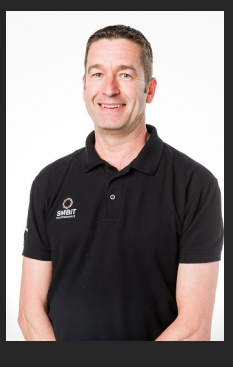
VOLUME 72
OCTOBER 2026
SYDNEY, NSW

Tech Talk

"Insider Tips to Make Your Business Run Faster, Easier and More Profitable"

INSIDE THIS ISSUE:

Why Your Employees Shouldn't Have Administrator Access	Page 1	Why Guest Wi-Fi Should Be Separate from Your Business Network	Page 2
Gadget of The Month	Page 1	Small Business IT Budget	Page 2
Personal Devices for Work?	Page 2	How Long Business Computers Last	Page 2
When You Cancel a Cloud Service	Page 2	Technology Trivia	Page 2



We love technology and we love helping people.

Give me a call today for a quick (non-salesy) chat to find out whether my team and I can help you better secure your data and get more out of your existing Technology!

Mark Giles

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

Administrator access often starts with one request. An employee needs to install a printer, update a specialist program, or change a setting on their computer.

Giving them administrator access gets the job done. The problem is that the access usually stays after the request has been completed.

From then on, the employee can approve other software installations and make changes that would normally require help from IT. If they install the wrong program or someone takes control of their account, those permissions can also be used to change the computer.

What administrator access allows someone to do

An administrator has more control over a computer than a standard user. On Windows, members of the local Administrators group have full control over the resources on that computer. According to Microsoft's guidance on local accounts, Microsoft recommends limiting the number of users in that group.

Depending on the computer and how it is managed, an administrator may be able to:

- Install and remove software
- Add drivers for printers and other equipment
- Create, change, or remove user accounts
- Change system settings
- Change permissions on files and folders
- Install services that continue running in the background
- Make changes to some security settings

Mac computers also have standard and administrator accounts. Apple says administrators can install and remove software, manage other users, and change settings. Apple recommends limiting the number of administrative users and using a standard account when administrator rights aren't required.

Standard accounts are suitable for everyday work

A standard account can still be used for normal business tasks, including:

- Reading and sending email
- Using a web browser
- Working in Microsoft 365 or Google Workspace
- Accessing approved business applications
- Joining online meetings
- Printing with an installed printer
- Opening and saving files
- Changing personal settings that do not affect other users

Some applications can be installed for one user without administrator access. Others need administrator approval because they add drivers, services, or files in protected parts of the computer. An employee should not receive permanent administrator access because one program needs an update. IT can approve the installation, deploy the update remotely, or use a separate administrator account for that task.

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. 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.

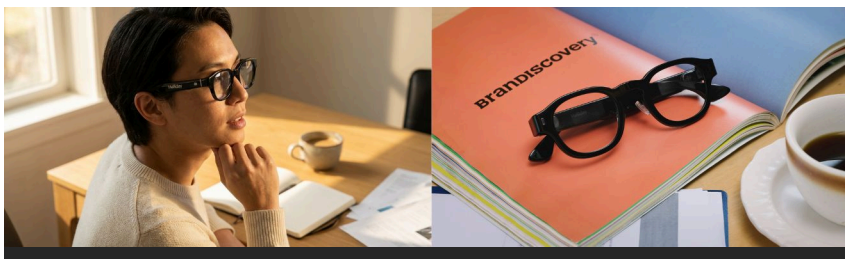
Keep a separate administrator account for approved technical work. Do not use it for email, web browsing, or everyday tasks, and protect it with multifactor authentication where the system supports it.

Check who has access now

Ask your IT provider to review the administrator accounts on every company computer and account.

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.



HALLIDAY G2 AI GLASSES

Halliday G2 is a pair of AI-powered glasses designed for live meetings, with a heads-up display that shows real-time translations, notes, and prompts in your line of sight.

It follows conversations across 45+ languages, tracks decisions and action items, and sends a summary when the meeting ends. A built-in voice assistant handles quick questions hands-free, while a 4-mic array and speakers manage calls and music. With no camera and encrypted data, it is built with privacy at the core.

VOLUME 72
OCTOBER 2026
SYDNEY, NSW

SHOULD EMPLOYEES USE PERSONAL DEVICES FOR WORK?

Allowing employees to use personal phones or computers can be convenient. They already know the device, and they can check email or join a meeting without carrying another piece of equipment.

But the business still needs to decide what work is allowed, which applications employees may use, and what happens to company information if a device is lost or an employee leaves.

Personal devices can be suitable for limited work when they meet your security requirements. Company-owned devices are a better choice for sensitive work, administration, or jobs that require large amounts of business data to be stored on the device.

What counts as a personal device used for work?

Bring your own device, often shortened to BYOD, includes reading company email on a personal phone, opening documents in mobile apps, or using a home computer to connect to a business system. Files may remain in the Downloads folder, and accounts can stay signed in after the work is finished.

Decide what employees may do

Set the rules according to the work and the information involved. You might allow employees to read email through an approved mobile app but require a company computer for customer database exports, payroll, system administration, or access to sensitive client records.

Staff should know which devices and applications are permitted, whether they may download files, and what they must do before selling or replacing the device.

Set minimum security requirements

A personal device should run an operating system that still receives security updates. It should have a screen lock, device encryption where available, current updates, and multifactor authentication on company accounts.

Keep business information inside approved applications or a managed work profile where possible. Device and app management tools can apply security settings and, on supported platforms, remove company data from managed apps. Tell employees what the business can see or remove before they enroll their device.

Plan for a lost device or departing employee

If a personal device is lost, IT may need to revoke active sessions, reset affected passwords and remove company information from managed apps.

When an employee leaves, disable their account at the agreed time and confirm that business information has been returned or deleted.

When to provide a company device

Use a company-owned device when an employee handles sensitive information, needs administrator access, stores a large amount of data locally, or requires specialist software. It is also the better choice when IT needs full control over updates, backups, applications, and security monitoring.

BYOD can work, but only when the rules are clear and the device can meet them.

WHAT HAPPENS TO YOUR DATA WHEN YOU CANCEL A CLOUD SERVICE?

Every cloud provider handles cancellations differently. One may leave your information available for a limited time, while another may restrict access as soon as the subscription ends. An account may become read-only, remain available only to an administrator, or be scheduled for deletion.

Check the provider's current documentation and your contract before canceling. Confirm when employees will lose access, how long the data will remain available, what the export contains, and whether you must request it while the subscription is active. If you bought the service through a reseller, check the cancellation process with the reseller as well.

Before you cancel:

1. List the information stored in the service, including attachments, comments, reports, audit records, and custom fields.
2. Export what the business needs and open a sample of every file type. Make sure attachments, dates, and customer or project details are complete.
3. If you are moving to another service, test the import before the old account closes.
4. Check website forms, payment tools, reports, mobile apps, automated workflows, and other systems connected to the service.
5. Confirm whether employees use the account to sign in to another application, then change those sign-ins first.

Your business may need to keep financial, customer, employee, or contract records for a set period. Check those requirements with the appropriate legal, accounting, or compliance adviser.

Ask the provider what it will delete from active systems and backups, when deletion will take place, and whether you need to close the account separately after canceling the subscription. Keep the confirmation with your other business records.

WHY GUEST WI-FI SHOULD BE SEPARATE FROM YOUR BUSINESS NETWORK

Guest Wi-Fi should give visitors internet access without allowing their devices to connect to your business computers, cameras, file storage, or network equipment.

A different Wi-Fi name and password do not prove that networks are separated. The router, wireless access points, and firewall must be configured so guest devices cannot reach the internal network.

Employee phones and personal laptops that only need internet access can normally use the guest network.

Ask your IT provider to test the guest Wi-Fi and confirm that it can reach the internet but cannot open internal systems or management pages. Most small businesses can use one internet connection while keeping these networks separate.

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.

Start with an inventory of computers, network equipment, software, cloud services, phone systems, websites, domains, backups, and support contracts.

Separate normal running costs from one-time purchases and projects.

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.

HOW LONG BUSINESS COMPUTERS LAST AND WHEN TO REPLACE THEM

Three to five years is a practical replacement range for many business computers, but age alone should not decide it. Start reviewing each device at three years, then check its security support, reliability, performance, warranty, and repair history.

Security comes first. Replace a computer if it cannot run an operating system that still receives security updates or the software your business requires. A computer that still runs well may need replacing if its operating system is no longer supported. Before an old computer is sold, donated, recycled, or returned, transfer the required data and have its storage properly erased.

Keep a replacement schedule with the purchase date, assigned user, warranty expiry, operating system, and review date for every computer.

Ask your IT provider to review your computers at least once a year. If you do not have an IT provider, feel free to reach out to us and we'll help you plan the replacements.

TECHNOLOGY TRIVIA

Each month you have a chance to win a $50 Amazon Gift Voucher by being the first person to email us with the answer to our Technology Trivia Question of the Month!

The Question This Month is:

What does PDF stand for?

The first person to email me at mark@phrixus.com with the correct answer gets a $50 Amazon Gift Card!

Last month's answer was *Image Maximum.*