

Alerts on WhatsApp and SMS

WhatsApp being the messaging app used by about 2 billion people worldwide has become the first choice of fraudsters and scammers. Recently financial frauds and leakage of sensitive information has become ubiquitous and getting executed through malicious link, social engineering or other innovative techniques.



Recent study alerts smartphone users and has listed **SOME** dangerous message lines that criminals send on SMS or WhatsApp to hack their devices or steal money. The report claims that 82% of Indians have clicked on or fallen for such fake messages. It claims that Indians receive nearly 12 fake messages or scams each day via email, text or social media daily. Here are **SOME such dangerous messages** that you should never click on

Common Modes used by Fraudsters



Latest Scams

- **My Phone has Broken**

Threat actors impersonates and texts from a new number claiming their “phone has broken”. Additionally they may say that the new number belongs to a friend in order to convince the victim. Finally, they ask to transfer money to purchase new phone. Always ask for proof of identity and do not transfer any money or personal information.

- **Wrong number Scam**

Here the attacker uses social engineering skills to befriend the victim after giving the excuse of either messaging by mistake or mistyping the mobile number of his/her friend. In all cases of message from an unrecognized person neither reply nor give out any personal details.



- **You've won a prize!**

This message may come with slight alterations as well, like specifying the award won. But there is a 99% chance that the message received is a scam and meant to steal receivers' credentials or money. In such cases never click on such suspicious links.

Never pay to
get a prize.
That's a scam.
ftc.gov/fakeprizes



- **Fake job notifications**

This is another dangerous message. Remember, job offers never come on WhatsApp or SMS. No professional company will ever approach you on these platforms, so it is a sure-shot scam. In such cases never click on such suspicious links.

- **Family Member Impersonation Scams**

Attackers impersonates as family/friends and Uses social engineering techniques to extort money/personal information. Confirm the identity of the impersonator in such cases.

- **Complete this Survey Scam**

Here users are promised of cash prizes or coupons in return of completing a survey. Think before participating and twice before paying for participation.

- **Bank alert messages with URL**

Bank alert messages received on SMS or WhatsApp asking users to complete KYC via a url/link in the message are scams. They are aimed to steal your money.



ENTER UPI PIN TO RECEIVE
MONEY IN YOUR ACCOUNT



Always cross-check and confirm the KYC status by directly communicating with your Home Branch

Scanning of QR Code or entering of UPI PIN is only required to make payment and not for receiving money

- **Fake missed delivery, or delivery problem, notification**



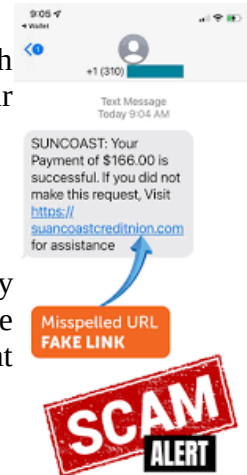
SMS or WhatsApp notifications around missed delivery or other delivery problems too are dangerous. This can be even when you have made the purchase.

- **Information about a purchase that you haven't made**

Any updates about a purchase that you haven't made is a scam. Such messages are written in a way to tempt recipients to click and get their phones hacked.

- **E-commerce site security alert, or notification messages regarding account updates**

E-commerce site security alert, or notification messages regarding any update in your account too are traps. Please note that any e-commerce company will never reach you on SMS or WhatsApp for such important alerts.



- **OTT subscription updates**

With OTT popularity increasing, scammers try to lure smartphone users with messaging around Netflix or other OTT subscriptions. These may be free offers or messages with urgency on subscriptions getting over.



General Safety Measures:

- Never click on suspicious links.
- Neither reply nor give out any personal details to any message from an unrecognized person
- Always ask for proof of identity and do not transfer any money or personal information.