Desktop Security

Nandeeshwar.B
CDAC Hyderabad

Why Security ?

" The olden phrase is always golden... Prevention is Better than Cure."

Desktop Security

BIOS Settings

- BIOS (Basic Input / Output System) Settings
  - Computers BIOS is the first program that runs when computer is started. You can tell the BIOS to ask for a password when it starts, thus restricting access to your computer

Why need for Securing Desktop

- We need to secure our desktop because a personal computer used without proper security measure that could lead to exploiting the system for illegal activities using the resources of such insecured computers
- These exploiters could be Virus, Trojans, Keyloggers and sometimes real hackers. This may result in data theft, data loss, personal information disclosure, stealing of credentials like passwords etc.

Starting from Installation

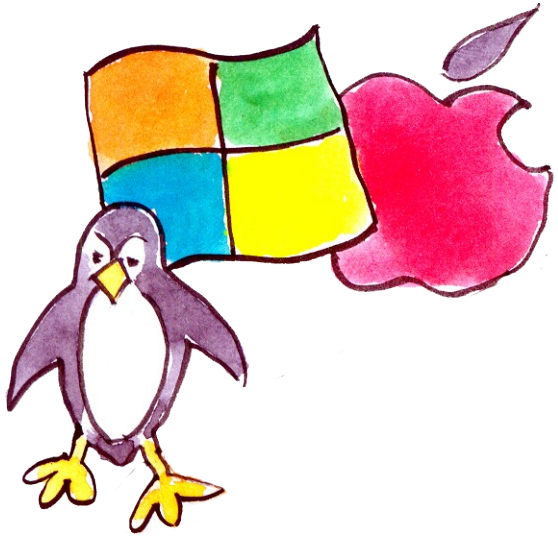
- Installation of Operating System get proper Licensed Operating System and read License agreement carefully before installing the OS.
- Switch on your personal computer and go to BIOS Settings

Look what is being installed

- Use the authorized software provided by the Vendor/official websites to install your
- Motherboard drivers
- Monitor drivers
- Audio & Video drivers
- Network drivers
- Any other software....

Operating System

- Operating System is the important program that runs on the computer
- It is responsible for us to secure the system by not allowing the unauthorized users to access the system



Data Security

- Enable Auto-updates of your Operating System and update it regularly.
- Strong password should be used for “Admin” Account on computer and for other important applications like E-mail client, Financial Applications (accounting etc).
- Backup: Periodically backup your computer data on CD / DVD or USB drive etc.. in case it may get corrupted due to HardDisk failures or when reinstalling/format ting the system.
- Recovery Disk: Always keep recovery disk suplied by Manufacturer / Vendor of the Computer System to recover the Operating System in the event of boot failures due to system changes such as uncerificated Drivers/unknown Software publisher.
- Startup programs should be monitored / controlled for optimal system performance.

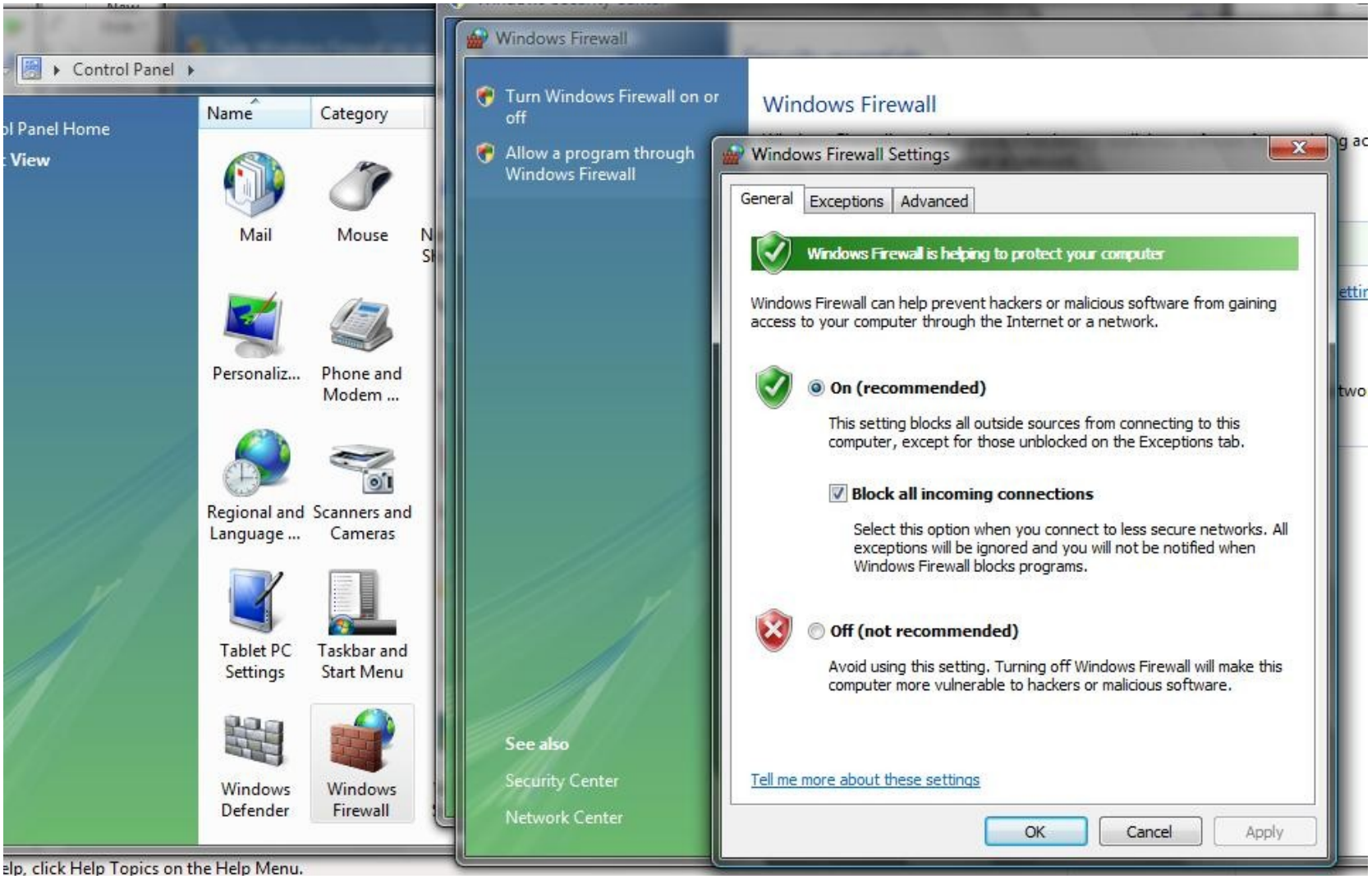
System Account Password

- Password represents the identity of an individual for an account

Firewalls

- When you leave your home, we will lock our doors for securing our property, and we can also secure our property from thieves
- *The same security is required for your computer since Internet connection leaves you vulnerable to hackers who want to access your personal information from your PC.*

How to enable firewall in windows?



Tips and Guidelines for securing the operating system

- Activate a password for the screen saver so that when ever the operations are not active it will lock the computer automatically after particular period of time.

- Always use a strong password for your operating system to protect the system from unauthorized users.
  - An example of a good password is Th!5iS@g0odP4s5wD

Tips and Guidelines

- Turn off file sharing in the computer when there is no need to access files in that system.
- Delete the software's and features of the operating systems which are not in use.

Tips and Guidelines

- Disable the default guest account so that it makes the unauthorized users harder to gain access to the system.
- Use an updated anti virus software to protect the operating system from a virus.

Tips and Guidelines

- Update the operating system with the latest patches mainly with critical security updates for the operating system.
- Backup critical data which will be helpful in case of operating system failure.

Tips and Guidelines

- Always make sure User accounts should set their passwords according to the defined security policies of an organization.
- Administrators should be careful while configuring the privileges, for an employee of the organization.
- Services and security polices should be reviewed daily.
- Always update the operating system with latest updates or patches and use updated antivirus
- And also make sure to enable a firewall of your PC to avoid access from hackers and always use tips and guidelines for secure PC.

Browser Security

Web browser

- For internet accessing we always use the application called web browser
- Update browsers Regularly

- Web browser is used to gain and access the information and also resources on the World Wide Web.

- It is a software application used to trace and display the web pages

Why Secure Your Browser

- Today, web browsers such as Internet Explorer, Mozilla Firefox, and Apple Safari (to name a few), are installed on almost all computers.
- Because web browsers are used so frequently, it is vital to configure them securely.
- Often, the web browser that comes with an operating system is not set up in a secure default configuration.
- Not securing your web browser can lead quickly to a variety of computer problems:
  - Spyware being

- Ideally, computer users should evaluate the risks from the software they use.

- Many computers are sold with software already loaded.

- Whether installed by a computer manufacturer, operating system maker

- The first step in assessing the vulnerability of your computer is to find out what software is installed and how one program will interact with another.

Various Threats from software attacks

- Many users have a tendency to click on links without considering the risks of their actions.
- Web page addresses can be disguised or take you to an unexpected site.
- Many web browsers are configured to provide increased functionality at the cost of decreased security.
- New security vulnerabilities may have been discovered since the software was configured and packaged by the manufacturer.
- Computer systems and software packages may be bundled with additional software, which increases the number of vulnerabilities that may be attacked.

- Third-party software may not have a mechanism for receiving security updates.
- Many websites require that users enable certain features or install more software, putting the computer at additional risk.
- Many users do not know how to configure their web browsers securely.
- Many users are unwilling to enable or disable functionality as required to secure their web browser.

Web Browser Features and Risks

- Attackers focus on exploiting client-side systems (your computer) through various vulnerabilities.
- They use these vulnerabilities to take control of your computer, steal your information, destroy your files, and use your computer to attack other computers.
- A low-cost way attackers do this is by exploiting vulnerabilities in web browsers.
- An attacker can create a malicious web page that will install Trojan software or spyware that will steal your information

- Rather than actively targeting and attacking vulnerable systems, a malicious website can passively compromise systems as the site is visited.
- A malicious HTML document can also be emailed to victims. In these cases, the act of opening the email or attachment can compromise the system.

- ActiveX allows applications or parts of applications to be utilized by the web browser.
- A web page can use ActiveX components that may already reside on a Windows system, or a site may provide the component as a downloadable object.
- This gives extra functionality to traditional web browsing, but may also introduce more severe vulnerabilities if not properly implemented.

- **Plug-ins** are applications intended for use in the web browser.
- Adobe Flash is an example of an application that is available as a plug-in.
- Plug-ins can contain programming flaws such as buffer overflows

- **Cookies** are files placed on your system to store data for specific websites.
- A cookie can contain any information that a website is designed to place in it.
- Cookies may contain information about the sites you visited, or may even contain credentials for accessing the site.
- Cookies are designed to be readable only by the website that created the cookie.
- Session cookies are cleared when the browser is closed, and
- Persistent cookies will remain on the computer

Usage of Web browsers

- Web browser is a software application that runs on internet and allows viewing the web pages, as well as content, technologies, videos, music, graphics, animations and many more.

Types of web browsers

- There are different types of web browsers available with different features.
- A web browser is a tool used not only on the personal computers but it also used on mobile phones to access the information.

Popular web browsers

- Microsoft Edge
- Mozilla Fire fox
- Google Chrome
- Safari
- Many More

Risks towards web browser

- There are increased threats from software attacks taking advantage of vulnerable web browsers.
- The vulnerabilities are exploited and directed at web browsers with the help of compromised or malicious web sites

How to secure your web browser

- Security zone
- Trusted sites
- In private browsing
- Tracking options
- Many more

Security Features

- Browse in in private mode
- Smart screen filter
- Tracking protection
- Delete browsing history

Security features

- Tracking
- Security zone
- Block forged websites
- Many more

Email Security

What is an email?

- Electronic mail in short email
- It is one of the widely used services of the internet.
- It is used to transmit the messages
- An email address is used to communicate

Risks involved

- Various techniques used by hackers to retrieve personal information and passwords
  - Spam
  - Fake emails
  - Lottery emails
  - Phishing emails
  - Many more

Different possible ways of Email threats

- Malicious Attachments
  - Malicious email attachments are an increasingly dangerous threat to corporate security. Disguised as documents, voicemails, e-faxes or PDFs, malicious email attachments are designed to launch an attack on the victim's computer when the attachment is opened. By opening or executing such attachments malicious code may download into your system and can infect your system.
- Always scan the attachments before you open them.
- Never click on links received in emails from strangers

Different possible ways of Email threats

- Double extensions
  - Another concept to bypassing file upload validation is for an attacker to abuse double extensions where an application extracts file extensions by looking for the '.' character in the filename, and extracting the string after the dot character. A file named filename.php.123 will be interpreted as a PHP file and it will be executed.
  - Use file upload forms with whitelisting approach. With this approach, only files that match a known and accepted file extension are allowed.

Different possible ways of Email threats

- Fake e-Mails
  - Sometimes e-Mails are received with fake e-mail address like services@facebook.com by an attachment named, “Facebook_Password_4cf91.zip and includes the file Facebook_Password_4cf91exe" that, the e-mail claims, contains the user's new facebook password. When a user downloads the file, it could cause a mess on their computer and which can be infected with malicious software.
- Always check and confirm from where the e-mail has been received, generally service people will never ask or provide your password to change.
- If you subscribe to e-mail or text alerts from your bank or financial institution, you should be familiar with the format, content, and address of these messages. Be suspicious of anything you receive that is out of the norm.

Different possible ways of Email threats

- Hoaxes
  - Hoax is an attempt to make the person believe something which is false as true. It is also defined as an attempt to deliberately spread fear, doubt among the users.
  - Since the e-Mail messages are transferred in clear text, it is advisable to use some encryption software like PGP (pretty good privacy) to encrypt email messages before sending, so that it can be decrypted only by the specified recipient only.
  - Since a backup is maintained for an e-Mail server all the messages will be stored in the form of clear text though it has been deleted from your mailbox. Hence there is a chance of viewing the information by the people who are maintaining backups. So it is not advisable to send personal information through e-Mails.
  - The most effective preventive strategy is to educate yourself and members within your organization on potential email security threats. Be sensible email users so that possible conflicts are avoided as much as possible.

Different possible ways of Email threats

- Phishing e-mails
  - These appear very authentic, and often include graphics and logos that are actually from your bank. There may even be a link that actually takes you to your bank's Web site. Even if you don't enter any personal information, clicking the link can infect your computer with data-stealing malware. Sometimes e-Mails are targeted at you by unknown users by offering gifts, lottery, prizes, which might be free of cost, and this may ask your personal information for accepting the free gift or may ask money to claim lottery and prizes it is one way to trap your personal information.
  - Look for grammatical errors in the e-mail
  - Always ignore free gifts offered from unknown users.

Fake / Phishing email

email says sent from RBI for two way authentication

From: [redacted] Sent: Tue 17-07-2012 15:14

To: [redacted]

Cc:

Subject: FW: Reserve Bank Of India: New OTP Alert Message

Attachments: NetBanking_Users.html (323 B)

From: Reserve Bank Of India [mailto:alert@rbi.org]
Sent: Tuesday, July 17, 2012 9:02 AM
Subject: Reserve Bank Of India: New OTP Alert Message

The New Online Security Platform

With a view to prevent online identity theft in internet banking a new security online Platform has been introduced wherein the customer would go through a 2-way Authentication factor before he/she properly logs into Internet Banking everytime

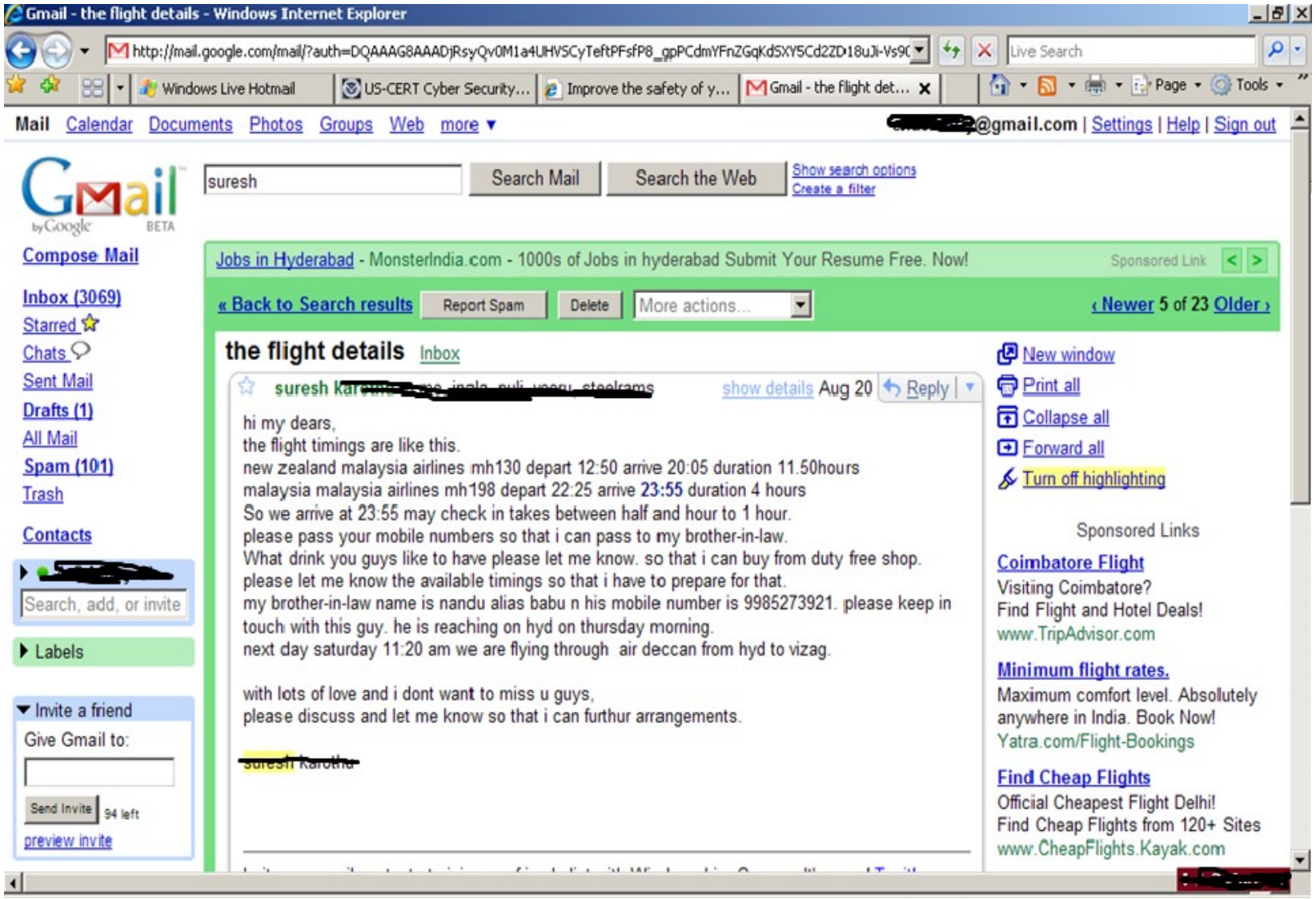
This security Platform is been introduced in view of the recent cyber attacks towards internet banking users

If you are using Internet Explorer please allow ActiveX for scripts.
to perform all data transfers securely.

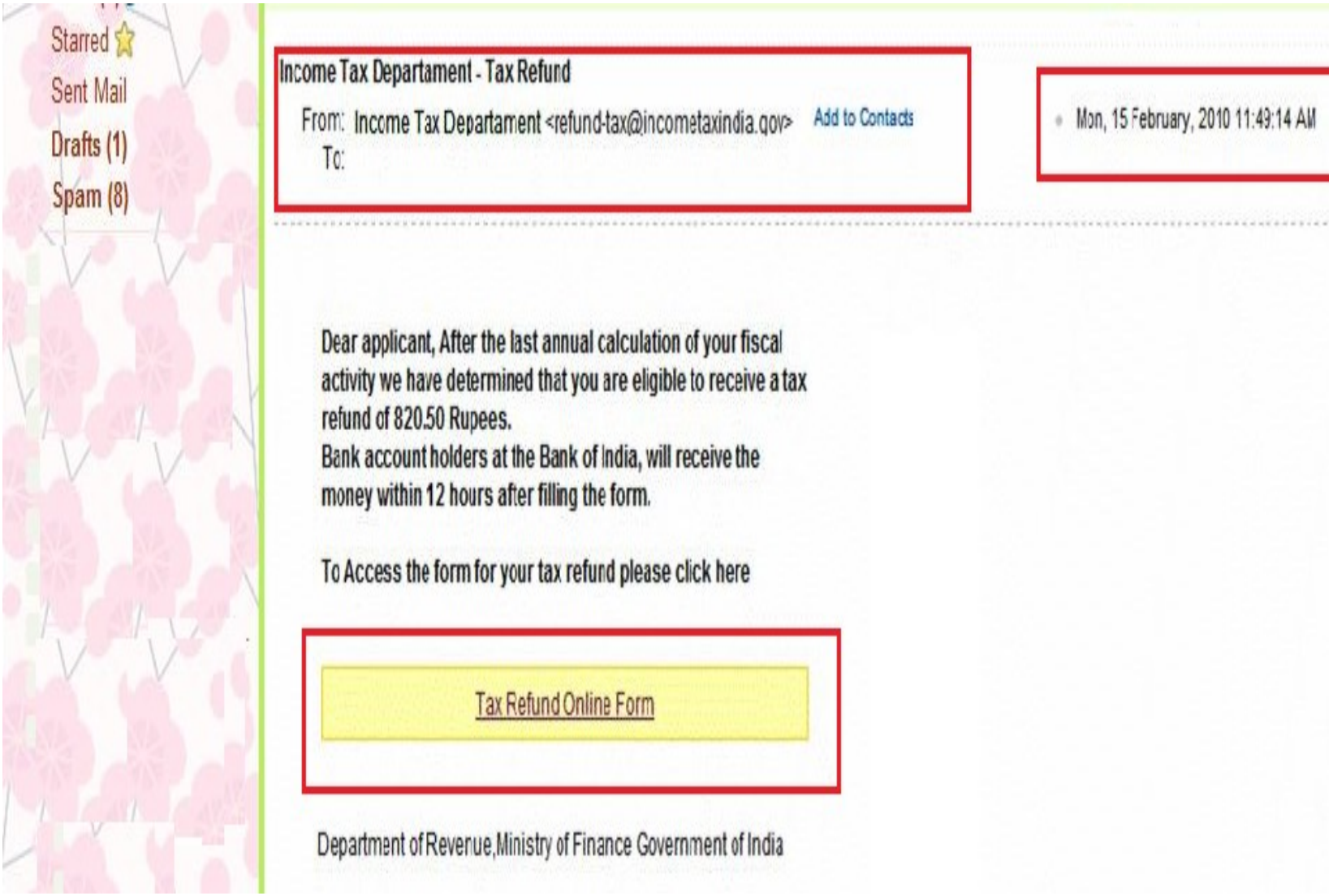
Kindly Download the attachment and update

Regards
RBI Online

One example


Gmail - the flight details - Windows Internet Explorer
http://mail.google.com/mail/?auth=DQAAAG8AAADjRsyQv0M1a4UHVSCyTeftPFsfP8_gpPCdmYFnZGqKd5XY5Cd2ZD18uJi-Vs9(
Live Search
Windows Live Hotmail
US-CERT Cyber Security...
Improve the safety of y...
Gmail - the flight det...
Page
Tools
Mail Calendar Documents Photos Groups Web more
@gmail.com | Settings | Help | Sign out
Gmail by Google BETA
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
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
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.
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

Example of Phishing email



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)

continuous

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
trps
Tax return

Income Tax Department

Department of Revenue, Ministry of Finance, Government of India

Home

- 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

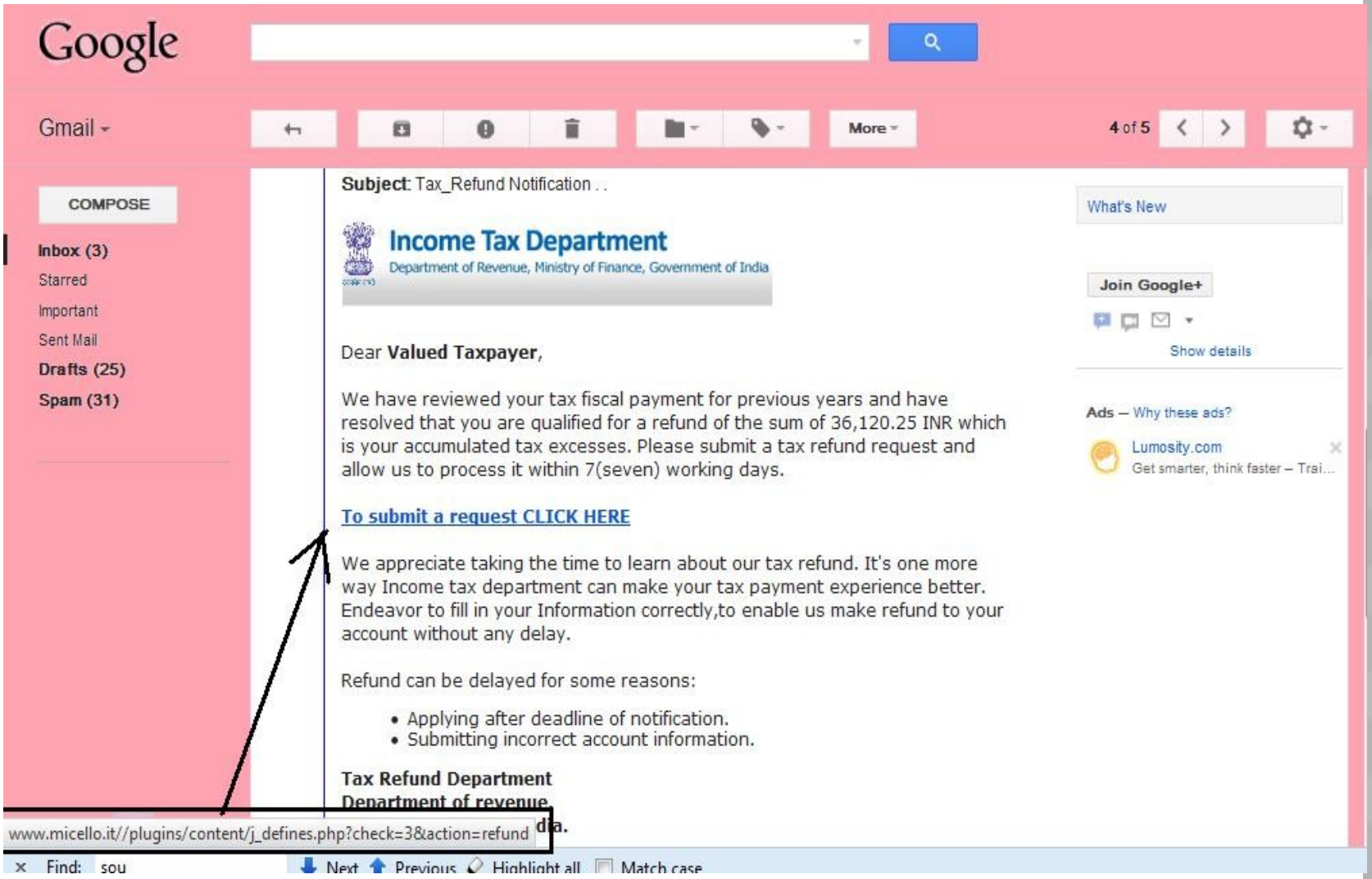
- Press Release
- Educational Institutions under section 10(23 C)
- Industrial Parks u/s 80 IA(4)(iii)
- Tax Information Network
- TIN Helpdesk
- Tax Calculator
- Departmental News
- Cadre Review and Restructuring of Income Tax Department

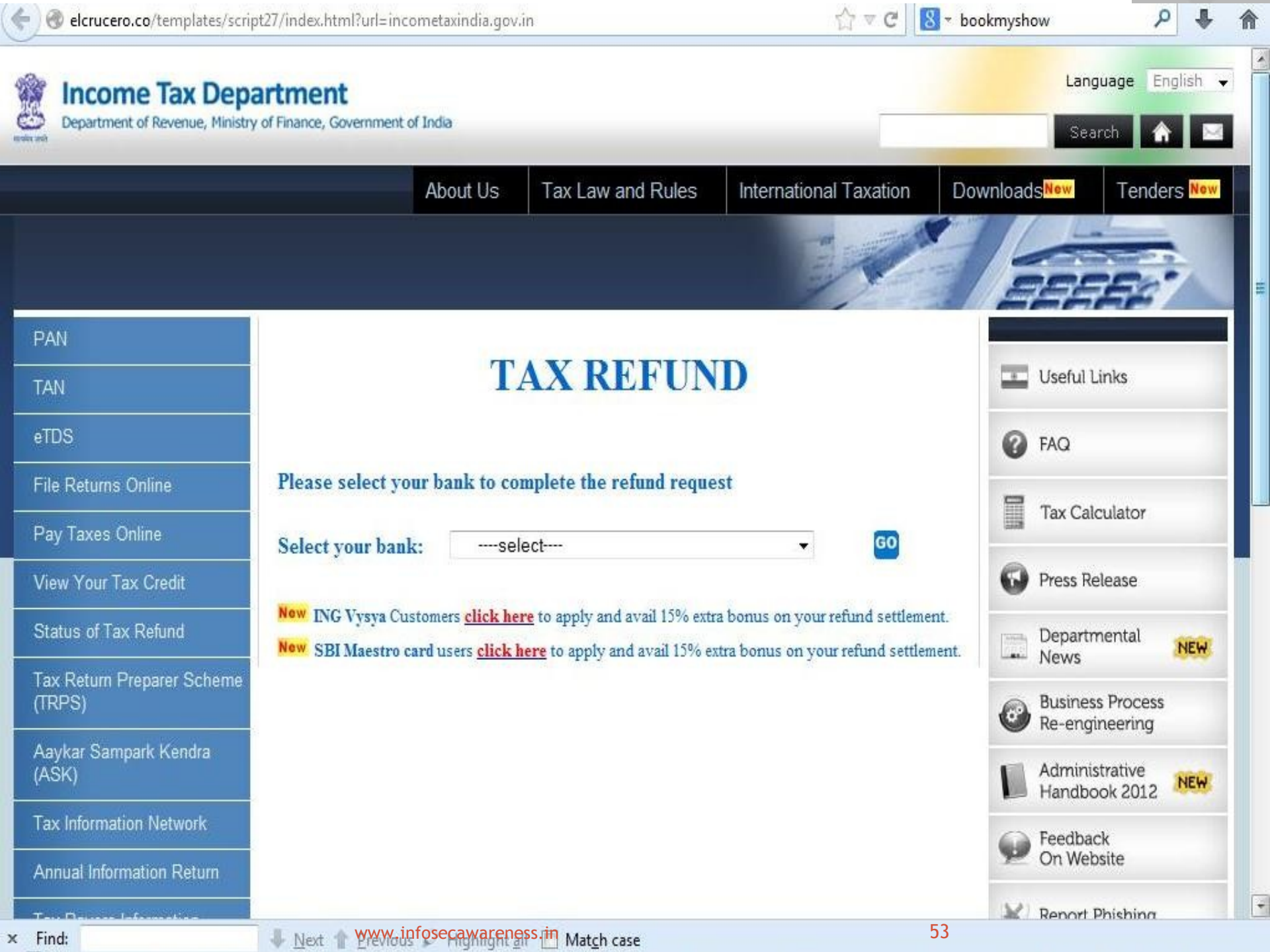
trps
TAX RETURN PREPARERS
Tax return

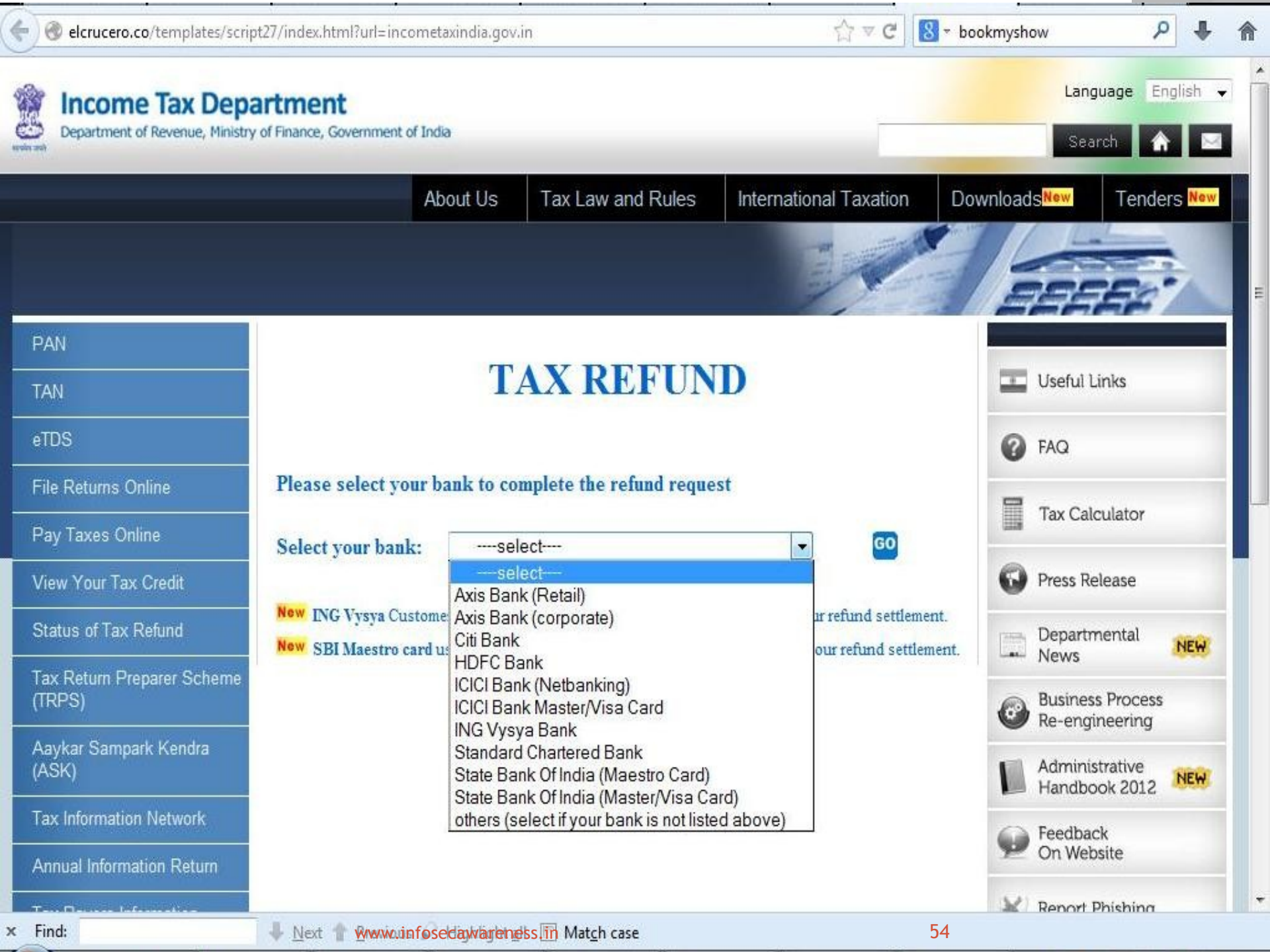
Original Website

How to recognize?

One more example of Phishing email




elcrucero.co/templates/script27/index.html?url=incometaxindia.gov.in
bookmyshow
Income Tax Department
Department of Revenue, Ministry of Finance, Government of India
Language English
Search
About Us
Tax Law and Rules
International Taxation
Downloads New
Tenders New
PAN
TAN
eTDS
File Returns Online
Pay Taxes Online
View Your Tax Credit
Status of Tax Refund
Tax Return Preparer Scheme (TRPS)
Aaykar Sampark Kendra (ASK)
Tax Information Network
Annual Information Return
TAX REFUND
Please select your bank to complete the refund request
Select your bank:
----select----
GO
New ING Vysya Customers click here to apply and avail 15% extra bonus on your refund settlement.
New SBI Maestro card users click here to apply and avail 15% extra bonus on your refund settlement.
Useful Links
FAQ
Tax Calculator
Press Release
Departmental News NEW
Business Process Re-engineering
Administrative Handbook 2012 NEW
Feedback On Website
Report Phishing
Find:
Next
Previous
Highlight all
Match case


elcrucero.co/templates/script27/index.html?url=incometaxindia.gov.in
bookmyshow
Income Tax Department
Department of Revenue, Ministry of Finance, Government of India
Language English
Search
About Us
Tax Law and Rules
International Taxation
Downloads New
Tenders New
PAN
TAN
eTDS
File Returns Online
Pay Taxes Online
View Your Tax Credit
Status of Tax Refund
Tax Return Preparer Scheme (TRPS)
Aaykar Sampark Kendra (ASK)
Tax Information Network
Annual Information Return
TAX REFUND
Please select your bank to complete the refund request
Select your bank:
----select----
GO
----select----
Axis Bank (Retail)
Axis Bank (corporate)
Citi Bank
HDFC Bank
ICICI Bank (Netbanking)
ICICI Bank Master/Visa Card
ING Vysya Bank
Standard Chartered Bank
State Bank Of India (Maestro Card)
State Bank Of India (Master/Visa Card)
others (select if your bank is not listed above)
New ING Vysya Custome
ur refund settlement.
New SBI Maestro card us
our refund settlement.
Useful Links
FAQ
Tax Calculator
Press Release
Departmental News NEW
Business Process Re-engineering
Administrative Handbook 2012 NEW
Feedback On Website
Report Phishing
Find:
Next
Match case
www.infosecawareness.in
54

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'.

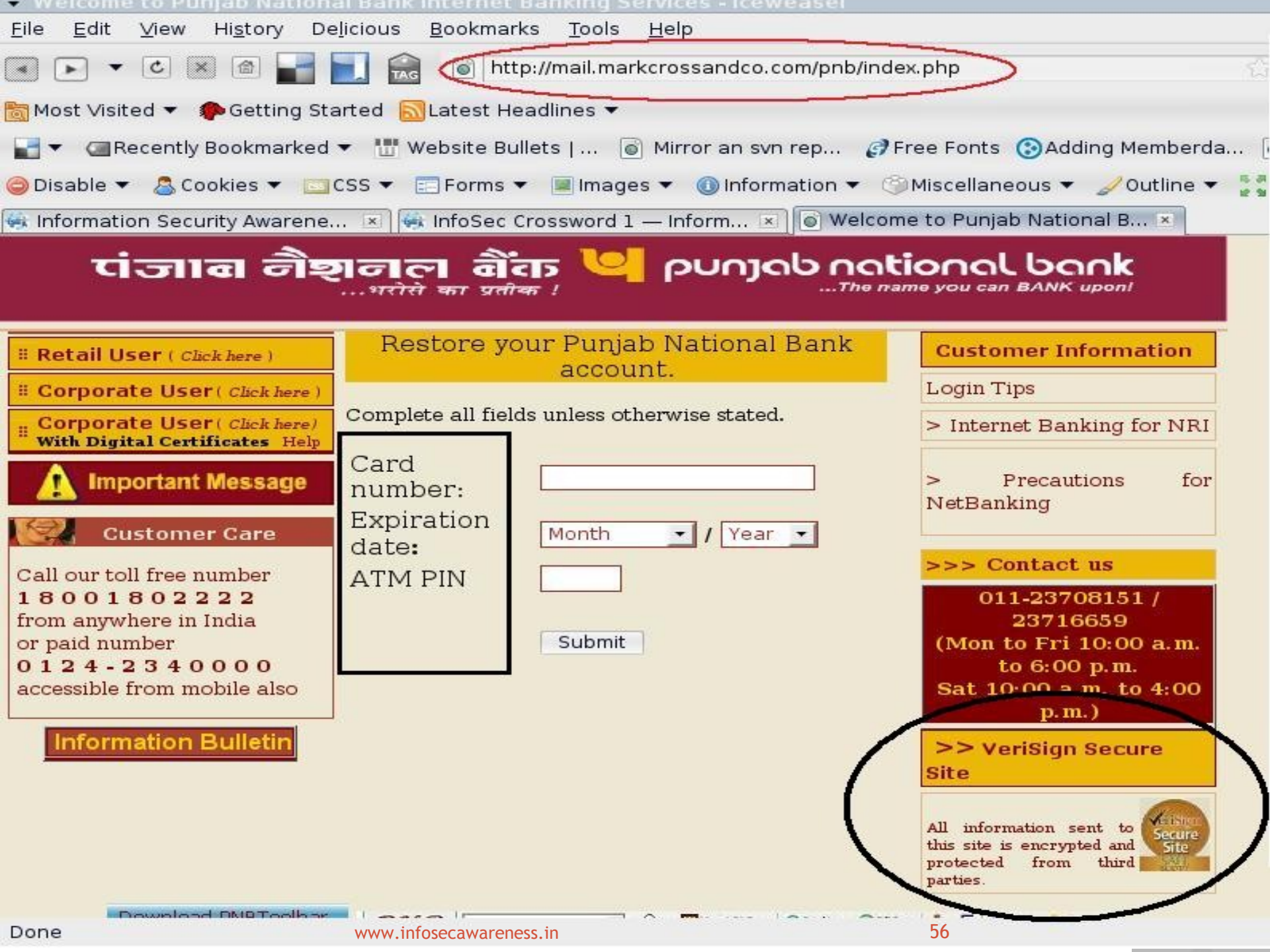
Most Popular

- Woman beaten by rail police for jumping queue
- Salman Khan comes to composer Pritam's rescue
- 10-year-old suspected of stealing paraded naked
- Model allegedly threatened by pimp to meet clients
- Picture special: Is this an air kiss gone

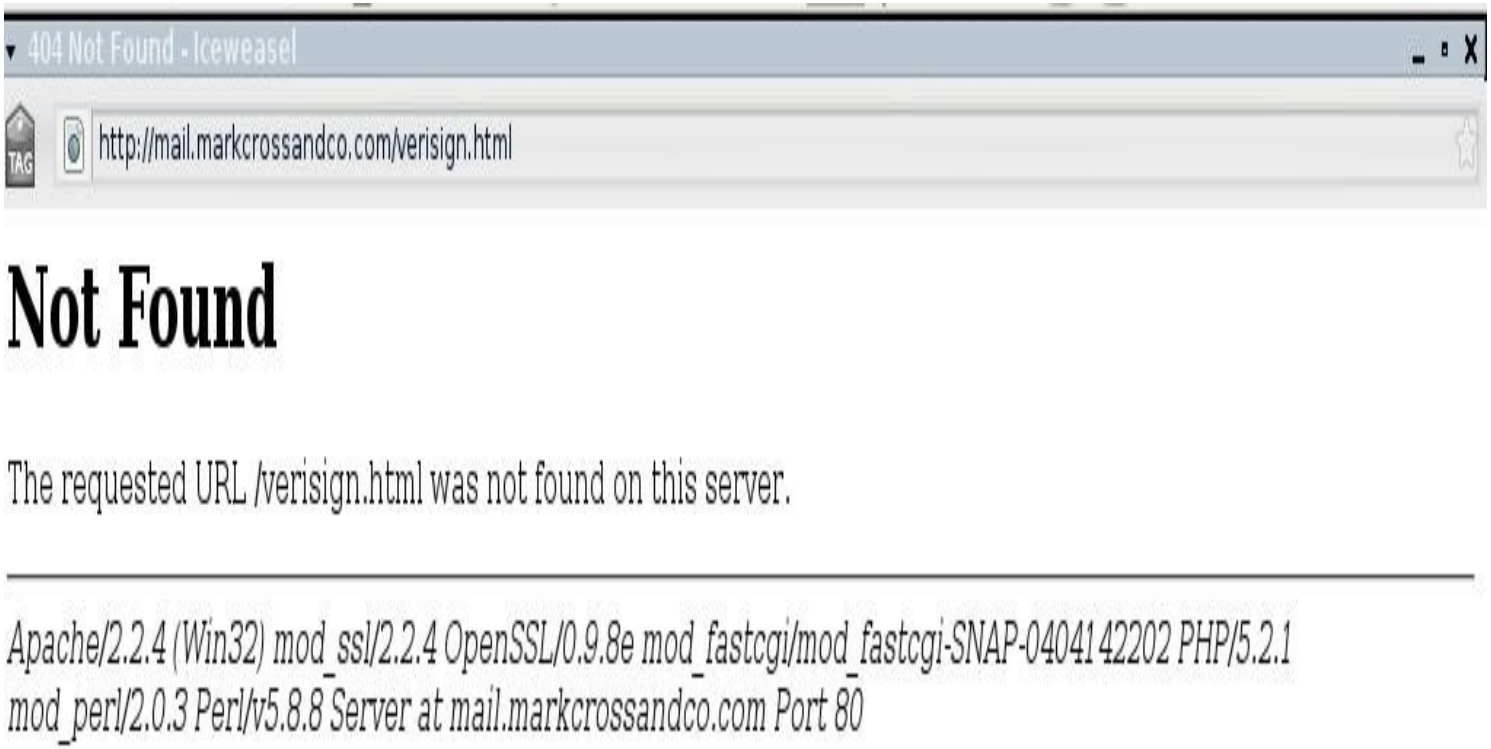
Download Software Free Trial
Write Any Kind of App In the Cloud In Multiple Languages. Learn More
Microsoft.com/Cloud/WindowsAzure
Ads by Google

Other Stories

- SRK fan tops CBSE
- Iconic Red fort was originally white
- No game plan on sports quota?
- Sachin Pilot held en route to Bhatta-Parsaul


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.
Secure Site
Done

Page went to not found page



Examples of phishing websites

- www.gmai1.com
- www.icici6ank.com
- www.bank0findia.com

Email Tracing

- Use of Email Headers to track
  - Cyberforensics.in

Secure Protocols

- Use of Secure Protocols
  - IMAPS (993)
  - POPS (995)
  - SMTPS (465/587)

Tips

- Don’t respond to emails received from strangers
- Don’t click on the links
- Check the URL before proceeding further
- Always follow email security and password policies
- So never reply and disclose any personal information because this might be scam or phishing.

Tips

- Always use strong password for your email account.
- Always use Anti-Spyware Software to scan the eMails for Spam.
- Always scan the e-Mail attachments with latest updated Anti-Virus and Anti-Spy ware before opening.
- Always remember to empty the Spam folder.

Malware

Your computer

- Viruses
- Worms
- Trojans
- Spyware

Yourself

- Online fraud
- Phishing
- Hoaxes
- Identity theft
- Spam

Your family

- Cyberbullies
- File sharing abuses
- Invasion of Privacy
- Disturbing Content
- Predators


Phishing
E-mail sent by online criminals to trick you into revealing personal information
Spam
Unwanted e-mail, instant messages, and other online communication
YOU'VE JUST WON!
Identity Theft
A crime where con artists get your personal information and access your cash and/or credit
Hoaxes
E-mail sent by online criminals to trick you into giving them money


cyberswachhtakendra.gov.in/index.html
certin
Handling Computer Security Incidents
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre
Ministry of Electronics and Information Technology Government of India
सत्यमेव जयते
Home
About Us
CERT-In
Security Tools
Alerts
Security Best Practices
Partners
FAQ's
Contact Us
Welcome to Botnet Cleaning and Malware Analysis Centre (Cyber Swachhta Kendra)
The " Cyber Swachhta Kendra " (Botnet Cleaning and Malware Analysis Centre) is a part of the Government of India's Digital India initiative under the Ministry of Electronics and Information Technology (MeitY) to create a secure cyber space by detecting botnet infections in India and to notify, enable cleaning and securing systems of end users so as to prevent further infections. The " Cyber Swachhta Kendra " (Botnet Cleaning and Malware Analysis Centre) is set up in accordance with the objectives of the "National Cyber Security Policy", which envisages creating a secure cyber eco system in the country. This centre operates in close coordination and collaboration with Internet Service Providers and Product/Antivirus companies. This website provides information and tools to users to secure their systems/devices. This centre is being operated by the Indian Computer Emergency Response Team (CERT-In) under provisions of Section 70B of the Information Technology Act, 2000.
Don't be Quick to Click, think before clicking on links received via email, social media etc.
Awareness is the key to the security
Why have I Reached this page?
You have reached this page because your computer / system / device is probably infected with malware called 'Bot' and could become a part of a botnet. If your computer / system / device is part of a botnet, the following could happen:
Information on your computer / system / device could be stolen
Your computer / system / device may be used to send out spam
What should I do?
To remove the malware, you need to scan your computer / system / device with the tools recommend below and take steps to improve the security of your computer / system / device.
We encourage you to visit the following page from the antivirus company Quick Heal who is providing free bot removal tools for this initiative.
Quick Heal


ISEA
Information Security Education & Awareness
www.infosecawareness.in


सी डैक
CDAC

THANK YOU