



PANTHEON Newsletter

WWW.PANTHEONCOMPUTERS.COM

MEET TATE!



What is something small that always makes your day better?

A walk and deep breathing

If you could instantly become an expert at one skill, what would it be?

Reverse Engineering

What is the best advice you have ever received?

To not take things at face value, always ask more questions, always be eager to learn

If you could have any job for one day, what would you choose?
General Manager of the Chicago Bears

TECH TIP OF THE MONTH

How to Keep Sensitive Information Secure at Your Desk

Cybersecurity is not only about passwords and suspicious emails. Sensitive information can also be exposed through papers left on a desk, an unlocked computer, or a conversation others can overhear.

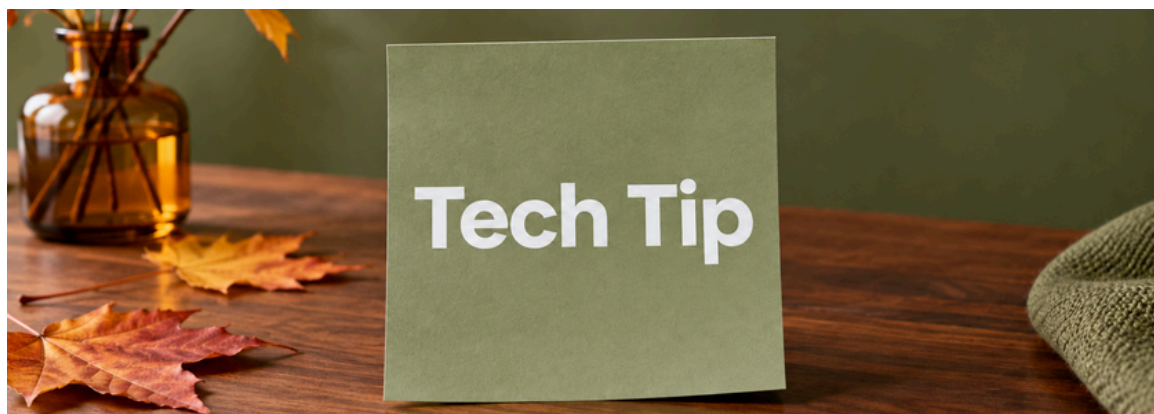
A few small habits can help protect company and client information throughout the day.

- Lock your screen when you step away. Even a quick trip to the printer or break room is enough time for someone to access an unattended computer.
- Keep sensitive documents out of sight. Client records, financial information, passwords, and employee details should not be left where visitors or coworkers can easily see them.

- Be mindful of where you talk. Avoid discussing confidential information in public spaces, on speakerphone, or where others may overhear.
- Pick up printouts promptly. Do not leave documents sitting on a shared printer longer than necessary.
- Secure paperwork when you are done. Store it in an appropriate locked location or use approved shredding when it is no longer needed.

Tech Tip: Make locking your screen a habit by pressing Windows + L every time you leave your desk.

If you think sensitive information may have been seen, shared, or left unsecured, notify your manager or IT provider as soon as possible.



LET'S CELEBRATE BIRTHDAYS!



Janella
09/05



Kyle
09/09



Dale
09/14



Kelsey
09/22



Jay
09/25



Juan
09/26



Dillon
09/26

Your Biggest Security Vulnerability May Already Be on the Payroll

Most people know their business depends on technology—but the biggest risk does not always come from a failed firewall or an outdated system. Sometimes, it starts with a convincing email, a rushed decision, or a phone call that sounds just legitimate enough to earn someone's trust.

In this featured article from our Q3 Pillar Magazine, Pantheon Director of Business Operations Nikki Dulas explores why employees are often the most targeted part of an organization's security posture—and why that does not make them the problem. Cybercriminals rely on urgency, authority, familiarity, and timing to turn ordinary human moments into opportunities.

The article looks at the role ongoing security awareness training, simulated phishing campaigns, and consistent follow-up play in reducing risk. Just as importantly, it highlights why employees need a culture where they can quickly report a suspicious message or admit they may have clicked something they should not have—without fear of embarrassment.

Even with strong security tools in place, people make judgment calls under pressure every day. The goal is not perfection; it is making mistakes harder to make, easier to catch, and faster to report. When employees understand what to watch for and know they will be supported when they speak up, they become an important part of the organization's defense.

A strong security strategy is built with both technology and people. It means helping employees recognize threats, make safer decisions, and respond quickly when something does not seem right.

Read the full article in our Q3 Pillar Magazine to learn how to strengthen your organization's human firewall. Reach out to Pantheon Computers if you would like a copy of the full magazine.

DAD JOKE OF THE MONTH:

Why did the scarecrow get promoted?

Because he was outstanding in his field.

