Mobile phones, roaming, hacking and rip-offs

After years of travelling with mobile phones, the whole business can still be a little bit fraught even in the EU and USA , especially if you don't want to be eavesdropped, hacked, ripped-off or otherwise inconvenienced.

Your phone connects to the outside world in three independent ways:-

1. Via the mobile telephone network, (i.e. masts and such). This covers 3G/ 4G and soon 5G and covers sending and receiving. This is also known as **roaming**. Different countries might use different frequencies but a modern phone should figure it out. Can involve large amounts of money.
2. Via a wireless router within range, (aka Wifi) and covers sending and receiving. Generally involves modest amounts of money and is often free.
3. Via GPS, in which case it only receives but it does mean that you can use free mapping apps like Navmii even with options 1 and 2 turned off, (more later). Free.

I will treat them one by one.

1. *Mobile telephone network.* So long as you are within range of a mast and you are allowed to use roaming, your phone will send and receive calls, send and receive text messages (aka **SMS**) and send and receive data (for example by accessing websites or sending and receiving email) and generally suck huge amounts of money from your account when you are away from home, especially in places like South America. Nowadays its possible to get packages of calls/SMS/data such that your allowance covers both the UK and EU/USA but make sure you know this, (and after B*$!xit it might no longer continue in the EU). Outside the UK/EU/USA, its down to individual deals. Calls and text messages are usually separated from data when roaming and your phone will allow you to turn off data roaming whilst still allowing calls and SMS. You should ALWAYS turn off data roaming because your allowance may be small or zero and mobile phones are forever automatically updating themselves by downloading new versions so that programmers can fix all the bugs they missed by rushing it out in the first place, and add all the new bugs so that it fails in new and exotic ways. If you really must use the mobile network to do a bit of browsing, make sure you turn off the automatic updating of apps. You should generally treat apps as assiduous gardeners treat weeds.

However, stopping it downloading mostly useless data doesn't stop you receiving yet another ambulance chasing phone call from a Birmingham number, (I'm not being unfair, ALL mine originate with Birmingham numbers). First of all you can only block them after you have received one and second, in many parts of the world, (such as South America), you get charged for both sending AND receiving phone calls, (a princely £1.80 a minute or part of a minute in Chile for example at the time of writing).

So, what can you do ? In short, switch your phone into Flight mode (the little airplane) when you get on your flight out and this blocks all calls, SMS and data coming down the mobile network. Its so satisfying that you might want to do this permanently, but if not, leave it in flight mode until you return home.

Another alternative is to choose the Phone app, go to settings and look for something like "Block Unknown Callers" and select it. Then add numbers you want to hear from using the + icon. Bear in mind you might forget somebody.

However, you probably want to continue communicating generally while you're away but without your bank account being emptied by "I'm ringing about the accident I'm hoping you have had" type of call, so this leads us to 2.

2. *Via a local wireless router, aka Wifi.* **To receive Wifi whilst your phone is in Flight Mode, just click on the Wifi icon.** Wifi is so ubiquitous today that its almost impossible to escape it. Unfortunately, most of them (hotels, cafes, hotspots … etc) are so badly protected that they are riddled with hackers and other lowlife all ready to steal everything you have. Whether they are protected or not, they will ask for your email address so they can send you endless marketing bumf or worse, sell it to a spammer. When you use Wifi, it is a relatively simple task to eavesdrop on everything you send or receive without you ever knowing. Even when you use a HTTP site leading to a secure HTTPS site, it can be hacked. (If you don't know what this means, don't worry, it just means that browsing through poorly secured Wifi is problematic for all kinds of reasons even when you might think it OK). Even worse, for emails, even though you might not mind third parties reading your words of wisdom, some local routers use servers which don't support security protocols, so that when your phone logs in with your username and password to get or send your emails, both finish up travelling across the internet without encryption so anybody can (and does) read them. (This occurs about once a week amongst my friends). Even worse, quite a few Wifi routers are set up to block free services like WhatsApp in a desperate bid to make you use their over-priced paying services.

You might think that all of this could lead to really widespread identity theft. It does, and welcome to the 21st century. (This does not include the massive amounts of data lost or stolen every year from companies to whom you entrust it by the way.) By and large "Cybersecurity" is an oxymoron.

So, what can you do ? Its slightly techy, but you can sign up for something called a VPN (Virtual Private Network) for about £50 a year. An example is witopia.net and there is lots of info on their website. There are others. On Android, using an app called openVPN, you can set your phone up such that everything coming in and out is encrypted. Just start it up and the rest is invisible. (It does this by opening a secure gateway called a tunnel between you and the destination and sending everything down it, email, browsing, …. It also has the benefit that such tunnels bypass attempts to block WhatsApp allowing you to use its phone, video and text messaging, (which are separately encrypted anyway).)

3. *GPS.* You don't have any control over this other than enabling it or disabling it but if you switch off 1. by using flight mode (to avoid expensive data downloading, nuisance calls and SMS) and you don't have any access to 2. because you are out of range or its expensive, you can still access GPS data. Some apps only use this channel to give you a basically free geographic service, (Navmii is one example although they make a small charge for downloading multiple maps – make sure you download them before you leave home though). So long as your phone can see enough satellites, it works wherever you are without troubling either 1. or 2.

You have one other alternative of course. Just switch it off until you get home and then you don't have to worry about charging it either.

** Disclaimer. I believe the above was accurate at the time of writing. All of it should be fine for Android phones but the principles are the same for iPhones. However, it's free advice and I don't warrant anything so you have been warned. I specifically do not endorse any of the products I mentioned. **