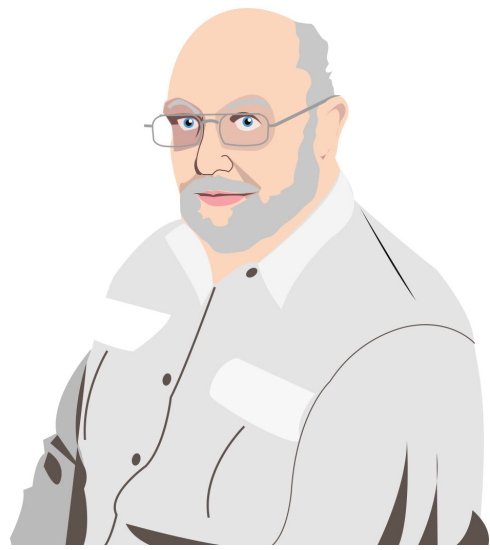# 10 Tips For Better
Cyber Security
by Tim O'Neill - The "Oldcommguy™"

Here are ten easy steps to implement Cyber Security on the home front. The last thing any IT professional wants to deal with is network security issues at home. Just like you institute corporate policies, your home network and users need to accept 'house rules' when it comes to cyber security.

1 Use Antivirus Software
Antivirus protection does not solve all your potential hacking and breaches but it does help. Sites like McAfee Total Protection, Trend Micro and Microsoft Security Essentials can check to see if you have any suspicious software.

2 Update Operating Systems Software Regularly
It's amazing how many viruses exploit outdated and vulnerable operating software, especially your core applications like Office, Adobe and virus protections. Get more info: https://www.us-cert.gov/

3 Turn Off Your Computer
Being always 'on' allows computers to be more susceptible to hackers, this is how computer camera's and microphones are hacked, as well as spyware or botnets.

4 Do NOT Share!
Not passwords, not computers, not mobile phones and not tablets. Here is another no brainer but it needs to be said out loud - Passwords need to be user-specific. Malware is often loaded onto 'lent' machines and tracking software is put on cell phones.

5 Don't Open Suspicious Emails
This takes discipline but phishing is the easiest way for a hacker to steal your passwords, account numbers, etc. Over 100 billion phishing emails are sent daily! Do not open any suspicious email or use embedded links to go to a site from an e-mail.

6 Check that the Site is Secure and Authentic
Verify you are shopping at an SSL encrypted site with HTTPS:// and a lock symbol in the url. Make sure there is a security seal by a third party like the McAfee SECURE trustmark. Double check the web address to make sure you are at the correct site, often SPAM email with to-good-to-be-true offers are spoofed versions.

7 Have a Family Cyber Security Policy
People are the weakest security link - make sure you and the people in your network follow a set plan.

8 Never Save Your Credit Card Number
One click purchasing sure is convenient, but if your credit card number is stored in a retail database there is a greater likelihood for it to be stolen.

9 Use Strong Passwords
A strong password is one that contains a mix of lower -and- upper-case letters, numbers and symbols. The longer the better. I suggest a core word that you add the above before and after. Do not save your passwords to your desktop or allow your computer to auto-save.

10 Be Cautious with Public WiFi
Make sure that you keep file sharing off. Assume that all public WiFi sites are hacked so do not do banking and other important duties on a public site. Even your home WiFi is easily hacked turn it off when you do not need it.

For more info on Cyber Securtiy, visit: https://www.dhs.gov/topic/cybersecurity