

The Tech Tribune

Anniversary

Congratulations to Dawn Hunt!

Dawn has been at our company for 5 years this month. She is our rock star accountant. Her position allows her to effectively manage all of our client accounts as well as performing overviews of the financial operations to ensure that we are running efficiently. Dawn has grown to be an indispensable part of our team. Thank-you, Dawn, for your commitment and dedication to continue to make Acts360 great!

August 2016



This monthly publication provided courtesy of Greg Sweers, CEO of ACTS360.

“As a business owner, you don’t have time to waste on technical and operational issues. That’s where we shine! Call us and put an end to your IT worries!”



The biggest block to protecting your company’s data is employee ignorance about cybersecurity. In fact, your employees are probably compromising your data right now and aren’t even aware of it.

In case you haven’t read the reports, a statement from one of the many companies recently forced to close its doors following a cyber-attack involving one of their own employees brings the point home:

“Code Spaces will not be able to operate beyond this point. The cost of resolving this issue and the expected cost of refunding customers who have been left without the service they paid for will put Code Spaces in an irreversible position both financially and in terms of ongoing credibility.”

Root cause of the disaster? Very

Employees Keeping Your Data Safe? Don’t Count On It

likely a phishing attack that one of their own team members unwittingly played a key role in. If you want even a ghost of a chance that your data remains safe and secure, you **MUST** be aware of the five ways your employees are probably putting your company at risk right now:

Risky Passcode Practices

A good rule of thumb is, if you can recall a password, it’s probably not safe. Require the use of a random password generator to keep weak passcodes from being the weak link in your data’s defenses. Invest in a company-wide password protection system. And wherever possible, use two-factor authentication for logins to critical sites.

Working Outside A Secured Network

It’s great that your team loves to collaborate. Just make sure

continued pg.2