NIKOLAY SHMAKOV *Managing Director, Res-Q IT*
Website res-q.com.au

Res-Q IT is a consultancy company located in Perth, Australia. Through our expert IT services delivered by a team of certified engineers, we help businesses by providing solutions for their every-day IT operations and Computer Support. Our services include set up and support of business phone systems, IT consultancy and support, web hosting and cloud-based solutions, and all things internet. When it comes to setting up systems for a business, whether it's an existing one or a startup, you can count on Res-Q IT Services. We take care of everything you need so that you never see

TIP 1. KEEP YOUR COMPUTERS UP TO DATE

If your computers are not up to date, then hackers can use that vulnerability to take control of your computers. Regularly updating your computers is a vital part in staying safe online.

TIP 2. INSTALL ANTIVIRUS

Your antivirus protection is only as good as its ability to detect any infected files in real-time scanning. It is important to understand that not every Antivirus software is good at detecting viruses. You must constantly stay alert and educate yourself and your staff about online safety.

TIP 3. MAKE SURE YOU LOCK YOUR COMPUTER WHEN IT IS NOT IN USE

If your computer is compromised, then hackers can access your files. If the computer is locked it creates an extra layer of difficulty for someone to access your favorite websites and potentially gain access to sensitive login information.

TIP 4. DO NOT ENGAGE IN ANSWERING PERSONAL QUESTIONS ON FACEBOOK

Social engineering is the psychological manipulation of people into performing actions, or divulging confidential information, as that can enable hackers to deduce the answers to your secret questions.

TIP 5. ENABLE MULTIFACTOR AUTHENTICATION FOR YOUR EMAIL ACCOUNTS

It is very important to add extra layers of protection to block access to your email accounts, particularly if the accounts are to be accessed by somebody else.

TIP 6. NEVER SHARE YOUR PASSWORDS WITH ANYONE

Nothing more to add to this tip really. You can have a secret place, such as a glass container buried in your garden with the master password to your password manager. All jokes aside: the only persons allowed to know about the place where you buried it is your very close family member, or your accountant.

TIP 7. GENERATE A NEW PASSWORD FOR EVERY SITE

It is tempting to use your favorite password for every site you use. However, if the resource gets hacked it then exposes the password combination (email + password) for access to other websites.

TIP 8. USE A PASSWORD MANAGER WHERE POSSIBLE

There are plenty of password managers out there. My favorite is LastPass. The master password can be securely locked in the container and buried in your garden

TIP 9. DOCUMENT HOW YOU RESTORE YOUR BUSINESS IF YOUR WEBSITE, COMPUTERS, OR OTHER IMPORTANT RESOURCE GOES DOWN

It is called the Disaster Recovery Plan. Detail what you need to do to get your computer, website, online shop or business documents back online - and how much time it will take. Write down the contacts and responsible people, as well as access details, for all these resources

TIP 10. BACKUP, BACKUP, BACKUP

You must have backups for all your documents. Regardless of how good you are, there is always a human factor in every cyber-attack. It is essential that your company's highly valuable classified data and assets are protected from its greatest threat: the enemy within the gates and outside.