



TALKING TECH

Helping your business

WHAT OUR CLIENTS SAY:

Very prompt service
and rectified issue.
Pleasant to work with.
Roxy
After-Care Aus.

They were great, my
issue was sorted in no
time at all. Thanks!
Melissa
FDNA Inc.

DID YOU KNOW?

The first webcam was invented at
Cambridge University to monitor a
coffee pot.

Researchers were tired
of wasting trips walking
down the hall to an
empty pot, so they set
up a camera to check
the coffee levels remotely.



DSP IT Solutions
(03) 9001 0817
182C Sladen Street
Cranbourne VIC 3977
sales@dspit.com.au
www.dspit.com.au

FROM SHANE'S DESK:



Welcome to the October newsletter,
crazy that we are already into the last
quarter of the calendar year!

Did you know that most technology
risks do not begin with a major
incident?

They often start with a small decision, such as leaving
administrator access in place, sharing sensitive information
with the wrong tool or overlooking an upcoming
technology expense.

The good news is that these risks can be reduced with a few
practical habits. Give people the access they need to do
their jobs, think carefully before entering business
information into AI tools, and review your IT costs regularly.

Taking a proactive approach today can prevent disruption
tomorrow and give your team greater confidence in the
technology they use every day.

If you are unsure where your business stands, reach out, our
team are always happy to help.



Shane Rajasinghe
General Manager

WHY YOUR EMPLOYEES SHOULDN'T HAVE ADMINISTRATOR ACCESS TO THEIR COMPUTERS

Administrator access often starts with a reasonable request. Someone needs to install a printer, update a program, or change a setting, so they're made an administrator on their computer. The task gets done, but the access stays.

From then on, that employee can approve software installations and make changes that normally require help from IT. If they download a fake installer or approve a harmful program, it may be able to install system components, change security settings, or affect other information on the computer.

For email, web browsing, documents, meetings, and most business applications, employees should use standard accounts. Administrator access should be reserved for approved IT work.

What administrator access allows

On Windows, members of the local Administrators group have broad control over that computer. They may be able to install software, add drivers, manage other local users, and change system settings or file permissions. Mac computers also have standard and administrator accounts, with similar differences in what each can change.

Why standard accounts are safer

Programs normally start with the permissions available to the person who launches them. If an employee can approve an administrator request on their own, harmful software may receive the same level of access.

Windows uses User Account Control to ask before many important changes. An employee using an administrator account can approve that request. A standard user is normally asked for administrator credentials, which gives IT an opportunity to check the program and where it came from.

Standard accounts still support normal work. Employees can use email, browsers, Microsoft 365 or Google Workspace, meetings, approved software, printers, and shared files.



How to handle software installations

Employees can still get software installed without keeping administrator access. Your IT team can install it remotely, approve a request when it is needed, or deploy updates to several computers at once.

Test specialist or older software before changing permissions across the business. If a program expects the user to be an administrator, your IT provider may be able to change its setup or find a supported alternative.

Keep a separate administrator account for approved technical work. Do not use it for email, web browsing, or everyday tasks, and protect it with multifactor authentication where the system supports it.

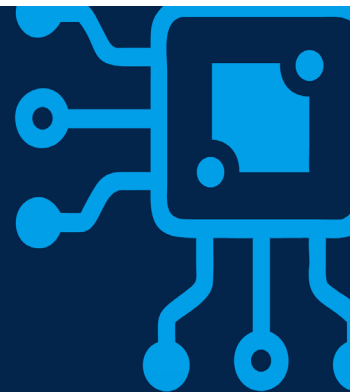
Check who has access now

Ask your IT provider to review the administrator accounts on every company computer, including former employees, shared logins, vendor accounts, and accounts created during the original setup.

Before removing access, confirm that IT still has a tested way to perform administrator tasks on every device.

Standard accounts let employees do their jobs without giving them or the software they run more control than normal work requires.

Never paste this into an AI tool



Not all business information belongs in AI.

Customer data

- Contact records
- Customer lists
- Personal details

Keep client information private.



Financial information

- Bank details
- Payroll
- Financial reports

Sensitive business data should stay protected.



Passwords & login details

- Passwords
- Security keys
- Logins

Never share account access information.



Confidential documents

- Contracts
- Proposals
- Internal reports

Private documents should remain private.



Legal or HR information

- Employee records
- Disciplinary notes
- Legal documents

Treat this information with extra care.



Company secrets

- Product plans
- Pricing
- Business strategy

Competitive information should stay in-house.



Before you paste, ask:

Would I email this to a stranger?

Would I post this on social media?

Would I be comfortable if this became public?

AI is powerful. But it doesn't need to know everything about your business.
Want to use AI without putting your business data at risk?

Get in touch.

DSP IT SOLUTIONS

SMALL BUSINESS IT BUDGET:

What to include and how to plan it

An IT budget should reflect the systems your business uses and the changes expected during the year. A general percentage of revenue cannot tell you whether you have allowed enough for a new employee, a failed laptop, or a software renewal.

Start with an inventory of computers, network equipment, software, cloud services, phone systems, websites, domains, backups, and support contracts. Record the cost, renewal date, contract owner, notice period, and number of licenses for each service.

Separate normal running costs from one-time purchases and projects. Recurring costs include software, IT support, internet, phones, backup, and security tools. One-time costs include new equipment, migrations, installations, office moves, and major upgrades.

Include onboarding and offboarding, staff training, backup testing, cybersecurity reviews, and equipment disposal. Keep a reserve for an urgent replacement or work outside a support agreement.

Review the budget every quarter against actual invoices. Check for unused licenses, new subscriptions, price changes, and projects that are costing more than expected.



OCTOBER TRIVIA QUESTION

Test your knowledge!

The answer to last month's question was d) 8.8km. It's not actually the tallest mountain! There are two volcanoes in Hawaii that are 10.2km but 4.2km of their height is submerged underwater. Do you know the answer to the question below? It will be in next month's Newsletter.

How long did the world's oldest cat, Creme Puff, live for?

- a) 38 years
- b) 29 years
- c) 39 years
- d) 27 years



DSP Communications

**Delivering better.
Better service.
Better phones & Internet.**

**VoIP Services
Business NBN
Business Mobile Phones
SIP & 3CX**

*Need help with your business
phones or internet?*

(03) 9008 6900

sales@dspcommunications.com.au

www.dspcommunications.com.au

TALKING TECH TIP

Turn a Picture into an Excel Table

In Excel for Microsoft 365, go to Data > From Picture and choose an image of a table.

Excel turns it into editable cells.



NEED A LAUGH

How many programmers does it take to change a light bulb?



None, it's a hardware problem!

