गोपनीय / CONFIDENTIAL
2269
29 NOV 2021
प्र.मु.आ.आ.का.का-I, आं.प्र. एवं तेलंगाणा/A.P. & Telangana, हैदराबाद/O/o. Pr.CCIT-I, Hyderabad

भारत सरकार/GOVERNMENT OF INDIA
वित्त मंत्रालय/MINISTRY OF FINANCE
आयकर विभाग/Income Tax Department
91025
26 NOV 2021
Pr. Chief Commissioner of Income Tax
Andhra Pradesh & Telangana.
Income Tax Towers
A.C. Guards, Hyderabad 500 004

K Murali Krishna, ITS
Director (Security)
Tel: 040-23233877
Email: dirs.ap-dgt-dot@gov.in

Department of Telecommunications
Ministry of Communications
Government of India
AP LSA, Hyderabad

Lr.No. APLSA/Sec/Public awareness/2021-22 **Dated: 25-11-2021**

Respected Madam/Sir, Greetings for the day!!!!

Subject: Mobile related security awareness pamphlet released by DoT, Hyderabad

DDC (Vig)
FW 29/11/21
Smt Nagajyoti
Pls circulate

The **vigilance awareness week** for the FY 2021-22 was celebrated by Department of Telecommunications, APLSA (comprising both Andhra Pradesh & Telangana State) from 25th Oct to 01st Nov 2021.

As part of celebrations, a bilingual pamphlet on **Mobile related Security** was released by Shri J.V. Raja Reddy, ITS, Deputy Director General (Administration) & Shri G. Gouri Sankar, ITS, Deputy Director General (Security), DoT, Hyderabad for general awareness & safety of public of Telangana & Andhra Pradesh.

The awareness pamphlet enumerates most commonly observed frauds such as OTP frauds, KYC frauds, Smartphone phishing, QR code scan frauds, fake call centres, sextortion crimes etc. along with precautionary measures, complaint reporting mechanism and do's/don'ts.

The pamphlet is hereby enclosed for your kind information, circulation among officials of your department & others for maximum awareness please.

Your's Sincerely

K Murali Krishna, ITS

To,
The Principal Chief Commissioner of Income Tax (AP & TS),
AC Guards,
Hyderabad-500004.

Department of Telecommunications

Ministry of Communications

Government of India

भारत दूरसंचार

INDIA TELECOM

सत्यमेव जयते

MOBILE RELATED SECURITY AWARENESS

Type	Description	Impact of Fraud	Preventive measures
QR Code Frauds	The fraudsters somehow convince victims to scan a QR code in order to receive money but instead of getting credited, money gets debited	Financial loss i.e., Illegal withdrawal of money from bank account	**1) You don't receive money when you scan a QR code.** 2) Do not scan QR Codes shared by anyone unless the objective is to pay
KYC Frauds	The fraudster may text, call or email stating: "Dear customer your Bank account has been suspended for KYC. Please complete your KYC in 10 min by immediately clicking on the link"	Clicking on the link may lead to illegal withdrawal of money, download of malware which may read victim's login credentials, OTP,CVV etc	1) Think before you click any link as banks never send link to update KYC 2) Do not share confidential data such as OTP, CVV, PIN with anyone, including bank officials 3) Avoid installation of remote access applications
OTP Frauds	Fraudsters get OTP by: 1) vishing (making voice call) 2) illegal SIM swap/cloning 3) changing the mobile number linked to bank account 4) bypassing OTP process since 3D international gateways don't ask for OTP	Financial loss i.e., Illegal withdrawal of money or unauthorised purchases from bank account	1) **Never share any OTP, card number & CVV on debit/credit card or bank details with others** 2) Be judicious before sharing your phone number with unknown persons
Mobile Tower Frauds	Fraudsters cheat public by submitting a fake NOC in the name of a government department for erecting tower & promise hefty monthly rent on grant of permission for erecting tower in their premise	Financial loss i.e. victim may pay some advance or application fee to the fraudster before installation of tower	Be extra careful whenever asked for advance or money in any form & verify the credentials of the person/company. DoT or any other Govt department does not issue any such NOC
Smishing in Smartphone	Victim receives SMS with a link directed to phishing websites, allowing hackers to access victim's mobile device	Financial loss i.e., Illegal withdrawal of money from bank account	1) Avoid clicking on suspicious links. 2) Do not share personal /banking details on such website or link as it may be fake

Type	Description	Impact of Fraud	Preventive measures
Fake Call Centres	Fraudsters put up fake contact numbers of various brands online. The victim fall into the trap & clicks on suspicious links or provides bank credentials to the fraudster	Financial loss i.e. victim ends up paying amount to the fraudsters	1) Use company's app or visit authorized website only 2) Do not click on the links sent by unknown persons
Sextortion Crimes	The criminals honey trap victim and later invite for a video chat, during which victim is recorded	The criminal extort money by threatening the victim that video will be uploaded on a public platform	1) Do not receive video calls from unknown persons 2) Do not share personal details with unknown people online
Loan/Job/Gift Fraud	The fraudsters call, send SMS or Email & lure victims to click on a suspicious link in the name of instant loan, job or gift	Financial loss as clicking on the link may lead to download of malware which may read bank details, OTP,CVV etc	1) Never click on suspicious links 2) Do not install unknown Apps

In case of any cyber fraud, one may also register complaint at https://cybercrime.gov.in, apart from reporting to the nearest police station.

Five - Do's

1) Install antivirus & also use it regularly. Uninstall unused & idle Apps on regular basis.

2) Be careful while installing e-wallet since there are many fake e-wallet apps.

3) Update the operating system on regular basis to enhance security of your device.

4) Limit the permissions proportional to the service provided by the App.

5) If you receive an "international call" with "local number", please register complaint on Department of Telecom Toll Free number **1963 or 1800110420** as such calls may pose serious threat to national security.

Five - Don'ts

1) Never store important and sensitive information on mobile & social media platforms.

2) Do not save passwords in mobile phone. If necessary, at least use some form of encryption.

3) Never lend your phone to unknown person.

4) Do not visit suspicious websites such as pornographic, gambling etc., which may render your phone vulnerable & lead to sextortion, financial loss etc.

5) Never connect to unknown Wi-Fi networks. In case connected, do not make financial transactions using such networks.

Issued in public interest by:

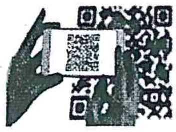
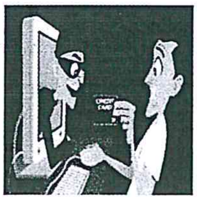
The Deputy Director General (Security), APLSA (comprising both Telangana & AP States), Department of Telecom, 5th floor, Telephone Bhavan, Saifabad, Hyderabad -500004.

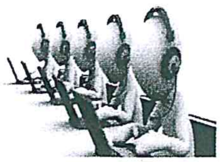
भारत दूरसंचार
INDIA TELECOM

టెలికమ్యూనికేషన్స్ విభాగం
కమ్యూనికేషన్ మంత్రిత్వ శాఖ
భారత ప్రభుత్వం

सत्यमेव जयते

మొబైల్ సంబంధిత భద్రతా అవగాహన

మోసాల రకాలు	వివరణ	మోసం ప్రభావం	నివారణ చర్యలు.
QR కోడ్ మోసాలు 	మోసగాళ్లు డబ్బును పంపిస్తాం అని QR కోడ్‌ని స్కాన్ చేయాలని బాధితులను ఎలాగోలా ఒప్పిస్తారు కానీ క్రెడిట్ పొందడానికి బదులుగా, డబ్బు డెబిట్ అవుతుంది.	ఆర్థిక నష్టం అనగా బ్యాంకు ఖాతా నుండి అక్రమంగా డబ్బు బదిలీ చేయడం.	డబ్బు స్వీకరించడానికి క్యూఆర్ కోడ్‌ని స్కాన్ చేయవద్దు. QR కోడ్ స్కాన్ అనేది చెల్లింపు చేయడానికి మాత్రమే, స్వీకరించడానికి కాదు.
KYC మోసాలు	మోసగాళ్లు ఈ విధంగా టెక్స్ట్, కాల్ లేదా ఇమెయిల్ చేయవచ్చు: "ప్రియమైన కస్టమర్ KYC కోసం మీ బ్యాంక్ ఖాతా సస్పెండ్ చేయబడింది. దయచేసి లింక్‌పై వెంటనే క్లిక్ చేయడం ద్వారా మీ KYC ని 10 నిమిషాల్లో పూర్తి చేయండి ".	ఆర్థిక నష్టం అనగా బ్యాంకు ఖాతా నుండి అక్రమంగా డబ్బు బదిలీ చేయడం మరియు లింక్ పై క్లిక్ చేయుడు వలన బ్యాంక్ లాగిన్ వివరాలు, OTP, CVV మొదలైనవి చదవగల మాల్వేర్ డౌన్‌లోడ్ కావచ్చు.	1) మీరు ఏదైనా లింక్‌ని క్లిక్ చేసే ముందు ఆలోచించండి. 2) కేవైసి ని అప్‌డేట్ చేయడానికి బ్యాంకులు ఎప్పుడూ లింక్‌ను పంపవు. 3) మీ OTP, CVV, ఏటీఎం పిన్ ని ఎవరికీ షేర్ చేయవద్దు, బ్యాంకు అధికారు లకు కూడా. 4) రిమోట్ యాక్సెస్ అప్లికేషన్‌లను ఇన్‌స్టాల్ చేయవద్దు.
OTP మోసాలు 	మోసగాళ్లు క్రింది విధముగా OTP పొందుతారు. 1)విషింగ్ (కాల్ చేసి మాయమాటలు చెప్పి) 2) మోసపూరిత సిమ్ మార్పిడి/సిమ్ క్లోనింగ్ 3) బ్యాంకు ఖాతాకు లింక్ చేయబడిన మొబైల్ నంబరును మార్చడం ద్వారా. 4) OTP ప్రక్రియను దాటవేయడం ద్వారా, ఎందుకంటే 3డి అంతర్జాతీయ గేట్వేలు OTPని అడగనందున.	ఆర్థిక నష్టం అనగా బ్యాంకు ఖాతా నుండి అక్రమంగా డబ్బు బదిలీ చేయడం.	1) ఓటీపీ ని ఎప్పుడూ షేర్ చేయవద్దు. 2) మీ ఫోన్ నంబర్‌ను తెలియని వ్యక్తులతో షేర్ చేయడం పట్ల భద్రతగా ఉండండి. 3) డెబిట్/క్రెడిట్ కార్డ్ నెంబర్, CVV మరియు పిన్ ఎవరితోనూ షేర్ చేయవద్దు.
మొబైల్ టవర్ మోసాలు	జారీ చేసిన నకిలీ NOC ని సమర్పించడం ద్వారా మోసగాళ్లు ప్రజలను మోసం చేస్తారు. టవర్ ఏర్పాటు కోసం ప్రభుత్వ శాఖ బాధితుడి ఆవరణలో టవర్ ఏర్పాటుకు అనుమతించిందని అలాగే ఎక్కువ నెలవారీ అద్దెకు హామీ ఇస్తారు.	ఆర్థిక నష్టం అనగా టవర్ ఏర్పాటుకు ముందు బాధితుడు మోసగాడికి కొంత అడ్వాన్స్ లేదా అప్లికేషన్ ఫీజు చెల్లించవచ్చు.	ఏదైనా రూపంలో డబ్బు అడ్వాన్స్ అడిగినప్పుడు మరింత జాగ్రత్తగా ఉండండి వ్యక్తి/కంపెనీ ఆధారాలను ధృవీకరించుకోండి. టెలికాం డిపార్ట్మెంట్ కానీ ఏ ఇతర ప్రభుత్వ సంస్థ కానీ ఎలాంటి NOC జారీ చేయదు.
స్మార్ట్ ఫోన్లో స్మిషింగ్	ఫిషింగ్ వెబ్‌సైట్‌లకు సంబంధించిన లింక్‌తో స్మార్ట్ ఫోన్ వినియోగదారుడికి ఎస్ఎంఎస్ చేయడమే స్మిషింగ్. ఆ లింక్ పై క్లిక్ చేసినపుడు హ్యాకర్లు మీ పరికరాన్ని యాక్సెస్ చేయగలుగుతారు.	ఆర్థిక నష్టం అనగా బ్యాంకు ఖాతా నుండి అక్రమంగా డబ్బు బదిలీ చేయడం.	1) మోసపూరిత లింక్ లపై క్లిక్ చేయకండి. 2) లింక్ లలో మరియు అటువంటి వెబ్‌సైట్లలో బ్యాంక్ ఇంకా వ్యక్తిగత వివరాలను ఎప్పటికీ నమోదు చేయవద్దు ఎందుకంటే అది నకిలీ కావచ్చు.

మోసాల రకాలు	వివరణ	మోసం ప్రభావం	నివారణ చర్యలు
నకిలీ కాల్ సెంటర్లు 	మోసగాళ్లు వివిధ బ్రాండ్‌ల నకిలీ సంప్రదింపు నంబర్లను ఆన్‌లైన్‌లో ఉంచారు. బాధితుడు ట్రాప్‌లో పడతాడు & అనుమానాస్పద లింక్‌లపై క్లిక్ చేస్తాడు లేదా మోసగాడికి బ్యాంక్ ఆధారాలను అందిస్తారు.	ఆర్థిక నష్టం అనగా బాధితుడు మోసగాడు అడిగిన ఫీజులను చెల్లిస్తాడు.	1) కంపెనీ యాప్‌ని ఉపయోగించండి లేదా అధీకృత వెబ్‌సైట్‌ను మాత్రమే సందర్శించండి. 2) తెలియని వ్యక్తులు పంపిన లింక్‌లపై క్లిక్ చేయవద్దు.
సెక్స్ టార్షన్ నేరాలు	నేరస్థులు బాధితుడిని హనీ ట్రాప్ చేస్తారు మరియు తరువాత వీడియో చాట్ కోసం ఆహ్వానిస్తారు, ఈ సమయంలో బాధితుడు రికార్డ్ చేయబడతాడు	నెట్‌లో వీడియో అప్‌లోడ్ చేయబడుతుందని బాధితులను బెదిరించడం ద్వారా నేరస్తుడు డబ్బులు వసూలు చేస్తాడు.	1) తెలియని వారి నుండి వీడియో కాల్‌లను స్వీకరించవద్దు. 2) ఆన్‌లైన్‌లో తెలియని వ్యక్తులతో వ్యక్తిగత వివరాలను పంచుకోవద్దు.
రుణం/ఉద్యోగం/బహుమతి మోసం	తక్షణ రుణం, ఉద్యోగం లేదా బహుమతి పేరుతో అనుమానాస్పద లింక్‌పై క్లిక్ చేయడానికి మోసగాళ్లు కాల్, ఎస్ఎంఎస్ లేదా ఇమెయిల్ చేసి బాధితులను ఆకర్షిస్తారు.	లింక్‌పై క్లిక్ చేయడం వల్ల ఆర్థిక నష్టం జరగవచ్చు. ఇంకా బ్యాంక్ వివరాలు, OTP, CVV మొదలైనవి చదవగల మాల్వేర్ డౌన్‌లోడ్ కావచ్చు.	1) అనుమానాస్పద లింక్‌లు ఎప్పుడూ క్లిక్ చేయవద్దు. 2)తెలియని యాప్‌లను ఇన్‌స్టాల్ చేయవద్దు.

సైబర్ క్రైమ్ నేరాలను సమీప పోలీస్ స్టేషన్ లో ఫిర్యాదు చేయడంతో పాటు సైబర్ క్రైమ్ పోర్టల్ https://cybercrime.gov.in లో కూడా నమోదు చేసుకోవచ్చు.

ఐదు – చేయవలసినవి

1) యాంటీవైరస్‌ని ఇన్‌స్టాల్ చేయండి & దీన్ని క్రమం తప్పకుండా ఉపయోగించండి. ఉపయోగించని మరియు పనిలేకుండా ఉన్న యాప్‌లను అన్‌ఇన్‌స్టాల్ చేయండి.

2) అనేక నకిలీ ఇ-వాలెట్ యాప్‌లు ఉన్నందున ఇ-వాలెట్‌ను ఇన్‌స్టాల్ చేసేటప్పుడు జాగ్రత్తగా ఉండండి.

3) మీ పరికరం యొక్క భద్రతను మెరుగుపరచడానికి ఆపరేటింగ్ సిస్టమ్‌ను రెగ్యులర్‌గా అప్‌డేట్ చేయండి.

4) యాప్ ద్వారా అందించబడే సేవకి సరిపడు వరకే అనుమతులు ఇవ్వండి.

5) మీకు "లోకల్ నంబర్" తో "ఇంటర్నేషనల్ కాల్" వచ్చినట్లయితే, దయచేసి టెలికాం డిపార్ట్మెంట్ టోల్ ఫ్రీ నంబర్ 1963 లేదా 1800110420 డైల్ చేసి ఫిర్యాదు నమోదు చేయండి, అలాంటి కాల్స్ దేశ భద్రతకు తీవ్రమైన ముప్పు కలిగిస్తాయి.

ఐదు- చేయకూడనివి

1) మొబైల్ & సోషల్ మీడియా ప్లాట్‌ఫారమ్‌లలో ముఖ్యమైన మరియు సున్నితమైన సమాచారాన్ని ఎప్పుడూ నిల్వ చేయవద్దు.

2) పాస్‌వర్డ్‌లను మొబైల్ ఫోన్‌లో సేవ్ చేయవద్దు. ఒకవేళ తప్పనిసరైతే, కనీసం ఏదో ఒక ఎన్‌క్రిప్షన్‌ని ఉపయోగించండి.

3) మీ ఫోన్‌ను తెలియని వ్యక్తులకు ఎప్పటికీ ఇవ్వవద్దు.

4) అశ్లీల, జూదం మొదలైన అనుమానాస్పద వెబ్‌సైట్‌లను సందర్శించవద్దు, ఇది మీ ఫోన్ కి హాని కలిగించేలా చేస్తుంది మరియు సెక్స్ టార్షన్ , ఆర్థిక నష్టానికి దారితీయవచ్చు.

5) మీకు తెలియని వై-ఫై నెట్‌వర్క్‌లకు కనెక్ట్ చేయవద్దు. కనెక్ట్ అయిన సందర్భంలో, అటువంటి నెట్‌వర్క్‌లను ఉపయోగించి ఆర్థిక లావాదేవీలు చేయవద్దు.

ప్రజా ప్రయోజనాల కోసం జారీ చేయబడింది:

డిప్యూటీ డైరెక్టర్ జనరల్ (సెక్యూరిటీ), ఏ పి ఎల్ స ఏ (తెలంగాణ మరియు ఆంధ్ర ప్రదేశ్ రాష్ట్రాలు రెండిటికి), టెలికాం డిపార్ట్మెంట్, 5 వ అంతస్తు, టెలిఫోన్ భవన్, సైఫాబాద్, హైదరాబాద్, తెలంగాణ-500 004.