SECURITY

STAY SECURITY SAVVY!

Don't Fall for Tech Support Scams

The Scam: Cybercriminals will contact you posing as a support technician from a company you know and trust. They'll tell you there's a problem and use remote support software to gain access to your computer. From there, they'll steal your information and potentially install malware or spyware to access your files later, without you knowing. Then, they'll charge for you for fixing the problem. ***Don't fall victim to their lies!***

Unexpected Phone Calls

If you ever get an unsolicited phone call from someone saying there's an issue with your computer, hang up immediately. ***Real tech support companies will never call you; you have to contact them first to get support for your computer.***

Suspicious Pop-Up Messages & Emails

Tech scammers will create convincing pop-up notifications online that look like security alerts or send frightening emails trying to get you to call them. Don't fall for it. ***Legitimate warning messages and security alerts will not contain phone numbers.***

Fear Tactics

The best tool in a tech scammer's arsenal is fear. They'll say anything to make you think you have to act now to fix a problem you don't have. Don't believe them. ***Don't let anyone try to scare you into making quick decisions, or giving up personal information over the phone, email, IM/chat, or during a remote support session.***

Unsolicited Remote Access & Support

Remote access and support software is an excellent tool for helping people when used responsibly by trained tech support providers. ***Remember, if anyone contacts you offering to remote into your computer to fix something, say NO. You should always be the one to initiate tech support.***

CALL 1300 700 187

MINO I.T.
MANAGED SERVICES

www.minoit.com.au