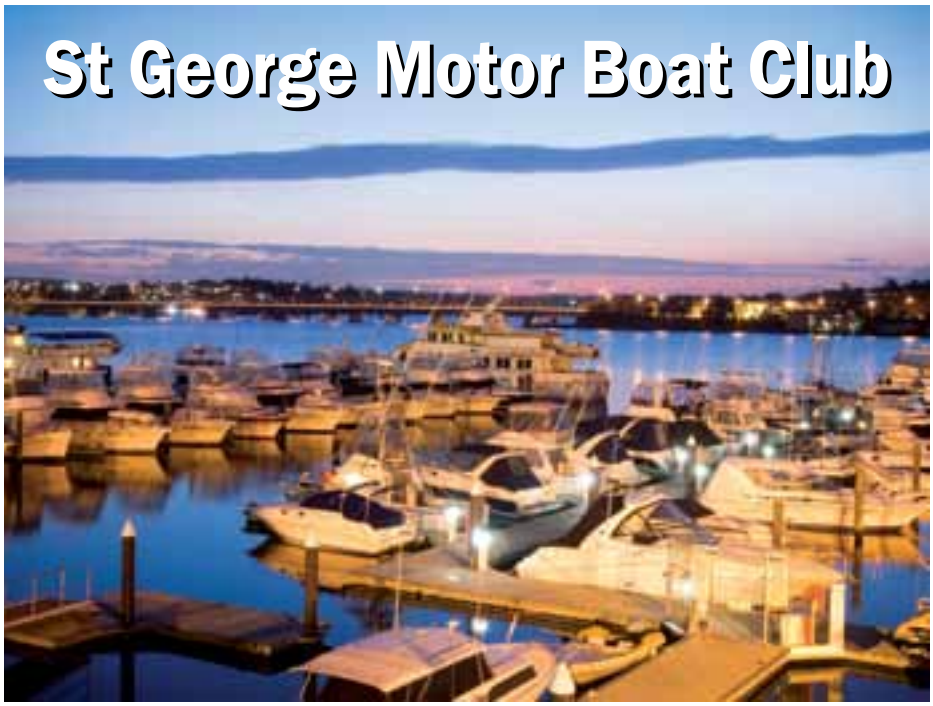
Club TECHNOLOGY UPDATE

Opening the door to labour and money saving technology

Issue 2

IT integral to 300% Growth

St George Motor Boat Club has gone from time warp to trendsetter in just four years, along the way growing membership by almost 300%, a transformation due in no small part to the can-do attitude and knowledge of specialist IT provider, Secom Technology.



Club CEO Adrian Vermeulen has nothing but praise for Secom Director Jason Drew who is now very much the club's go-to-man when it comes to change.

When Adrian joined the club from Cabramatta Leagues Club four years ago, Secom was the incumbent IT firm and Adrian admits that, like all suppliers at the time, he made them jump through hoops to prove themselves.

"They did that and more and the more I asked of them the more I realised what an underutilised resource they had been," Adrian said.

"As a result, today we involve Jason in all of our think tanks and when I start throwing balls in the air he'll quickly tell me which ones are worth catching but he'll even go away and come back with ways of catching others.

"The relationship has gone to another level these days. Jason's virtually part of our executive team and we involve him in all of our future planning," he said.

Adrian admits that he has a soft spot for technology and takes great pride in the fact that St George Motor Boat Club is now very much a leader in this area, from a unique card access secure marina to the tracking of cost and profit centres and member activity.

He is constantly coming up with new theories, challenges and wish lists and is pleased that when he confronts Jason with the challenges Jason's eyes light up as opposed to rolling in his head.

Where initially Secom Technology worked only on specific projects, now the firm is very much seen as the club's interface with other technology providers such as software companies.

"I know what I want but don't know the terms for it, but Jason does. On matters of integration he not only liaises with the other software companies such as BevLink and Independent Gaming, but he ensures that they are answerable and don't have any outs."

INSIDE: Beware Wireless Hot Spots' Dangers - Page 2

Continued page 3 >>

Wireless Hot Spot Data Scavengers

Beware The Evil Twins

Rogue wireless hot spots have become the latest threat by cyber criminals and hackers to both personal and corporate data security.

Just as the rise in mobile technology has provided flexibility in computing we couldn't have dreamed of ten years ago, so too has it provided more avenues to access our data.

Our phones have more processing power and capacity than the desktop computers we were using ten years ago. All this has meant that we can get our email, send files amongst other things virtually anywhere that has an internet connection.

A growing threat is the rise of "Evil Twins", a term used to describe a rogue hotspot that disguises itself as a legitimate one.

These evil twins are wifi access points set up by cyber criminals or hackers with the purpose of capturing data or users' transaction details such as passwords, bank account details and anything else they can access.

For example you may be sitting in a cafe that offers a free wireless connection.

When you go to access the connection you will see two that appear to relate to the cafe, Jumbuck and Jumbuck 1. Jumbuck 1 has the strongest signal so you connect to it unaware that you are actually connecting to an evil twin, a rogue wifi access point that can cause you harm.

These access points are quite simple for cyber criminals to set up and for that reason they are propagating quickly.

It can be as simple as plugging a special USB thumb drive into their laptop and with a little programming they can appear to be a legitimate hotspot.

The hacker then uses software to monitor all the traffic going through, looking for logins, account numbers, credit card numbers etc.

Some of the more sophisticated evil twins may ask you to authenticate by downloading their viewer ware.

When this is done, you are loading a virus or key logging malware onto your machine which they are able to access at any time.

Naturally, evil twins are more likely to be found where people are likely to use credit cards such as shopping centres and cafes near tourist attractions and airports.

So how do you protect yourself?

The easiest way to ensure that you are not connecting to an evil twin is to confirm the exact name of the wireless hotspot you are connecting to by approaching a staff member on the premises.

Also, if you are connecting to your desktop via remote access, ensure that it is by (VPN) virtual private network and the VPN is encrypted.

As with any internet usage, avoid downloading anything that you are not 100% sure of. Often downloads, especially free downloads, contain malware and invite the perpetrator into your machine.

It is also good practise to do any type of banking transactions behind a firewall. If you do have to use a credit card, ensure the site has adequate protection and that your anti-virus program and spyware is up to date.

Whilst the threat of cybercrime is present you can avoid it happening to you by making yourself aware and taking some simple precautions.

- 40 million MasterCard and Visa cards compromised in late 2007 by a hacker
- 26.5 million names, social security numbers and birthdates lost by the US Department of Veterans Affairs in 2005 when a worker's notebook was stolen
- 1.2 million Bank of America charge cards compromised in 2008 when back-up tapes were lost
- A Western Australian man recently had his home sold while he was overseas and they were about to sell another of his properties

SAFEGUARDS At a Glance

- Have a firewall
- Have a segregated network
- Have Anti-Virus on all PC's & Servers
- Ensure Anti-Virus is updated
- Limit the use of USB's
- Scan all USB's / Floppy discs before use
- Advise staff not to open unfamiliar emails
- Avoid downloading free software
- Advise staff not to download PDF's or plugins from random websites
- Give all staff an individual login and confidential password
- Don't allow people to share passwords
- Limit the amount of people who have the system administration password to CEO/GM and Duty Managers
- Apply Group Policy protection to files. Staff should only have access to files or information they require to do their job.
- Policy of not sharing passwords
- Ensure passwords are alpha numeric
- Avoid using "password", "admin" or "blank"

Continued from page 1 >>

Supplier Helps Bottom Line

During the relationship Secom's own key projects for the club have included:

- Development of a vehicle tracking system for the club's courtesy bus. The system allows the club to track vehicle movements and send customer pickup details direct to the vehicle's on-board GPS system.
- Implementing a complete wireless marina access control system securing access to the Marina via proxy gate control.
- Implementing an in-house secure web based document storage system with iPad integration for Directors, removing the need to print monthly 80-page board reports for each director.

Adrian said that nothing the club has done has been a case of technology for its own sake. His decisions are based solely on Return on Investment and the worth of these decisions is reflected in the club's 300% membership growth in just four years.

"Even something simple like developing a system that allows staff to control the jukebox volume from their iPad has a benefit. It not only adds to our seamless level of services, but it ensures staff are available for customers rather than having to go to the jukebox."

Adrian said that one of his greatest joys from the relationships he has developed with Secom Technology and other suppliers comes from the fact he is now able to work to a Triple Bottom Line.

"I love to stand up at the AGM and say not only did we make a good profit, but we also developed this and that, measurably reduced our green footprint and put back to the community in these ways.

"These things are a source of great pride for me personally and should be for every member of our club and its staff," Adrian added.

A further measure of the club's growth and success is the recently acquired approval to add 78 berths to the marina, effectively making it half as big again.

Club Security Basics That Are Often Overlooked

The trust between club managers and IT companies is an imperative, particularly given that they have access to all of the club's data and systems.

But what if you have a falling out? What if the company doesn't conduct rigorous pre-employment checks? What if your one-man-band supplier is sick or uncontactable?

If something went wrong, could your club function?

To avoid potential issues regarding your IT network and crucial data systems, ask yourself the following questions.

1. Do you have access to all of the passwords?

Every machine and device on your network has (or should have) a password. If your current provider is the only one who knows what they are, then that person/company is the only one able to view, change or update system settings. You should also know the passwords to all of your third party IT providers - the gaming, membership, POS and accounting software packages.

2. Do you have the product keys to your software?

Product keys are long, alpha numeric codes, usually printed on the back of the softwares packaging. They are required to install the software. Once installed, you don't need them again... unless your system has issues and you need to reinstall the program. Always make sure they are stored on your premises in a secure location but with copies off site, also secured.

3. Do you know where all the installation software is stored?

Taking a few minutes to organise and store software disks in a secure place can save you a considerable amount of money in the event that you need to restore a program on your computer. If you don't have the disk, you may be required to purchase the software again.

4. Do you know all the equipment on your network?

The idea of learning about, and keeping track of, all of the servers, workstations and peripherals on your network may seem overwhelming but it's important information to maintain. To be in a position to recycle or refurbish equipment that may no longer be suitable for its initial purpose but will suit a new project, you need a full inventory of existing and decommissioned equipment.

5. Do you know how to protect yourself from an ugly security breach if your IT company leaves?

Best practice is to, as soon as is humanly possible, disable their access, including remote access to your network. If you are unable to do this, have your new IT company do this before you advise your existing IT company that they will no longer be looking after your network.

It is best practice to have available all the relevant information you need to maintain your IT network, and to ensure your club runs with minimal interruption, if there is ever a need to replace your IT services providers.

IT providers who are confident in the quality of their services will welcome the opportunity to provide you with the answers.

How Secure Is Your Club's IT System?

Could cyber criminals be viewing your banking and member's data without you knowing?

Ring **1300 78 1224** for your **FREE** Network Security Audit

All audit participants receive The Essential Guide To Preserving Your Critical Data And Computer System

secom TECHNOLOGY

PO Box 541, Sans Souci NSW 2219 AUSTRALIA
P: 1300 781 224 F: 1300 134 840
W: www.secomtech.com.au E: support@secomtech.com.au