Threats to My Computer - who'd be interested in my PC? – Rob Neary

Recently one of our Probus members contacted me with considerable angst and distress as the family PC was unable to be started and there was a message on the computer screen demanding a password to start the machine.
Prior to this, the member had been harassed by a caller from "Microsoft" claiming that the machine was infected and needed to be cleaned. The caller was quite aggressive and as a result of being bullied by the caller, our Probus member relented with the result that the machine and the member had become victims to "ransomware".
The situation worsened when, even after paying to have the password sent, the perpetrators didn't respond with the required password but had raided the small, but not insignificant, account of our Probus member for every cent.
The member now had a machine that would not start up beyond the screen demanding the password and the member had also lost the money from the account.

I relate this story to you because it is important to understand that:
1. Microsoft will never ring you unless you have managed somehow to contact them;
2. Never allow an external organisation to have access to your computer; and
3. Never give away details of any accounts to anyone by email or phone – close known relatives might be an exception – but my advice is to stick to the rule.

The dilemma for the member was that even if the machine were "unlocked" would the perpetrator have left anything on the machine to trace any activity such as banking or funds payment to credit cards.
The rectification and true cleaning of the machine required around six hours of work.

So, why would anyone be interested in your PC?
Answer: we are now more reliant on the internet for information, dealing with utility companies such as power and water and we now move money around using our computers. Unfortunately this leaves a "digital trail" in the computer and so really clever and dishonest persons can "unearth" this trail if they have access to your computer.

How do I stop them?
Answer:
Firstly, ensure that your machine has an up-to-date antivirus and malware detection program (see accompanying tables for independent company results for common antivirus products).

Secondly, make sure your machine has all of the system updates loaded – whether it's a Mac or a PC, android or IOS tablet – as these updates "close" some of the ways in which the "baddies" can get into your machine.

Thirdly, *stop using CC* in your emails. If you wish to send that great joke or photo to a number of people, use To: to send a copy to yourself and ***then BCC: a copy to all your friends and/or relatives*** that you wish to share the email with. This stops your email address being hacked by baddies and will eventually stop a lot of the spam or unwanted email landing on your device.

Fourthly, remove the spam before it comes into your email program, use a product like Mailwasher Pro (www.firetrust.com) to look at your mail before you bring it onto your PC or tablet. There is a free version for one email account. If you wish to run it with two or more you will be required to buy a license. Fortunately, Nick at Firetrust has a special offer for Probus members until November 2015.
Simply click this link: https://secure.firetrust.com/cart/items/add/mw2010-1-0/promo/probus and you'll receive a special Probus price for a lifetime license for Mailwasher Pro. When this is set up, you can delete unwanted email before you bring the selected emails onto your device into your email program.

Fifthly, tighten up your security. Our member's PC was easily accessible because there was no password on the user account. I know it's a nuisance to type a password to go into your account especially if you're the only one using it, but it affords the baddies "carte blanche" access to your PC. And don't use 1234! Yahoo did a survey of its email accounts and the password use by some huge majority was 123456! If you were a baddie, what would you start with if you were trying to break into a computer?

Microsoft states that any password less that fifteen (15) characters long is at risk. I can't remember 15 characters but I can do ten (10). Microsoft also states that the password must be made by using upper and lower case letters, numbers and punctuation to be effective.

Here's a little sample of ten (10) character passwords that would register as strong by some evaluating programs:

1) r?becaM@Mu
2) 2) nunaPh*dr4
   and
3) CHeqe2Raz? .

You can make one up too, for example: 19!J0hN*Fr@nK+38 – year of birth separated by name and/or initials but substituting zero for "o" and the "@" for the "a". Ladies you also have your maiden name to play with. So long as it isn't easily guessed.

There are other areas on your computer that need to be checked as well. Many computers are set to allow remote access to them as the default setting. This needs to be altered to the "no access" setting. Each operating system has a different place for this. You can "google" "turn off remote access for XP, Vista, WIN7, WIN8, Mac OSX .. whatever your operating system is" – then do it.

With an up-to-date computer operating system (or tablet OS) and an up-to-date good quality anti-virus product and a strong user password, you should make the "breaking into" your PC more difficult. Remember to turn off the remote access too.

Below are the result of independent testing of common anti-virus suites.

This Dennis Technology Labs report aims to compare the effectiveness of anti-malware products provided by well-known security companies. The products were exposed to internet threats that were live during the test period. This exposure was carried out in a realistic way, closely reflecting a customer's experience.
These results reflect what would have happened if a user was using one of the products and visited an infected website. Results are for January - March 2015

TOTAL ACCURACY RATINGS

Product	Total Accuracy Rating	Percentage	Award
Kaspersky Internet Security 2015	1017	100%	AAA
Norton Security	1000	98%	AAA
Avast! Free Antivirus	991	97%	AAA
Trend Micro Titanium Internet Security	988	97%	AAA
ESET Smart Security 8	971	95%	AAA
McAfee Internet Security	940	92%	AA
AVG Anti-Virus Free 2015	904	89%	A
Panda Free Antivirus	791	78%	C
Microsoft Security Essentials	745	73%	-