Beware of Fake KYC whatsapp messages with MTNL Name and Logo

It has come to our notice that MTNL Name and Logo is being misused by some unknown persons on pretext of KYC, with an intention to commit financial fraud. In this regard following may be noted:-

- MTNL has not authorized any agency or any individual to carry out any KYC activity.
- MTNL do not carry out any KYC verification over Whatsapp.

Be Vigilant in case you receive such message:-

- Do not share personal information,
- Do not click on unverified link,
- Do not download any app,
- Report to Cyber Crime Delhi Police, 1930

For Customer Awareness

https://twitter.com/DelhiPolice/status/1549329104968617984?t=Jg-RXQmL_9QXTuH4S5oZcA&s=08

Millennium Post

Cyber fraud through misuse of MTNL name, logo; alerts issued

OUR CORRESPONDENT

NEW DELHI: Citing an increase in cyber frauds through misuse of the MTNL's name and logo, the Delhi Police on Tuesday alerted mobile customers against WhatsApp messages received on the pretext of KYC updation.

Taking to Twitter, the Delhi Police said that the state-run telecom service provider does not carry out KYC verification over WhatsApp and advised mobile customers not to respond to such fraudulent messages.

"In case you receive such messages — be careful — Dear Customer, Your MTNL Sim Card, Addhar, e-KYC has been suspended. Your sim card would be blocked within 24 hours. Call immediately," the Delhi Police said.

"Beware! There is a sharp spike in fraudulent incidents wherein @MTNLOfficial's name & logo are being used to commit cyber fraud.

"Mobile customers receive WhatsApp messages from miscreants on the pretext of KYC updation to retrieve confidential information," the Delhi Police tweeted from its official handle.

To avoid falling prey to such scams, the Delhi Police asked people not to share personal information in case they receive such messages and warned them from clicking on unverified links.

Police officials said one should not download any apps that appear suspicious and most importantly MTNL does not carry out KYC verification over WhatsApp.

ठगी | साइबर जालसाज लोगों को चूना लगाने के लिए नया हथकंडा अपना रहे, दिल्ली पुलिस ने अपने ट्विटर हैंडल से इसके बारे में लोगों को सचेत किया

सिम ब्लॉक होने के मैसेज व्हाट्सऐप पर भेजकर धोखाधड़ी

नई दिल्ली, प्रमुख संवाददाता। साइबर जालसाज लोगों को चूना लगाने के लिए आए दिन कोई न कोई नया हथकंडा अपना रहे हैं। अब केवाईसी नहीं होने पर सिमकार्ड ब्लॉक करने के मैसेज व्हाट्सऐप पर भेजकर लोगों को झांसे में ले रहे हैं। इस बारे में सर्विस प्रोवाइडर यूजर्स को एडवाइजरी जारी कर रहे हैं। दिल्ली पुलिस ने भी अपने ट्विटर हैंडल से लोगों को बताया कि इस तरह से केवाईसी अपडेट के लिए एमटीएनएल की तरफ से कोई भी संदेश नहीं भेजा जाता है। यह सब साइबर जालसाज कर रहे हैं। ऐसे व्हाट्सऐप मैसेज से सावधान रहिए।

ट्वीट कर संदेश दिया : पुलिस ने ट्वीट कर यूजर्स को बताया कि एमटीएनएल व्हॉट्सऐप पर केवाईसी वेरिफिकेशन नहीं करता है। व्हॉट्सऐप पर आने वाले ऐसे फर्जी संदेशों का जवाब नहीं दें। हालांकि ऐसे संदेश दूसरे सर्विस प्रोवाइडर से भी आने की सूचना है। इसके मद्देनजर विभिन्न सर्विस प्रोवाइडर ने इस भी इस बारे में एडवाइजरी मैसेज भेजना शुरू कर दिया है।

ऐसे लिंक होते हैं फर्जी

1 केवाईसी अपग्रेड मैसेज के साथ रजिस्ट्रेशन के लिए आने वाले लिंक

2 बैंक के फर्जी ऐप को डाउनलोड करने के नाम पर आए लिंक

3 फर्जी शॉपिंग साइट्स पर लुभावने ऑफर वाले लिंक

क्लिक न करें ऐसे लिंक पर

दिल्ली पुलिस ने निजी जानकारी शेयर नहीं करने की अपील की और कहा कि वह वेरिफिकेशन लिंक पर क्लिक न करें। बदमाश वॉट्सऐप पर केवाईसी अपडेट कराने के लिए संदेश भेजते हैं और इस बहाने गुप्त सूचना प्राप्त कर लेते हैं।

1930 पर या नजदीकी साइबर थाने में सूचित करें

पुलिस ने बताया कि ऐसी कोई भी ऐप डाउनलोड नहीं करें जो संदेहास्पद हो। अगर इस तरह का अपराध होता है तो 1930 पर या साइबर थाने में सूचित करें।

इन सब तरीकों का प्रयोग कर रह सकते हैं सुरक्षित

1 लिंक, डोमेन नाम या ईमेल एड्रेस में स्पेलिंग की गलतियों पर जरूर ध्यान दें। साइबर क्रिमिनल आमतौर पर उस तरह का ईमेल यूज करते हैं जो नामी कंपनियों का हो, बस वे मामूली सा हेर-फेर कर देते हैं, जिससे वह वास्तविक लगे।

2 किसी भी ऐसे लिंक पर क्लिक करने से पहले बार-बार सोचें, जिसे देखकर इसमें आपको कुछ भी संदिग्ध लगे। उस पर बिल्कुल भी क्लिक न करें। साथ ही आप साइबर सेल को भी जरूर सूचित करें।

3 अपनी जानकारी संभालकर रखें। अगर कंप्यूटर/स्मार्टफोन में इस तरह की जानकारी है तो उसे पासवर्ड या पैटर्न से सुरक्षित करें और पासवर्ड लिखकर रखने की आदत न डालें। सिस्टम को शट डाउन करने या किसी साइट पर हैं तो उसे लॉगआउट करने के बाद ही उससे बाहर निकलें।

साइबर अपराध की शिकायतें

2018	13,200
2019	23,300
2020	37,280
2021	38,110