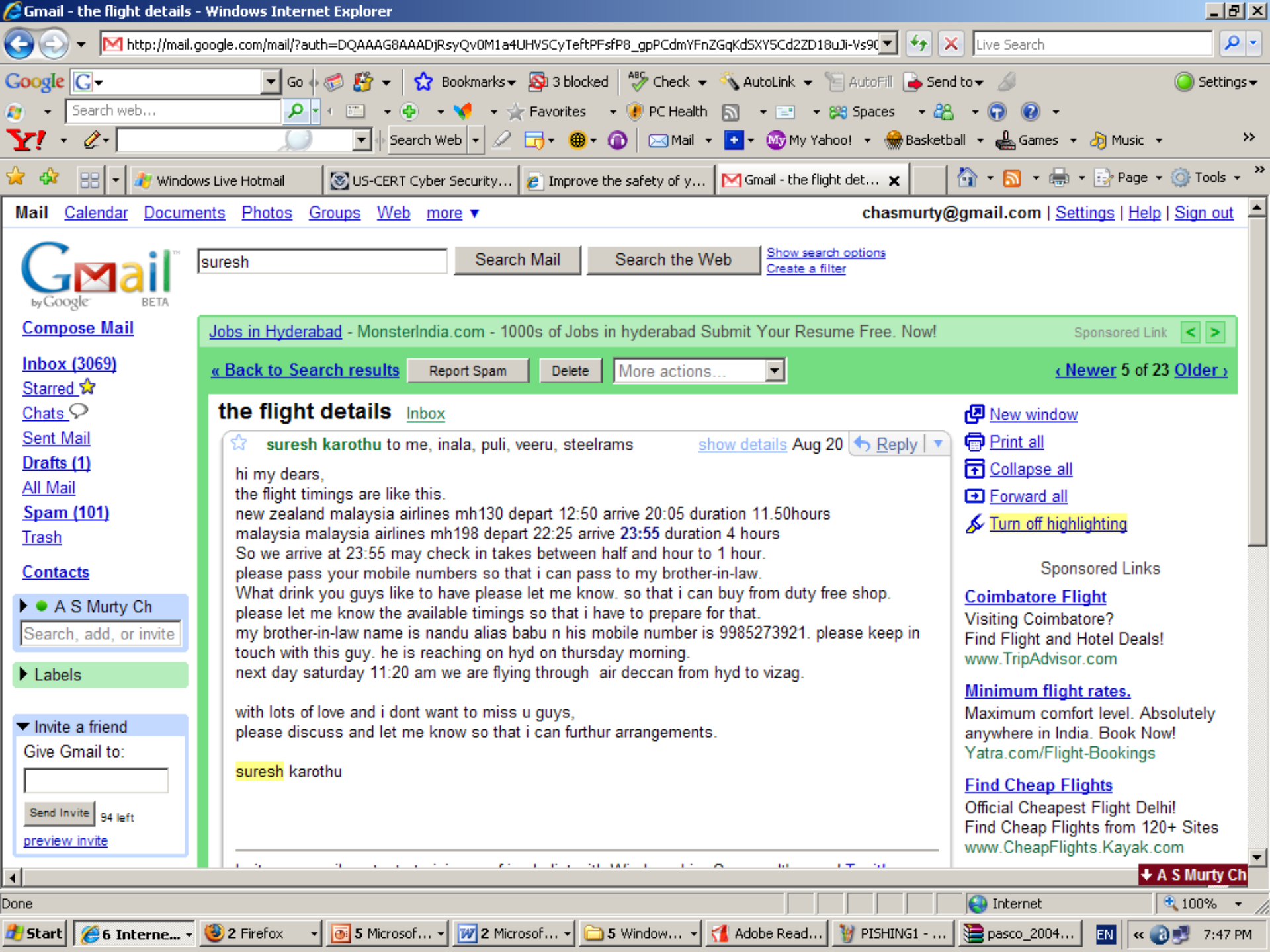
www.infosecawareness.in

Hardware Keylogger

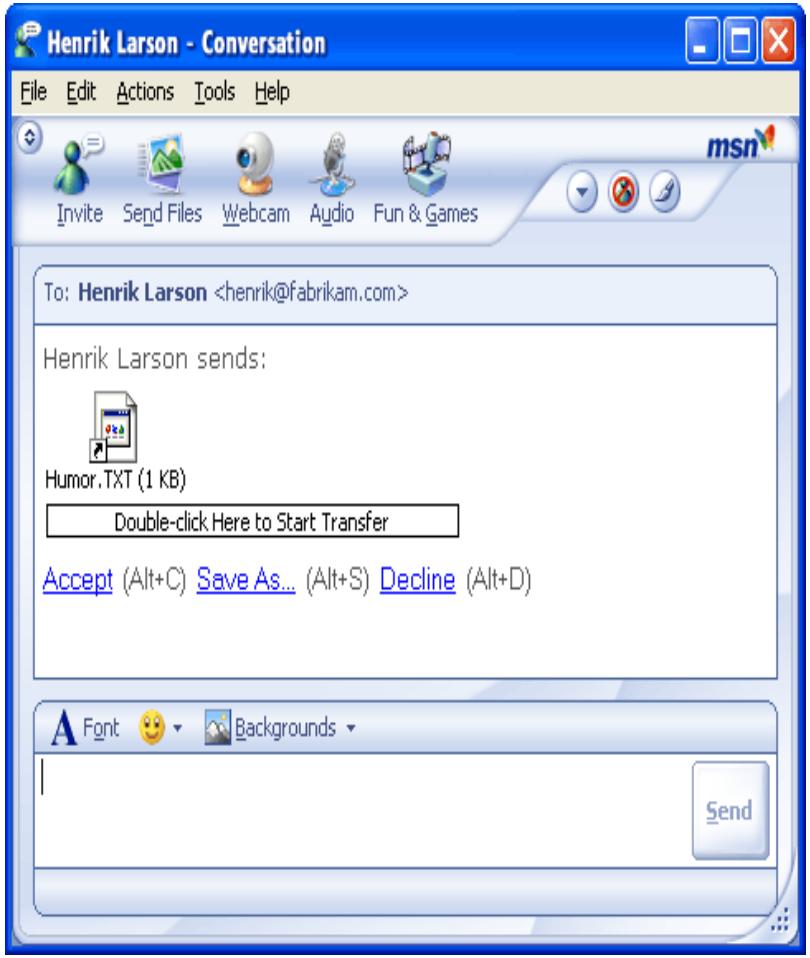
- Hardware keylogger attached to CPU

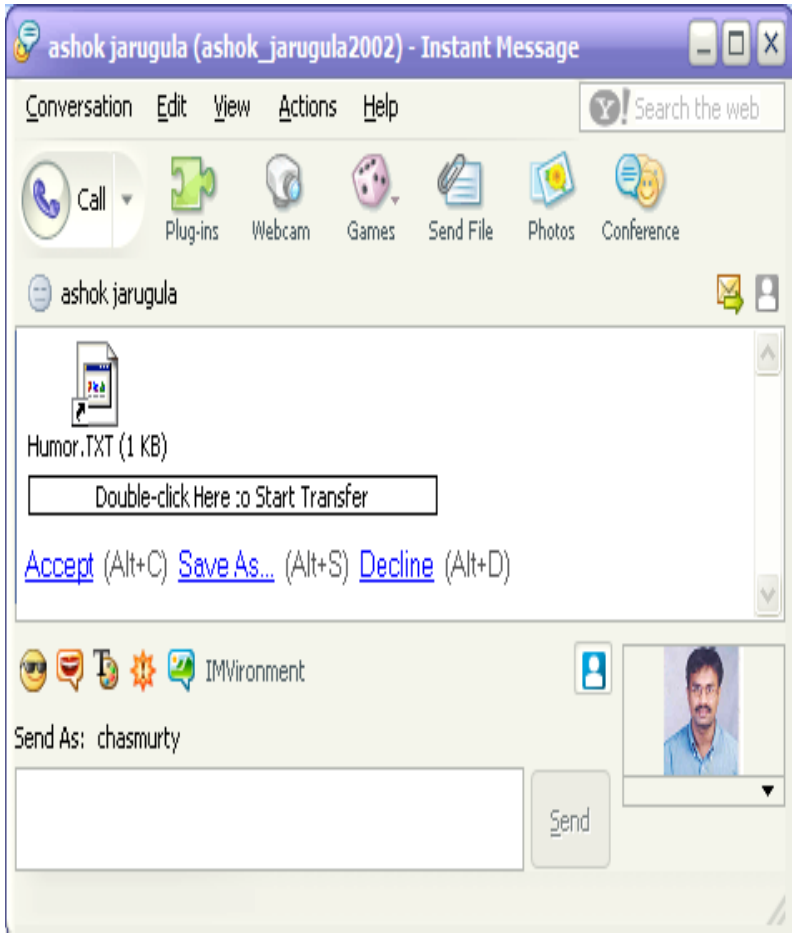


www.infosecawareness.in


Gmail - the flight details - Windows Internet Explorer
http://mail.google.com/mail/?auth=DQAAAG8AAADjRsyQv0M1a4UHVSCyTeftPFsfP8_gpPCdmYFnZGqKdSXY5Cd2ZD18uJi-Vs9C
Live Search
Windows Live Hotmail
US-CERT Cyber Security...
Improve the safety of y...
Gmail - the flight det...
Mail Calendar Documents Photos Groups Web more ▼
chasmurty@gmail.com | Settings | Help | Sign out
suresh
Search Mail
Search the Web
Show search options
Create a filter
Compose Mail
Inbox (3069)
Starred
Chats
Sent Mail
Drafts (1)
All Mail
Spam (101)
Trash
Contacts
A S Murty Ch
Search, add, or invite
Labels
Invite a friend
Give Gmail to:
Send Invite
94 left
preview invite
Jobs in Hyderabad - MonsterIndia.com - 1000s of Jobs in hyderabad Submit Your Resume Free. Now!
Sponsored Link
« Back to Search results
Report Spam
Delete
More actions...
‹ Newer 5 of 23 Older ›
the flight details
Inbox
suresh karothu to me, inala, puli, veeru, steelrams
show details Aug 20
Reply
hi my dears,
the flight timings are like this.
new zealand malaysia airlines mh130 depart 12:50 arrive 20:05 duration 11.50hours
malaysia malaysia airlines mh198 depart 22:25 arrive 23:55 duration 4 hours
So we arrive at 23:55 may check in takes between half and hour to 1 hour.
please pass your mobile numbers so that i can pass to my brother-in-law.
What drink you guys like to have please let me know. so that i can buy from duty free shop.
please let me know the available timings so that i have to prepare for that.
my brother-in-law name is nandu alias babu n his mobile number is 9985273921. please keep in touch with this guy. he is reaching on hyd on thursday morning.
next day saturday 11:20 am we are flying through air deccan from hyd to vizag.
with lots of love and i dont want to miss u guys,
please discuss and let me know so that i can furthur arrangements.
suresh karothu
New window
Print all
Collapse all
Forward all
Turn off highlighting
Sponsored Links
Coimbatore Flight
Visiting Coimbatore?
Find Flight and Hotel Deals!
www.TripAdvisor.com
Minimum flight rates.
Maximum comfort level. Absolutely anywhere in India. Book Now!
Yatra.com/Flight-Bookings
Find Cheap Flights
Official Cheapest Flight Delhi!
Find Cheap Flights from 120+ Sites
www.CheapFlights.Kayak.com
A S Murty Ch
Done
Internet
100%
Start
6 Interne...
2 Firefox
5 Microsof...
2 Microsof...
5 Window...
Adobe Read...
PISHING1 - ...
pasco_2004...
EN
7:47 PM

Looks like....





www.infosecawareness.in

5 steps to help avoid instant message viruses

- **Be careful downloading files in IM**
- **Update your software** patches
- **Make sure you're using an updated version of your IM software**
- **Use antivirus software and keep it updated**
- **Use antispyware software and keep it updated**

www.infosecawareness.in

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 passwor
- Erase your tracks
- Don't enter sensitive information into a public computer
- Force Cyber Cafe Owner to allocate you a computer loaded with updated antivirus software

www.infosecawareness.in

InSecurity Complex
By Elinor Mills

```
Starting Nmap 4.76 ( http:
Initiating Ping Scan at 16
Scanning 192.169.1.1 [2 po
Completed Ping Scan at 16:
Read data files from: /usr
```

August 6, 2009 4:32 PM PDT

Twitter, Facebook attack targeted one user

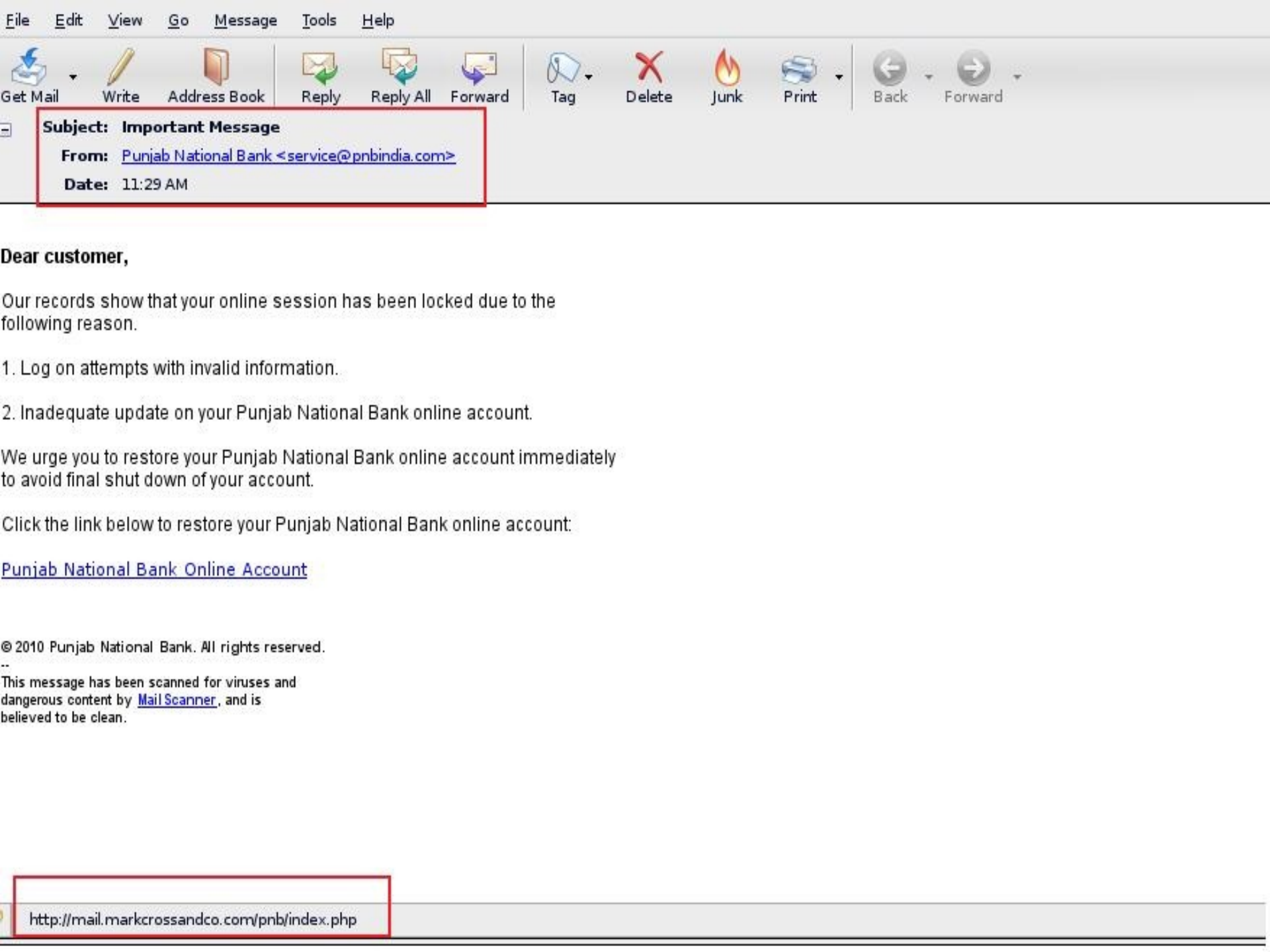
by Elinor Mills

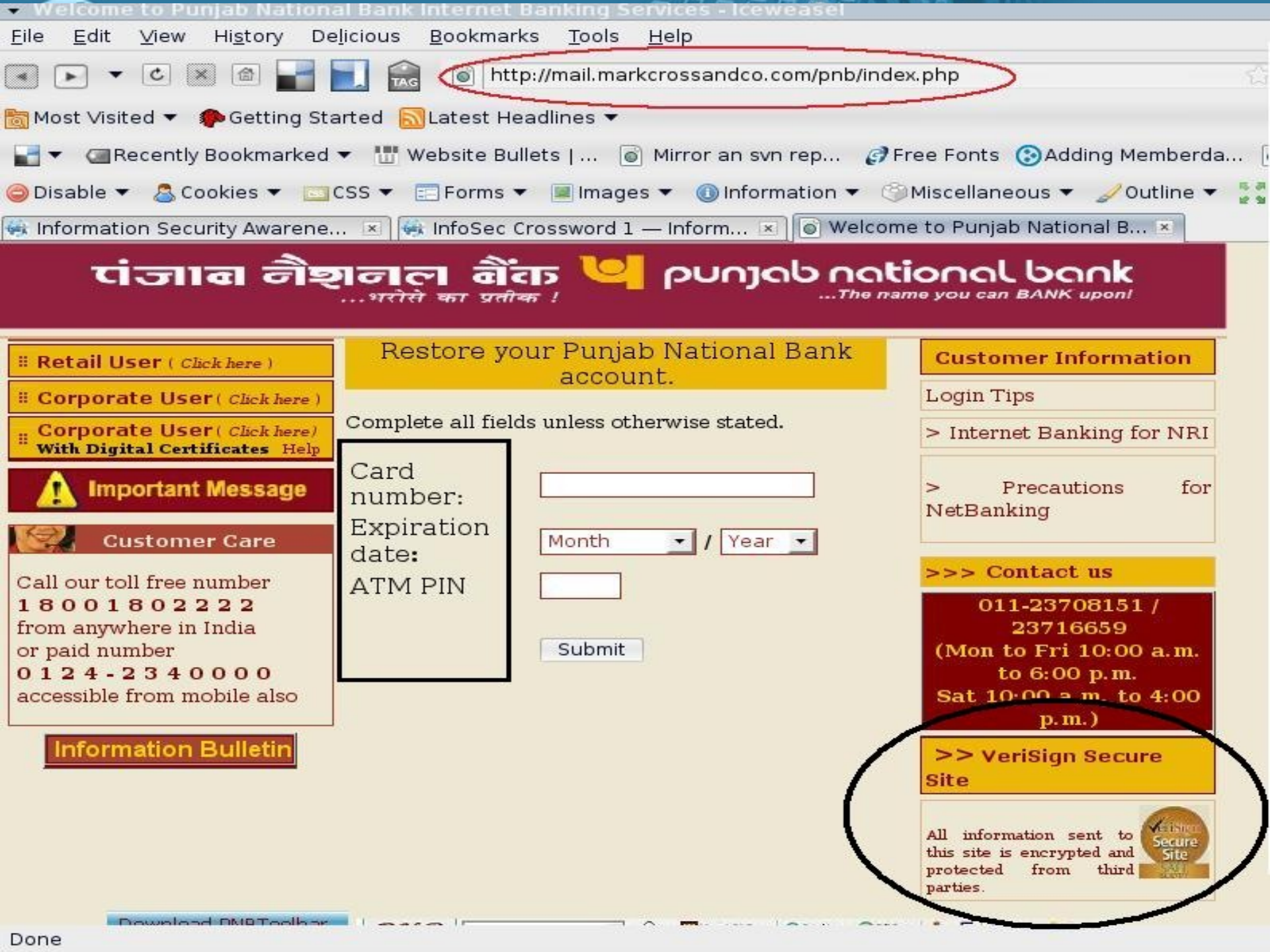
A Georgian blogger with accounts on Twitter, Facebook, LiveJournal, and Google's Blogger and YouTube was targeted in a denial-of-service attack that led to the sitewide outage at Twitter and problems at the other sites on Thursday, according to a Facebook executive.

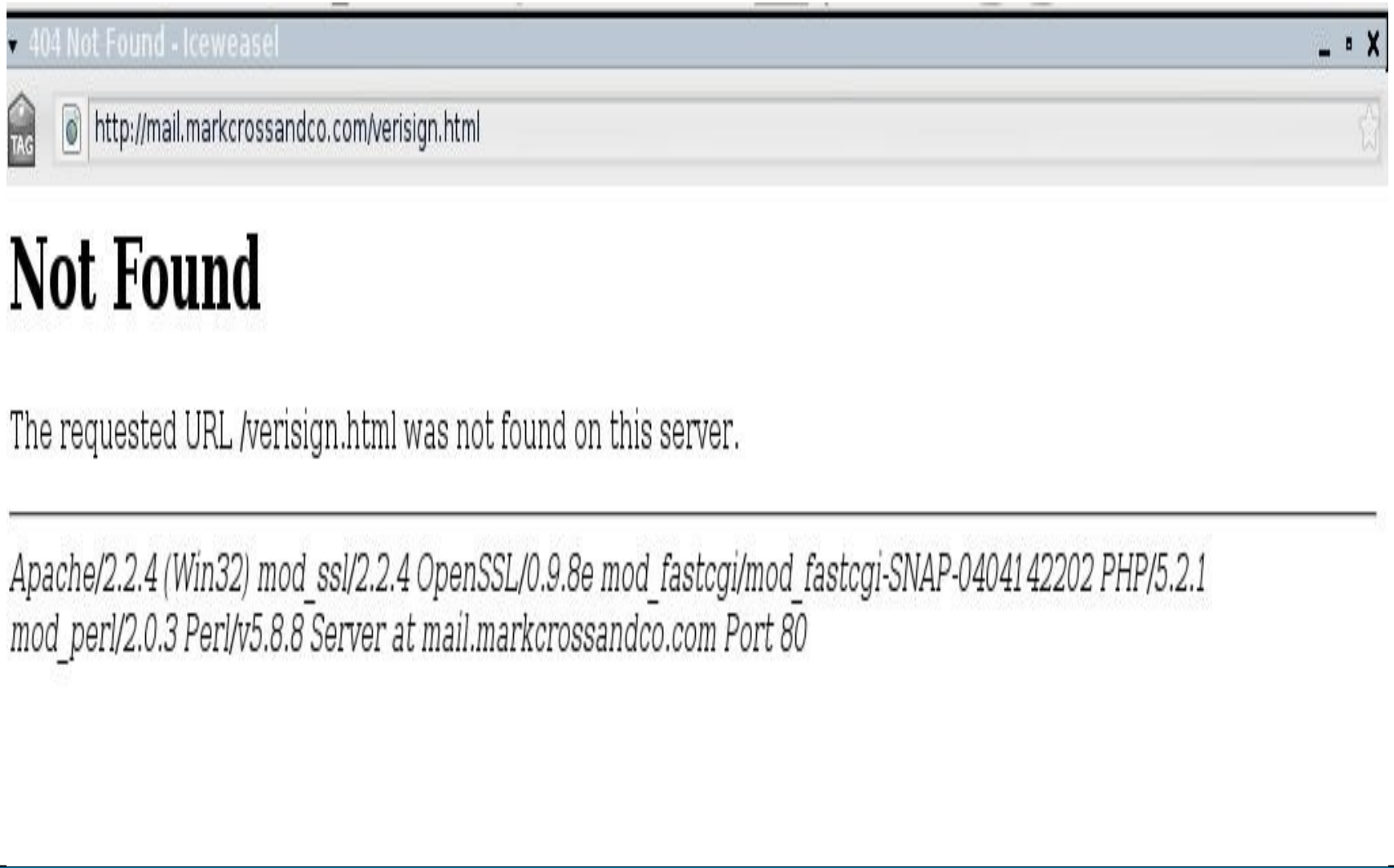
970 diggs
digg it

The blogger, who uses the account name "Cyxymu," (the name of a town in the Republic of Georgia) had accounts on all of the different sites that were attacked at the same time, Max Kelly, chief security officer at Facebook, told CNET News.

"It was a simultaneous attack across a number of properties targeting him to keep his voice from being heard," Kelly said. "We're actively investigating the source of the attacks, and we hope to be able to find out the individuals involved in the back end and to take action against them, if we can."


File Edit View Go Message Tools Help
Get Mail Write Address Book Reply Reply All Forward Tag Delete Junk Print Back Forward
Subject: Important Message
From: Punjab National Bank <service@pnbindia.com>
Date: 11:29 AM
Dear customer,
Our records show that your online session has been locked due to the following reason.
1. Log on attempts with invalid information.
2. Inadequate update on your Punjab National Bank online account.
We urge you to restore your Punjab National Bank online account immediately to avoid final shut down of your account.
Click the link below to restore your Punjab National Bank online account:
Punjab National Bank Online Account
© 2010 Punjab National Bank. All rights reserved.
--
This message has been scanned for viruses and dangerous content by Mail Scanner, and is believed to be clean.
http://mail.markcrossandco.com/pnb/index.php


Welcome to Punjab National Bank Internet Banking Services - Iceweasel
File Edit View History Delicious Bookmarks Tools Help
http://mail.markcrossandco.com/pnb/index.php
Most Visited Getting Started Latest Headlines
Recently Bookmarked Website Bullets | ... Mirror an svn rep... Free Fonts Adding Memberda...
Disable Cookies CSS Forms Images Information Miscellaneous Outline
Information Security Awarene... InfoSec Crossword 1 — Inform... Welcome to Punjab National B...
पंजाब नैशनल बैंक ...भरोसे का प्रतीक !
punjab national bank ...The name you can BANK upon!
Retail User (Click here)
Corporate User (Click here)
Corporate User (Click here) With Digital Certificates Help
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
Restore your Punjab National Bank account.
Complete all fields unless otherwise stated.
Card number:
Expiration date:
ATM PIN
Month / Year
Submit
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.
VeriSign Secure Site
Done



www.infosecawareness.in

Spoofed e-Mail

Folders: caughtspam Go

Refresh • New Message • Empty Trash • Folder Management • Vacation Message • Spa

Disk Space Used: 108.2 MB

[1 - 25 of 59

Status	Date (▼)	From	Subject	Si
	12/08/09 22:30	AMERICAN ONLINE LOTTERY	AMERICAN ONLINE LOTTERY!! (YOU HAVE WON USD1,300,000,00)	6
	12/08/09 16:18	plholidays	[illegible]	28
	12/07/09 22:52	DR SANUSI LAMIDO	Fund Transfer Notification usd$7.2million	21
	12/07/09 00:49	info@whitesmokemail.com	{Disarmed} Cyber Monday Re-Run! 24 Hours Only	10
	12/05/09 15:27	info@whitesmokemail.com	{Disarmed} Can Cyber Monday be Beat? Check Inside...	29
	12/04/09 16:00	Suresh Ramasubramanian	{Disarmed} [India-InfoSec] Nigerian trying to catch sbi gold accounts	27
	12/04/09 11:33	Prasanthi Kothamasu	FW: WHY RATAN TATA IS RESPECTED THE MOST?	41
	12/04/09 01:30	info@whitesmokemail.com	{Disarmed} Can Cyber Monday be Beat?	24
	12/03/09 01:11	info@whitesmokemail.com	{Disarmed} Unbeatable Price Via Our Live Chat / Call Center	22
	12/01/09 17:49	Royal Bank of Scotland Group PLC	Account Notice!!!	8
	11/30/09 23:45	Parth Mahar	{Disarmed} RE: [India-InfoSec] Virus attack in many rooms at a time, says IIM B director	35
	11/30/09 22:21	Sunbelt Software	{Disarmed} Upcoming Webinars from Sunbelt Software	11
	11/28/09 18:03	coca cola	YOU HAVE WON!!!	218
	11/27/09 21:29	MINISTRY OF FINANCE	[SPF:fail] OUTSTANDING PAYMENT APPROVED	6
	11/13/09 19:03	srivalli j.	RE: Offer from R G B C - Kerala	17
	11/12/09 14:05	Prasanthi Kothamasu	FW: BEAUTY OF KONKAN	5

www.infosecawareness.in

After Opening mails

Euro Million [sicclaimdept@luckymail.com]

Extra line breaks in this message were removed.

Sent: Thu 29-10-2009 16:04
To: undisclosed-recipients:

Attn Web/Internet user!!!

This is to notify you that your email address was entered during the annual Euro Milliones Lottery selection Draw and have won the sum of 470,000 euros.

Contact below claim officer on e-mail for immediate process of your claim; Remember to quote these numbers below for verification by the company.

REF: ESP/WIN/008/02/10/MA
BATCH: EURO/1007/444/606/09

You should include Your Name, Address, Age, Occupation, Nationality and Phone numbers.

Mr. ANTONIO GUZMAN (Claim Officer)
E-mail: sicclaimdept@luckymail.com
Tel: 0034634151884

Best regards,
Dr. Maria Jose Muyor.
Euro Milliones Lottery

www.infosecawareness.in

Email Trace - Trace Email and Track Email tool - Windows Internet Explorer
http://www.ip-adress.com/trace_email/
ip address location
Powered by Google Search Total Care Shop Mail Messenger News
Web Search Translate to Check Grammar Games TV Channels Hot Offer
Favorites Scenarios for Internet Ethics Suggested Sites Get More Add-ons
Email Trace - Trace Email and Track Email tool
Page Safety Tools

For email tracing copy and paste an email header in this field:

```
X-CDAC-PUNE-MailScanner-From: sicclaimdept@luckymail.com
X-CDAC-MailScanner-Spam-Status: No
X-Spam-Checker-Version: SpamAssassin 3.0.3 (2005-04-27) on
mailhub.cdac.in
X-Spam-Level: **
X-Spam-Status: No, score=2.2 required=3.0
tests=FORGED_RCVD_HELO,
        ROUND_THE_WORLD,UNDISC_RECIPS,YOU_WON autolearn=no
version=3.0.3
Status:  O
```

Trace Email Sender | Clear

What is an email header?

The email header is the information that travels with every email, containing details about the sender (including the IP address), route and receiver.

How to view the email header?

This depends on your email program. We made a little tutorial for some email programs and freemailers. Click here.

Email Trace - Trace Email and Track Email tool - Windows Internet Explorer

http://www.ip-adress.com/trace_email/#result

ip address location

Powered by Google | Search | Total Care | Shop | Mail | Messenger | News

Web Search | Translate to | Check Grammar | Games | TV Channels | Hot Offer

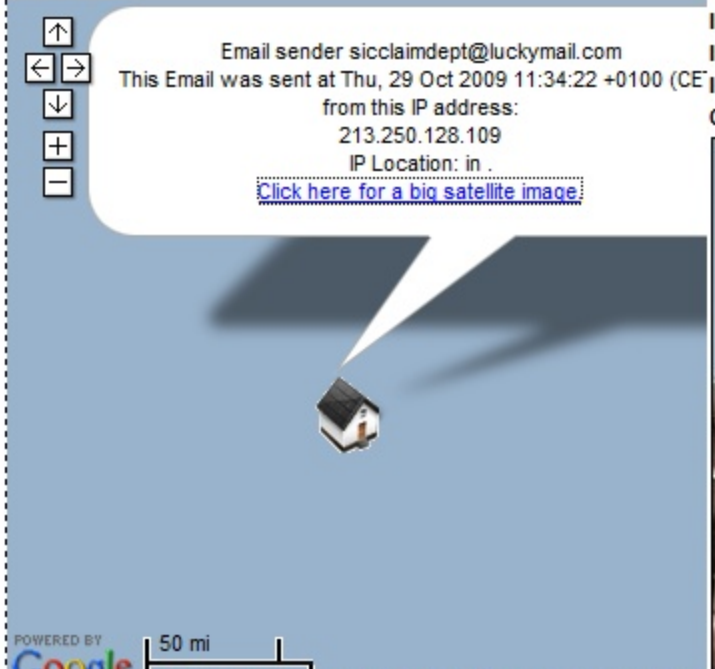
Favorites | Scenarios for Internet Ethics | Suggested Sites | Get More Add-ons

Email Trace - Trace Email and Track Email tool

Page | Safety | Tools

Email Tracing succesful!

The email sender
sicclaimdept@luckymail.com
used at Thu, 29 Oct 2009 11:34:22 +0100 (CET)
the IP address: **213.250.128.109** from , .



Email Sender IP address location & IP address info:

IP address [?]:	213.250.128.109 [Copy] [Whois]
IP address country:	n/a
IP address state:	n/a
IP address city:	n/a
IP address latitude:	n/a
IP address longitude:	n/a
ISP of this IP [?]:	n/a
Organization:	n/a

NIITcareers.com/GNP Ads by Google

SHARE

Folders: INBOX Go

Reply • Reply to all • Forward • Print View • Save to file

Date: Sunday, December 6 2009 03:52

From: Irish National Lottery <mel1000@stanford.edu>

To: undisclosed-recipients@ , @

Reply-To: Tedd Moyles <tedd.moyles03@live.in>

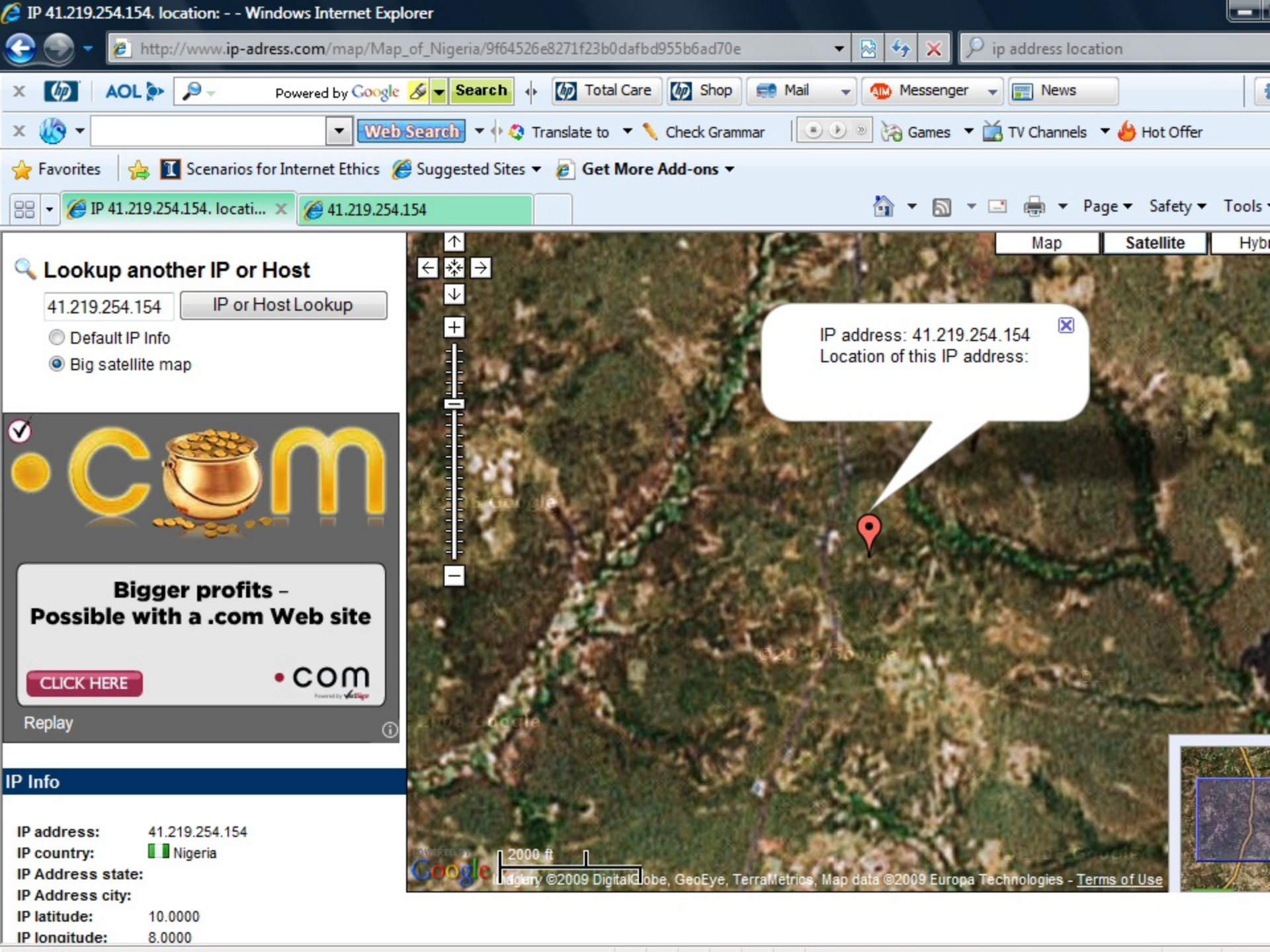
Subject: Registration Z720633X

Full Headers: Display Headers

Irish National Year Offer@2009(Registration Z720633X). 47 Meadow Vale, Sligo, Ireland Your email was selected as winner of 700,000 Pounds(GBP) in cash Credited to file KTU/9023118308/03 for claims Name:Age:sex:Occupation:Country: Home Address:Phone No :Regards Mr .Rooney James. Online Co-ordinator Email:tedd.moyles03@live.in for claim

--

This message has been scanned for viruses and dangerous content by MailScanner, and is believed to be clean.


IP 41.219.254.154. location: - - Windows Internet Explorer
http://www.ip-adress.com/map/Map_of_Nigeria/9f64526e8271f23b0dafbd955b6ad70e
ip address location
Powered by Google
Search
Total Care
Shop
Mail
Messenger
News
Web Search
Translate to
Check Grammar
Games
TV Channels
Hot Offer
Favorites
Scenarios for Internet Ethics
Suggested Sites
Get More Add-ons
IP 41.219.254.154. locati...
41.219.254.154
Page
Safety
Tools
Lookup another IP or Host
41.219.254.154
IP or Host Lookup
Default IP Info
Big satellite map
Bigger profits –
Possible with a .com Web site
CLICK HERE
Replay
Map
Satellite
IP address: 41.219.254.154
Location of this IP address:
2000 ft
Imagery ©2009 DigitalGlobe, GeoEye, TerraMetrics, Map data ©2009 Europa Technologies - Terms of Use
IP Info
IP address: 41.219.254.154
IP country: Nigeria
IP Address state:
IP Address city:
IP latitude: 10.0000
IP longitude: 8.0000

41.219.254.154 - Windows Internet Explorer
http://www.ip-adress.com/whois/41.219.254.154
ip address location
Powered by Google Search Total Care Shop Mail Messenger News
Starcomms Nigeria (v4 allocation) Web Search Translate to Check Grammar Games TV Channels Hot Offer
Favorites Scenarios for Internet Ethics Suggested Sites Get More Add-ons
IP 41.219.254.154. location: - 41.219.254.154
Page Safety Tools
Internet Security

41.219.254.154 Whois Information

```
% This is the AfriNIC Whois server.

% Note: this output has been filtered.

% Information related to '41.219.254.0[Who Is IP][trace][Reverse IP Search] - 41.219.254.255[Who Is IP][trac
[Reverse IP Search]'

inetnum: 41.219.254.0[Who Is IP][trace][Reverse IP Search] - 41.219.254.255[Who Is IP][trace][Reverse IP Search]
netname: ORG-SA57-AFRINIC-20050513
descr: Assigned to Lagos dial-pool customers
country: NG
admin-c: NS4-AFRINIC
tech-c: CM9-AFRINIC
status: Assigned PA
mnt-by: STARCOMMS-MNT
mnt-lower: STARCOMMS-MNT
source: AFRINIC # Filtered
parent: 41.219.192.0[Who Is IP][trace][Reverse IP Search] - 41.219.255.255[Who Is IP][trace][Reverse IP Search]

person: NAVNEET SINGH
address: Plot 1261, Bishop Kale Close, off Saka Tinubu
address: Victoria Island, Lagos, Nigeria
phone: +234-1-804-1234
fax-no: +234-1-811-0301
e-mail: navneets@starcomms.com[Who Is Domain][trace][Reverse DNS Search]
nic-hdl: NS4-AFRINIC
source: AFRINIC # Filtered

person: Catalin Miclaus
address: Plot 1261C, Bishop Kale Close, off Saka Tinubu
phone: +234-1-8041234
```

Stanford.edu - Stanford - Windows Internet Explorer
http://www.ip-adress.com/whois/stanford.edu
ip address location
Search
Total Care
Shop
Mail
Messenger
News
Web Search
Translate to
Check Grammar
Games
TV Channels
Hot Offer
Favorites
Scenarios for Internet Ethics
Suggested Sites
Get More Add-ons
Stanford.edu - Stanford
41.219.254.154
Page
Safety
Tools

Not registered?
It's free!
sign up now >

Make ip-adress.com to your homepage

My IP address: 210.212.218.253 Details
Last IP Lookup: 41.219.254.154 Details
Distance between this IP address locations: 5465 miles
Hyderabad <-> Details

Webhosting Reviews
Hosting Solution
IP Address Management
Remote IP Address
Cheap Internet Service
Internet Security

stanford.edu IP:
171.67.216.15

stanford.edu server location:
Stanford in United States

stanford.edu ISP:
Stanford University

Stanford.edu - Stanford Whois Information

```
--------------------------

Domain Name: STANFORD.EDU

Registrant:
Stanford University
The Board of Trustees of the Leland Stanford Junior University
241 Panama Street, Pine Hall, Room 115
Stanford, CA 94305-4122
UNITED STATES

Administrative Contact:

Domain Admin
```

Thank You

www.infosecawareness.in