



MAHARASHTRA GOVERNMENT
SPECIAL INSPECTOR GENERAL OF POLICE MAHARASHTRA
CYBER, WORLD TRADE CENTER, CUFFE PARED-400005
Email: sp.cbr-mah@gov.in



Income Tax Return Cyber Scam Advisory

As the financial year comes to a close, individuals and businesses are increasingly targeted by cybercriminals exploiting the Income Tax Return (ITR) filing and refund process. To address this growing threat, **Maharashtra Computer Emergency Response Team (MHCERT)** has prepared a citizen awareness advisory detailing key cyber fraud tactics and protective measures.

Key Highlights of the Advisory:

- **Common ITR Cyber Frauds:** Tax refund scams, phishing attacks, impersonation of tax officials, and fraudulent ITR services.
- **Modus Operandi of Cybercriminals:**
 - Phishing emails and messages luring users with fake refund offers.
 - Creation of counterfeit ITR websites and mobile apps.
 - Fraudsters posing as tax officials to extract personal and financial information.
 - Offering deceptive ITR filing services to steal sensitive data.
- **How to Protect Yourself:** Verifying sources before sharing information, avoiding links in unsolicited messages, using official tax portals, and enabling multi-factor authentication for financial accounts.

We encourage individuals and organizations to remain vigilant and share this advisory within their networks to prevent falling victim to these scams.



Income Tax Return Cyber Scam Advisory

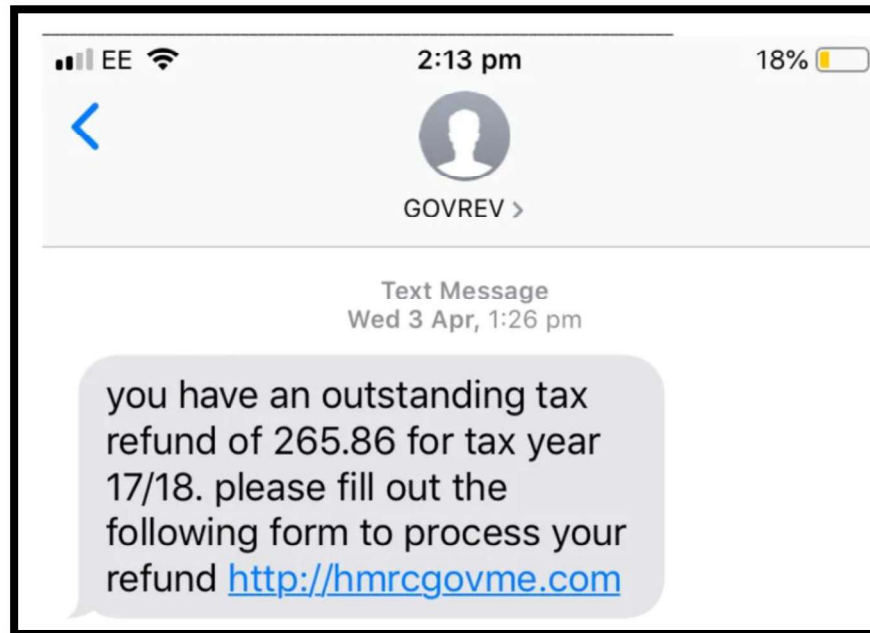
MH CERT

Advisory ID: CERTMH_CA_2025_01

Date: 26th March 2025

This Page is intentionally left blank

What Is Income Tax Return Scam?



Cybercriminals are capitalizing on tax season, with scams targeting individuals under the guise of Income Tax Return (ITR) filing assistance. As the tax deadline approaches, fraudsters are increasingly using deceptive messages and websites to trick people into revealing sensitive information, with the promise of helping them file their returns or offering tax-related benefits.

Common tactics include phishing emails or text messages that appear to be from the Income Tax Department, offering help with ITR filing or claiming a refund. These messages often contain fake links that lead to counterfeit websites designed to steal personal information or install malware on devices. Some fraudsters even impersonate tax professionals, sending messages about incomplete filings or demanding immediate action, prompting victims to share their details or make payments.

Scammers may set up fake customer service numbers or call centers, claiming to assist with ITR filing or tax-related queries. These fake agents ask for sensitive financial information, such as bank account details or Aadhaar numbers, which are later used to commit fraud.

Notable ITR Cyber Frauds

₹13cr tax refund scam detected in Andhra

U Sudhakar Reddy / Jul 1, 2023, 08:17 IST



ITR refund scam: Income Tax Dept warns taxpayers against falling prey to cyber fraudsters

The I-T Department, in a social media post, said a man lost ₹1.5 lakh after clicking on a "fake income tax refund message".



CID busts cyber criminal involved in IT refund scam worth crores

CID officers have uncovered evidence indicating that Rajegowda embezzled Rs 3.6 crore

ED attaches IPS officer's flat in Mumbai in Rs 263 crore ITR fraud case

The ED has already filed a prosecution complaint in September 2023 against Adhikari and 10 others.

Alert! IRS Officer Falls Victim to Online Reward Points Fraud via Deceptive Messages

A 48-year-old IRS officer with the Income Tax Department fell victim to an online reward points fraud, resulting in a loss of Rs 48902.



Modus-Operandi



Phishing emails and messages: Scammers send emails or messages disguised as official communication from the Income Tax Department. These often contain links to fake websites that mimic the real ITR portal, where they steal login credentials and other sensitive information.

Fake refund offers: Scammers may offer fake tax refunds or claim to help expedite the refund process. They may ask for personal details or bank account information, which they then use for fraudulent activities.

Impersonating tax officials: Scammers may call or visit individuals posing as tax officials. They may threaten legal action or demand immediate payment to avoid penalties.

Creating fake ITR websites or apps: Scammers may create fake ITR filing websites or apps that look legitimate. These platforms may steal user data or install malware on their devices.

Offering fraudulent ITR services: Scammers may offer ITR filing services at unusually low prices or make unrealistic promises. They may file incorrect returns or misuse personal information for illegal purposes.

How to Protect Yourself

Verify the sender: Always check the sender's email address or phone number to ensure it is legitimate. The Income Tax Department never asks for sensitive information via email or message.

Be cautious of links/Attachments: Do not click on links/Attachments in suspicious emails or messages. Instead, type the official website address directly into your browser.

Never share personal information: Do not share your login credentials, PAN details, bank account information, or other sensitive information with anyone.

Be wary of unrealistic offers: Be sceptical of anyone offering unusually high refunds or promising to expedite the ITR process through unofficial channels.

Use official channels: File your ITR through the official Income Tax Department website or authorized tax professionals.

SAVE THESE 24x7 HELPLINE NUMBERS & REPORT

- 1945 & 1930
- <https://mhcyber.gov.in/> (MAHARASHTRA CYBER CRIME PORTAL)
- www.facebook.com/MahaCyber (MAHARASHTRA CYBER FACEBOOK)
- www.instagram.com/mahacyber(MAHARASHTRA CYBER INSTAGRAM)
- www.x.com/mahacyber1(MAHARASHTRA CYBER X ACCOUNT)