Social Engineering Techniques and Preventive Measures

By

Karanpreet Kaur

Cyber Security Expert

CDAC, Mohali

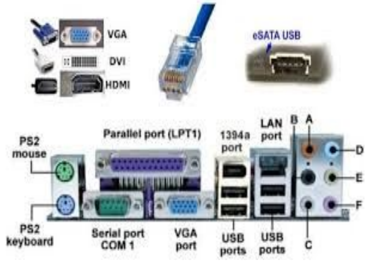
Objectives

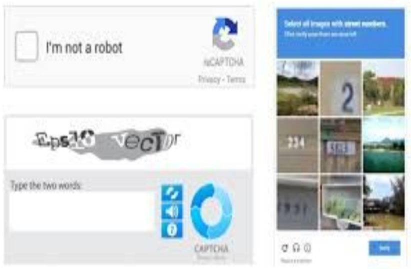
The objective of this presentation is to educate and create awareness amongst the community on use of Technology, Internet Media and its implications on possible cyber crimes.

- Understand the principles of social engineering
- Define the goals of social engineering
- Recognize the signs of social engineering
- Identify ways to protect yourself from social engineering

Home Security

Cyber Security





□ I'm not a robot

reCAPTCHA

Privacy - Terms

Type the two words:

CAPTCHA

Types of Hackers

1) **White Hat** – Good guys. Report hacks/vulnerabilities to appropriate people.
2) **Black Hat** – Only interested in personal goals, regardless of impact.
3) **Gray Hat** – Somewhere in between.

Script Kiddies

- Someone that calls themselves a ‘hacker’ but really isn’t

Ethical Hacker

- Someone hired to hack a system to find vulnerabilities and report on them.
- Also called a ‘**sneaker**’

What is Social Engineering

1. At its core it is manipulating a person into knowingly or unknowingly giving up information; essentially 'hacking' into a person to steal valuable information.

    - Psychological manipulation

    - Trickery or Deception for the purpose of information gathering

What is Social Engineering

2. It is a way for criminals to gain access to information systems. The purpose of social engineering is usually to secretly install spyware, other malicious software or to trick persons into handing over passwords and/or other sensitive financial or personal information

What is Social Engineering

3. Social engineering is one of the most effective routes to stealing confidential data from organizations, according to Siemens Enterprise Communications, based in Germany. In a recent Siemens test, 85 percent of office workers were duped by engineering.

“Most employees are utterly unaware that they are being manipulated,” says Colin Greenlees, security and counter-fraud consultant at Siemens.

What are they looking for

- Obtaining simple information such as your pet's name, where you're from, the places you've visited; information that you'd give out freely to your friends.
  - Think of yourself as a walking computer, full of valuable information about yourself. You've got a name, address, and valuables. Now categorize those items like a business does. Personally identifiable data, financial information, cardholder data, health insurance data, credit reporting data, and so on…

What are they looking for

- Take a close look at some of the 'secure' sites you log into. Some have a 'secret question' you have to answer, if you cannot remember your username or password. The questions seem pretty tough for an outsider looking into trying to hack into your account.
  - ✔ What's the name of your first pet?
  - ✔ What is your maiden name?
  - ✔ When was your mother/father born?
  - ✔ Where were you born?

Do these sound familiar?

Tactics

1. **Pretexting** – Creating a fake scenario

2. **Phishing** – Send out bait to fool victims into giving away their information

3. **Fake Websites** – Molded to look like the real thing. Log in with real credentials that are now compromised

4. **Fake Pop-up** – Pops up in front of real web site to obtain user credentials

Social Engineering methods

0 Dumpster Diving

0 Shoulder surfing

0 Baiting

0 Vishing

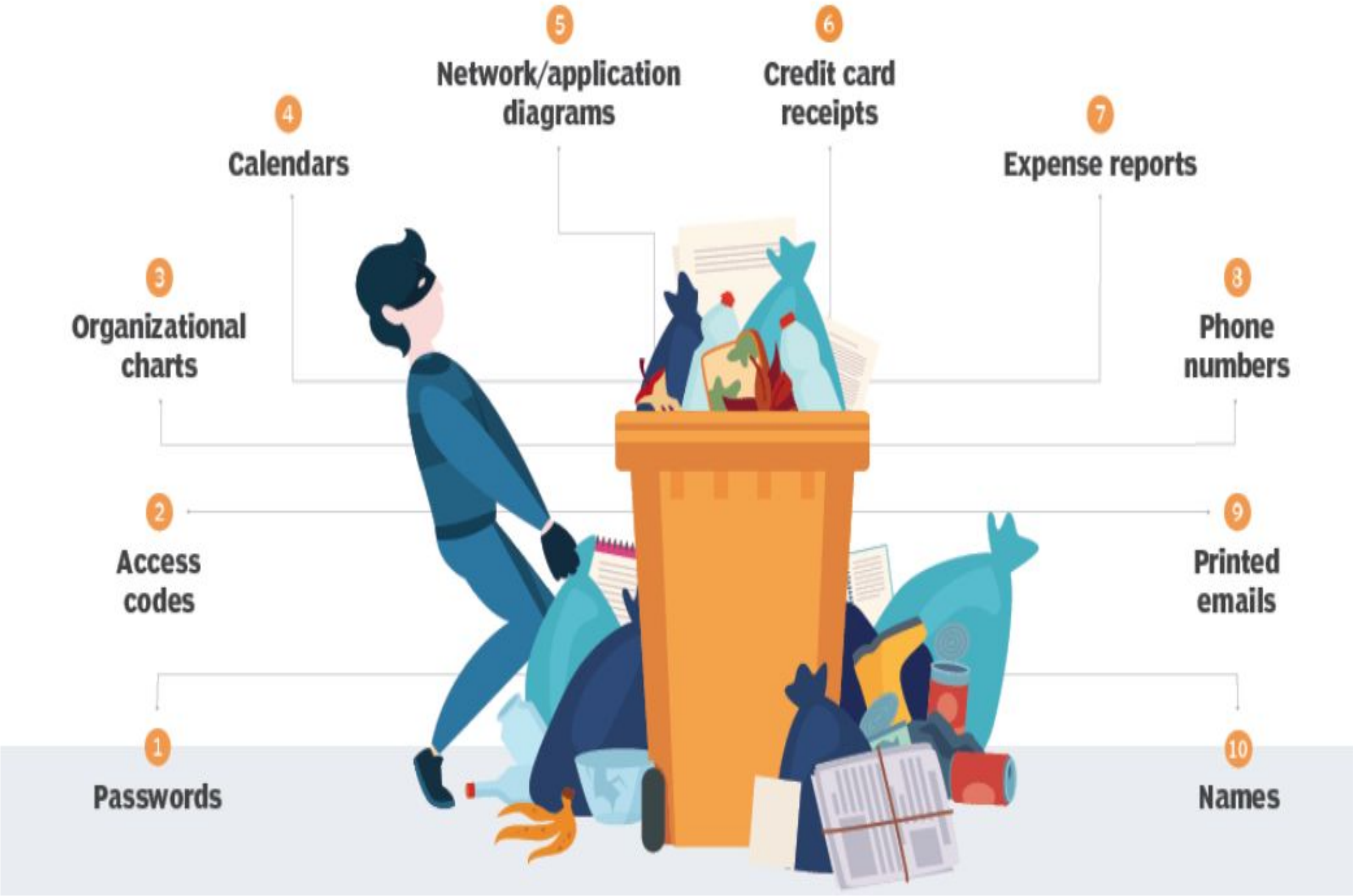
0 Phishing

0 Whaling

The Social Web
Social Networking
Micro blogging
Publishing
Photo Sharing
Aggregation
Audio
Video
Live-casting
RSS
Mobile
Crowd sourcing
Virtual Worlds
Gaming
Search
Conversation Apps.
Ning
twitxr
twitter
PLURK
slideshare
Picasa
flickr
digg
Google Reader
iTunes
viddler
justin.tv
blogtalkradio
USTREAM
FeedBurner
callwave
Aol Mobile.
TweetBrain
Kaneva
Second Life
World of Warcraft
Ask
bing
Google
Created by Mirna Bard
www.mirnabard.com

Dumpster diving

This entails combing through someone else's trash to find treasures—or in the tech world, discarded sensitive information that could be used in an illegal manner. Information that should be securely discarded includes, but is not limited to:



1 Passwords

2 Access codes

3 Organizational charts

4 Calendars

5 Network/application diagrams

6 Credit card receipts

7 Expense reports

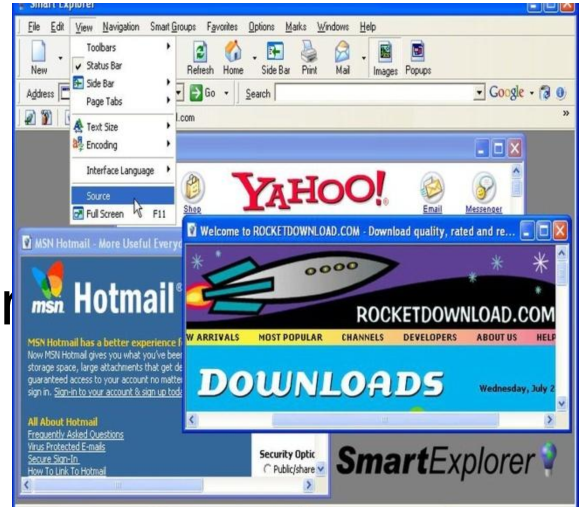
8 Phone numbers

9 Printed emails

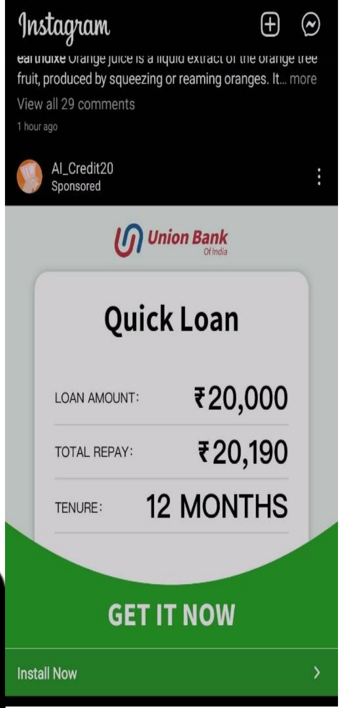
10 Names

www.isea.gov.in

Types of Social Engineering



MSN Hotmail has a better experience f
Now MSN Hotmail gives you what you've beer
storage space, large attachments that get de
guaranteed access to your account no matte
sign in. Sign-in to your account & sign up tod



earthuxe Orange juice is a liquid extract of the orange tree fruit, produced by squeezing or reaming oranges. It... more

View all 29 comments

1 hour ago

AI_Credit20
Sponsored

Union Bank Of India

Quick Loan

LOAN AMOUNT: ₹20,000

TOTAL REPAY: ₹20,190

TENURE: 12 MONTHS

GET IT NOW

Install Now

Technical Social Engineer

- Phishing
- Vishing
- Spam mails
- Popup window
- Interesting Software

Non-Technical

- Impersonation / Pretexting (retrieving the information via influencing)
- Dumpster Driving
- Spaying
- Acting as Technical expert

www.isea.gov.in

www.InfoSecawareness.in

Hello, Welcome to Amazon International Women's Day 2022 Giveway!

Complete the short quiz and win an Exclusive Gift from Amazon.

Question 1 of 4: Do you know Amazon?

YES

NO

Comments

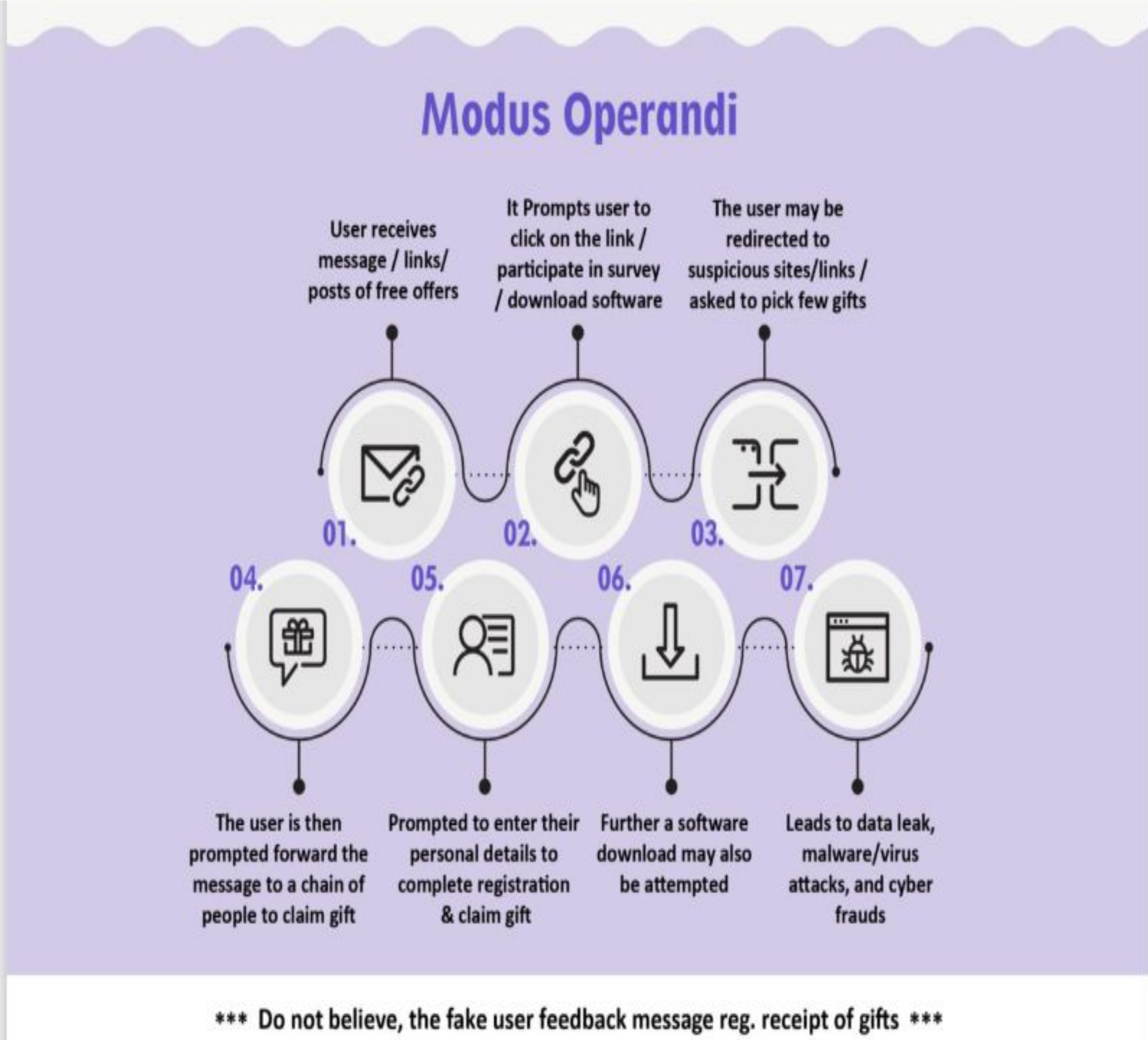
Cari Lewis
I received it today, thank you very much!

Meredith Price
I thought it was a scam, but it arrived this morning.

FRAUD ALERT

Amazon International Women's Day 2022 Giveaway Message is fake

Amazon International Women's Day 2022 Giveaway message which is widely being circulated on Social Media Apps is fake



Modus Operandi

01. User receives message / links/ posts of free offers

02. It Prompts user to click on the link / participate in survey / download software

03. The user may be redirected to suspicious sites/links / asked to pick few gifts

04. The user is then prompted forward the message to a chain of people to claim gift

05. Prompted to enter their personal details to complete registration & claim gift

06. Further a software download may also be attempted

07. Leads to data leak, malware/virus attacks, and cyber frauds

*** Do not believe, the fake user feedback message reg. receipt of gifts ***

Warning Signs

01. Tweaked website or email id of the sender

02. No genuine website would ask to share the link with your contacts

03. Creating unrequired urgency to share details

04. Requesting for unrelated personal details

05. Can sound too good to be true

Social Engineering

Any act that influences a person to take actions that or may not be in their best interest.

How it happens:

Fraudsters are able to trick people by playing on their emotions and getting people to act before they think, something people often do in an emotional state.

Example:

- **Desire to please**: Pretending to be your boss or other authority figure and telling you to do something that is critical, right away.
- **Trust:** Pretending to be a close friend or relative.
- **Fear of scarcity**: Saying offers are limited and/or will end soon.
- **Threats to wellbeing**: Pretending that access to critical resources such as your bank account , Card number, OTP etc
- **Greed/Entitlement**: Saying you won something or you are getting a free gift.

Social engineering is information security's weakest link

Social Engineering attacks

Phishing: Phishing uses emails that appear to come from legitimate sources to trick people into providing their information or clicking on malicious links and put end users into one of the emotional states that causes them to act without thinking.

Vishing: Attackers use phone calls to trick victims into handling over data. They may pose as bank managers or other trusted entities to supply your credentials and other important data.

Smishing: Uses SMS text messaging to get you to divulge information or

click on a malicious link.

Spear Phishing: Similar to phishing but the attacker customizes the email specifically for an individual to make the phish seem more real. They often target key employees with access to critical and/or confidential data

Quid Pro Quo: Pretends to be a service provider who keeps calling people until they find someone who actually requested or needs the service.

Baiting: Attackers setup traps such as USB drives , Malicious links, free download offers to entice users

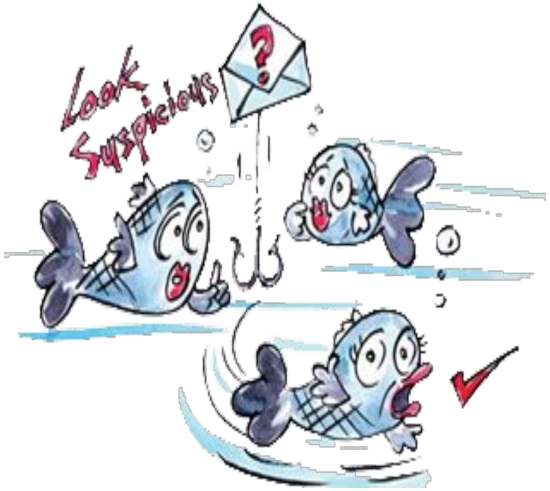
Whaling : Attackers target high ranking employees to gain access to high value data . Government agencies are frequently targeted

AI Powered Malware : AI can be used to bypass antimalware solutions and in some cases and even impersonate senior members of staff

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 attempting to acquire sensitive information such as
  - usernames
  - passwords
  - credit card details

BEWARE! YOU CAN BE NEXT VICTIM OF PHISHING



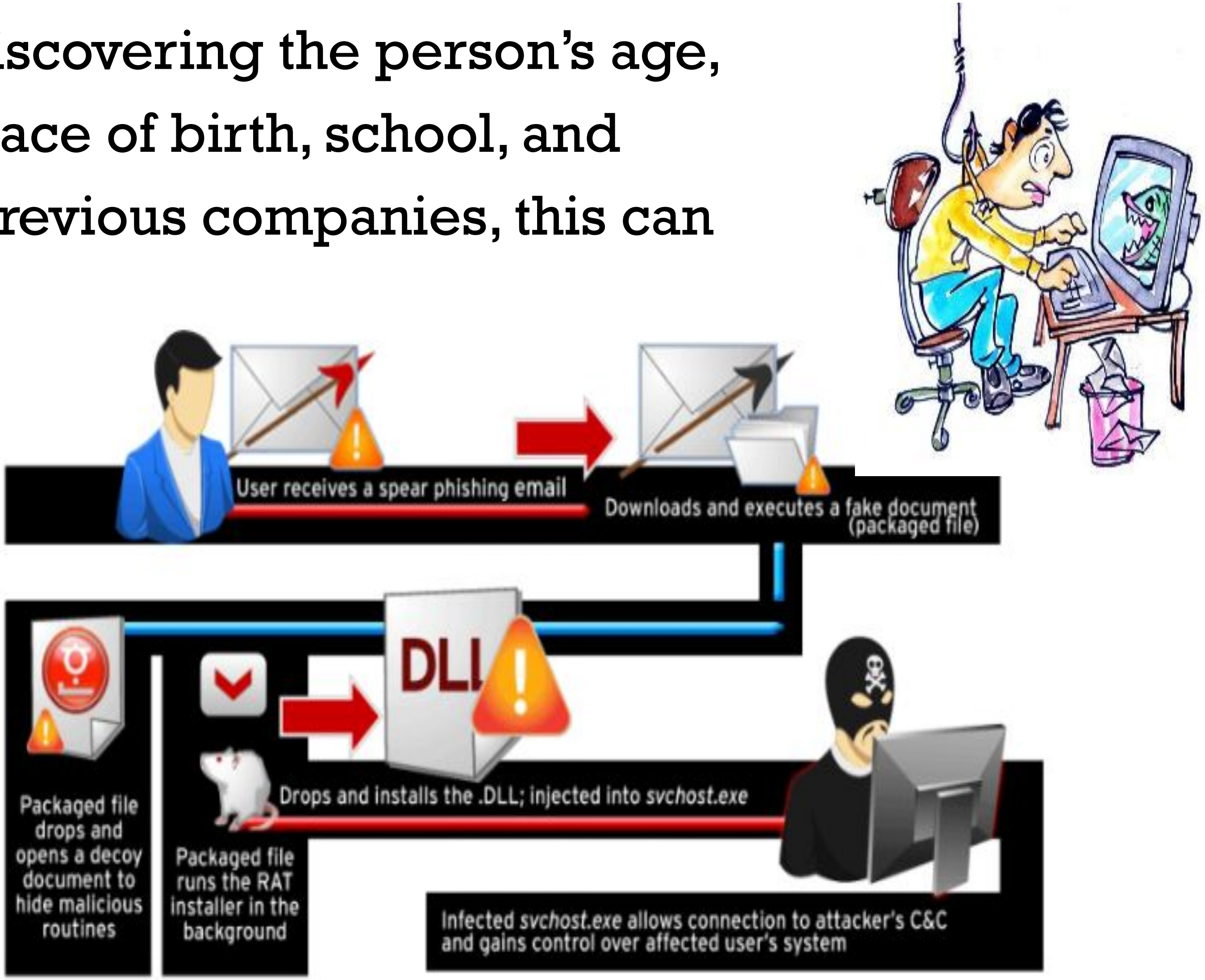
Spear phishing attack

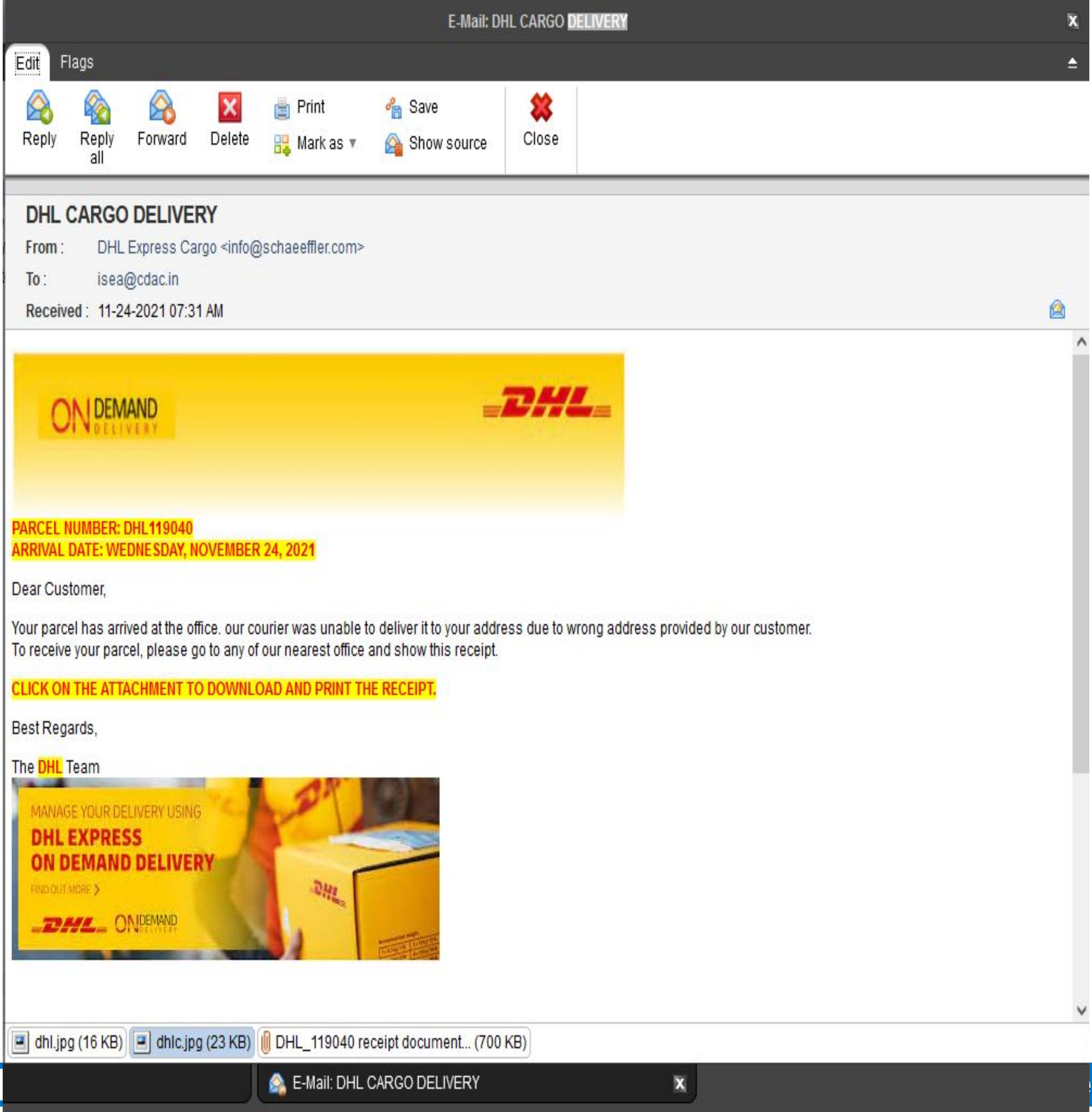
0 Discovering the person’s age,

0 place of birth, school, and

0 previous companies, this can

0 a
ir


User receives a spear phishing email
Downloads and executes a fake document (packaged file)
DLL
Drops and installs the .DLL; injected into svchost.exe
Packaged file drops and opens a decoy document to hide malicious routines
Packaged file runs the RAT installer in the background
Infected svchost.exe allows connection to attacker's C&C and gains control over affected user's system



DHL CARGO DELIVERY

From : DHL Express Cargo <info@schaeeffler.com>

To : isea@cdac.in

Received : 11-24-2021 07:31 AM

PARCEL NUMBER: DHL119040
ARRIVAL DATE: WEDNESDAY, NOVEMBER 24, 2021

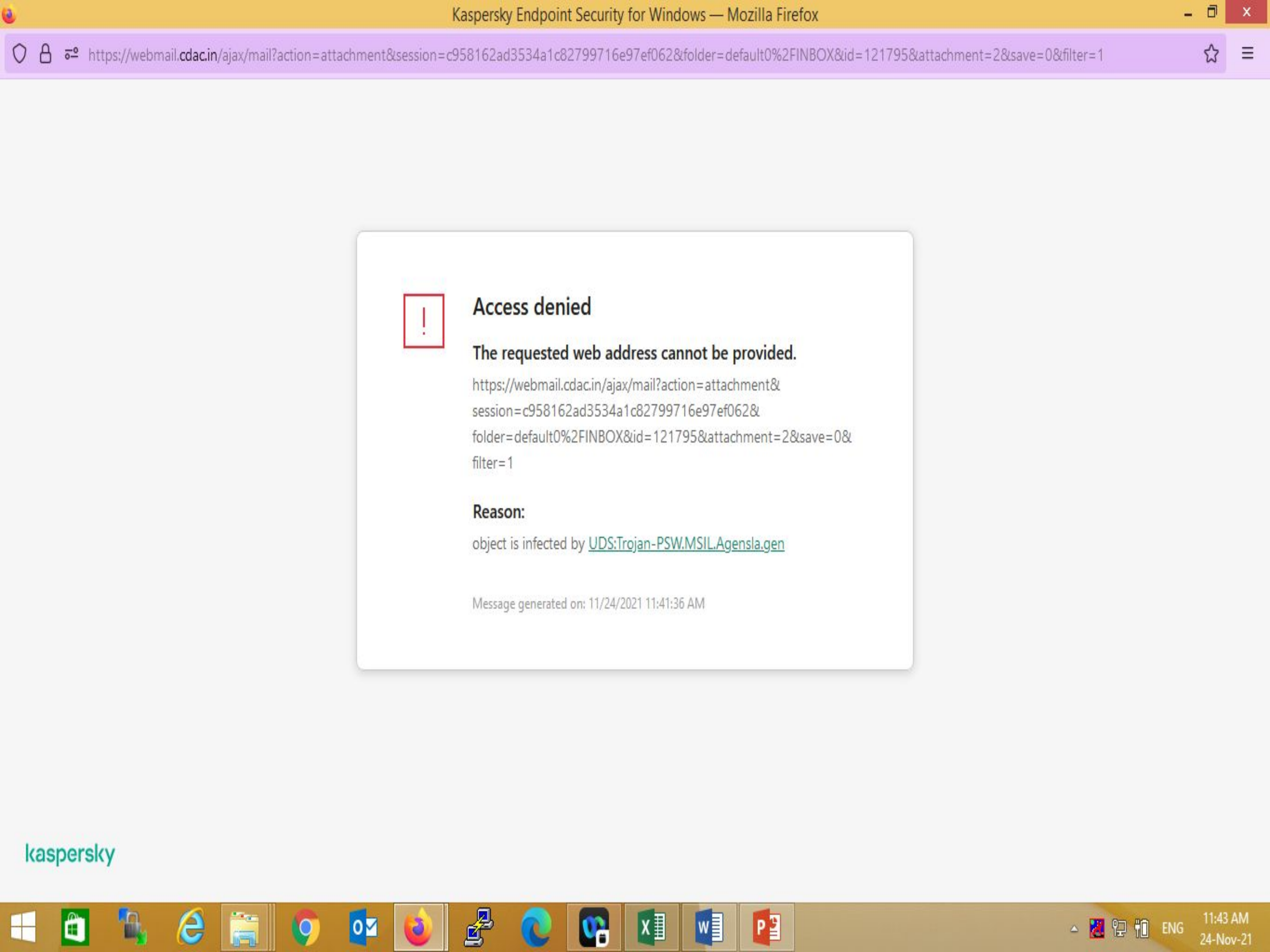
Dear Customer,

Your parcel has arrived at the office. our courier was unable to deliver it to your address due to wrong address provided by our customer.
To receive your parcel, please go to any of our nearest office and show this receipt.

CLICK ON THE ATTACHMENT TO DOWNLOAD AND PRINT THE RECEIPT.

Best Regards,

The DHL Team


Kaspersky Endpoint Security for Windows — Mozilla Firefox
https://webmail.cdac.in/ajax/mail?action=attachment&session=c958162ad3534a1c82799716e97ef062&folder=default0%2FINBOX&id=121795&attachment=2&save=0&filter=1

Access denied

The requested web address cannot be provided.

https://webmail.cdac.in/ajax/mail?action=attachment&
session=c958162ad3534a1c82799716e97ef062&
folder=default0%2FINBOX&id=121795&attachment=2&save=0&
filter=1

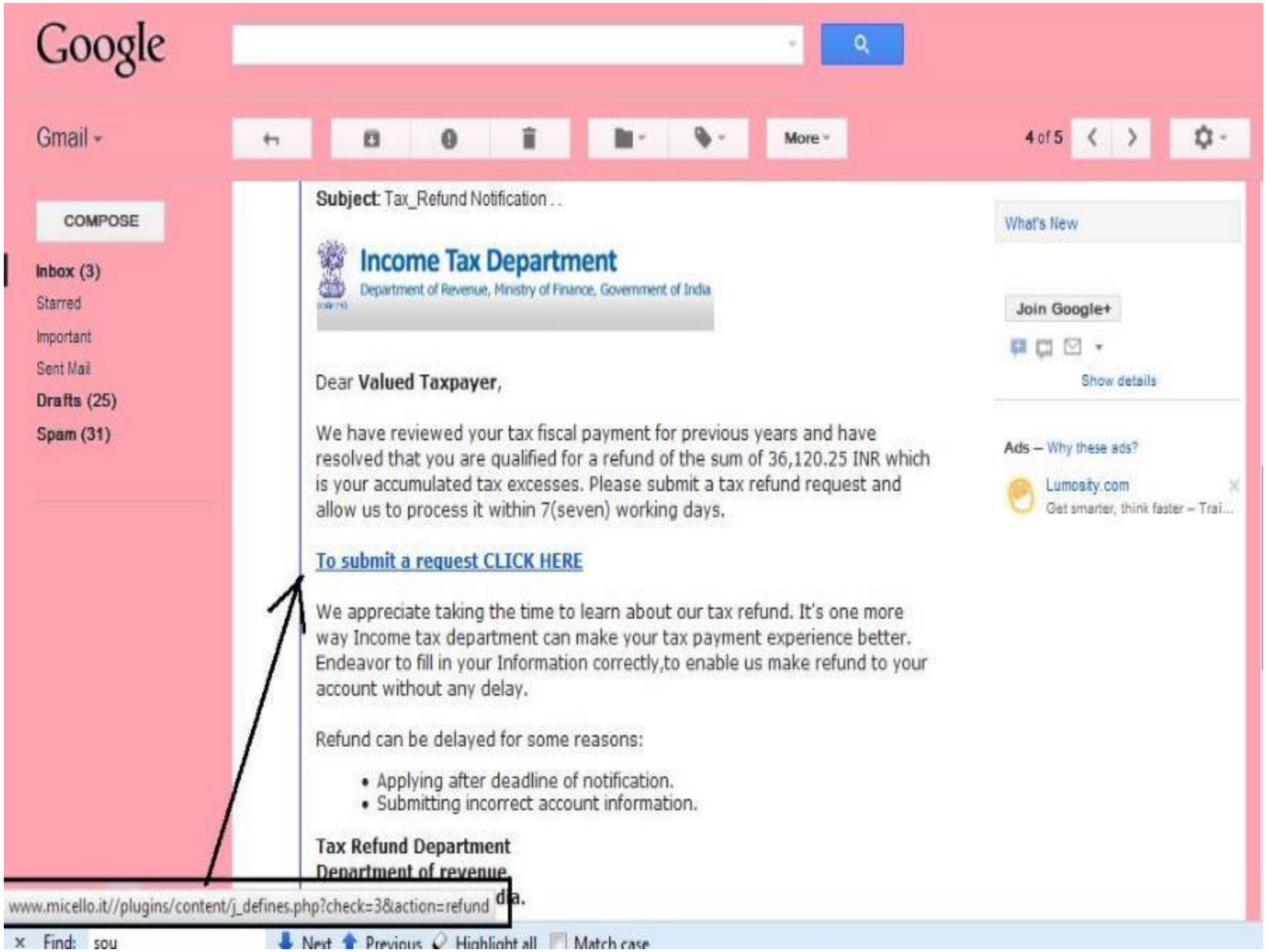
Reason:

object is infected by UDS:Trojan-PSW.MSIL.Agensla.gen

Message generated on: 11/24/2021 11:41:36 AM

kaspersky
ENG
11:43 AM
24-Nov-21

Example of Phishing e-Mail



Subject: Tax_Refund Notification . .

Income Tax Department

Department of Revenue, Ministry of Finance, Government of India

Dear **Valued Taxpayer**,

We have reviewed your tax fiscal payment for previous years and have resolved that you are qualified for a refund of the sum of 36,120.25 INR which is your accumulated tax excesses. Please submit a tax refund request and allow us to process it within 7(seven) working days.

To submit a request CLICK HERE

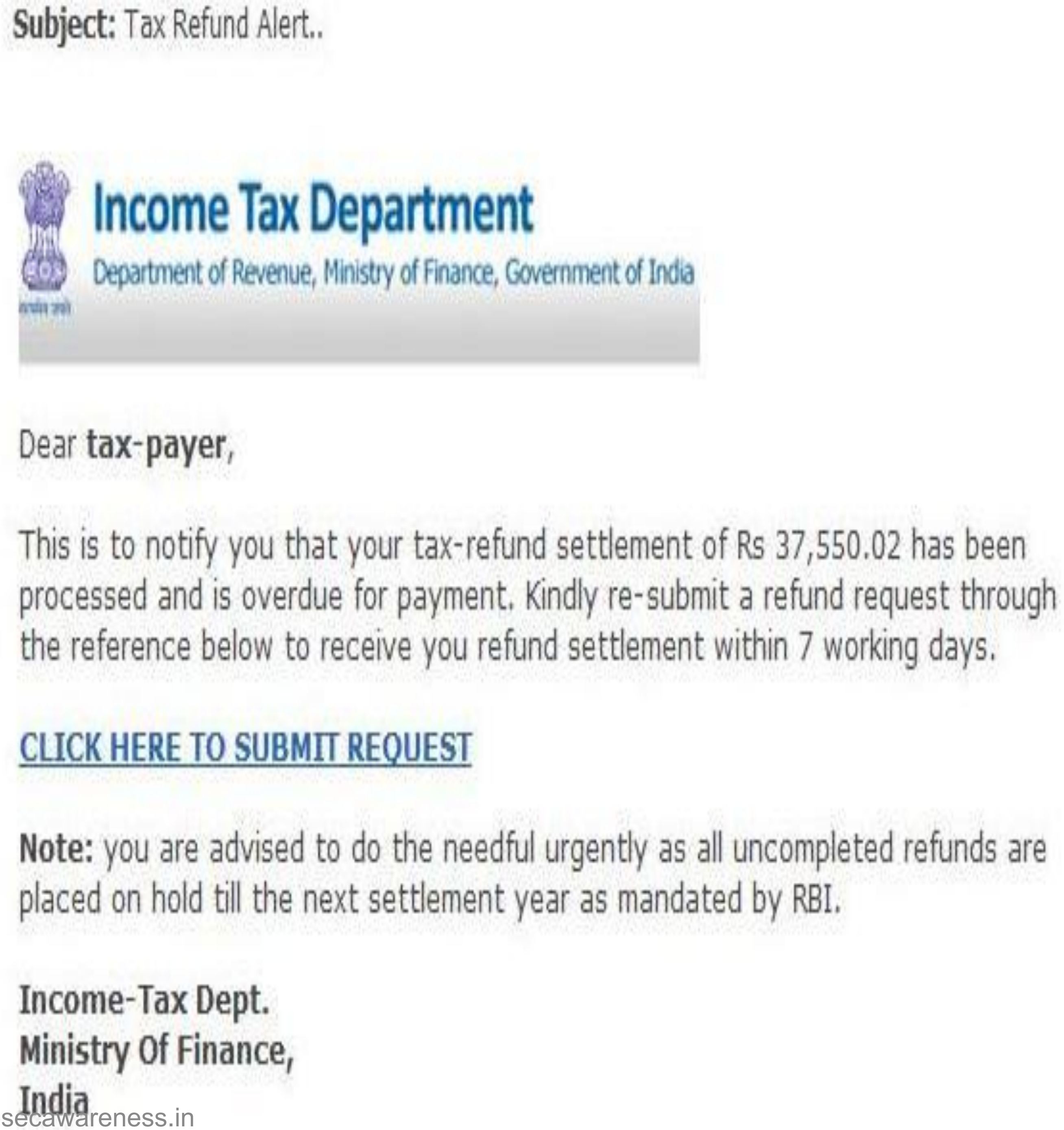
We appreciate taking the time to learn about our tax refund. It's one more way Income tax department can make your tax payment experience better. Endeavor to fill in your Information correctly,to enable us make refund to your account without any delay.

Refund can be delayed for some reasons:

- Applying after deadline of notification.
- Submitting incorrect account information.

Tax Refund Department
Department of revenue
dia.

www.micello.it//plugins/content/j_defines.php?check=3&action=refund



Subject: Tax Refund Alert..

Income Tax Department

Department of Revenue, Ministry of Finance, Government of India

Dear **tax-payer,**

This is to notify you that your tax-refund settlement of Rs 37,550.02 has been processed and is overdue for payment. Kindly re-submit a refund request through the reference below to receive you refund settlement within 7 working days.

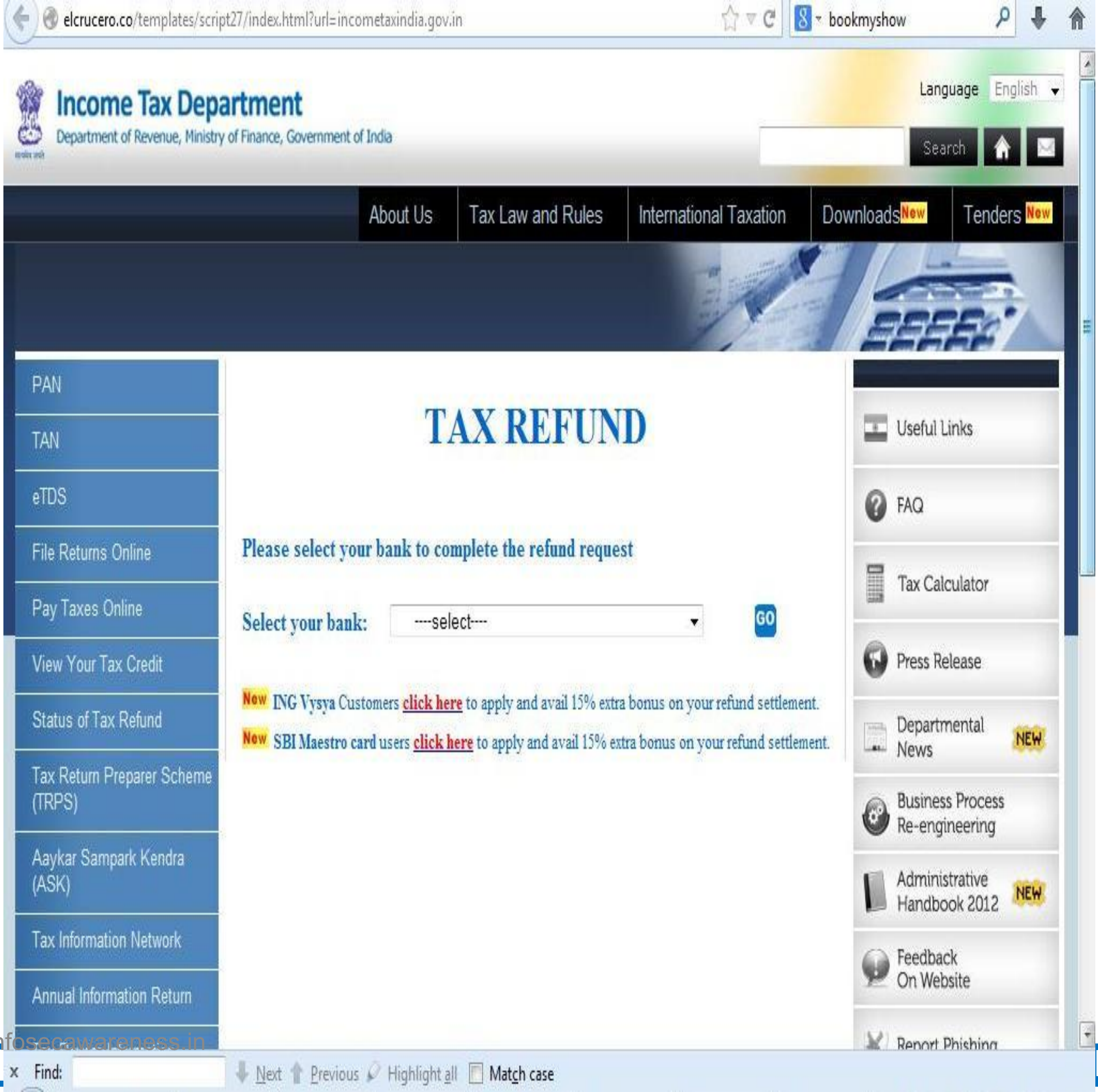
CLICK HERE TO SUBMIT REQUEST

Note: you are advised to do the needful urgently as all uncompleted refunds are placed on hold till the next settlement year as mandated by RBI.

Income-Tax Dept.
Ministry Of Finance,
India

www.isea.gov.in

www.InfoSec awareness.in



elcrucero.co/templates/script27/index.html?url=incometaxindia.gov.in

Income Tax Department

Department of Revenue, Ministry of Finance, Government of India

TAX REFUND

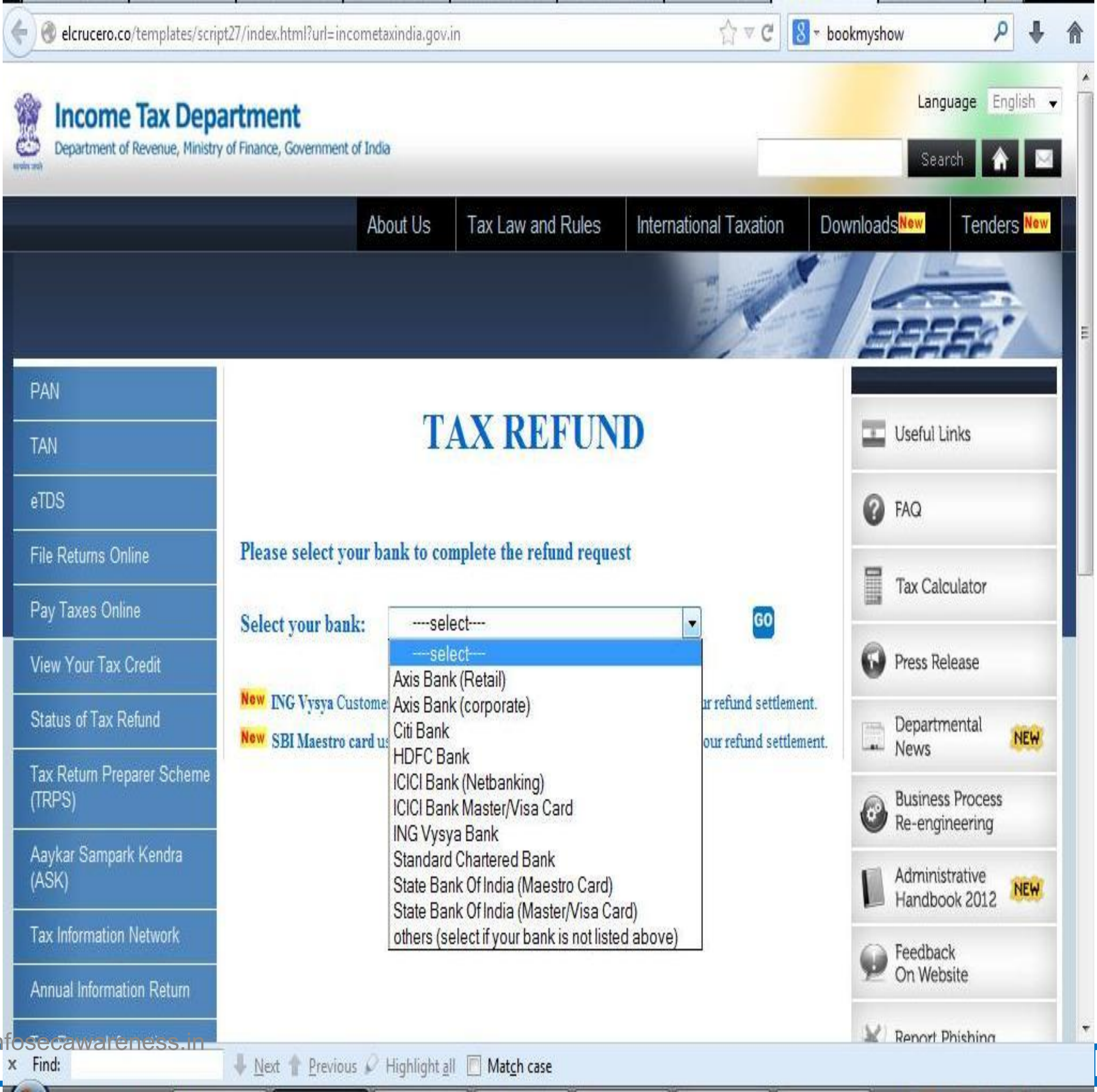
Please select your bank to complete the refund request

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.

No. 1800 4



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 … r refund settlement.

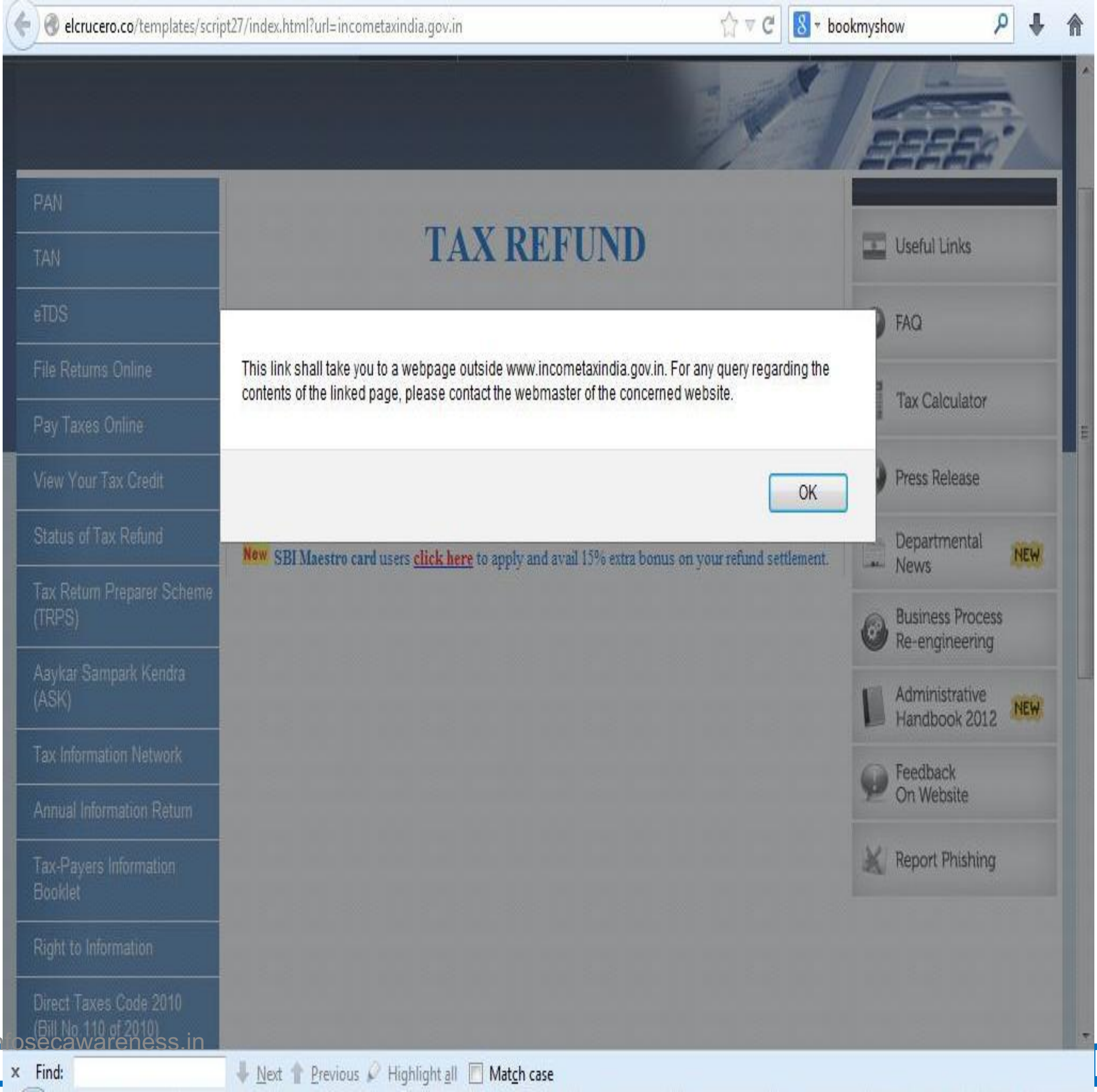
New SBI Maestro card us … our refund settlement.

- 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 Previous Highlight all □ Match case

www.isea.gov.in

www.InfoSec awareness.in


elcrucero.co/templates/script27/index.html?url=incometaxindia.gov.in

TAX REFUND

This link shall take you to a webpage outside www.incometaxindia.gov.in. For any query regarding the contents of the linked page, please contact the webmaster of the concerned website.

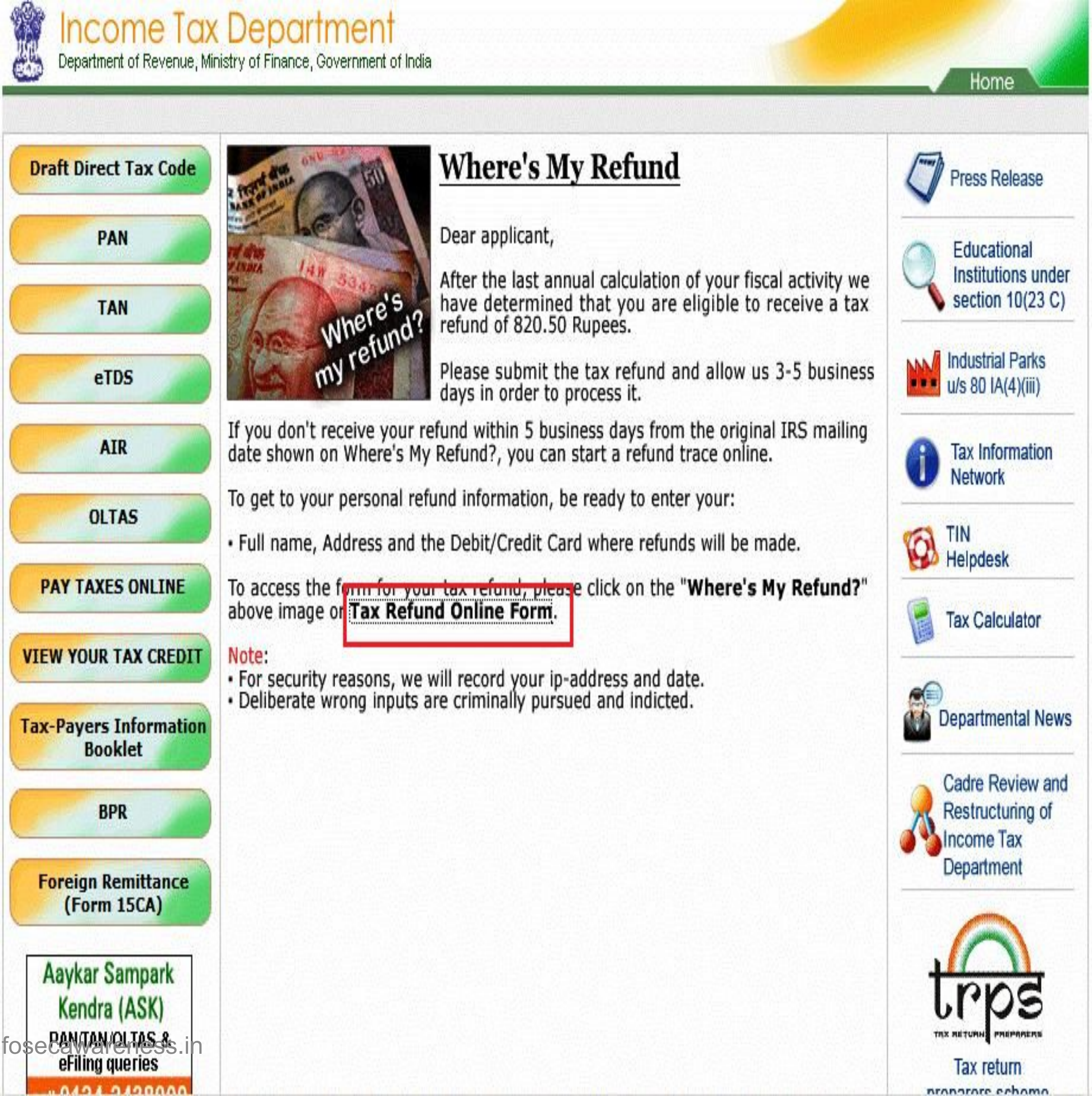
OK

New SBI Maestro card users click here to apply and avail 15% extra bonus on your refund settlement.

No. 1800 4

www.isea.gov.in

www.InfoSecawareness.in


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
Where's my refund?
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 preparers scheme

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.

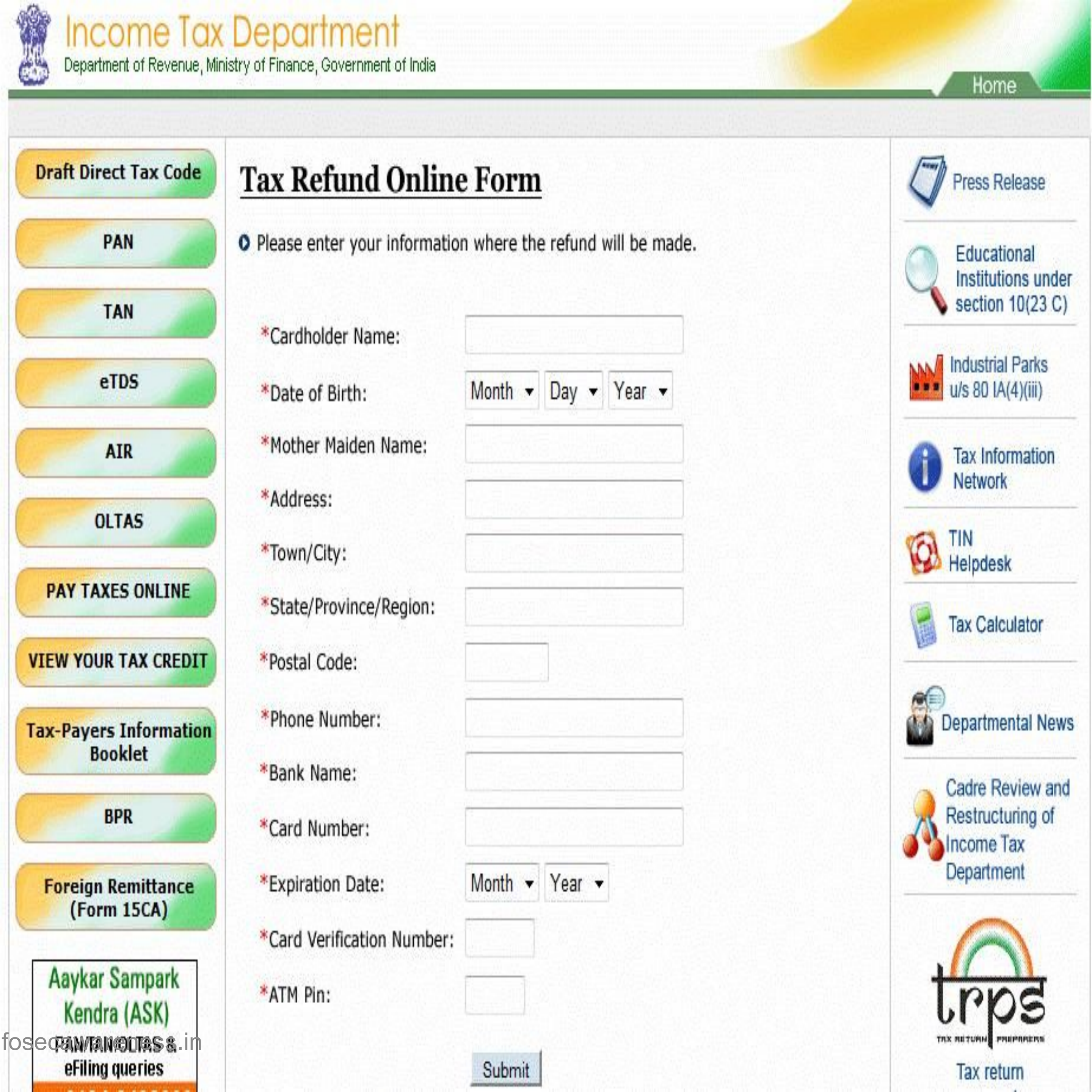
To access the form for your tax refund, please click on the "**Where's My Refund?**" above image or **Tax Refund Online Form**.

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

No. 1800 4

www.isea.gov.in

www.InfoSecawareness.in



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
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

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:

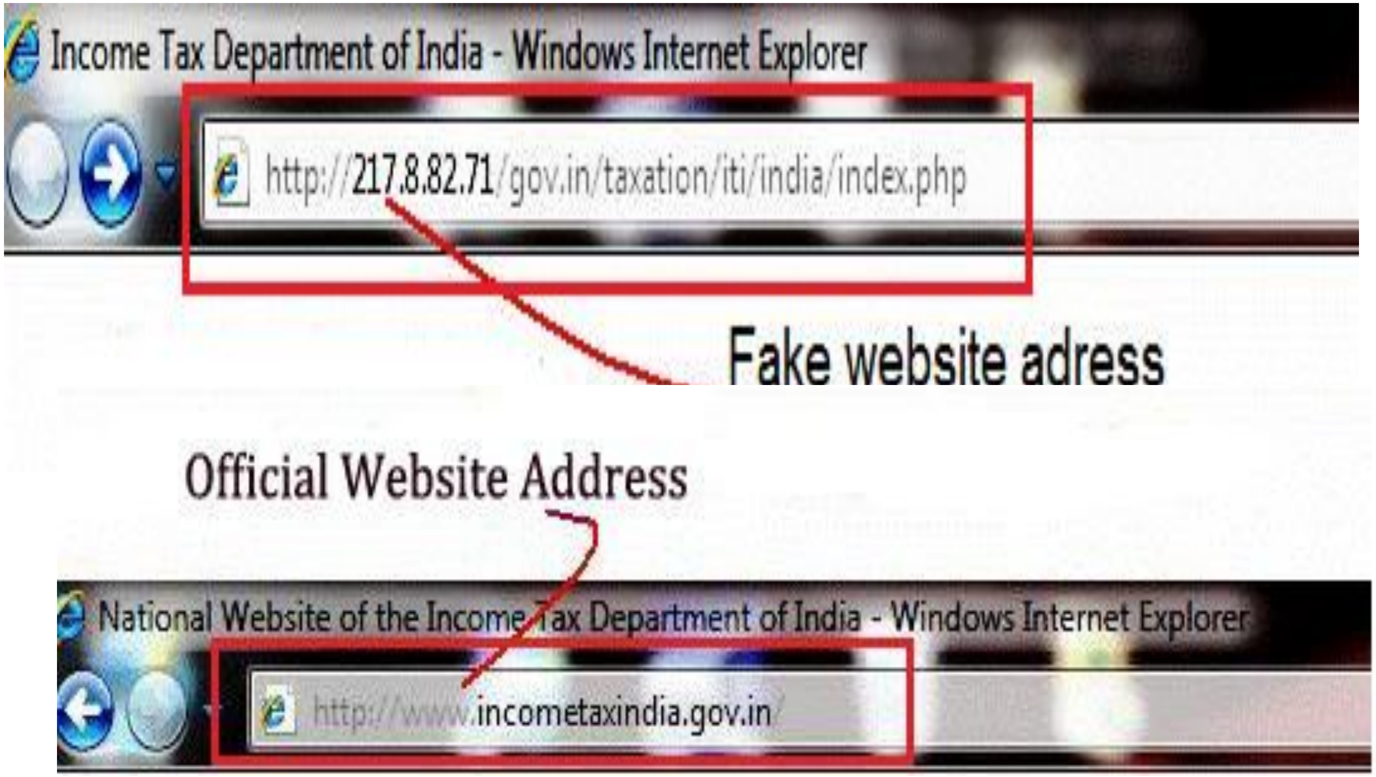
Submit

No. 1800 4

www.isea.gov.in

How to recognize??

www.InfoSec awareness.in



Income Tax Department of India - Windows Internet Explorer

http://217.8.82.71/gov.in/taxation/iti/india/index.php

Fake website adress

Official Website Address

National Website of the Income Tax Department of India - Windows Internet Explorer

http://www.incometaxindia.gov.in/

Vishing & Smishing

Vishing - Phone calls made by fraudsters to steal your personal information and sensitive information

- they communicate

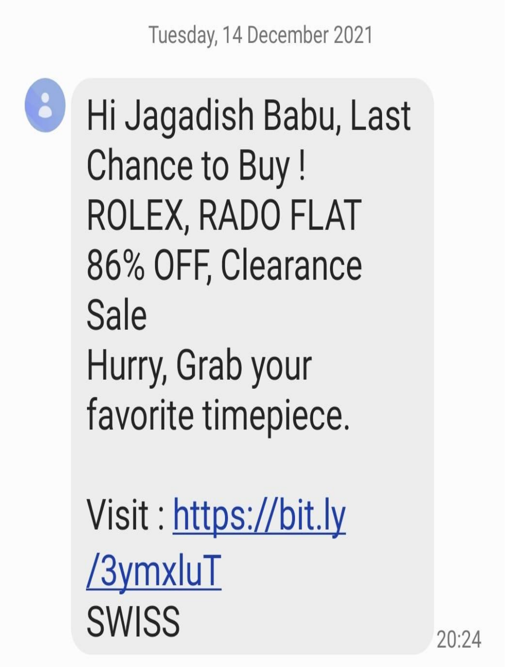
- as bank officer
- referring your shopping

OR

you may land up callin phishing number

through search engines

Vishing & Smishing

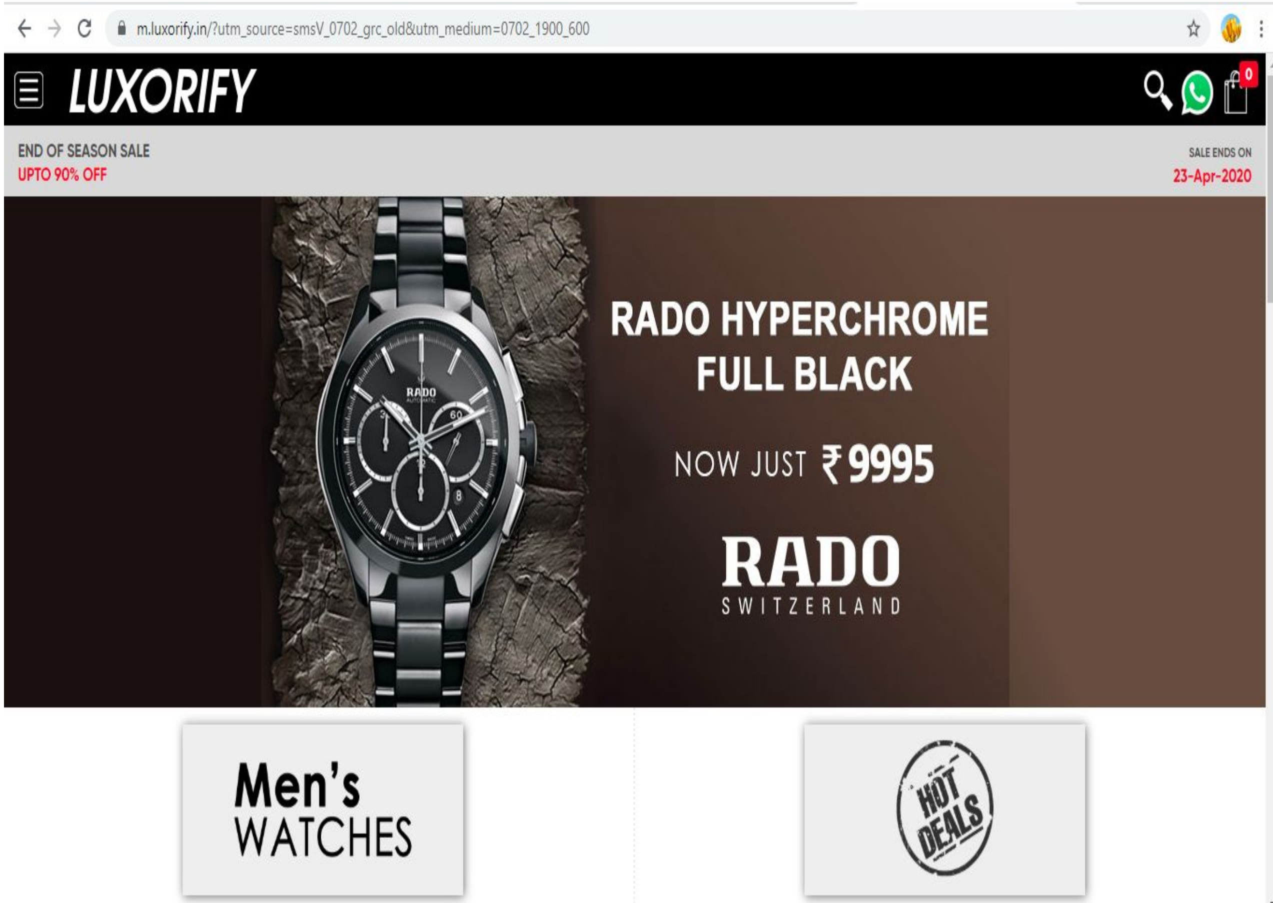


Tuesday, 14 December 2021

Hi Jagadish Babu, Last Chance to Buy !
ROLEX, RADO FLAT 86% OFF, Clearance Sale
Hurry, Grab your favorite timepiece.

Visit : https://bit.ly/3ymxluT
SWISS

20:24



m.luxorify.in/?utm_source=smsV_0702_grc_old&utm_medium=0702_1900_600

LUXORIFY

END OF SEASON SALE
UPTO 90% OFF

SALE ENDS ON
23-Apr-2020

RADO HYPERCHROME FULL BLACK
NOW JUST ₹9995
RADO
SWITZERLAND

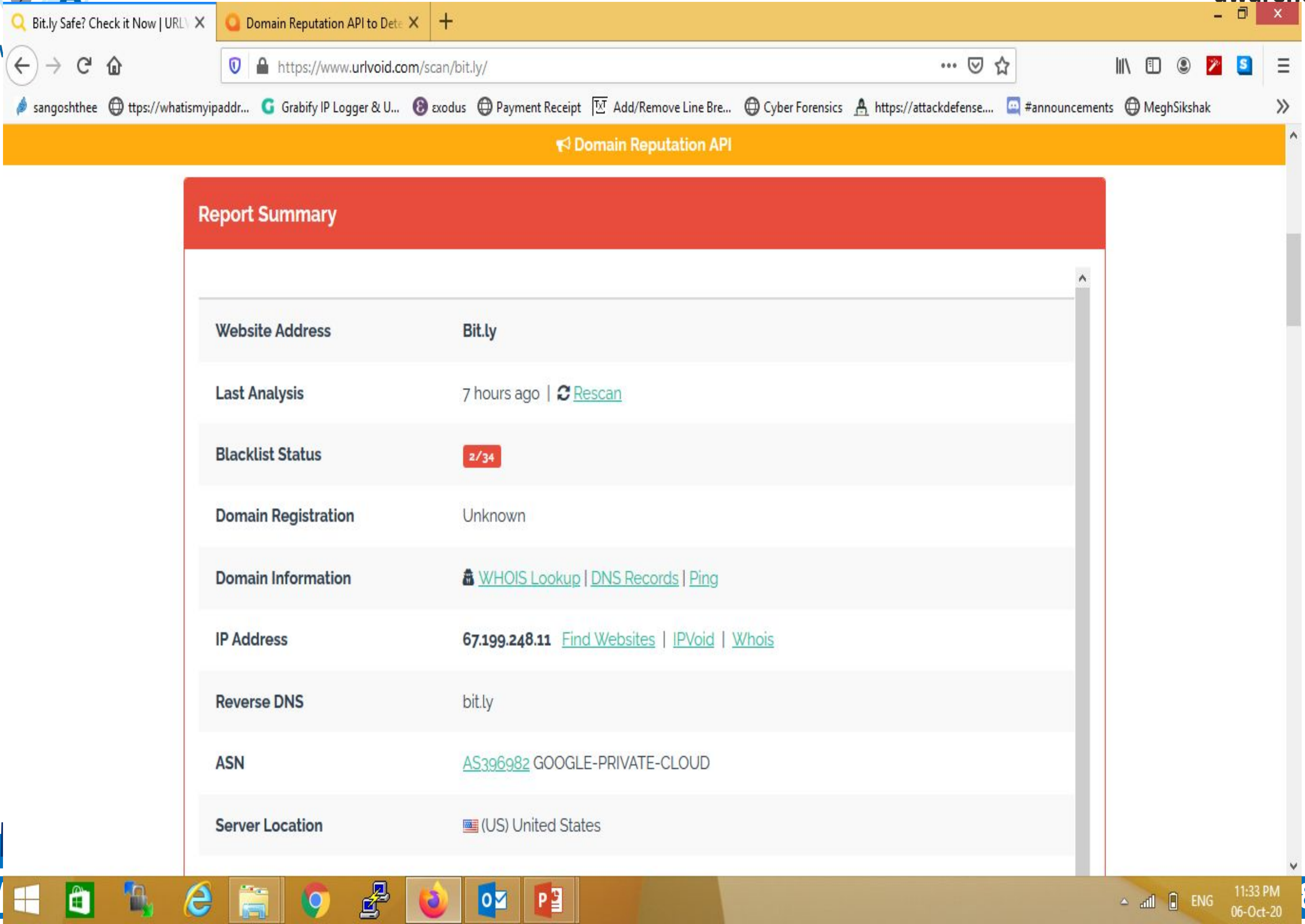
Men's WATCHES

HOT DEALS

Hi Jagadish Babu, Last Chance to Buy !ROLEX, RADO FLAT 86% OFF, Clearance SaleHurry, Grab your favorite timepiece.Visit :

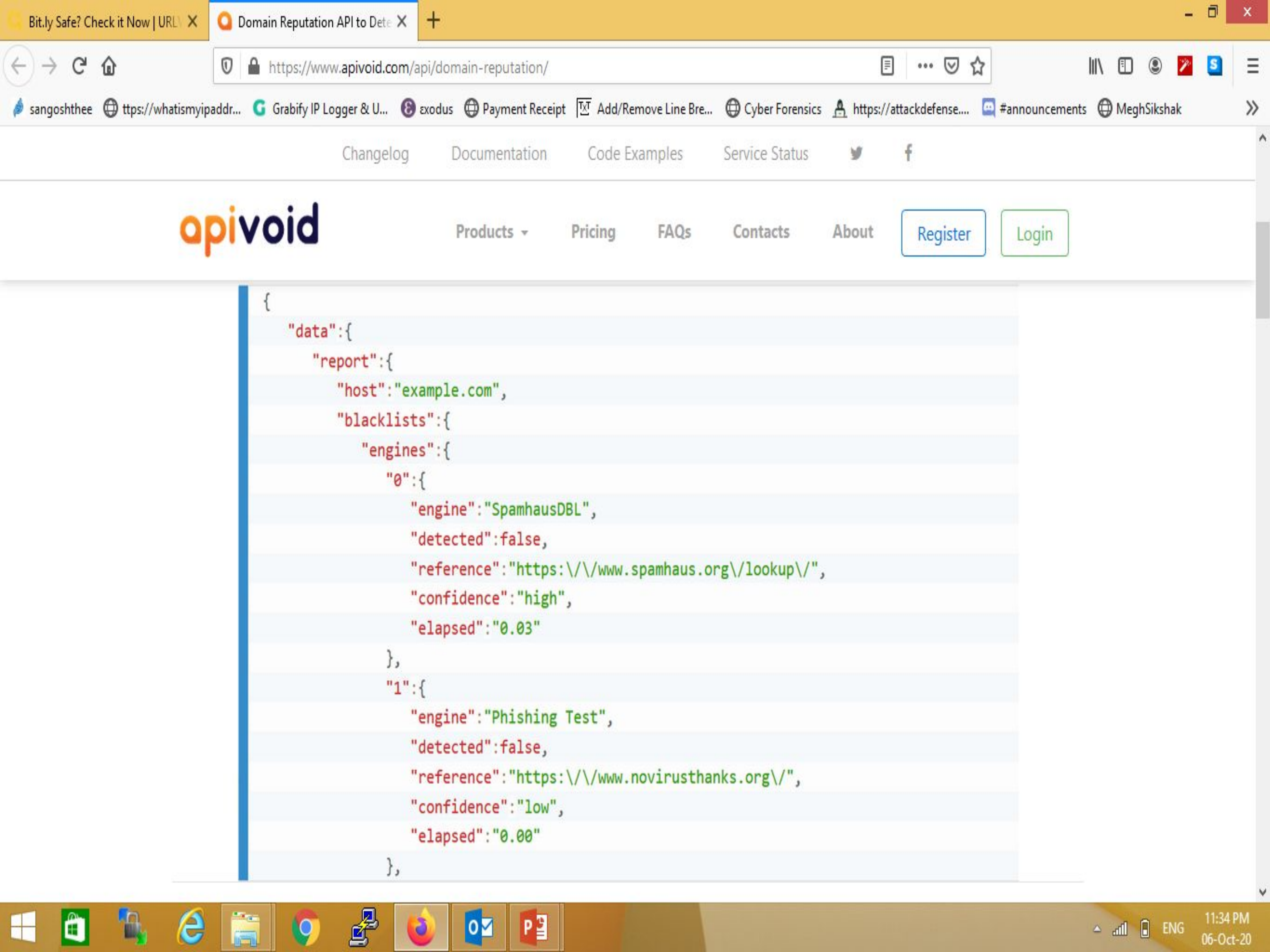
https://bit.ly/3ymxluTSWISS

www.InfoSecawareness.in



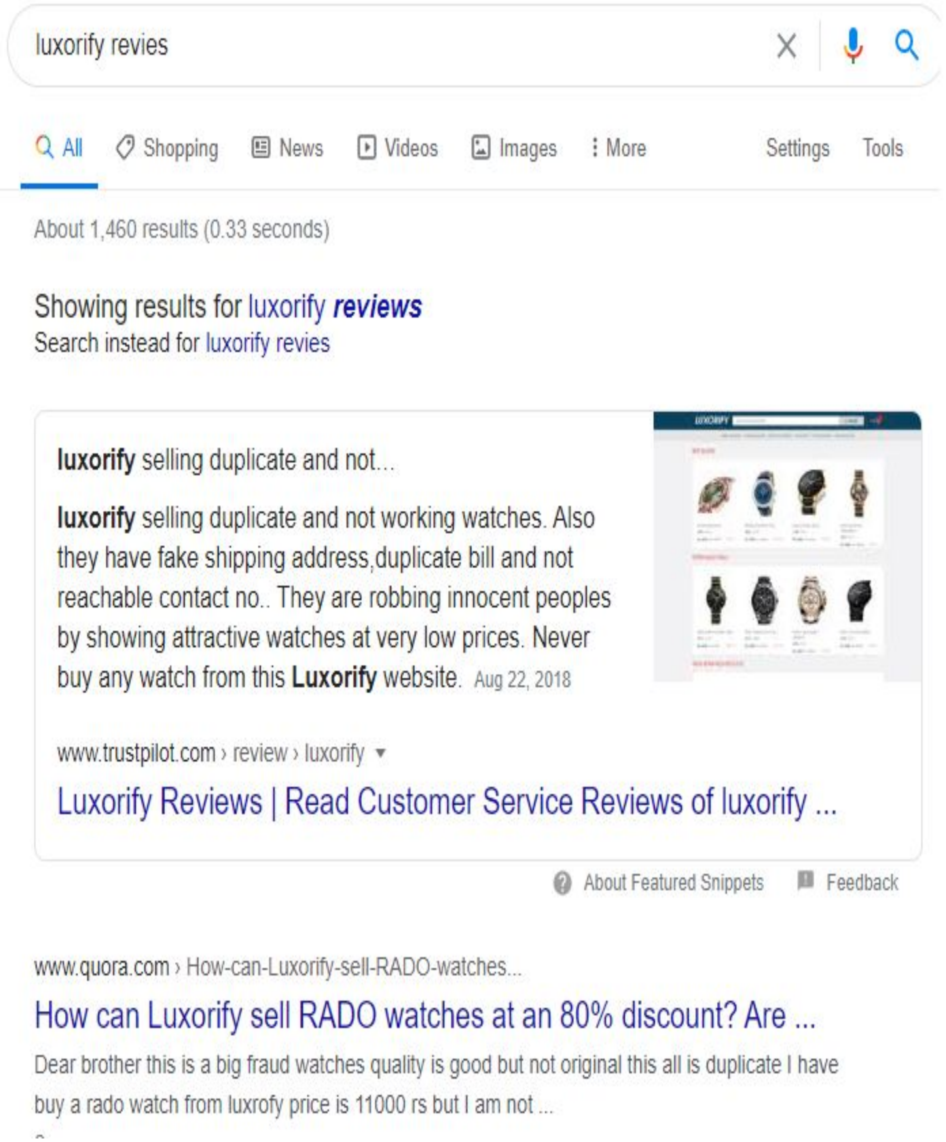
Report Summary

Website Address	Bit.ly
Last Analysis	7 hours ago | Rescan
Blacklist Status	2/34
Domain Registration	Unknown
Domain Information	WHOIS Lookup | DNS Records | Ping
IP Address	67.199.248.11 Find Websites | IPVoid | Whois
Reverse DNS	bit.ly
ASN	AS396982 GOOGLE-PRIVATE-CLOUD
Server Location	(US) United States



```
{
  "data":{
    "report":{
      "host":"example.com",
      "blacklists":{
        "engines":{
          "0":{
            "engine":"SpamhausDBL",
            "detected":false,
            "reference":"https:\/\/www.spamhaus.org\/lookup\/",
            "confidence":"high",
            "elapsed":"0.03"
          },
          "1":{
            "engine":"Phishing Test",
            "detected":false,
            "reference":"https:\/\/www.novirusthanks.org\/",
            "confidence":"low",
            "elapsed":"0.00"
          },
```

Check on Reviews ...



About 1,460 results (0.33 seconds)

Showing results for luxorify ***reviews***
Search instead for luxorify revies

luxorify selling duplicate and not...

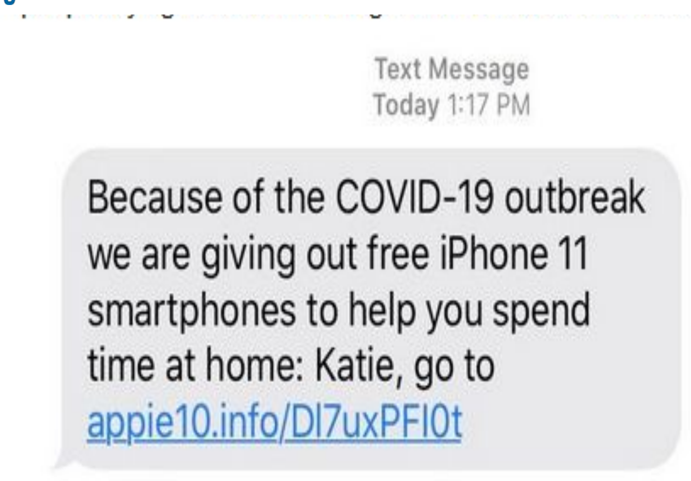
luxorify selling duplicate and not working watches. Also they have fake shipping address,duplicate bill and not reachable contact no.. They are robbing innocent peoples by showing attractive watches at very low prices. Never buy any watch from this **Luxorify** website. Aug 22, 2018

www.trustpilot.com › review › luxorify ▾
Luxorify Reviews | Read Customer Service Reviews of luxorify ...

www.quora.com › How-can-Luxorify-sell-RADO-watches...
How can Luxorify sell RADO watches at an 80% discount? Are ...

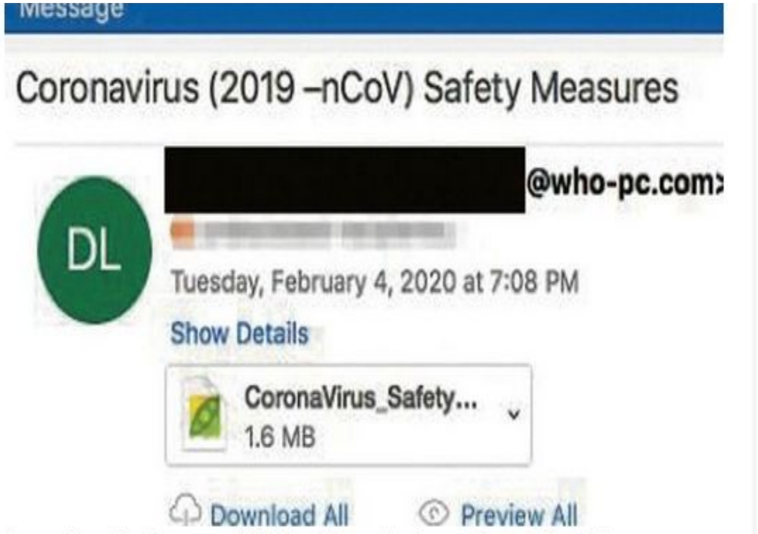
Dear brother this is a big fraud watches quality is good but not original this all is duplicate I have buy a rado watch from luxrofy price is 11000 rs but I am not ...

Another Example for smishing



Text Message
Today 1:17 PM

Because of the COVID-19 outbreak we are giving out free iPhone 11 smartphones to help you spend time at home: Katie, go to appie10.info/Dl7uxPFI0t



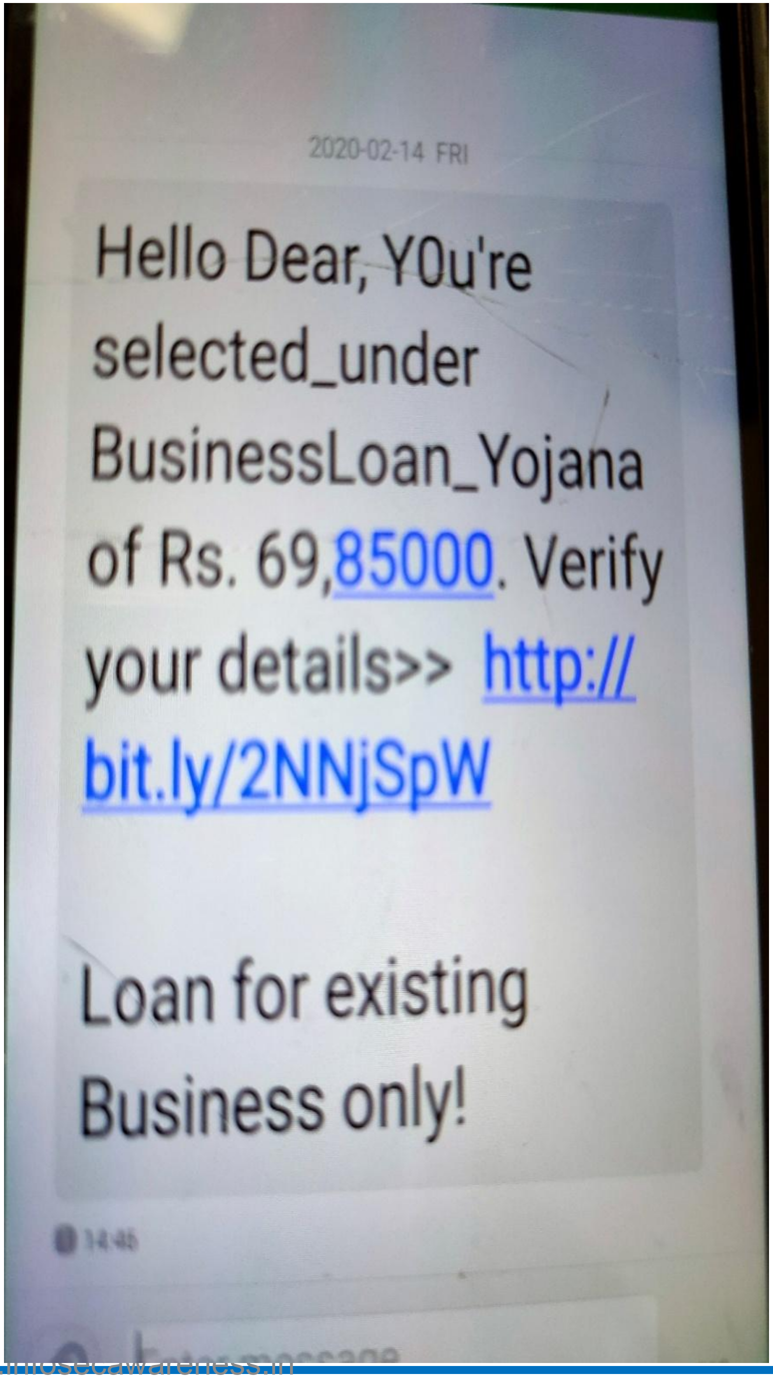
Message

Coronavirus (2019 –nCoV) Safety Measures

DL [redacted]@who-pc.com>

Tuesday, February 4, 2020 at 7:08 PM

An email sent in the name of WHO with an attachment that will install the AgentTesla Keylogger to record all keystrokes and send them to attackers. (Proofpoint)

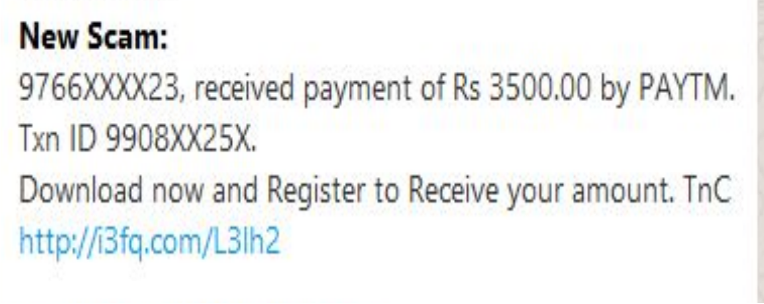


2020-02-14 FRI

Hello Dear, Y0u're selected_under BusinessLoan_Yojana of Rs. 69,85000. Verify your details>> http://bit.ly/2NNjSpW

Loan for existing Business only!

14:46



New Scam:

9766XXXX23, received payment of Rs 3500.00 by PAYTM. Txn ID 9908XX25X.

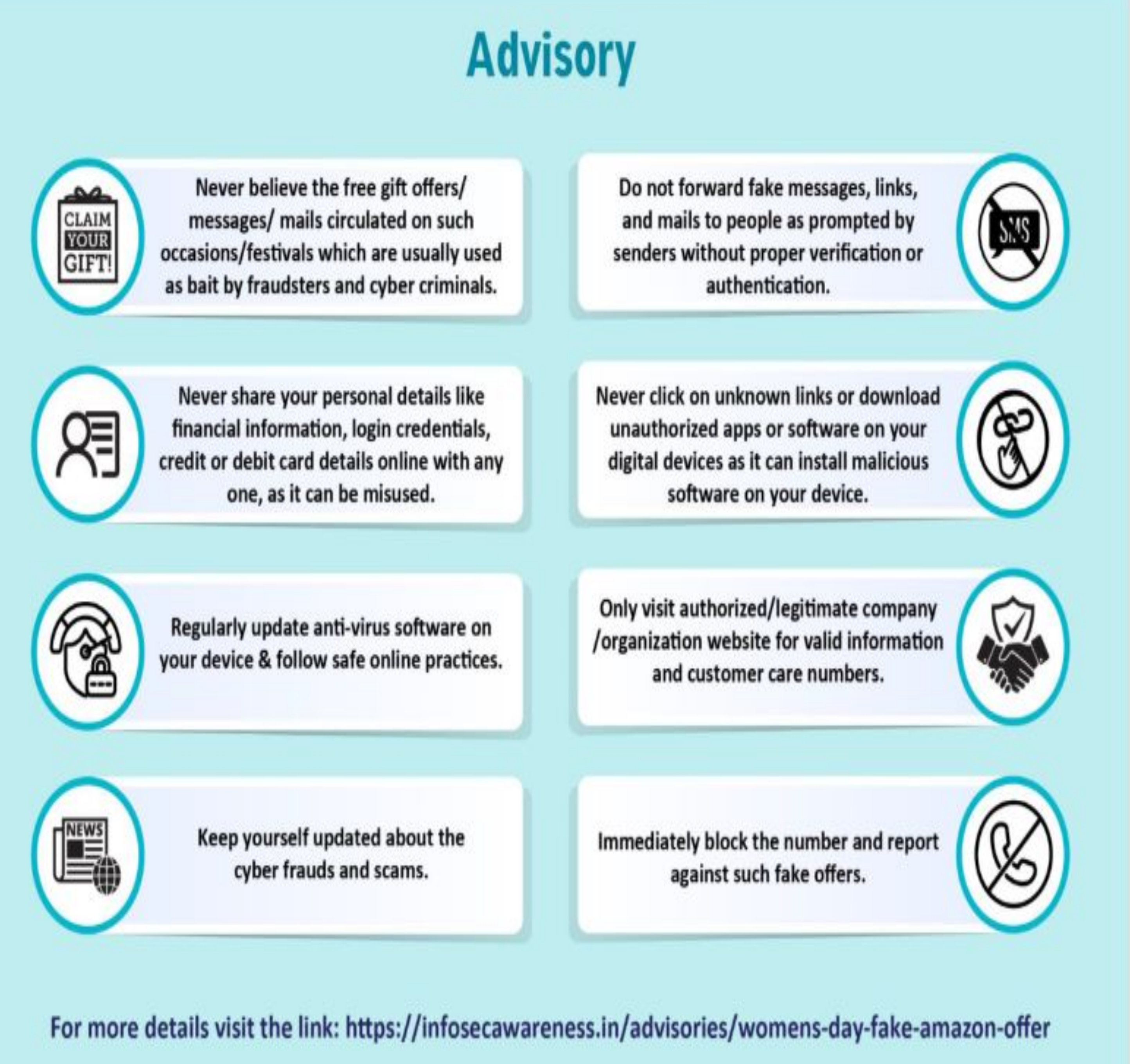
Download now and Register to Receive your amount. TnC http://i3fq.com/L3lh2

Tips to avoid Vishing & Smishing

- Never reveal any information over phone calls
- Call the original company like bank, shopping toll free and enquire about the calll received
- Avoid picking calls from unknown numbers
- Never respond to sms recevied from unknowns
- Avoid clicking links received on sms

www.isea.gov.in

www.InfoSecawareness.in



Advisory

CLAIM YOUR GIFT!

Never believe the free gift offers/ messages/ mails circulated on such occasions/festivals which are usually used as bait by fraudsters and cyber criminals.

Do not forward fake messages, links, and mails to people as prompted by senders without proper verification or authentication.

SMS

Never share your personal details like financial information, login credentials, credit or debit card details online with any one, as it can be misused.

Never click on unknown links or download unauthorized apps or software on your digital devices as it can install malicious software on your device.

Regularly update anti-virus software on your device & follow safe online practices.

Only visit authorized/legitimate company /organization website for valid information and customer care numbers.

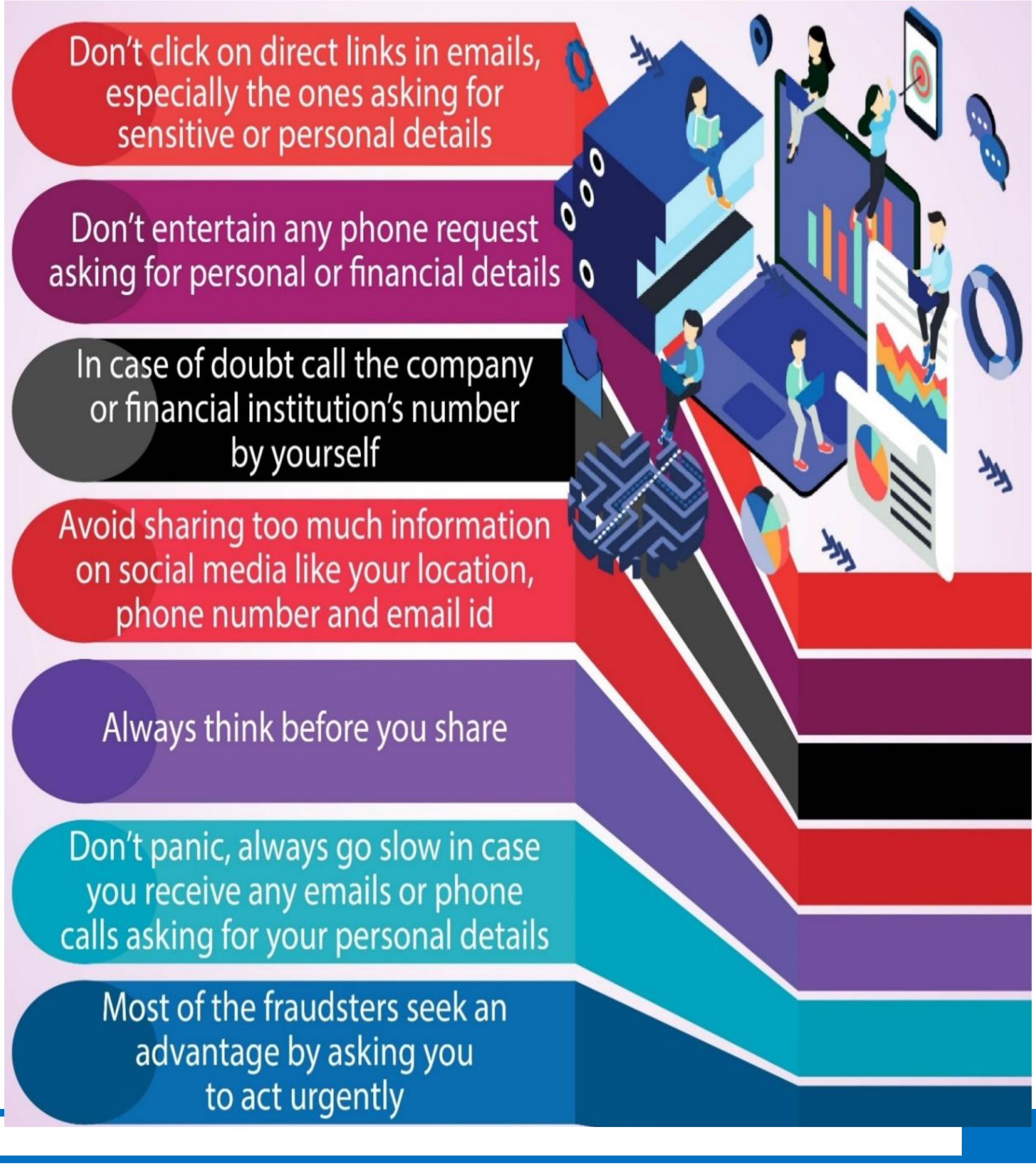
NEWS

Keep yourself updated about the cyber frauds and scams.

Immediately block the number and report against such fake offers.

For more details visit the link: https://infosecawareness.in/advisories/womens-day-fake-amazon-offer

Tips to Stay Safe



Don't click on direct links in emails, especially the ones asking for sensitive or personal details

Don't entertain any phone request asking for personal or financial details

In case of doubt call the company or financial institution's number by yourself

Avoid sharing too much information on social media like your location, phone number and email id

Always think before you share

Don't panic, always go slow in case you receive any emails or phone calls asking for your personal details

Most of the fraudsters seek an advantage by asking you to act urgently

Protecting Yourself

A security aware culture can help employees identify and repel social engineering attacks

- Recognize inappropriate requests for information
- Take ownership for corporate security
- Understand risk and impact of security breeches
- Social engineering attacks are personal
- Password management
- Two factor authentication
- Physical security
- Understand what information you are putting on the Web for targeting at social network sites

Google
MySpace
Personal Blogs
Twitter
Facebook
LinkedIn

Protecting Yourself

1. Network defenses to repel virus
   - Virus protection (McAfee, Norton, Symantec, etc…)
   - Email attachment scanning
   - Firewalls, etc…
2. Organizations must decide what information is sensitive
3. Security must be periodically tested
4. Contact your security office immediately if you have any concerns at work

Safety Tips

1) Use antivirus software (AVAST, AVG…..)
2) Insert firewalls , pop up blocker (Windows, Comodo)
3) Uninstall unnecessary software (Adwares)
4) Maintain backup (Weekly/Monthly)
5) Use secure connection (HTTPS)
6) Open attachments carefully
7) Use strong passwords , don't give personal information unless required.

FREE AVAST ANTIVIRUS FOR ONE YEAR –

https://www.avast.com/registration-free-antivirus.php

Any Enquiry

karanpreet@cdac.in

THANK YOU