CENTRAL RESERVE POLICE FORCE

MAR, 2025

CYBER BYTE

NPCI warns users against call merging scams

How to react against call merger scam

FRAUD ALERT
FRAUD ALERT
FRAUD ALERT

"SpyLend" Android malware found on Google Play enabled financial cyber crime and extortion

1. CYBER GEEKS NEWS

A. NPCI warns users against call merging scams.

Indian authorities have issued a warning about a new scam being employed to steal money from people. In this latest way to scam people, fraudsters deceive users by merging calls and getting access to their One- Time Passwords (OTPs). This enables scammers to carry out unauthorized transactions and steal money.

National Payments Corporation of India (NPCI) has also warned users about this new scam through its X account. In this latest post, they mentioned that scammers are using call merging to cheat users.

While sharing this information, NPCI also advised people to be more careful and explained how this scam works and how to avoid it. The scammer calls a victim claiming that they received their number through a friend. The scammer then requests the victim to add his "friend" who is calling from a different number. Once the call is merged, it leads to the unsuspecting user being unknowingly connected to a genuine OTP verification call from their bank.

The scammer tricks the users into revealing OTP. Once the OTP is out, the transaction will be completed leading to a financial loss.

B. Tampering or Spoofing of Mobile Numbers, IPs, IMEI, and SMS Headers is a Criminal Offense: DoT

दूरसंचार विभाग
Department of Telecommunications

Telangana

DoT cautions about misuse of telecom resources

The Ministry of Communications said that the Telecommunications Act 2023 enforces stringent penalties for misuse of telecom resources.

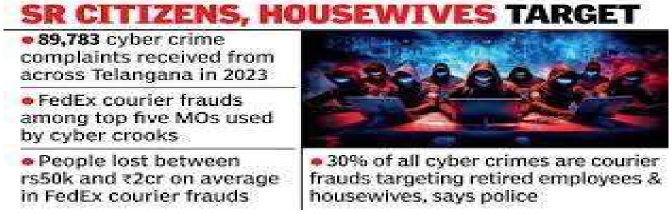
The Department of Telecommunications (DoT) has issued a stern warning against the misuse of telecom resources, including tampering or spoofing of mobile numbers, IP addresses, IMEI numbers, and SMS headers. The DoT emphasized that such activities violate the Telecommunications Act, 2023, which prescribes stringent penalties for offenders.

Fraudsters are increasingly exploiting telecom resources for cybercrime and financial fraud. Miscreants have been found using illegally acquired Subscriber Identity Module (SIM) cards and SMS headers to send bulk fraudulent messages. Some individuals also procure SIM cards in their names and distribute them to others, often unknowingly aiding cybercriminals.

Additionally, cases have surfaced where SIM cards are obtained using fake documents, fraud, or impersonation. In some instances, Points of Sale (PoS)—the entities responsible for issuing SIM cards—have been complicit in facilitating such illegal procurements, effectively abetting the offence. Cybercriminals have also been found modifying telecommunication identifiers, such as the Calling Line Identity (CLI)— commonly referred to as a phone number— using mobile apps and other means.

2. CYBER FRAUDS

(A) New cyber fraud targets unemployed youth, students, housewives:


SR CITIZENS, HOUSEWIVES TARGET

- 89,783 cyber crime complaints received from across Telangana in 2023
- FedEx courier frauds among top five MOs used by cyber crooks
- People lost between rs50k and ₹2cr on average in FedEx courier frauds
- 30% of all cyber crimes are courier frauds targeting retired employees & housewives, says police

The government has issued an alert about a new cyber fraud scheme called the '**Pig Butchering Scam**' which targets unemployed youth, students, and vulnerable individuals. Victims not only lose money but are also forced into cyber slavery.

This was also highlighted in the latest annual report published by the Union Ministry of Home Affairs, adding that unscrupulous individuals and entities have been noticed using Google services platforms to initiate these crimes.

According to reports from the cyber intelligence wing, a new online fraud module known as '**Pig Butchering Scam**' or '**Investment Scam**' has been noticed, which targets unemployed youths, housewives, students, and needy people, who are made to either lose large sums of money daily or are enticed to do cyber slavery.

It is believed that such fraud first originated in China in 2016. In such fraud modules, miscreants target gullible individuals with whom they first build trust over time and then convince them to invest in cryptocurrencies or some other lucrative scheme before stealing the money collected.

(B) SpyLend Android malware found on Google Play enabled financial cyber-crime and extortion:

CYFIRMA researchers discovered an Android malware, named "**SpyLend**", which was distributed through Google Play as Finance Simplified. The malware targets Indian users with unauthorized loan apps, enabling predatory lending, blackmail, and extortion.

The loan apps poses as a financial tool, it lures users with easy loan promises but demands excessive permissions to access contacts, call logs, SMS, photos, and location. The app redirects users to external links for APK downloads, bypassing Google Play security. Once installed, it accesses photos, videos, and contacts, capturing clipboard data to steal sensitive information.

The researchers discovered that the malicious app uses a custom C2 server, with an admin panel in English and Chinese. The malware exploits APIs to access files, contacts, call logs, SMS, and installed apps.

3. TIP OF THE MONTH

A. How to react against call merger scam.

A **call merger scam** (also known as a **call spoofing scam**) is when scammers use software or techniques to disguise their phone numbers, making it look like they are calling from a legitimate or trusted source, such as a bank, government agency, or even a local number. Here are some steps to protect yourself and respond if you suspect you're a victim of a call merger scam:

1. **Don't Answer Unknown Calls.**

   If you receive a call from an unfamiliar number, especially if it's an international or suspiciously local- looking number, don't answer. Scammers often use call spoofing to make their number appear familiar to you.

2. **Hang Up Immediately if You Suspect a Scam.**

   If you answer a call and the person on the other end seems suspicious or requests personal information, hang up immediately. Do not engage with the caller.

3. **Don't Share Personal Information**

   Scammers may ask for sensitive information like Social Security numbers, account details, or passwords. Never give out personal information over the phone, especially if you didn't initiate the call.

4. **Verify the Call's Legitimacy.**

   If the caller claims to be from a legitimate organization (like your bank or a government agency), hang up and call the official number of that institution to verify the request. Always use trusted contact details from official websites or documents.

5. **Use Call Blocking and Screening Apps.**

   Many smartphones and apps have built-in call screening or blocking features. Consider using third-party apps like Truecaller, Hiya, or Nomorobo to block or identify suspicious calls.

6. **Report the Scam.**

- Report the scam to your phone provider. Many service providers offer features to help block fraudulent calls.
- You can also report the scam to local authorities or consumer protection agencies, such as:
  - www.cybercrime.gov.in (NCRP portal).
  - Cybercrime helpline number 1930.
  - https://www.cert-in.org.in

7. **Use Caller ID Services.**

   Enable your phone's caller ID services, or use apps that can identify potentially malicious calls, so you can better screen who is calling.

8. **Block the Number.**

   If you receive a scam call, most smartphones allow you to block the number directly from the call log. However, since scammers can use different numbers each time, blocking one number may not prevent further scams.

9. **Educate Others.**

   Share information about call merger scams with friends and family, especially those who might be more vulnerable, such as elderly relatives. Awareness is key to reducing the impact of these scams.

(B) How the lost phones can remotely be locked to protect data and prevent unauthorized access.

Depending on whether you're using an **Android** or an **iPhone**:

For Android Phones:

1. **Use Google's Find My Device:**

- Go to Find My Device on a web browser.
- Sign in using the Google account linked to your lost phone.
- After signing in, you'll see a list of devices associated with your account. Select your lost phone from the list.

You'll have several options:

Play Sound: If your phone is nearby, you can make it ring to help find it.

Secure Device (Lock): Choose this option to lock your phone. You can set a new password, PIN, or pattern to lock the device and prevent others from accessing it. You can also display a message on the lock screen with your contact information (like a phone number or email) in case someone finds it.

Erase Device: As a last resort, if you're sure you can't recover your phone, you can erase all its data remotely. However, this should only be done if locking the device is not an option and you want to protect your data.

Alternative: Use Samsung's Find My Mobile (Samsung Phones):

If you're using a Samsung phone, you can also use Find My Mobile.

Log in with your Samsung account.

Choose your lost device and select the "Lock" option to secure your phone remotely.

For iPhones:

1. Use Apple's Find My iPhone:

Open iCloud.com on a web browser or use the **Find My** app on another Apple device.

Sign in with your Apple ID.

Select your lost iPhone from the list of devices.

Choose **Mark as Lost**. This will lock your phone with your existing passcode and display a custom message (you can enter your contact information in case someone finds it). Apple Pay will also be disabled when you enable "Mark as Lost."

Play Sound: You can make the phone play a sound if it's nearby.

Erase iPhone: If you believe you won’t recover the phone and want to protect your personal data, you can choose the "Erase iPhone" option, which will erase all data on your device remotely. Note that once you erase it, you won’t be able to track the phone anymore.

Activation Lock: If you have "Find My" enabled, **Activation Lock** will prevent anyone from using your iPhone even if they erase it. It will require your Apple ID and password to reactivate the device.

General Tips:

- **Report to your carrier**: You can inform your mobile carrier about the lost phone. They can disable your SIM card to prevent unauthorized use of your mobile number and may also help track the device.
- **Change passwords**: If you think your phone is lost permanently or contains sensitive data, change the passwords for important accounts, such as your Google, Apple ID, email, and banking apps.
- **File a police report**: In case of theft, report the phone as stolen with the police, especially if it contains valuable or sensitive information.

By following these steps, you can lock your lost phone and secure your personal information remotely.

Holi Milan Samaroh

Tribute to Pulwama

38th National Games

Women's Day

GOLF MEDAL WINNER

15th AIPDM COMMANDO
TEAM WITH DG CRPF