Your security on-line

There are many dangers lurking on-line and few security measures in place protecting your information at a public Internet access location. Security becomes your own responsibility. Here are some hints to keep yourself safe:

- Make sure no one is peering over your shoulder when you log into your operating system, email, Instant Messenger, or other accounts.

- Be on the watch for suspicious behaviour and never leave your computer unattended.

- Minimize the amount of sensitive, personal data you can access from a public computer.

- Change any passwords you feel are weak.

- Don't do your online banking or trading at a public computer. Save it for a more safe and controlled environment.

- Protect yourself against online fraud by only doing business with websites that have security features like a padlock icon, green address bar or the address bar has an s after http:// so it reads https://

- When you're in a public Internet access point, you cannot know whether there are hackers prowling the network so don't forget to LOG OFF when you finish.

- Make wise computing decisions. Always avoid using public Internet access for important communications or transactions.

Free public Internet access available

Community Support Frankston provides FREE public Internet access to people showing identification during open hours:

9:00 am — 4:00 pm
Monday, Tuesday, Wednesday and Friday
1:00 pm — 4:00 pm Thursday

Location: 35 Beach Street,
FRANKSTON, VICTORIA
Corner of Lewis St, opposite Tyrepower.
(Melways Map 100A Ref: F6)
For more information see the Community Support Frankston brochure:
Abuse by Cyberstalking

COMMUNITY SUPPORT FRANKSTON
Inc. Reg. No. A0000431J   ABN 95 426 151 625

Tailored information for Sole Parents
Project funded by FaHCSIA

Security on a shared computer

October 2018

free public Internet access

●chat & web-mail●
●how to avoid scams●
●online security hints●

COMMUNITY
SUPPORT
FRANKSTON

35 Beach Street, Frankston
Phone: 9783 7284

Community Support Frankston provides free public Internet access. Here is some basic information about how to protect your identity, bank details, credit cards and any sensitive information when using the public computers.

Instant Messaging (chat)

There are many types of instant messaging programs available (i.e. MSN, AOL, Yahoo) and most instant messages still travel unencrypted across the Internet, exposing your conversation to anyone who can find a way to listen in. Instant Messenger attachments, just like email attachments, can carry destructive viruses, Trojan horses, and worms. Some worms use Instant Messenger software to send themselves to every person in your friend list.

What you can do

- Reject all messages from people who are not in your Friend list.

- Do not open attachments or click on web links within your Instant Messenger program unless it is from a known person and you expect it.

- Never send personal information or attach files using Instant Messenger.

- If a person on your friend list is sending strange messages, files, or web site links terminate your Instant Messenger session immediately.

Phishing (fishing)

Phishing is an online con and phishers are con artists and identity thieves. They use spam, malicious websites, email and instant messages to trick people into giving them sensitive information, such as bank or credit card accounts. Their site looks identical to the real one because they use pictures and logos from the genuine website.

- Phishers pretend to be genuine companies, your financial institution, a company you do business with, or even someone in your address book

- They request sensitive information such as PIN, bank account, Tax file, Centrelink numbers or date of birth and direct you to a malicious website when you reply.

- Phishers use emotional language, scare tactics or urgent requests to entice you to respond

- Their fraudulent messages are often not personal to you even though they use your name in the title

What you can do

- Be extremely wary of emails asking for confidential information.

- Immediately delete any email informing you have won a lottery (and you didn't buy a ticket), received an inheritance (from someone you've never met and/or who lives in a foreign country) or wants help to move money from overseas into your account.

- Consider disabling the email's preview pane and reading emails in plain text.

- Discard email that threatens to close an account or suspend your privileges.

- Confirm the authenticity of a suspicious request before responding by email.

Web Based Email

▶▶▶ Spam

- Spam is a serious security concern as it can be used to deliver Malware

- Messages that do not include your email address in the TO: or CC: fields are common forms of spam

- Spam can contain links to web sites with inappropriate content

What you can do

If you suspect email is spam delete it, never respond as it gives the spammer your email address and spam messages will increase.

▶▶▶ Malware

- May appear to come from someone you know so it can trick you into opening an attachment

- May give no symptoms of infection on your PC but it is gathering information about you

- May reduce performance or cause your computer to reboot

What you can do

- Only open attachments you are expecting from someone you trust

- Most web-based email will allow you to scan attachments for viruses prior to opening

- Don't click on unknown links (hover your mouse over the link for a few seconds—and it will reveal where you are being linked to. Make sure it matches the one you see in the email.)

- Delete all unwanted email without opening

www.frankston.net