PROTECT YOURSELF FROM UNWANTED INTERNET USAGE

The internet is a fascinating medium allowing access to information and entertainment in the fastest and most convenient form ever available. Of course as with any popular medium there are some people who target others using the Internet with unsolicited advertising or other activities that were not initiated by the end user. All of these activities generate Internet traffic. TransACT has various anti spam and anti virus programs running on its email service that block many of these unwanted activities before they reach our users email accounts. However, it is impossible to prevent or block all activities.

Don’t leave Peer-to-Peer Applications running unattended

Our experience is that a vast majority of usage queries directly relate to those users that have installed and use Peer-to-Peer applications such as Kazaa, eDonkey, iMesh, etc.

The nature of these programs makes tracking the amount you have downloaded very difficult. When using these types of applications to download software, the download process may slow down or stall for some period of time, then resume. Depending on the size of the file you are downloading and the client you are getting the file from, the time taken from starting the download to finishing could be anywhere from a few seconds to a few days.

If you do not wish to remove your Peer-to-Peer application, then make sure you have fully closed it down when you have finished using it, otherwise any downloads that are in progress will continue. Generally, with most of these applications, clicking on the close button (the little ‘X’ in the top right corner), will only minimise it to the system tray (where your speaker icon and time is).

This does not actually close the application completely – to do so you’ll have to right-mouse click on the relevant system tray icon and select ‘Close’. Or you can generally go to the ‘File’ menu option and select ‘Close’ from there.

Be aware that many Peer-to-Peer applications install additional software, commonly referred to as adware, spyware and malware. This software may continue to download from the Internet even after your Peer-to-Peer application has been closed, commonly to display popup advertising.

Some Peer-to-Peer applications allow your computer to act as a “router” or “hub”. This means that while you may not be downloading; other users of the Peer-to-Peer network may be downloading via your computer. If your computer is used by more than one person, be aware of the software that they install on it. While you may not use Peer-to-Peer software, a relative or friend may have installed it on your PC. If you share your computer – regularly check the list of installed applications.

Install an Anti Virus program on your PC

One of the most prolific and dangerous activities on the internet is the distribution of “virus” type programs. Virus programs are not only unwanted and dangerous they also generate usage against your account which was not initiated by you.

Whilst TransACT’s anti-spam and anti-virus software will detect and clean a large proportion of these programs travelling through the email system, viruses can still spread through other means such as some web pages, through encrypted email that can't be scanned, from floppy disks/CD’s, directly via the Internet from another computer, etc. It is your responsibility to ensure you have appropriate protection in place for your systems from virus threats. Therefore we strongly advise you to install and run a reputable anti-virus product on your PC.

TransACT will charge for usage that is generated by virus type programs.

Enhance your protection from unwanted activates with a firewall
A firewall is similar to installing a fence around your pool to keep people out. It is important to configure your firewall correctly. Windows XP has an excellent and easy to configure software firewall but there are 3rd party programs available to run on other operating systems.

For more information we suggest that you consult with an IT technician and investigate a combination software firewall + anti-virus solution.
Hardware firewalls are another way of enhancing security. Again, an IT technician can advise you on the best steps to take to secure your connection.

After using the Internet, log-off by closing all Internet software
Some of the programs you have running on your PC generate Internet traffic as part of their normal operation. Sometimes they may be doing this in the background.
When you have finished with your internet activities disconnect by:-

- Placing the modem into standby mode by pressing the button on the top.
- If you are a **HomeTALK customer** as well, then your modem should not be placed into standby, instead to ensure that you are no longer connected to the internet, disconnect your computer from the cable modem (cat-5 or USB) – or switch off your computer.

Be careful with e-mail from sources you do no know
Be careful when opening e-mails from people you don’t know. They may contain harmful viruses or programs that can damage your computer settings. Make sure you set your anti-virus program to scan email and keep your anti-virus programs virus definitions up to date.

Update your software regularly
Software companies release patches from time to time (such as Microsoft do for the Windows operating systems) to overcome security holes in their product as they are identified. It is important to keep your software up to date with the latest security patches to minimise the possibility of your Internet connection being compromised. These patches are usually, but not always, provided free of charge to you via the software supplier’s website. Automatic updates should be seen as necessary investment. You should however be aware that updates do contribute to your Internet usage.

Be aware when downloading software off the Internet
Software can contain viruses or have the ability to change your computer’s settings and should therefore be scanned before being loaded onto your computer. Software should only be installed from reputable sources which will reduce unwanted applications being installed. Again, these unwanted applications may cause you to unknowingly download data.

Don't leave your web browser open on a page with automatically refreshing content

Some web sites need a lot of traffic to flow between your PC and their site to function. There are some web pages that automatically refresh themselves after a certain time period, eg banner advertisements that reload every minute or so. If you leave your browser on a page like this for a long period of time, they could end up costing you a lot of money. WhitePages and YellowPages are examples of pages that exhibit this behaviour.