Cyber Security Centre of Excellence
West Bengal

Department of Information Technology & Electronics
Government of West Bengal

An advisory on Suspected Fraud Communications (An advisory on registering spam callers)

What are Suspected Fraud Communications (spam calls)?

Spam calls are unsolicited phone calls that are typically made for commercial or fraudulent purposes. These calls often involve automated dialling software and may be made from fake or spoofed phone numbers. They can be disruptive, annoying, and even dangerous, as they may be used to scam or defraud individuals. However, these Fraud Communications are messages (calls, SMS, WhatsApp) that try to trick us into revealing personal details or sending money. These communications typically aim to deceive individuals into providing personal information, financial details, or access to sensitive accounts, which can then be used for malicious purposes such as identity theft, financial fraud, or unauthorized access to accounts. Common types of spam calls include:

1. Telemarketing calls: Unsolicited sales calls from companies trying to sell products or services.

2. Robocalls: Automated calls that play a pre-recorded message, often trying to sell something or ask for personal information.

3. Scam calls: Calls from fraudsters posing as representatives from banks, government agencies, or other organizations, trying to trick people into revealing sensitive information or making payments.

4. Phishing calls: Calls aimed at tricking individuals into revealing sensitive information, such as passwords or credit card numbers.

5. Political calls: Unsolicited calls from political campaigns or organizations, often made during election seasons.

6. Imposter scams: This call uses emotional manipulation and family ties to trick the victim into sending money to the person on the other end of the call.

How to detect spam calls? *Red Flags are*

1. **Urgency:** They create a sense of urgency to pressure you into acting quickly without thinking clearly.
2. **Threats:** Threaten us with consequences if we don't comply.
3. **Offers that Seem Too Good to Be True:** Unrealistic deals or prizes are a red flag.
4. **Unusual Grammar or Spelling Errors:** Legitimate organizations typically have professional communication.
5. **Requests for Personal Information:** Banks and other institutions won't ask for sensitive details via SMS or calls.

How to Protect Our self from Fraud Communication?

1. **Stay Calm:** Don't panic. While fraudulent communications can be concerning, staying calm will help us to think clearly and take appropriate action.
2. **Verify the Source:** If we receive an email, text message, or phone call that seems suspicious, verify the sender's identity. Check email addresses, phone numbers, or website URLs for any irregularities or inconsistencies.
3. **Do Not Respond:** Avoid responding to suspicious communications or providing any personal or financial information. Legitimate organizations will never ask for sensitive information via email, text, or phone without prior verification.
4. **Contact the Organization Directly:** If we suspect the communication is from a legitimate organization but are unsure, contact them directly using official contact information from their website or other trusted sources. Confirm whether they sent the communication.
5. **Do Not Click on Links or Download Attachments:** Avoid clicking on links or downloading attachments from suspicious emails or text messages. These could contain malware or lead to phishing websites designed to steal our information.
6. **Educate Yourself:** Stay informed about common types of scams and fraud tactics. Being aware of the latest scams can help us to recognize and avoid fraudulent communications in the future.
7. **Protect our Devices:** Ensure that our computer, smartphone, and other devices have up-to-date antivirus software and security patches installed. This can help prevent malware and other security threats.

8. **Warn Others:** If we receive a suspicious communication, consider warning others, especially friends, family, and colleagues who may also be targeted by similar scams.
9. **Stay Vigilant:** Remain vigilant and skeptical of unsolicited communications, especially those that request sensitive information or payment. Trust your instincts and err on the side of caution.
10. **Report Suspected Fraud:** Report suspected fraud to the appropriate authorities or organizations. This may include our bank or financial institution, or the relevant authorities.

The government of India launched the **Chakshu** portal and under the **Sanchar Sathi** initiative. The portal aims to empower subscribers to report suspected fraud calls and messages, as well as instances of leaked phone numbers by businesses.

Chakshu - Report Suspected Fraud Communication

In the world the technology changes every day, today we are more dependent on gadgets like mobile, laptop or tablet. Be it village or city, we can order any item sitting at home with just one click. In this era of modern technology and Artificial Intelligence (AI), cyber thugs are also active. Which can clear our bank account in the blink of an eye through SMS, link or other methods. The Government of India keeps launching apps from time to time to save people from these cyber frauds. Recently the government has launched 'Chakshu' portal and Digital Intelligence Platform (DIP). The aim of this digital intelligence platform is to prevent misuse of smart gadgets in cybercrimes and financial frauds. Also, its aim is to ensure that the accounts of users doing online transactions remain secure. On the Chakshu portal, people can upload details of possible cyber fraud messages or calls. Due to which law and enforcement agencies will be able to take action against them even before fraud occurs. The combined efforts of Chakshu and the Digital Intelligence Platform are expected to bolster the detection and prevention of cyber fraud.

Remember, it's always a good idea to be vigilant and skeptical when receiving unsolicited calls!

সাইবার ক্রাইম প্রতিরোধ করবে সরকারের চোখ *(Chakshu)*

LINK: https://sancharsaathi.gov.in/sfc/Home/sfc-complaint.jsp

How to Use Chakshu Portal to Report Spam Calls, fraud

1. Log in to the 'Sanchar Saathi' portal at sancharsaathi.gov.in
2. Select the 'Chakshu' option under 'Citizen Centric Services.'
3. Review the disclaimer and the uses of 'Chakshu,' then click 'continue for reporting.'
4. Fill out the form with details such as the medium, category, and timing of the suspected fraud communication.
5. Add personal details, verify with OTP, and submit the complaint.

What can we report on Sanchar Saathi - Chakshu Portal:

1. Check mobile connections issued in their name and report unnecessary or unauthorized connections.
2. Report stolen/lost mobile handsets for blocking and tracing.
3. Verify the authenticity of mobile handsets when purchasing new or used devices.
4. Report incoming international calls displaying Indian telephone numbers as caller ID.
5. Check details of licensed wireline Internet Service Providers.