

## Scams

Scams seem to be in the news all the time at the moment whether they are online scams, telephone scams or even from people who visit your house. When we hear about something too often we start to switch off and ignore the message, thinking we have heard it all before. But when it comes to online scams, this is not a topic where you have heard it all before; online scams are constantly evolving as technology advances. This article will discuss some of the scams which are currently affecting Grenfell residents and ways you can protect yourself.

Most people assume that websites are legitimate when in actual fact there is no governing body overseeing the internet to ensure all website are legitimate and in the best interests of the user. In fact anyone including scammers can have a website and can publish anything they like no matter if it's true and because of the range of free website templates available even dangerous scam websites can look and function like an expensive professional website. This is dangerous for unsuspecting internet users as it means users need to always be aware of scams to avoid becoming a victim. Always make sure you think twice before signing up for an offer, or replying to an email where you are being offered money or prizes as these are classic indications that a scammer is at work.

In recent months I have received many reports from local residents who received a phone call supposedly from Microsoft or other well known computer companies. The caller informs you that your computer has been infected by a virus but that they will help you go through the steps to remove the virus from your computer. In actual fact these callers do not remove a virus; you didn't have had a virus to start with. Instead they force you to unwittingly modify and reduce security settings on your computer which allows them access to all of your computer files. Recently I met with a lady who inadvertently went through these steps with a caller. When they asked her to pay the large fee for supposedly removing the virus from her computer she replied she was unable to afford the fee. As a result they deleted her photos and files from her computer while she was watching and there was nothing she could do to stop them. While there are companies that do offer phone support for your computer, they will not ring you, they always allow you to contact them. In addition the fee will often be charged in advance or on a per minute basis, you should never find out an unexpected charge at the end of a call.

Many computers I have had come in for repairs lately have had fake antivirus programs installed on them. Each customer has come in with the same story "my computer tells me it's full of viruses and it won't let me do anything until I buy the program". These fake antivirus programs tell you that your computer is infected but in reality the program itself is the only infection. These programs do look legitimate and their names are similar to real antivirus programs you may have heard of. These can be tricky programs to remove and occasionally I have had to fully reinstall windows to fix the problem. If you think you have purchased a fake antivirus program, contact your bank immediately to see if they can reverse the payment. Secondly remove the program from your computer. If you are unsure how to remove the program, bring your computer to the Internet Centre where I can do it for you.

Another scam I have experienced recently was an email scam from WEB SUPPORT telling me that my mailbox limit has been exceeded. The email read:

"IT Service, You have exceeded the limit of your mailbox set by your IT Service, and you will be having problems in sending and receiving mails. To prevent this, please click on the link below to reset your account. Failure to do this, will result in limited access to your mailbox. Warning!!! Do not send your username and password via email. Regards, IT Service."

Because of my experience I know our emails are not hosted with this company so I knew that this was a scam and I never clicked on the link. To prove the point I logged into the host of my email and I could see that my mailbox was empty. If I was to visit the link suggested in the scam email I would have had to enter my details and then my email would be used to send out spam. If you do not know the sender of an email or you receive an email offering you money or asking you to confirm details such as your email address or banking details, delete the email straight away. These are classic indicators of a scam. Do not even reply to these emails. Replying to these emails confirms that your email is active and you will receive even more spam.

To ensure your computer remains virus free it is important to install an antivirus program. Another name for antivirus is internet security. When buying an antivirus program I recommend you acquire one with a full security suite, rather than just a basic antivirus as comes with free versions of internet security. A full security suite will include things like a Firewall, Anti-Spam, Anti-Malware and Link-Scanner. This will protect you and your computer against a wider range of potential problems on the internet.

Once you have internet security you will need to keep it up to date. Companies that sell internet security sporadically release updates to patch up weak spots in response to scammers developing new threats that bypass the existing levels of internet security.

A good Internet Security that I use on my own computer and that I am happy to recommend is AVG.

AVG is available at the Internet Centre from \$69.95 for 12 months protection, or 24 months protection for \$104.95. A two year contract offers better value for money and means you don't have to worry about researching and renewing your internet security again in a year's time.

You should familiarize yourself with your internet security program so you know what the legitimate updates looks like and so you can identify the warning signs of a virus should they appear. Signs that your computer is infected are: running slow than usual, directing you to a different website from the one you were trying to visit, programs not running properly and more frequent pop-ups. If your internet security program tells you there is a virus on your computer, perform a full system scan straight away to ensure that there are no other viruses on your computer. If any other internet security program tries to install or warns you of viruses on your computer, close it immediately and run your antivirus software. Never click on anything that offers a free scan or install something from websites that say your computer has errors. These are all classic techniques used by scammers to trick you.

If you think you have a virus or if you have questions about internet security give Josh a call on 02 6343 1720, email on [grentech@grenfell.org.au](mailto:grentech@grenfell.org.au), find us on Facebook or pop into the Grenfell Internet Centre in the Community Hub Building on Main Street.