The Tech chronicle

## Coffee Anyone?

What keeps most offices running smoothly from day to day? Coffee of course.

We don't only keep your system up and your security in check, but we are pleased to announce that one of our clients has graciously offered a 10% discount on some coffee choices.

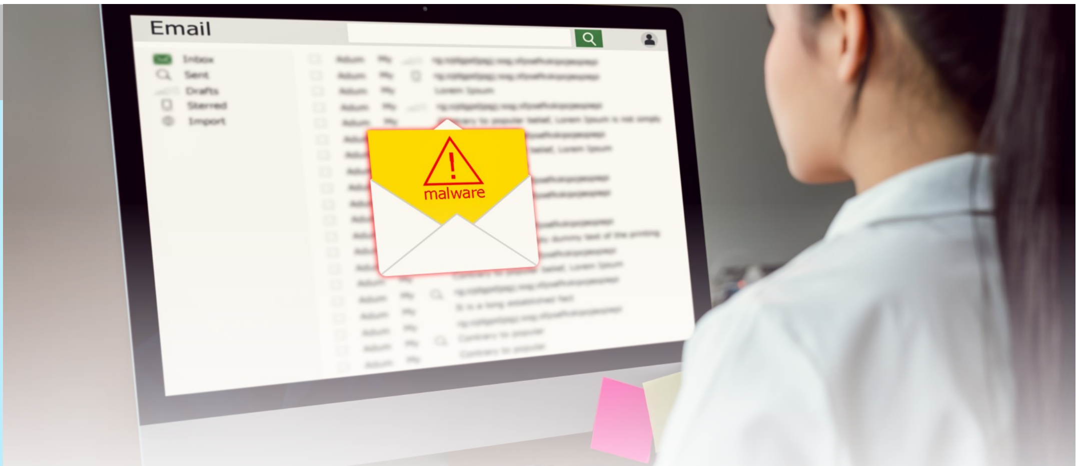
This is a one-time use coupon, but reach out and give them a try.

Once you're set, cheers to you, and enjoy a nice cup o' joe.

June 2021

This monthly publication provided courtesy of Carlos Soto. Franchise owner since 2005.

Our Mission: To build a community of successful-minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.



# Don't Let Your Employees Become Your Biggest Vulnerability

A couple years ago, *TechRepublic* ran a story with the following headline: "Employees Are Almost As Dangerous To Business As Hackers And Cybercriminals." From the perspective of the business, you might think that's simply inaccurate. Your company strives to hire the best people it can find – people who are good at their jobs and would never dream of putting their own employer at risk.

And yet, many employees do, and it's almost always unintentional. Your employees aren't thinking of ways to compromise your network or trying to put malware or ransomware on company computers, but it happens. One Kaspersky study found that 52% of businesses recognize that their employees are "their biggest weakness in IT security."

Where does this weakness come from? It stems from several different things and varies from business to business, but a big chunk of it comes down to employee behavior.

**Human Error**

We all make mistakes. Unfortunately, some mistakes can have serious consequences. Here's an example: an employee receives an e-mail from their boss. The boss wants the employee to buy several gift cards and then send the gift card codes to them as soon as possible. The message may say, "I trust you with this," and work to build urgency within the employee.

The problem is that it's fake. A scammer is using an e-mail address similar to what the manager, supervisor or other company leader might use. It's a phishing scam, and it works. While it doesn't necessarily compromise your IT security internally, it showcases gaps in employee knowledge.

*Continued on pg.2*

*Continued from pg.1*

Another common example, also through e-mail, is for cybercriminals to send files or links that install malware on company computers. The criminals once again disguise the e-mail as a legitimate message from someone within the company, a vendor, a bank or another company the employee may be familiar with.

It's that familiarity that can trip up employees. All criminals have to do is add a sense of urgency, and the employee may click the link without giving more thought.

**Carelessness**

This happens when an employee clicks a link without thinking. It could be because the employee doesn't have training to identify fraudulent e-mails or the company might not have a comprehensive IT security policy in place.

Another form of carelessness is unsafe browsing habits. When employees browse the web, whether it's for research or anything related to their job or for personal use, they should always do so in the safest way possible. Tell employees to avoid navigating to "bad" websites and to not click any link they can't verify (such as ads).

> **"One Kaspersky study found that 52% of businesses recognize that their employees are 'their biggest weakness in IT security.'"**

Bad websites are fairly subjective, but one thing any web user should look for is "https" at the beginning of any web address. The "s" tells you the site is secure. If that "s" is not there, the website lacks proper security. If you input sensitive data into that website, such as your name, e-mail address, contact information or financial information, you cannot verify the security of that information and it may end up in the hands of cybercriminals.

Another example of carelessness is poor password management. It's common for people to use simple passwords and to use the same passwords across multiple websites. If your employees are doing this, it can put your business at a huge risk. If hackers get ahold of any of those passwords, who knows what they might be able to access. A strict password policy is a must for every business.

**Turn Weakness Into Strength**

The best way to overcome the human weakness in your IT security is education. An IT security policy is a good start, but it must be enforced and understood. Employees need to know what behaviors are unacceptable, but they also need to be aware of the threats that exist. They need resources they can count on as threats arise so they may be dealt with properly. Working with an MSP or IT services firm may be the answer – they can help you lay the foundation to turn this weakness into a strength.

## FREE Report: 12 Little-Known Facts Every Business Owner Must Know About Data Backup And Disaster Recovery

PROTECT YOUR DATA

"12 Little-Known Facts Every Business Owner Must Know About Data Backup, Security And Disaster Recovery"

Discover What Most IT Consultants Don't Know Or Won't Tell You About Backing Up Your Data And Recovering It After A Disaster

**You will learn:**

- The only way to know for SURE your data can be recovered if lost, corrupted or deleted – yet fewer than 10% of businesses have this in place
- Seven things you should absolutely demand from any off-site backup service
- Where many backups fail and give you a false sense of security
- The #1 cause of data loss that businesses don't even think about until their data is erased

**Claim your FREE copy today at http://go.ctmaryland.com/12facts**

## 2FA—What is it?

Two-factor authentication (2FA) improves on security for anytime you use online services.

2FA is a method of establishing access to an online account or computer system that requires the user to provide two different types of information.

When you login to a secure site, you input your username and then your password.  With 2FA, after the password you will be asked to provide a code, normally found on your smartphone app, which changes automatically every 45 seconds (depending on the method being used).

Soon, Google may force all users to use 2FA for security.  In the near future, Google will push Gmail and Google account holders to use 2FA by automatically enrolling them.

If you choose not to use 2FA you will make your accounts easier to hack and less secure.

Keep building up your resistance to hack attacks by using strong passwords and 2FA.

Keeping your passwords fresh will also help.  We recommend changing all (yes, all) your passwords every 90 days.

Need more info?  Give us a call, let's talk about it works.

# From Start-Ups To Best Places To Work: How Culture Changes Everything

There are two parts to culture: people and systems. On the people side, consider the "Empathy Accountability Continuum." Empathy is at one end of the spectrum and accountability at the other.

Then, based on who you are dealing with and the context of the conversation, figure out where you need to be on that continuum. The more you get to know someone, the easier it becomes to choose the right moment in time to lean toward either empathy or accountability.

How do you know where to land on the scale? Be curious about the people on your team as well as people in the world around you. Ask what they are doing and how they are doing it.

A big part of maintaining curiosity and understanding also comes from being calm and connected. You can't have a connection with your people unless you are calm. It's part of being a leader within your organization.

To that effect, you need to be able to lead yourself and know where you are on the Empathy Accountability Continuum. We can't lead others unless we can lead ourselves. So, we have to understand our own fears and concerns. Then it becomes easier to make those connections.

On the systems side of things, you have to "discover the core": your core purpose and core values, which tell you what is important to you and your business.

As part of that, you also need to document the future. Plan, strategize and put it into writing. Where are you going? What is your vision?

What is your BHAG (big, hairy, audacious goal)? What is your 10-year obsession?

Once you plan and put your future into writing, you have to execute relentlessly. This is how you make sure you get there. Live your system – use daily rituals like huddles and make sure they are useful. You should be constantly talking about your core values and goals.

Of course, as part of building a strong culture, you need a robust recruiting process. Find the right people and keep them engaged. Have a multistep and multiperson process when hiring and use a scorecard (a very detailed job description) when recruiting.

When you bring it all together – people and systems – be sure to show more love. Make sure there is peer recognition and recognition from leadership on a regular basis. Send them cards on their anniversary or birthday. Even have a budget for when bad stuff happens in people's lives.

But don't rush your culture. Take it one piece at a time – do something every day to work at it and build something great.

*Tristan White is the founder and CEO of The Physio Co, a unique health care company based in Australia. While he's led The Physio Co, the company has been ranked one of Australia's 50 Best Places To Work for 11 consecutive years. In building this fast-growing company, White authored the book* Culture Is Everything *and started a podcast,* Think Big Act Small. *Learn more at TristanWhite.com and see his Petra Coach webinar at* ***PetraCoach.com/from-start-up-to-best-places-to-work-how-culture-changes-everything-with-tristan-white***

### Are You Stuck In The Self-Employment Trap?

Many people go the self-employment route in order to have more control over their days, in search of a better work/life balance. But reality soon becomes very different: long hours while you pour everything into the business. This leads to burnout. What actions can you take to avoid or escape this trap?

**Delegate More Tasks.** This is hard to do, especially when you want things to go just right. Turn your attention to hiring one or more employees who are up to the challenge and can meet your needs. It might take a while to find the ideal match, but it's worth it to find someone who can take on crucial tasks and help you achieve your goals.

**Inspect Your Systems And Processes.** Across the board, you need systems and processes in place. When you have a framework to follow, it makes it much easier to reclaim your time and energy. Inc., *Feb. 18, 2021*

*"I think we're named after computer passwords."*

### Make The Most Of Your Remote Workforce

More people are working at home. With a spread-out workforce, businesses face new challenges that they didn't face with the traditional in-office model. Now, as businesses adapt, they are looking for waysto get more out of their remote workforce.

**1. They're Reorganizing.** Businesses are taking a hard look at their internal structure, along with systems and processes. They're shifting the way they hire by raising their expectations. Along with that, they're redoing the way they onboard and train. They're relearning to do everything remotely, and tools like Slack and Zoom are taking center stage.

**2. They're Investing In Technology.** Businesses are bringing new tools and tech into the mix. They're investing in communication and collaboration tools. They're relying heavily on the cloud and VPNs. They're also buying devices like laptops and PCs for their remote workforce to ensure everyone is using the same, approved technology – which makes support and security more efficient. *Inc., Feb. 27, 2021*

### Use Technology To Make Your Business Stand Out

Today's workforce is more tech-savvy than ever before. This means your business should be as well. You want to attract good talent, and leveraging your own tech prowess can be a way to do just that.

Think about how you engage with social media. Is it something that's just there or is it something you're using to actively reach out and connect with customers, potential customers and your community? TikTok, for example, relies on a powerful algorithm to reach specific audiences. Businesses can take advantage of that to get content, including ads, to relevant eyes. According to Hootsuite, TikTok pushes for five million daily impressions for certain ads.

Taking it a step further, you can mix AI with human communication. Chatbots are more advanced than ever and can seriously impact lead generation. Chatbots also direct users to real people to continue the conversation on specific terms. Basically, there are more ways to customize how you communicate, and it's worth investing in. *Forbes, March 12, 2021*

# IT Scramble

1. RUTSTCIRRAENUF ____________________
2. ORAFTEWS ____________________
3. URSIV ____________________
4. ATMGEEYB ____________________
5. EBMRRICYCE ____________________
6. SUCEYRIT ____________________
7. CAPKUB ____________________
8. RYOMEM ____________________
9. IEBRF ____________________
10. ETOBRO ____________________
11. PUCETMRO ____________________
12. BTAGGII ____________________
13. WEBSROR ____________________
14. RAODTMEOBRH ____________________
15. AOJTNR ____________________
16. PRIPAEHLRE ____________________
17. RGCSPIAH ____________________
18. YSWPAER ____________________
19. KICOOE ____________________
20. ANDROADBB ____________________
21. MAELRAW ____________________
22. RSPODWSA ____________________
23. TENRETIN ____________________
24. IARLFELW ____________________
25. KWRTNOE ____________________

10% off these items with Computer Troubleshooters coupon code: CTMD
*One-time use only

Barrie House House Blend Extra Bold Single Serve Capsules, 24 ct

Barrie House 100% Colombian Single Serve Capsules, 24 ct

Barrie House Clay Avenue FTO Single Serve Capsules, 24 ct

Barrie House Descafeinado FTO Single Serve Capsules, 24 ct

This month we have a scramble puzzle for you.

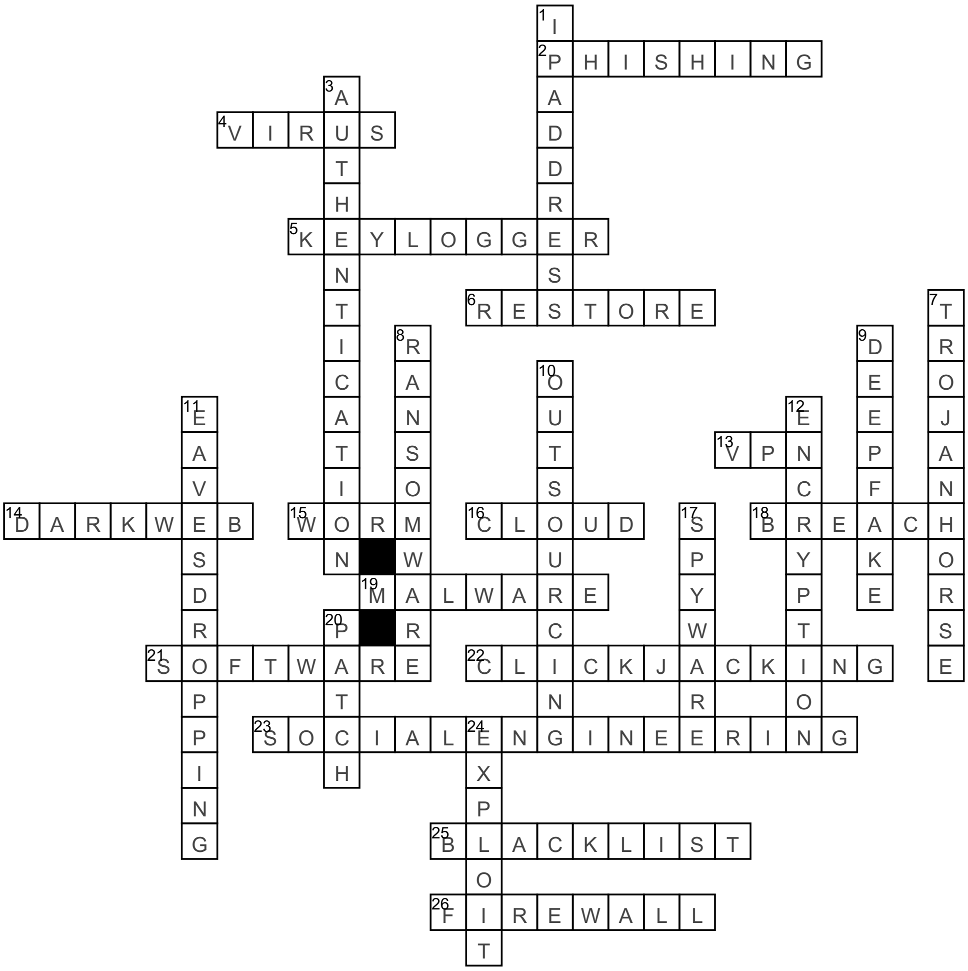
Figure out what IT word is scrambled.

We will provide you with the answer in next month's newsletter.

In the meantime, here is the coupon the newsletter was referencing you to use.

Give Coffee Etc. a chance to bring you peace of mind on their services, as well as a great cup of coffee.

# Cyber Security Terms



**Across**

**2.** A technique used by hackers to obtain sensitive information

**4.** A type of infection aimed to corrupt, erase or modify information on a computer before spreading to others

**5.** Any means by which the keystrokes of a victim are recorded as they are typed into the physical keyboard

**6.** The process of returning a system back to a state of normalcy

**13.** The acronym for a tool that allows the user to remain anonymous while using the internet by masking the location and encrypting traffic

**14.** What describes the deepest part of the internet where few dare to tread safely

**15.** An infection that can replicate itself in order to spread the infection to other connected computers

**16.** What technology allows a user to access files or services through the internet from anywhere in the world.

**18.** The moment a hacker successfully exploits a vulnerability in a computer or device, and gains access to its files and network

**19.** An umbrella term that describes all forms of malicious software designed to wreak havoc on a computer

**21.** What is a set of programs that tell a computer to perform a task.

**22.** A hacking attack that tricks victims into clicking on an unintended link or button

**23.** A technique used to manipulate and deceive people to gain sensitive and private information

**25.** A security mechanism prohibiting the execution of those programs on a known malicious or undesired list of software

**26.** A defensive technology designed to keep the bad guys out.

**Down**

**1.** What is the internet version of a home address for your computer

**3.** The process of proving an individual is a claimed identity

**7.** A piece of malware that often allows a hacker to gain remote access to a computer

**8.** A form of infection that prevents you from accessing your files holding your data hostage

**9.** An audio or video clip that has been edited and manipulated to seem real or believable

**10.** The action of obtaining services from an external entity

**11.** The act of listening in on a transaction, communication, data transfer or conversation

**12.** The process of encoding data to prevent theft by ensuring the data can only be accessed with a key

**17.** A type of infection that functions by looking at user activity without their knowledge

**20.** An update or change or an operating system or application

**24.** A malicious application or script that can be used to take advantage of the computer's vulnerability