

Social Engineering Attacks and Security Measures



CIET, NCERT

Leading a Secured Digital Life.....



Information Security
Education & Awareness
Project Phase - II

M Jagadish Babu ,
Project Manager - ISEA,
C-DAC, Hyderabad

PURPOSE OF ISEA



Information Security Education & Awareness

Ministry of Electronics and Information Technology
Ministry of Communications and Information Technology
Government of India

- Generation of Core Research manpower
 - Formal, Non Formal Courses
 - Faculty Training
 - Short term/Specialized courses for Professionals
- Training for Government Personnel
- Awareness Campaign

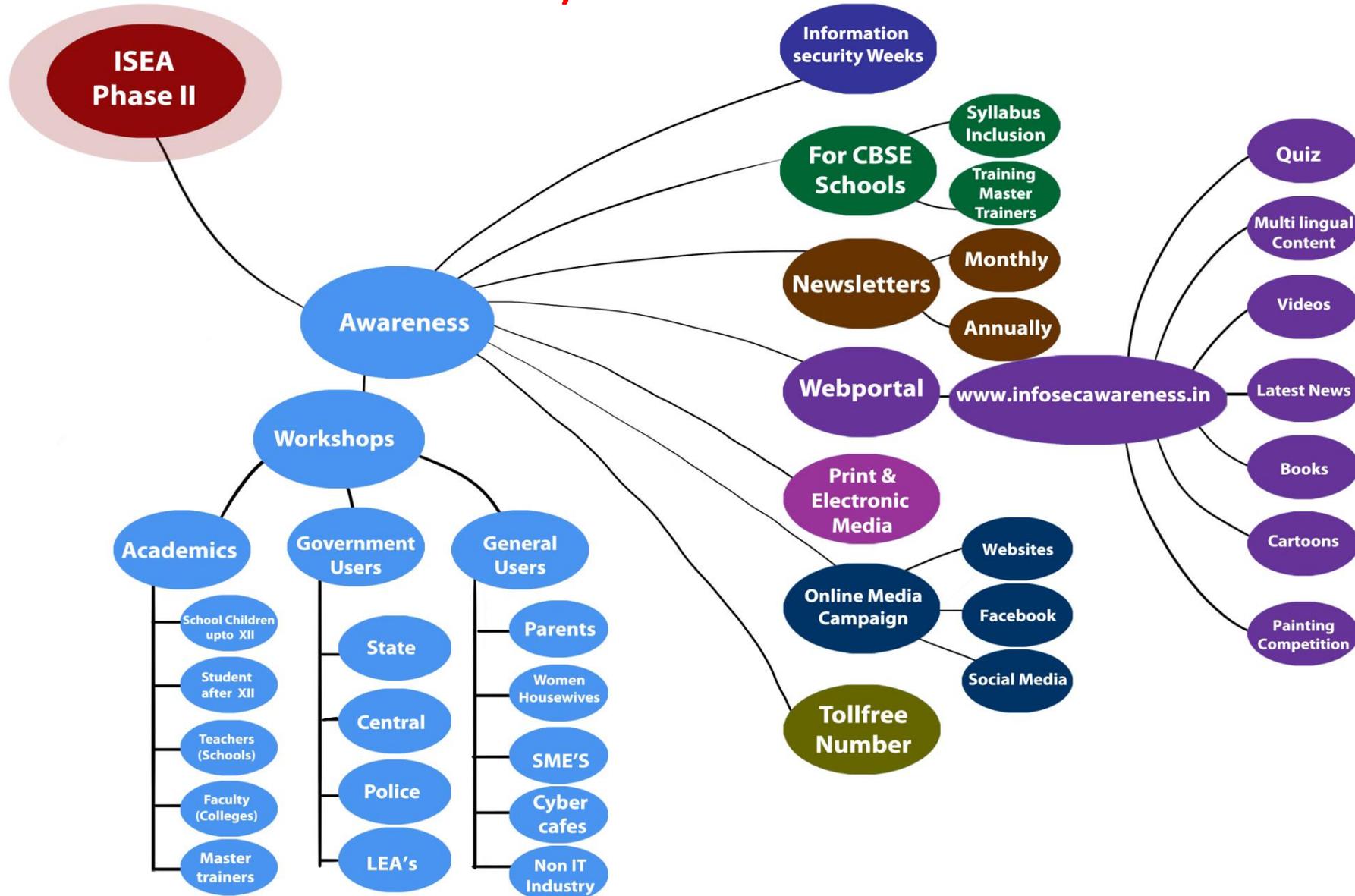
Implementation Structure

Area	Category	No's	Description
Academic	ISRDCs	4	IISc. Bangalore, IIT – Bombay, Madras, Guwahati
	RCs	7	IIT-Roorkee, Kharagpur ; NIT-Jaipur, Surathkal, Rourkela, Surat, Warangal
	PIs		
	Category I	23	10 NITs, 5 IIITs, 2 CoE, etc.
	Category II	13	13 CDAC & NIELIT Centres
	Category III (Special Category)	5	5 State Technical Universities -Gujarat, West Bengal, Tamil Nadu, Madhya Pradesh and Telangana
	Total	52	

Area	Category	No's	Description
GOT	Implementing Agencies	16	12 CDAC & NIELIT Centres, ERNET, NIC, CERT-In, STQC

Area	Category	No's	Description
Awareness	--	1	CDAC Hyderabad (through RCs, PIs, etc.)

Delivery Mechanism



2021 This Is What Happens In An Internet Minute



Created By:
@LoriLewis
@OfficiallyChadd



www.isea.gov.in



www.isea.gov.in

Ten human negligence errors that can cause threat to any workplace:



www.
InfoSec
awareness.in



www.
InfoSec
awareness.in



Nature of crime

www.isea.gov.in

www.
InfoSec
awareness.in

1. Fake online sites on the pretext of supplying food, medicine, oxygen & other essentials
2. Luring people into online transactions & hacking accounts
3. Creating fake social media accounts of influential officers, deceiving public using their names
4. Filming & circulating pornographic material online/blackmailing by threatening to share images of intimate moments

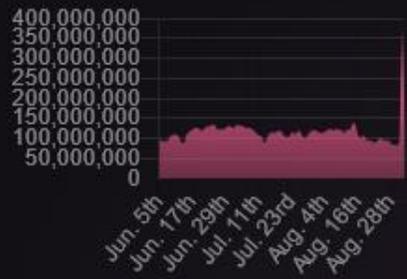


LIVE CYBER THREAT MAP

86,543,181 ATTACKS ON THIS DAY

**DON'T WAIT TO BE ATTACKED
PREVENTION STARTS NOW >**

RECENT DAILY ATTACKS



TOP TARGETED COUNTRIES

Highest rate of attacks per organization in the last day.

- Mongolia
- Nepal
- Indonesia
- Bolivia
- Nigeria

TOP TARGETED INDUSTRIES

Highest rate of attacks per organization in the last day.

- Education
- Government
- ISP/MSP

TOP MALWARE TYPES

Malware types with the highest global

ATTACKS Current rate 4

- Content Protection Violation
09:50:43 United States → CA, United States
- Content Protection Violation
09:50:43 United States → NC, United States
- Content Protection Violation
09:50:42 United States → NC, United States
- Content Protection Violation
09:50:42 United States → Netherlands
- Content Protection Violation
09:50:42 United States → Philippines

Source : <https://threatmap.checkpoint.com>

Toll Free No. 1800 425 6235



www.isea.gov.in

Types of Social Engineering

Technical Social Engineering

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



Non-Technical

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

Click here to access SBI Internet Banking

<https://sbionline.com>

www.
InfoSec
awareness.in



<https://sbiOnline.in>



Toll Free No. 1800 425 6235

40% fell victim to a phishing attack in the past month

The global shift to remote work has exacerbated the onslaught, sophistication, and impact of phishing attacks, according to Ivanti. Nearly three-quarters (74%) of respondents said their organizations have fallen victim to a phishing attack in the last year, with 40% confirming they have experienced one in the last month.



Eighty percent of respondents said they have witnessed an increase in volume of phishing attempts and 85% said those attempts are getting more



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

www.isea.gov.in

www.
InfoSec
awareness.in

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 handing 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



www.isea.gov.in

[www.
InfoSec
awareness.in](http://www.InfoSecawareness.in)

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

Hello [redacted]ail.com, **Income Tax** Refund ALERT! I-T Department issues Rs 51,531 cr refund till 23 August 2021   Inbox x  



Income Tax Refund ALERT <info@e.decorx.in> [Unsubscribe](#)
to me ▾

Sep 1, 2021, 2:15 PM (2 days ago)   

[Dear](#) [redacted],

Income Tax Refund ALERT! I-T Department issues Rs 51,531 cr refund till 23 August 2021

Income tax refunds of Rs 14,835 crore have been issued in 2,170,134 cases and corporate **tax** refunds of Rs 36,696 crore have been issued in 128,870 cases.....[\[Read More Info\]](#)

For FY2021-22, ITD has issued refunds:: 

[FULL DETAILS](#)



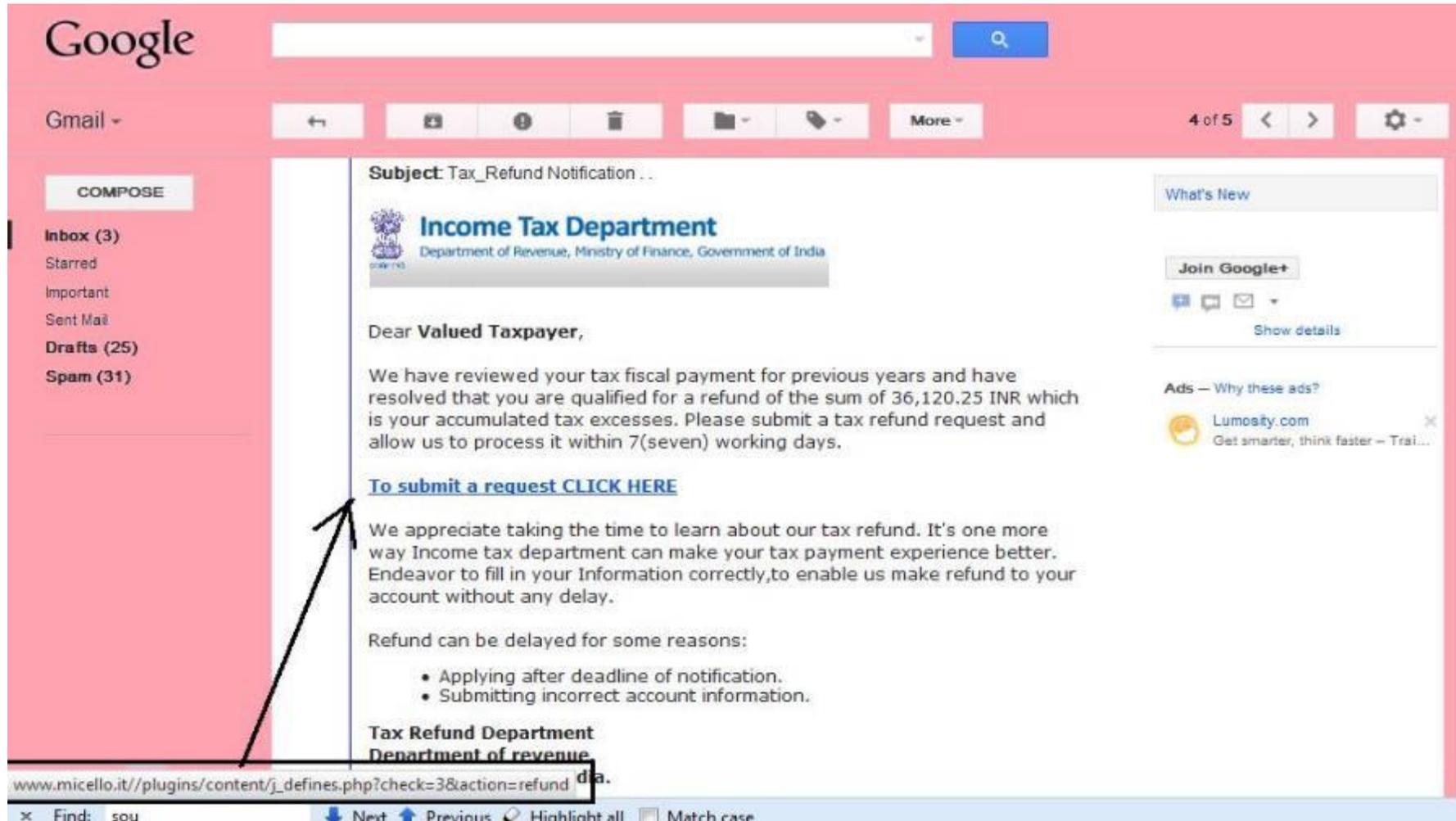
Phishing

- 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**



Example of Phishing e-Mail



Subject: Tax Refund Alert..



www.isea.gov.in

www.
InfoSec
awareness.in



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**



- 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:

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



Income Tax Department

Department of Revenue, Ministry of Finance, Government of India

Language English

Search [Home] [Email]

www.**InfoSec** awareness.in

- 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---
- 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)

GO

New ING Vysya Customer
New SBI Maestro card us

our refund settlement.
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



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.

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



www.isea.gov.in

Draft Direct Tax Code

PAN

TAN

eTDS

AIR

OLTAS

PAY TAXES ONLINE

VIEW YOUR TAX CREDIT

Tax-Payers Information Booklet

BPR

Foreign Remittance (Form 15CA)

Aaykar Sampark Kendra (ASK)
PAN/TAN/OLTAS & eFiling queries
☎ 0124-2438900



Where's My Refund

Dear applicant,

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

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

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

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

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

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

Note:

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



Press Release



Educational Institutions under section 10(23 C)



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



Tax Information Network



TIN Helpdesk



Tax Calculator



Departmental News



Cadre Review and Restructuring of Income Tax Department



Tax return preparers scheme

Draft Direct Tax Code

PAN

TAN

eTDS

AIR

OLTAS

PAY TAXES ONLINE

VIEW YOUR TAX CREDIT

Tax-Payers Information
Booklet

BPR

Foreign Remittance
(Form 15CA)

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

Tax Refund Online Form

Please enter your information where the refund will be made.

*Cardholder Name:

*Date of Birth: Month Day Year

*Mother Maiden Name:

*Address:

*Town/City:

*State/Province/Region:

*Postal Code:

*Phone Number:

*Bank Name:

*Card Number:

*Expiration Date: Month Year

*Card Verification Number:

*ATM Pin:

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



www.isea.gov.in

Another example of Phishing website for banking

https://csctrater.com.br/wp-content/plugins/sbi.html

SBI ONLINE | SBI Home Loan | About OnlineSBI | Forms | Net Banking Branches

Home | Products & Services | How Do I

Personal Banking

[CONTINUE TO LOGIN](#)

ALWAYS keep your computer free of malware	ALWAYS change your passwords periodically	NEVER respond to any communication seeking your passwords	NEVER reveal your passwords or card details to anyone
---	---	---	---

FOR YOUR OWN SECURITY

Please ensure the following before logging into OnlineSBI <ul style="list-style-type: none">→ The URL in your browser address bar begins with "https".→ The address or status bar displays the padlock symbol.→ Click the padlock to view and verify the security certificate.→ The address bar turns green indicating that the site is secured with an SSL Certificate that meets the Extended Validation Standard.→ (SSL is compatible for IE 7.0 and above, Mozilla Firefox 3.1 and above, Opera 9.5 and above, Safari 3.5 and above, Google Chrome).	Beware of Phishing attacks <ul style="list-style-type: none">→ Phishing is a fraudulent attempt, usually made through email, phone calls, SMS etc seeking your personal and confidential information.→ State Bank or any of its representative never sends you email/SMS or calls you over phone to get your personal information, password or one time SMS (high security) password. Any such e-mail/SMS or phone call is an attempt to fraudulently withdraw money from your account through Internet Banking. Never respond to such email/SMS or phone call. Please report immediately on report.phishing@sbi.co.in if you receive any such email/SMS or Phone call. Please lock your user access immediately, if you have accidentally revealed your credentials. Click here to lock.
---	---

By clicking on "Continue to Login" button, you agree to the Terms of Service (Terms & Conditions) of usage of Internet Banking of SBI. [CONTINUE TO LOGIN](#)

VeriSign | Privacy Statement | Disclosure | Terms of Service (Terms & Conditions)

© State Bank of India (APM Id: Serv_Tran_552) | Site best viewed at 1024 x 768 resolution in IE 10 +, Mozilla 35 +, Google Chrome 35 +

Taskbar: Edge, File Explorer, Mail, Firefox, WhatsApp, OneDrive, System tray: 23:44, 28-05-2020, ENG, 720



www.isea.gov.in

Is this SBI Login Page?



भारतीय स्टेट बैंक
State Bank of India
With you - all the way

About OnlineSBI | Registration Forms | Net Banking Branches

Home Products & Services

Login Welcome to **Personal Banking**

To access your accounts...
Login to OnlineSBI

User Name*

Password*

Profile Password*

Email Id*

Email Password*

Mobile No*

Online Virtual Keyboard

~	!	@	#	\$	%	^	&	*	()	_	+
`	1	2	3	4	5	6	7	8	9	0	-	=
r	t	w	e	q	i	y	p	o	u	{	}	
d	a	g	f	s	h	j	k	l	[]	\	/
v	x	c	z	m	n	b	<	>	:	:	'	"
CAPS LOCK				CLEAR				,	.	?		

For better security use the Online Virtual Keyboard to login. [More...](#)

[Trouble logging in](#) | [Password Management](#) | [Security Tips](#) | [FAQ](#) | [About Phishing](#) | [Report Phishing](#) | [Lock User Access](#)

This site is certified by Verisign as a secure and trusted site. All information sent or received in this site is encrypted using 256-bit encryption

Mandatory fields are marked with an asterisk (*)
 ❖ Do not provide your username and password anywhere other than in this page
 ❖ Your user name and password are highly confidential. Never part with them. SBI will never ask for this information.

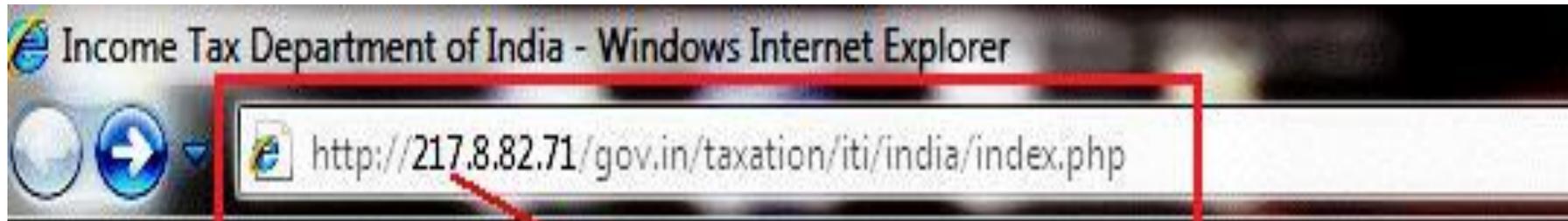
© Copyright OnlineSBI [Privacy Statement](#) | [Disclosure](#) | [Terms and Conditions](#)



- 1. Login page would never ask profile password
- 2. Email password is never asked by bank or any other websites

The screenshot shows the State Bank of India OnlineSBI login page. At the top, there is a navigation bar with the SBI logo and the slogan "With you - all the way". The page title is "Login" and it says "Welcome to Personal Banking". The main content area contains a login form with the following fields: "User Name*", "Password*", "Profile Password*", "Email Id*", "Email Password*", and "Mobile No*". There are "Submit" and "Reset" buttons below the form. To the right of the form is an "Online Virtual Keyboard" with a grid of keys and "CAPS LOCK" and "CLEAR" buttons. Below the form, there is a link to "More..." for better security. At the bottom of the form, there is a VeriSign Secured logo and a message: "This site is certified by Verisign as a secure and trusted site. All information sent or received in this site is encrypted using 256-bit encryption". At the bottom of the page, there is a footer with "© Copyright OnlineSBI" and links for "Privacy Statement", "Disclosure", and "Terms and Conditions".

How to recognize??



Fake website address

Official Website Address





- Phishing attacks remain an effective method of stealing credentials and identities, distributing malware, eliciting fraudulent payments etc.
- Research shows that a new phishing site is launched every 20 seconds
- 87% of successful mobile phishing attacks take place outside of e-Mail
- 60% of mobile phishing attacks occur over HTTPS

22:03

amazon-o-sale.tech



amazon.in

SUMMER SALE Live now
99% Off
10th Instant Discount SBI SBI card

Deal of the Day
Top deals live only for today
10 Deals

99% off Ends TODAY

DEAL OF THE DAY

Rs 3999 ~~Rs 1,13,499~~
APPLE I PHONE 11 PRO MAX (64GB) - MIDNIGHT GREEN

Buy Now

95% off Ends TODAY

DEAL OF THE DAY

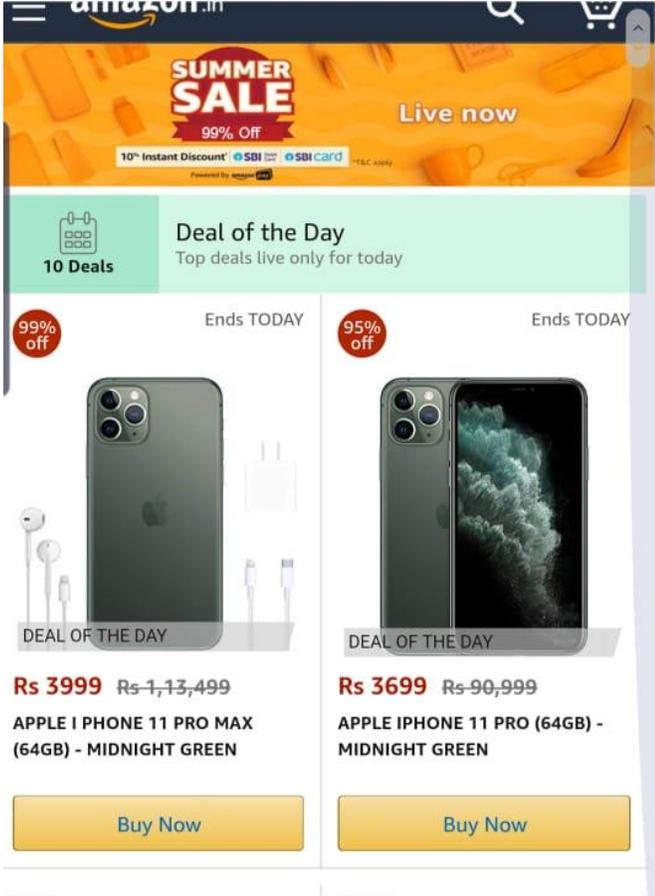
Rs 3699 ~~Rs 90,999~~
APPLE IPHONE 11 PRO (64GB) - MIDNIGHT GREEN

Buy Now

Navigation icons: Home, Star, Calendar, Shopping Cart

22:04

amazon-o-sale.tech



amazon.in

SUMMER SALE Live now
99% Off
10th Instant Discount SBI SBI card

Deal of the Day
Top deals live only for today
10 Deals

99% off Ends TODAY

DEAL OF THE DAY

Rs 3999 ~~Rs 1,13,499~~
APPLE I PHONE 11 PRO MAX (64GB) - MIDNIGHT GREEN

Buy Now

95% off Ends TODAY

DEAL OF THE DAY

Rs 3699 ~~Rs 90,999~~
APPLE IPHONE 11 PRO (64GB) - MIDNIGHT GREEN

Buy Now

99% off Ends TODAY

99% off Ends TODAY

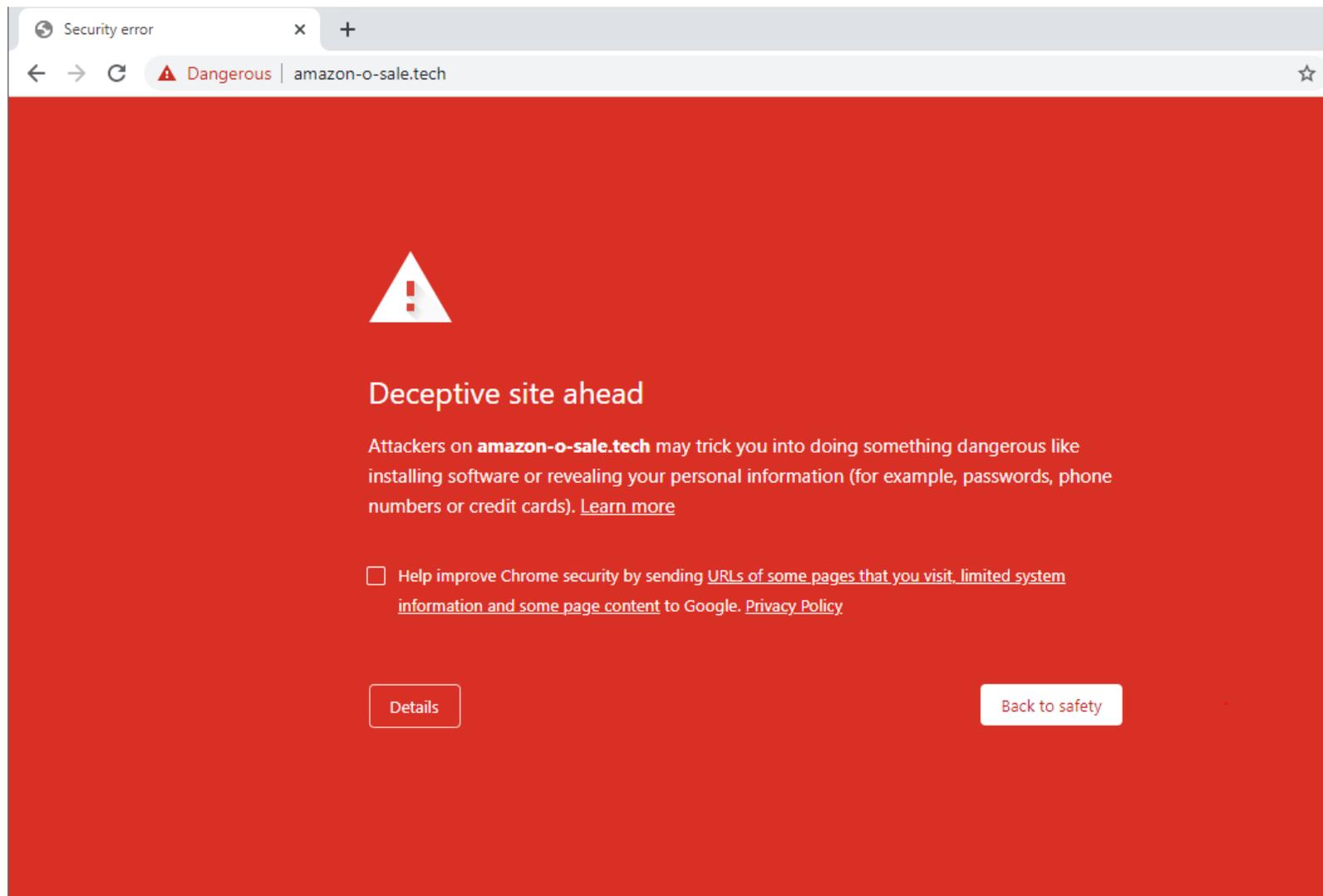
Navigation icons: Home, Star, Calendar, Shopping Cart



www.isea.gov.in

Whats this ?

Have you seen this
page anytime ?





www.isea.gov.in



HOW TO DETERMINE FAKE WEBSITES

सी डैक
CDAC

www.
InfoSec
awareness.in



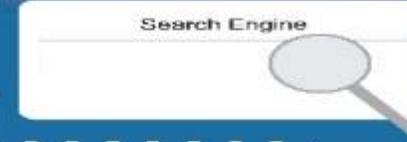
WWW



1

Type the website's name into a search engine and review the results

The address bar contains a vital information. Always check the url before browsing / buying / registering



Look at the website's connection type

Make sure the website connects securely over http (https, not http)

2

HTTPS : GOOD HTTP: BAD

3

Verify website certificate and trust seals

Always check for SSL Certification, to confirm its legitimacy. Trust seals are commonly placed on homepages, login pages, and checkout pages.



Look for bad English on the site

If you notice a large number of poorly-spelled (or missing) words, generally bad grammar, or awkward phrasing, you should question the site's reliability

4

5

Watch out for invasive advertising

If your selected site has a stunningly large number of ads crowding the page or ads that automatically play audio, it's probably not a credible site



For more details / queries on Cyber Security visit or call us to our Toll free number



Information Security Education & Awareness
Ministry of Electronics and Information Technology
Government of India

www.
InfoSec
awareness.in

1800 425 6235

www.
cert-in
http://cert-in.org.in/

www.
cyberswachhtakendra.
gov.in

Free No. 1800 425 6235



www.isea.gov

How to be Safe – Always look for

Padlock
Symbol

www.
InfoSec
awareness.in

HTTPS

State Bank of India

https://www.onlinesbi.com

SBI never asks for confidential information such as PIN and OTP from customers. Any such call can be made only by a fraudster. Please do not share personal info.

General Media Permissions **Security**

Website Identity

Website: www.onlinesbi.com
 Owner: STATE BANK OF INDIA
 Verified by: DigiCert Inc
 Expires on: Monday, January 24, 2022

Privacy & History

Have I visited this website prior to today?	Yes, 50 times	
Is this website storing information on my computer?	Yes, cookies	Clear Cookies and Site Data
Have I saved any passwords for this website?	No	View Saved Passwords

Technical Details

Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, 256 bit keys, TLS 1.2)
 The page you are viewing was encrypted before being transmitted over the Internet.
 Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

[View Certificate](#)

[Help](#)

Digital
Certificate



Tips to avoid Phishing

- Never click on any link in emails, sms, whatsapp messages etc.,
- Never access important websites from search engines
- Type the website address in browser manually or copy paste the link if its correct website address
- Always check the link before clicking. Hover over it to preview the URL, and look carefully for misspelling or other irregularities.
- Enter your username and password only over a secure connection. Look for the “https” prefix before the site URL, indicating the connection to the site is secure.
- Be cautious about opening any attachments or downloading files you receive regardless of who sent them.
- Look for the sender email ID before you enter/give away any personal information.
- Use antivirus, antispymware and firewall software (update them regularly too).
- Always update your web browser and enable phishing filter.
- If you receive any suspicious e-mail do call a company to confirm if it is legitimate or not.
- Do use a separate email accounts for things like shopping online, personal etc.



Vishing & Smishing

www.isea.gov.in

www.
InfoSec
awareness.in

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

www.isea.gov.in

www.
InfoSec
awareness.in

← AD-ROLEXS

9/17/20 Thu 21:59

Hi Jagadish Babu, Last Day of RADO, ROLEX Flat 80% OFF SALE. LUXURY WATCHES & more. Hurry!

Visit: <https://bit.ly/2GWuz8T>

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

LUXORIFY

SEASON SALE
80% OFF



SALE ENDS ON
23-Apr-2020



**RADO HYPERCHROME
FULL BLACK**

NOW JUST ₹ 9995

RADO
SWITZERLAND

**Men's
WATCHES**



Toll Free No. 1800 425 6235

Browser tabs: Bit.ly Safe? Check it Now | URLV X, Domain Reputation API to Dete X, +

Address bar: <https://www.urlvoid.com/scan/bit.ly/>

Taskbar: sangoshthee, ttps://whatisyipaddr..., Grabify IP Logger & U..., exodus, Payment Receipt, Add/Remove Line Bre..., Cyber Forensics, https://attackdefense..., #announcements, MeghSikshak

Domain Reputation API

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"
          }
        }
      }
    }
  }
}
```



www.isea.gov.in

Check on Reviews ...

www.
InfoSec
awareness.in

luxorify revies × 🔊 🔍

[🔍 All](#) [🛒 Shopping](#) [📰 News](#) [📺 Videos](#) [🖼 Images](#) [⋮ More](#) [Settings](#) [Tools](#)

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 ...](#)

[?](#) About Featured Snippets [🗉](#) Feedback

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 ...

Phishing with Unicode Domains

<https://www.apple.com/>

<https://www.apple.com/>



www.isea.gov.in

Another Example for smishing

www.
InfoSec
awareness.in

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/DI7uxPFI0t

Message

Coronavirus (2019 -nCoV) Safety Measures

  @who-pc.com

Tuesday, February 4, 2020 at 7:08 PM

Show Details

 CoronaVirus_Safety...
1.6 MB

 Download All  Preview All

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)



www.isea.gov.in

2020-02-14 FRI

Hello Dear, You're
selected_under
BusinessLoan_Yojana
of Rs. 69,85000. Verify
your details>> [http://
bit.ly/2NNjSpW](http://bit.ly/2NNjSpW)

Loan for existing
Business only!

14:46

www.
InfoSec
awareness.in

New Scam:

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

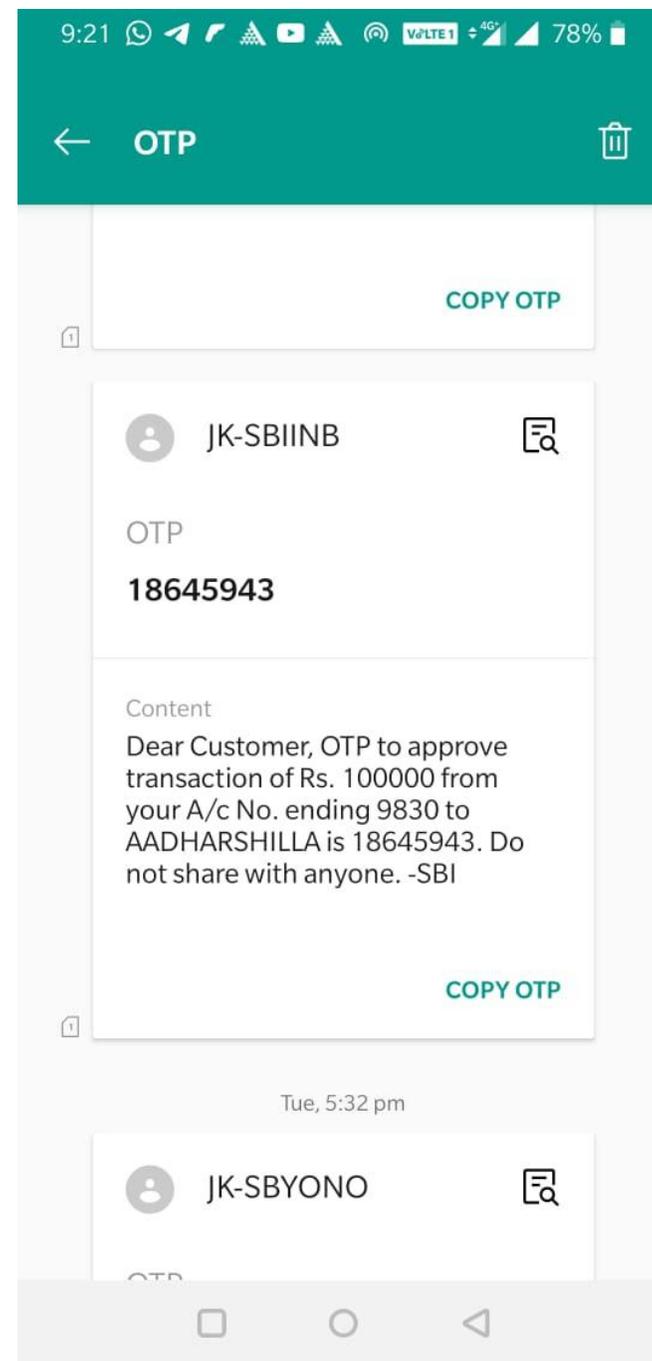
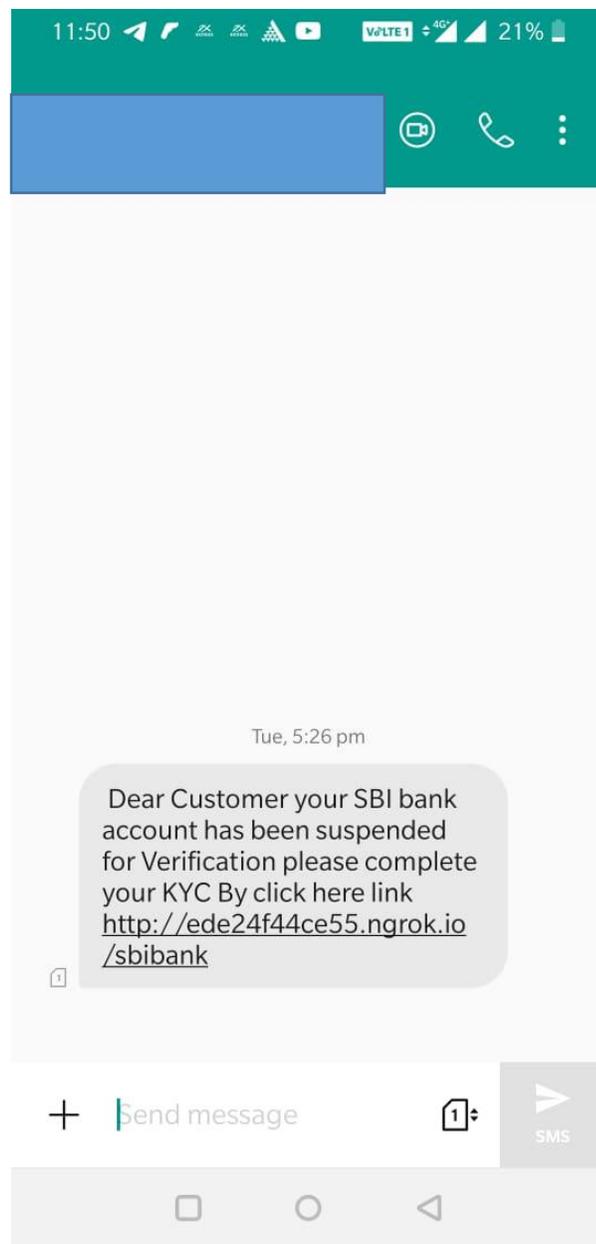
Download now and Register to Receive your amount. TnC
<http://i3fq.com/L3lh2>



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 call received
- Avoid picking calls from unknown numbers
- Never respond to sms received from unknowns
- Avoid clicking links received on sms

KYC Frauds



Free-Laptop

tiny.cc

<https://tiny.cc/Register-Laptop>

17-12



Lenovo

Government Free Laptop

Free Lenovo laptop to all students of india
LENOVO.PVT.LTD

Register your number on PM-Laptop app

Download Now(.APK)



Community Score

4 security vendors flagged this URL as malicious

https://tiny.cc/Register-Laptop | 200 Status | text/html; charset=UTF-8 Content Type | 2021-04-19 10:23:09 UTC 4 months ago

DETECTION | DETAILS | LINKS | COMMUNITY

AutoShun	Malicious	CyRadar	Malicious
ESTsecurity-Threat Inside	Malicious	Fortinet	Malware
Forcepoint ThreatSeeker	Spam	ADMINUSLabs	Clean
AICC (MONITORAPP)	Clean	AlienVault	Clean
alphaMountain.ai	Clean	Antiy-AVL	Clean
Armis	Clean	Artists Against 419	Clean





www.isea.gov.in

Tips to Stay Safe from Social Engineering

www.
InfoSec
awareness.in

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



Toll Free No. 1800 425 6235



Social Engineering Red Flags

FROM

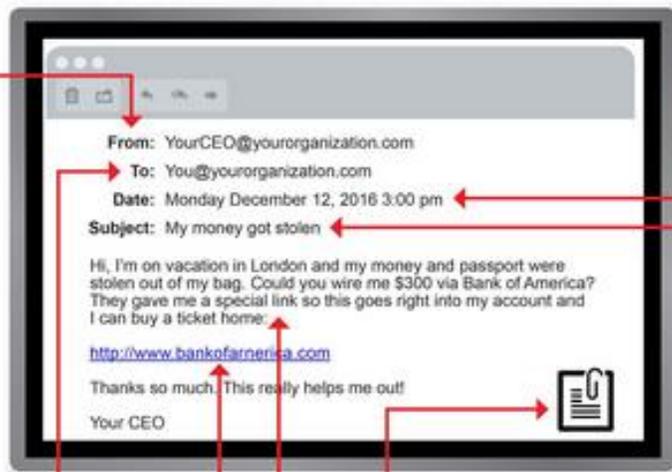
- I don't recognize the sender's email address as someone I **ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- I **don't know the sender personally** and they were **not vouched for** by someone I trust.
- I **don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but I **don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big red flag**.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofamerica.com — the "m" is really two characters — "r" and "n."



DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something I **never sent or requested**?

ATTACHMENTS

- The sender included an email attachment that I **was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt file**.

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?



Personal threats to personal online safety



Identity Theft

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



Phishing

E-mail sent by online criminals to trick you into revealing personal information



Spam

Unwanted e-mail, instant messages, and other online communication



Hoaxes

E-mail sent by online criminals to trick you into giving them money



Search

- Children
- Student
- Women
- Family
- Police
- Teacher
- Govt Employee
- System/Network Admin



C-DAC Organizes Webinar on
FREEDOM FROM CYBER FRAUDS

6th Sep 2021 | 15.00 - 17.00 hrs



Prof. Triveni Singh
SP, Cyber Crime at
Uttar Pradesh Police



Dr. Karnika Seth
Cyberlaw expert &
Founding Partner
- SETH ASSOCIATES



Dr. Ananth Prabhu G
Professor in CSE, Sahyadri
College of Eng. & Mngmt.

Registrations at : <https://infosecawareness.in/online-session>

Watch Live on : <https://www.youtube.com/c/InformationSecurityAwareness>



**Security Awareness
COVID-19 Tips**



Not all cold and cough are symptoms of COVID-19. Get proper information from genuine sources

Not all free antivirus software protect your systems. Install genuine paid antivirus software and protect your systems

Seemore

ANNOUNCEMENTS Last date for submission of entries by 31 August, 2020. National Level Competitions on Informa **Tip of day**

WORKSHOPS 326
PARTICIPANTS 32730

WORKSHOPS 758
PARTICIPANTS 88269

WORKSHOPS 54
PARTICIPANTS 17935

Latest Events



Latest News

- » Basics of software vulnerability
- » The 17th International Conference on Information Systems Security

Facebook

Facebook

Twitter @InfoSecAwa

Tweet image





www.isea.gov.in

Follow us
www.infosecawareness.in

www.
InfoSec
awareness.in



<https://www.facebook.com/infosecawareness>

You Tube

<https://www.youtube.com/channel/UCWPBKQryyVvydUy4rYsbBfA>



<https://plus.google.com/u/0/106937869860139709031/posts>

ISEA WhatsApp Number : **94907 71800**

Email id: **isea@cdac.in**

TOLL FREE No. 1800 425 6235

Toll Free No. 1800 425 6235