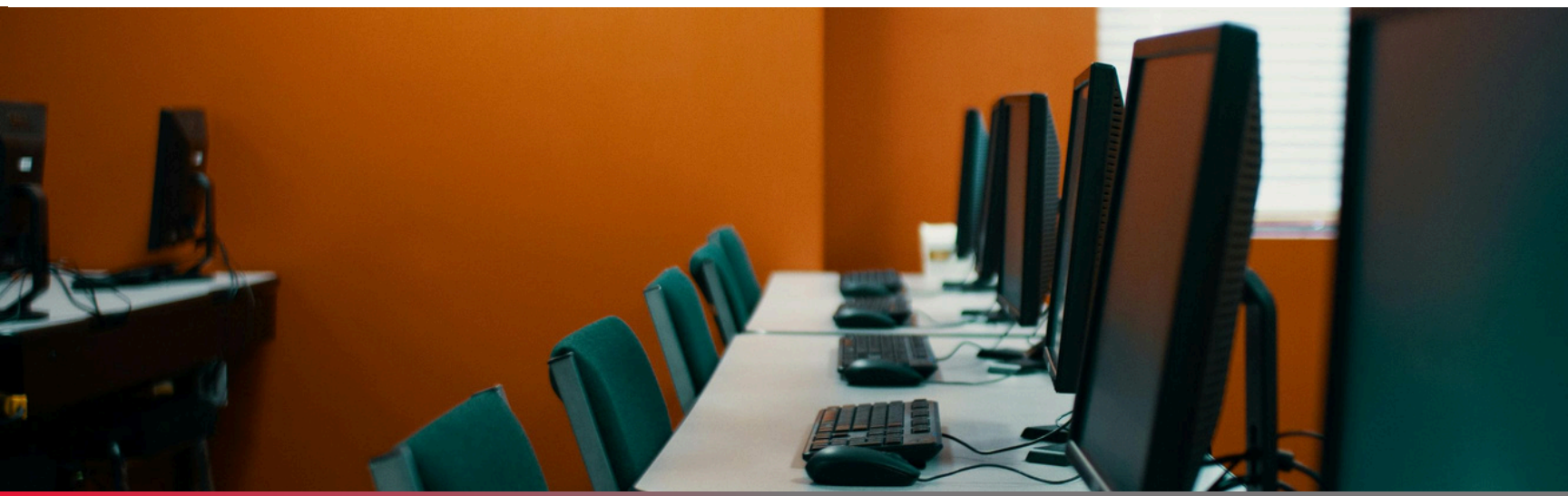
PEGGNET COMPUTERS



# 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!

Christopher McManus
Founder & CEO

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

Administrator access often starts with a simple 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 quickly. The problem is that the access often stays long after that task is finished.

Once an employee has administrator access, they can approve software installations and make changes that would normally require help from IT. If the wrong program is installed or someone takes control of the employee's account, those permissions can also give that person more control over the computer. For a business, limiting those permissions is a practical way to reduce unnecessary risk while still giving employees the access they need to do their jobs.

**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 resources on that computer. 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
- Change 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 administrative users and using a standard account when administrator rights aren't required.

**Standard accounts are suitable for everyday work**

Most employees don't need administrator access to handle their normal work. A standard account can still be used for everyday 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 to protected parts of the computer. An employee shouldn't receive permanent administrator access just because one program needs an update. IT can approve the installation, deploy the update remotely, or use a separate administrator account for the task.

**How to handle software installations**

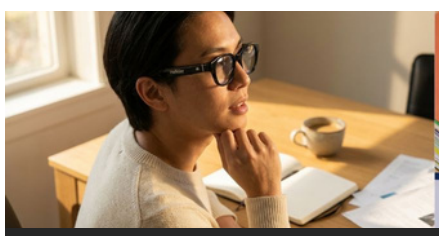
Employees can still get the software they need without keeping administrator access. Your IT team can install it remotely, approve a request when needed, or deploy updates across several computers at once. If a program expects administrator access, your IT provider may be able to change its setup or identify a supported alternative.

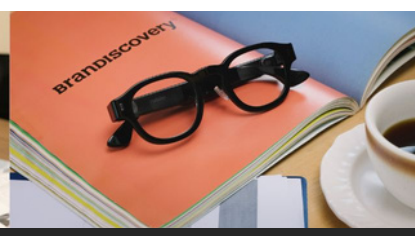
Keep a separate administrator account for approved technical work. Don't use it for email, web browsing, or everyday tasks, and protect it with multifactor authentication where the system supports it.

**Check who has access now**

Ask your IT provider to review administrator accounts on every company computer and account. Before removing access, confirm that IT has a tested way to perform administrator tasks on every device.

The goal isn't to make employees' jobs harder. It's to give them the access they need for everyday work without giving their accounts, or the software they run, more control than necessary.






## 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.

PEGGNET COMPUTERS

# SHOULD EMPLOYEES USE PERSONAL DEVICES FOR WORK?

Allowing employees to use personal phones or computers for work 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 clear rules about what work is allowed, which applications employees can use, and what happens to company information if a device is lost or an employee leaves.

Personal devices can work for limited business tasks 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 called 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.

The concern isn't simply the device itself. Files can remain in the Downloads folder, and accounts can stay signed in after the work is finished.

## Decide what employees may do

Set the rules based on the work being done 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.

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

## Set minimum security requirements

A personal device used for work should meet basic security requirements. It should run an operating system that still receives security updates and have a screen lock, device encryption where available, and current updates. Multifactor authentication should also be enabled 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.

Employees should also understand what the business can see or remove before they enroll a personal 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.

Having this process decided in advance makes these situations much easier to handle.

## When to provide a company device

A company-owned device makes more sense 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 it shouldn't be an informal arrangement. The rules need to be clear, employees need to understand them, and the device needs to meet the security requirements your business has established.

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

Canceling a cloud service may sound straightforward, but what happens to your business data afterward depends on the provider. Some providers keep information available for a limited time, while others restrict access as soon as the subscription ends. Your account may become read-only, remain available only to an administrator, or be scheduled for deletion.

Before you cancel, check the provider's current documentation and your contract. Confirm when employees will lose access, how long your data will remain available, what the export includes, and whether you need to request it while the subscription is still active. If you purchased the service through a reseller, check the cancellation process with them as well.

Before closing the account, take a few practical steps:

1. **Know what is stored there.** Make a list of the business information you need, including attachments, comments, reports, audit records, and custom fields.
2. **Export what you need and check it.** Open a sample of each file type and make sure attachments, dates, and customer or project details are complete.
3. **Test the move.** If you're switching providers, test the import while you still have access to the original service.
4. **Check connected systems.** Review website forms, payment tools, reports, mobile apps, automated workflows, and other systems that depend on the service.
5. **Check connected sign-ins.** If employees use the account to sign in to another application, change those sign-ins before closing the old account.

Your business may also have requirements for keeping financial, customer, employee, or contract records. Check those requirements with the appropriate legal, accounting, or compliance adviser.

Finally, ask the provider what will be deleted from active systems and backups, when deletion will occur, and whether the account must be closed separately. Keep that confirmation with your business records.

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

Guest Wi-Fi should give visitors internet access without giving their devices access to your business network. Guests should not be able to reach business computers, cameras, file storage, or network equipment.

A different Wi-Fi name and password alone do not guarantee that separation. Your router, wireless access points, and firewall need to be configured so guest devices can reach the internet without reaching internal systems.

The same approach can work for employee phones and personal laptops that only need internet access. Keeping those devices on the guest network can limit what they can reach inside the business environment.

It is worth having your IT provider test the setup. They should confirm that a device connected to guest Wi-Fi can access the internet but cannot open internal systems or network management pages.

Most small businesses can use one internet connection while keeping guest and business networks separate. The goal is simple: give visitors the access they need without giving their devices a path into the systems your business depends on.

# SMALL BUSINESS IT BUDGET: WHAT TO INCLUDE AND HOW TO PLAN IT

An IT budget should reflect the systems your business relies on and the changes you expect during the year.

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

Separate regular operating costs from one-time purchases and planned projects.

Include onboarding and offboarding, employee training, backup testing, cybersecurity reviews, and equipment disposal. Keep some room in the budget for an unexpected replacement or work outside your support agreement.

Review the budget each quarter against actual invoices. Look 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 make the decision. Start reviewing each device around three years, then look at its security support, reliability, performance, warranty, and repair history.

Security should always come first. Replace a computer if it cannot run an operating system that still receives security updates or support the software your business needs. Even if an older computer still performs well, it may need replacing when its operating system is no longer supported.

Before an old computer is sold, donated, recycled, or returned, make sure required data is transferred and the storage is properly erased.

Keep a replacement schedule that includes 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, reach out to us. We can help you plan replacements before an aging computer becomes a business problem.

# TECHNOLOGY TRIVIA TIME

Each month, you have a chance to win a $50 Amazon gift card by answering our Technology Trivia Question of the Month!




**TAKE THE QUIZ & WIN**

***Click below to answer this month's Technology Trivia question and enter for your chance to win.***

**Click Here**

LAST MONTH'S ANSWER

***Image Maximum***