thebuzz

Buzz Insurance Security Statement

Online security

The protection of your personal information is a priority for us. We take all reasonable precautions to protect your personal information from loss, misuse, unauthorised access, modification or disclosure.

How can you be sure your personal information is secure?

The information you provide to us via this website is encrypted as it travels between your computer and our computers. We use a strong form of encryption (secure socket layer - SSL), making it almost impossible for others to access your information. Two ways of knowing when you are using a secured section of our website is to look for the small padlock symbol in the bottom right hand corner of your browser and secondly the web address in your browser window will start with “https” instead of “http”.

Your personal information is stored on our computer systems which are protected from unauthorised access by a combination of technologies (firewalls, secure logon processes, encryption and intrusion monitoring technologies). We use an industry recognised payment service provider to process any insurance payments you make using this website. The service provide is required to protect your personal information on our behalf.

Communicating with us via the internet

Our website enables you to communicate with us electronically using the internet. We need your email address in order to respond to your communications with us, however we will not utilise your email address for the purposes of sending unsolicited email messages (referred to as Spam).

We will not ask you to provide or confirm personal information via email. An email purporting to come from us that asks for this information should be discarded as it’s likely to be an attempt to steal your personal details (referred to as 'phishing').

Securing your personal computer

There are three things you can do to secure your online experience:

- Antivirus and Spyware Protection. Install a commercial quality antivirus/spyware protection software package on your PC. All of the commercial packages can be configured to automatically update themselves with the latest patterns and protection so you are always up to date.
- Firewall. Make sure you have an active Firewall. A Firewall is a device that prevents unauthorised users from accessing or connecting to PCs or networks. Most firewalls also enable some internet content filtering, blocking of advertisements and SPAM email as well as providing logging and alerting of intrusion attempts. Most of the publicly available PC Security packages provide antivirus, antispyware and firewall protection all bundled into the one package
- PC Operating System. Keep you PC’s operating system up to date with the latest updates. Both Apple and Microsoft provide automated means to download and install the latest updates providing the best protection against security flaws

The Buzz Insurance
388 George St, Sydney
NSW 2000, Australia
www.thebuzzinsurance.com.au

thebuzz

Securing your wireless connection

If you use a wireless network at home, taking a few extra minutes to configure the security features will protect you and your wireless network.

Don't broadcast your SSID

The SSID (Service Set Identifier) is constantly broadcast which allows you to locate your WLAN (Wireless Local Area Network) quickly and easily. It also allows anyone else (even neighbours) to also see your WLAN. Turning off this broadcast does not affect your WLAN's performance and makes it invisible to others.

Establish an access list for your router

Most WLAN routers allow you to establish an access list. This means that you enter or select which devices you want to allow access to your WLAN usually based on the devices MAC address, a unique 12 character code. The router's interface will display what devices are connected or trying to connect and their respective MAC address and you use this information to add the devices you want to the router's protected access list. This feature is also known as "MAC Filtering".

Enable encryption

By far the best and most secure way to protect your WLAN is to enable encryption. All wireless devices will support encryption of one form or another. The two main standards are WEP (802.11's Wired Equivalency Privacy) and WPA (Wi-Fi Protected Access) or WPA2. WPA is stronger and is built into Windows XP and virtually all modern wireless hardware and operating systems.

Secure your WLAN router's administrator's interface

If your SSID is being broadcast, then even neighbours are able to see your WLAN and if they have a similar model router to you, would be able to call up your router's administrator's interface. Most systems ship with a weak default password like "password" or none at all, so your first action should be to change this password to something robust. Remember, someone attempting to hack into your system will have an unlimited number of attempts at guessing your password.

Disable remote administration

Most WLAN routers have the ability to be administered via the internet. Unless you absolutely need this ability, it is best to disable this feature.

For more information about the way we deal with your personal information, please see our Privacy Charter

The Buzz Insurance
388 George St, Sydney
NSW 2000, Australia
www.thebuzzinsurance.com.au