



Introduction

When dealing with the Internet, it is imperative to ensure the security and privacy of ALL one's data. Information on how to do this is offered below.

Securing the wireless network

Wireless devices broadcast via radio waves, which are sent out by a transmitter. This means that any receiver within range (and tuned to the transmission frequency) will receive the signal. Thus, when personal information is to be transmitted, it must be guarded against un-authorized access (usually referred to as 'eavesdropping'). There are a number of security/privacy risks inherent in wireless communication, as outlined below:

Risks related to Bluetooth

Bluetooth devices communicate using short-range wireless signals and operate on a frequency band between 2.4 GHz to 2.4835 GHz, achieving speeds of up to 1 Mbps. They can be used to link a mobile phone to a headset, a keyboard or a mouse to a computer and a laptop to a printer. The use of Bluetooth technology presents the following security/privacy threats:

- **Bluesnarfing**, which is the un-authorized access to personal data, such as; calendars, contact lists, emails, text messages, pictures or videos
- **Bluebugging**, which allows an unauthorized person to take control of another person's phone – allowing them to listen in to conversations, make calls and send messages
- **Bluejacking**, which is the sending of unsolicited messages, via the Bluetooth technology, to other Bluetooth-enabled devices.
- In order to protect against such risks, Bluetooth users are advised to ensure that all such devices are protected by default passwords, and that all Bluetooth functions are turned off when not in use.

Mobile phones

Because they can be used for voice transmission, as wireless modems and as web browsers, mobile phones can be accessed by unauthorized persons to obtain personal data.

Wi-Fi

Wireless Fidelity (Wi-Fi) is wireless data network, which allows Wi-Fi-enabled devices (such as PCs or mobile phones) to connect to the Internet – at such time as they are in the vicinity of the wireless data network. Offering low-cost implementation and high-access use, WiFi areas are sometimes termed 'hot spots' and are typically deployed in public areas – such as airports, universities, bookstores, coffee shops, offices and hotels. In the interests of security and safety, users of Wi-Fi are advised to encrypt all data before transmission. Small organizations are also advised to consider the use of **WiFi Protected Areas**, while the larger organizations are advised to consider the use of **Virtual Private Networks (VPN)**



Securing wireless networks

Any device within a wireless network can serve as an illicit entry point to the entire network if it is not properly protected. It is therefore vital to secure the entire network rather than to secure specific devices. Users wishing to secure their wireless network are advised to:

- Encrypt all data during transmission
- Use antivirus and anti 'spy ware' software as well as firewalls
- Turn off identifier broadcasting. Change the identifier of the router from the default
- Change the router pre-set password
- Allow only specific computers to access the network
- Turn off the wireless network when it is not in use.

Identity theft

Identity theft is the theft of a person's name, PIN number, ID card number, credit card number or other personal data. The usual means by which identity theft is accomplished is by 'Phishing', whereby a fraudulent but credible e-mail is sent to the victim – soliciting all such personal data as is required. Once this personal data is obtained, it can be used to access funds, run up accounts or to facilitate a broad range of fraudulent practices. There are a number of indications that identity theft has been perpetrated. They are as follows:

- The appearance of invoices or proof of purchase regarding items that the user did not purchase
- Calls from debt collection agencies relating to same
- Apparent redirection of utility bills and other important correspondence
- The erosion of the user's credit rating.

What to do if you become a victim of identity theft

- Place a fraud alert on your credit reports
- Close any accounts that have been accessed
- File a police report
- Notify the relevant regulatory authority.

Spam scams

Most people are resigned to the fact that they receive 'spam' (unsolicited 'junk' mail). Such mail can, however, prove a serious security risk. Some spam messages, for instance, request the provision of personal data – which can lead to identity theft, as outlined above. Others invite entry to websites – which can, in themselves, offer a wide range of personal and security risks; yet others are designed to perpetrate a specific 'scam', which has been deliberately designed to defraud the victim of his/her money.

To avoid becoming a victim of 'spam' scam:

- Protect your personal information
- Know who you are dealing with
- NEVER act impulsively
- Obtain all promises, guarantees or agreements in writing first.
- Disregard any offer that asks you to pay for anything in advance
- Consider the use of a 'spam filter'

How to respond to such scams

The best way to respond to all such scams is NOT to respond, never to send funds, never to volunteer ANY personal or financial information and to remember that things which sound 'too good to be true' generally are.