Wi-Fi Best Practices – Things that we all must do to keep our Wi-Fi networks secure:

- Most Wi-Fi routers by default have all the security options turned off. This means that anyone and everyone can use your wireless network without your knowledge and permission. The first thing that you must and have to do is turn lots of security options on in your Wi-Fi router.

- If you do not follow what is happening around and your wireless internet is misused in some ways, you are held personally responsible. People in a radius of 500 feet in all directions will also be held responsible, thus it is in your best interest to make sure that there are no insecure wireless networks in your surroundings. We already have had two cases in a month where an insecure wireless network has been misused and there will be more to follow.

- When you access the configuration pages of your router using a web browser, you will be asked to give a password. Normally the password by default is either blank or a well known word like 'admin' or 'password' depending upon the make of the router. Please change the default password, because even if you have the best security enabled, if a person knows the router's administrator password, the bad guy would disable the security, use your internet account with impunity and then re-enable the security. So, we are saying this again that please change the default password for the web enabled administrator's account of the router. This is the most important thing you must and have to do.

- No matter what the manufacturers of wireless routers tell you, one of the most difficult jobs in the world is to get your wireless router securely connected to the internet. At times, it has taken us over 3 hours to get everything right. As the TV ads say, don't do this alone at home, this applies to configuring routers also. Use expert help.

- The problem with security is that most people do not understand how to secure a wireless router. You must be very careful when you ask someone else to secure your router as you have no way of finding out how much they know. There is no formal qualification that assures enough knowhow on securing wireless networks anywhere in the world.

- You need to secure your Wi-Fi network for two reasons, one nobody that you do not approve off should be able to use your internet connection and second the data that leaves your wireless network must be garbled or unreadable or to use the right word, be encrypted. If your data does not leave your computer in an encrypted form, then anyone in a 500 feet radius could read username and password of your internet account, web mail account, e-banking account, share broking account, e-commerce account etc and then may use that information to act as 'you'. He could steal all your money or read your e-mail or transfer your shares and you would not even know.

- Think three times before you use a free wireless account or hot spot because other people can also see what you are doing if the hot-spot is not properly set up.

- As Windows likes connecting to a wireless network without asking you first, please make sure that you do not allow anyone else to share your computer/hard disk. Make sure that sharing is off.

- The computer industry will never get anything right the first time. The initial method for security for wireless networks is called **WEP** or **Wired Equivalent Privacy**. In plain English this means that WEP can be broken,

WEP is very easy to crack, WEP does not work, WEP is a mistake, WEP is something that you must not use at all. Even your worst enemies must not use WEP as it can be cracked at times in 10 minutes flat using free tools available on the internet. We are saying it again, WEP has nothing to do with wireless security and the government must ban the use of WEP. Read our lips, do not use WEP at all. WEP means an insecure wireless network.

- Please use the latest security, which is called **Wi-Fi Protected Access** or **WPA**. You could use **WPA** or **WPA2**, which is equally good and it makes no difference which one you use. As of today, nobody has been able to crack WPA security. Tomorrow is however another day. Enable WPA on your router and sleep well at night.

- Normally you would learn a lot of wireless jargon along the way, the full form is **WPA-PSK**, **PSK** is **pre shared key**. A password that you cannot remember is a key and pre shared means that your router and the machines that connect to it have to share or use the same key. We use lots of jargon for no rhyme or reason.

- Every router has a name by default. It is a good security hygiene to change this default name of the router or network name. Why should anyone know what router you are using? The minute a bad guy knows it, he can try and use a vulnerability on your router and then attack your router. The less he/she knows about your router the safer you are. This router name or network name is called the **SSID** or **Secure Set ID**. There is nothing secure about this name nor does it represent a set. We love confusing you by using words that have no basis in reality at all.

- Every wireless router would broadcast its SSID at regular intervals to tell wireless clients that they are around. It is a good idea to **disable SSID broadcasts** so that bad guys do not know that your router is around. This would not stop your laptop from connecting to the wireless network as it has connected in the past and it remembers the SSID of the router.

- This, however, is not a thing that will stop a bad guy from knowing about your router. A bad guy could use free network sniffers to find out about the existence of your wireless router. The whole idea is that the more you stop the bad guy from getting to know about you, the better it is for you and the safer you are.

- A wireless router creates what is technically called an **AP** or an **Access Point**. The computers that connect to an AP is called a station. A station along with an AP is called for some weird reason a **BSS** or **Basic Service Set**.

- Every desktop computer or laptop has a wireless card which has a unique number burned into the card. This number is unique not only on earth but within the solar system. This number is called the **machine number** or **MAC address** or **Ethernet address**. Technically **MAC** is the **Media Access Control address** and not machine address but we will not try and get nit picky about terminology. It is a very good idea to note down the MAC addresses of all the computers that you will connect to your Wi-Fi router. Then you must set access control on for your router and instruct it to only allow those MAC addresses that belong to the machines that you own. No other machine will be allowed access.

- You must be wondering that when we have WPA security enabled, why do we need another level of security. The first e-security principle is that we must never rely on only one layer of security as it will fail one day or the other. So, always have more than one layer of security active. It is

also called the onion defense, as onions have multiple layers unlike an egg that has only one layer as a defense mechanism.

- To find out the MAC address, use the command Ipconfig /ALL in a command or shell prompt. The BSSID is the MAC address of the router.

- There is no such thing as 100% percent security. You may follow all these rules and yet someone may hack your wireless security. All that we are doing is lowering the probability of someone breaking your security defenses. After all people do get killed by lighting but the odds are low. This is why we would ask you to switch your router off when you are not using it for a long time.

- Physical protection of your router is also very important. Someone, who has physical access for say 15 seconds to the router, would use the cheapest ball point pen and reset your router as the reset button is normally at the back of the router. This would remove all the security options you have set and router will restart with no security.

- If you allow a technician to come and change some settings on the router make sure that he does not steal your passwords or change the security settings. Trust no one in this world, when it comes to security.

- Most people do not use a computer only to connect to their Wi-Fi router, they also use mobile phones. I for instance use Internet phone on my mobile phone to talk to another mobile phone in India and abroad and use my Wi-Fi connection to do so. It saves a lot of money and the voice clarity is better. You must understand the security system on your mobile phone also. You cannot be paranoid enough.

- All machines that connect to the internet using your wireless router are using your IP address. There is no way for investigators to know which machine actually sent out the mischief e-mail. This is why the owner of the router is suspect.

- As wireless routers do not cost a lot of money, for under Rs. 3000, you can buy a very good router, they have extremely poor logging systems. The wireless routers find it difficult to save a copy of all traffic that flows through them. It is a very good idea and something that we must all do is to turn all the logging and saving of data by the wireless router on. Some of them have an option of sending you an email of the log data when the logs get full. The more log data you give the investigators, the easier you make it for them to catch the culprit. Lots of wireless routers actually save a copy of all unique computers that have connected to them in the past. This helps investigators actually pin point all the machines that were on your network in the immediate past.

- All wireless routers have different ways on configuring security. The basic principles are what we have enumerated above. The problem is that their user interfaces are as different as chalk is from cheese. This confuses anyone, who is trying to configure a router for the first time.

- The latest wireless routers have wizards that help you set them up and also a one button push security. They claim that the wizard would set up your router if you simply follow simple steps that a ‘panchivi’ fail student can do. They also claim that if you push a button on the router and computer, security gets set up automatically without human intervention. All this is true but in our case as the phases of the moon were not aligned as advertised, things do not work as expected. Use the latest wizards and one button claims out but bear in mind that it may not

work for you. Like it never works for us. Take claims with a tablespoon of salt in our line of work.

This is version 1.0 of the security steps you need to take and very soon we will come back with version 2.0.

Security is a journey which will never end.

It is not a question whether your wireless network will be broken into or not. The real question is ‘when will it be broken into?’
