Public Health and Safety in the use of Mobile Communications

Mobile services are already an everyday part of many people's lives. They are transforming the way we live, work and communicate, and helping change people's lives for the better by creating access to services and enabling economic development.

The exponential growth in mobile services has also given rise to health concerns with regard to exposure to emissions from telecom towers and mobile phones.

The report will take you through the basics of what are Electro Magnetic Fields (EMF), how mobile telecommunication services are provided, what are the safety standards for EMF, the latest scientific reviews, the views of some experts in this field as well as address some of frequently asked questions and some common myths and facts .

Click here to read more. Spread the word and share with your friends today.

Important communication from TRAI

TRAI prohibits using personal numbers for telemarketing purposes. Please ensure your number is not involved in such activities.

DNSChanger Malware threat

Some customers may face a connectivity disruption because of a malware infection due to DNSChanger in their machines. If the machine is infected, it will also infect the router and cause the traffic to go to a false DNS server. In USA, the law enforcement agencies are identifying and shutting down these false servers. This is a step to protect global users of Internet. The advisory from CERT.in provides you directions to check if your system is infected and, if so, enables you to correct it. Click here for more details from CERT.in.

Alert on malware protection

There is a reported increase in malicious activity by fraudsters in the telecommunication world. Complex malware, such as bot-nets may infect your systems and cause interruption or data-leak. Please keep your anti-virus updated and run frequent scans to prevent such infection. Click here for more details from CERT.in.

Don'ts

We would like to issue a general advisory to caution Indian telecom customers who are being arbitrarily targeted by calls fraudulently claiming the recipient customer as being a Prize/Lottery Winner.

In these types of phone frauds, the customer returns a missed call to a +92 or +375 country code and inadvertently reaches a fraudster pretending to be representative of airtel or another Indian mobile operator and informs the customer of having won some lottery/prize money. The fraudster then attempts to trick the customer into divulging sensitive personal information and to pay a commission to receive the winnings. Such commission is usually asked to be paid via an international OTH operator's recharge vouchers.

To protect all our mobile subscribers from such malicious activities which may result in substantial increase in your phone bill, airtel would like to advise the following:

- Do not respond to any unexpected calls from a number with the +92 or +375 country code. Click here for more details
- Do not respond to any suspicious missed calls from unknown numbers. In case of such suspicious calls, please report the same to us immediately at 121@in.airtel.com.
- Do not get lured into any financial transactions or divulge any personal information like IMEI, Bank Account number and other information to callers offering prize money or lottery winnings. Also do not respond to any instructions to dial an international number to get the prize money.
- This luring may also be done through SMS messages offering prize money and seeking personal details on a specified email ID. Please do not respond to these.
- Do not respond to any SMS/Email from unknown sources prompting you to call on a number or go to a site offering free download of content/movie clips/pictures.
Do's

- Avoid going from your mobile browser to sites which offer unreliable and questionable content.
- If you inadvertently access any of these sites, close any/all pop-up windows that may have opened.
- You should not download and/or install any software from sites where there are a large number of pop-up windows. Read everything carefully before clicking OK, especially when you are going to download something.
- Please be aware that certain websites use mobile or fixed line number to make outgoing calls. This is an illegal activity. Do not post your mobile number or fixed line number on the websites unless you are very sure that the site is secure.
- Do not delete data from your browser’s history files, to enable you trace back problems, if necessary.
- Keep Bluetooth connectivity off when not required and keep the security feature of your handset on high mode.
- Periodically check the icons on your handset and ensure that no new icons have appeared that has not consciously been installed by you.
- Check your Mobile bill regularly for any anomaly (to check for Outgoing International Calls). You may subscribe to daily unbill alerts by sending ‘SUNB’ to 121 to check on your usage.
- Format your handset if you feel that unintentionally any of the above may have happened with you, this will remove malicious software from your handset.
- Refrain from sharing any personal information, identity proof or making any payments to people promising lottery or other unexpected awards.

Cyber Security Awareness

Mobile phones are becoming ever more popular and are rapidly becoming attractive targets for malicious attacks. Mobile phones face the same security challenges as traditional desktop computers, but their mobility means they are also exposed to a set of risks quite different to those of a computer in a fixed location. For more information, please visit DotY website at Mobile phones are becoming ever more popular and are rapidly becoming attractive targets for malicious attacks. Mobile phones face the same security challenges as traditional desktop computers, but their mobility means they are also exposed to a set of risks quite different to those of a computer in a fixed location. For more information, please visit DotY website at www.secureyourelectronics.in.

In respect of frauds related to installation of Mobile Tower

It has come to our notice that some companies/agencies/individuals cheat general public by promising hefty monthly rental payment and ask them to deposit money in their personal/companies account as security deposit/application fee/registration charges/stamp duty/government tax under Telecom Act/clearing of the advance payment etc., in lieu of leasing/renting the premises of individuals for installation of mobile tower or for any other purpose. After collecting the money these companies/agencies/individuals become unreachable. These companies/agencies/individuals at times issue fake and misleading advertisement or communications in violation of our trademarks and other intellectual property rights. In view of this we “Bharti Airtel Limited” hereby caution the public at large that:

- A mobile tower may be installed by either Telecom Service Provider (TSP) or Infrastructure Provider (IP-1) as per their licensing/registration conditions. The updated list of TSPs and IP-1 is available on DoT website i.e. www.dot.gov.in. The public at large are cautioned that before they entertain any offer for installation of tower, they should verify the authenticity of TSP/IP-1 from DoT website and the concerned TSP/IP-1.
- In case any company/agency/individual is asking for advance or for application fee or for money in any form before actual installation of tower, public is hereby cautioned to be extra careful and verify the credentials of the company.
- Any person or entity found fraudulently involved in such activity like i) taking advance etc., in the name of installation of mobile towers, ii) using name/logo/recommendations of Bharti Airtel Limited is liable to be prosecuted under applicable law. If any person comes across any such fraudulent activity then he/she may report the incident to local police authorities. In addition or alternatively the local TEC Cell may also be contacted whose contact details are available on DoT website i.e. www.dot.gov.in.
- Anyone dealing with such companies/agencies/individuals will be doing so at his/her own risk and Bharti Airtel Limited shall not be held responsible for any claim or loss or damages, whatsoever, suffered directly or indirectly.

Issued in the public interest by Bharti Airtel Limited, Registered Office: Bharti Crescent, 1, Nelson Mandela Road, Vasant Kunj, Phase II, New Delhi 110070, India. Tel: +91 11 4666 6100. Fax: +91 11 41666 6137, e-mail: 121@in.airtel.com, website: www.airtel.in DIN: L74899DL 1995PLC0070609