CETech
IT Hassle Free
1425 Mount Read Blvd Suite 125
Rochester, NY 14606

Who Else Wants To Win A $25 Gift Card?

You can be the Grand Prize Winner of this month's Trivia Challenge Quiz! The first two people to correctly answer this month's trivia question will receive a $25 Amazon gift card. One winner per company per quarter. Call us now with your answer!

What do we call a collection of two or more computers that are located within a limited distance of each other and that are connected to each other directly or indirectly?

A) Internet
B) Intranet
C) Local Area Network
D) Wide Area Network

Email us at **chill@cetechno.com** or call us now with your answer! **585-441-0055**

3 Technology Truths For Transforming Your Business

1. You have to keep up. Tech changes fast. By the end of this year, 5G will be more widely available – along with devices that can use it. More businesses will be relying on artificial intelligence to supplement productivity and customer interaction, putting them light-years ahead of the competition that lags behind.

2. You have to invest. Change comes with cost. If you aren't willing to invest in new tech, then you will fall behind, and so will your support and security. If you run into any problems, then you could be in big trouble.

3. Don't fall behind on cyber security. It's easy to forget about cyber security when things are running smoothly and working as intended. But cybercriminals never stop. They are always looking for a way in, and if you fall behind the times on your IT security, then you make it easier for them. Keep your data and your customers as secure as possible. *Inc., July 30, 2019*

HOW MALWARE CAN CRIPPLE YOUR BUSINESS

Every year, the number of malware attacks on small businesses increases. *Symantec's 2018 Internet Security Threat* Report found that between 2017 and 2018, malware increased by 54%.

The term "malware" covers a number of different malicious programs, including ransomware, spyware, viruses, worms, Trojan horses and more.

In many cases, malware is designed to take over your computer. It may be programmed to look for specific data or it may give a hacker remote access to your files. In the case of ransomware, it lock you out of your computer until you pay the hacker a ransom. After that, the hacker may give you back control – or they might delete everything on your hard drive. These are not good people. If you don't invest in cyber security, then hackers can destroy your business. It's already happened to countless businesses across the country. It's estimated that websites experience up to 58 cyber-attacks every day. Protect yourself before it's too late. *Small Business Trends, Oct. 12, 2019*

CE BITS & BYTES
INSIDER TIPS TO MAKE YOUR BUSINESS RUN FASTER, EASIER AND MORE PROFITABLY
July 2020

WHAT'S NEW

Thank You Rochester!

With nearly 40,000 votes by the local business community, we are extremely honored to be a Rochester Business Journal "Reader Rankings" winner in two categories:

Best Cybersecurity Company
&
Best IT Outsourcing Firm

Thank you to our clients and everyone who voted for us! All winners will be celebrated online this year through category-specific daily video rollouts honoring all winners and revealing the top winner in each group.

We look forward to the announcement of the Category Winners in late July!

585-441-0055

3 Critical Cyber Security Protections EVERY Business Must Have In Place NOW To Avoid Being Hacked

Five years ago, you might have had state-of-the-art security protecting your business and network. You had the latest malware protection, highly rated firewalls and a great data backup plan. Maybe you even had a handbook on how to address cyberthreats. You were set. But then you forgot to do one crucial thing: you didn't stay up-to-date with your IT security policy.

This is a trap countless businesses fall into. They invest in great cyber security once. Five years ago, this was fantastic. The problem is that cyberthreats are constantly evolving. Methods used by hackers and cybercriminals have come a long way in the past five years.

Criminals stay on top of what's going on in the IT security industry. They are always looking for new ways to steal your data and make a quick buck at your expense.

What can you do to stay up-to-date in an ever changing digital world? Here are three things every business must do to protect itself.

Understand The Threats
It's easy to assume that hackers are trying to get into your network the "old-fashioned" way. You might picture them hacking your network trying to get your passwords and usernames or breaking through your firewall protection. While some hackers will do this (it's easy for them if you use simple passwords), many of today's cyber - criminals rely on social engineering.The most common form of social engineer-

-- Continued on page 2

... continued from cover

ing is the phishing scam. The criminal sends you or your employees an e-mail, hoping someone will click a link or open an attached file.Cyber- criminals have gotten VERY sophisticated. These e-mails can mimic the look of a legitimate e-mail from a legitimate business, such as the local bank you work with or another company you buy from (or that buys from you). Social engineering is all about tricking people.

This is why you need a cyber security handbook – one that is regularly updated. It's something you can reference. Your team needs to know how to identify a phishing e-mail, and you need to have procedures in place for what to do if a questionable e-mail shows up. This helps keep your employees from becoming the weak link in your security setup.

Update, Update And Update
From software to hardware, you must-

> ***"Proactive monitoring means your network is being watched 24/7."***

stay updated. There is no such thing as "one-and-done" when it comes to network security. Something as simple as a wireless router can DESTROY your security if it's not regularly updated. Hackers are always looking for vulnerabilities in both hardware and software, and when they find them, they WILL exploit them.

What happens when a piece of hardware (like a router) is no longer supported by the manufacturer? This occurs all the time, particularly as hardware ages. Manufacturers and developers drop support for their older technology so they can focus on their newer products. When they drop support for a product you use, this is a good indicator that you need to replace that piece of hardware. The same applies to software.

You might balk at the cost of buying new technology, but in the long run, the cost is well worth it. Think of the cost of buying a new router versus the cost of cleaning up after a data breach. Some small businesses never recover after a hack – it's just too expensive. Keep your malware software updated, keep your firewall updated, keep your cloud backups updated and keep all your devices and software UPDATED!

Invest In Proactive Network Monitoring
When it comes to the security of your network and overall business, being proactive can make a huge difference.

Proactive monitoring means your network is being watched 24/7. Every little ping or access to your network is watched and assessed. If a threat is found, then it can be stopped.

The great thing about proactive network monitoring is that you can customize it. Want to know about every threat? You can request a real-time report. Only want updates once a day or once a week? That can be done too! This approach means you have one less thing to think about. Someone is always keeping an eye on your network, making sure the bad guys stay out.

You might think, "How am I going to do all this?" You don't have to go it alone – and you shouldn't. Work with an IT services firm. Work together to find the best solutions for your business. When you work with IT specialists, you can rest assured your team will be updated on today's threats. You'll know your network – and everything connected to it – is updated. And you'll know someone is watching over you. That's the ultimate peace of mind.

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

You'll 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 https://www.cetechno.com/12facts

> "I've found everyone very helpful and responsive. Doreen is terrific and has helped us out many times. I highly recommend!"
>
> Julieray Romano
> Brighton Volunteer Ambulance

CARTOON of the MONTH

"Remember, once you get past my secretary, assistant, and security, my door is always open."

SHINY NEW GADGET OF THE MONTH

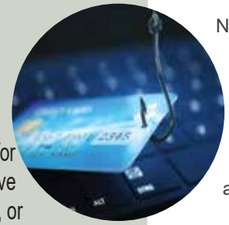
FitTrack – A Smart Scale That Does More

The bathroom scale isn't always the most useful device in the home. FitTrack is a smart scale that aims to change that. It's a different kind of bathroom scale that gives you much more than a single number.

Traditional bathroom scales don't tell you anything about what's happening in your body. FitTrack does. It gives you an "inside look" into what's going on inside your body. It measures your weight, body fat percentage, body mass index, muscle and bone mass, hydration and more. In fact, it tracks 17 key health insights.

The advanced scale pairs with the FitTrack app, which you can download to your smartphone and connect to the smart scale. All you do is step on the scale with your bare feet – the scale actually reads electrical signals from your body – and it sends the results to your phone. Simple and useful. Learn more about FitTrack at **bit.ly/2VOg7Vs.**

Have You Received A 'Smishing' Text?



Smishing, or SMS phishing, is similar to phishing. With phishing, scammers send fraudulent e-mails with links or attachments. The goal is for the recipient to share sensitive details, like bank passwords, or to install malware on their computer so the scammer can ultimately steal or extort money from them.

With smishing, the scammer sends a text message instead. Scammers often pose as banks or government agencies (like the IRS or the Social Security Administration). The text may say your accounts have been compromised or that you're owed money — all you have to do is click the link in the text and share sensitive information.

The best thing to do is delete these types of text messages. Never respond and never click on anything in the message.

CETech's Client Spotlight:

Love Beets is a true labor of love from the husband and wife team, Guy and Katherine Shropshire. The Shropshire family, known for growing salad vegetables in England, decided to purchase a small beet factory with the hopes of sharing a family favorite with others. They knew they wanted to find a way to attract younger people to beets, so the family got to work experimenting with unique marinated beet recipes.

In October 2010, Guy and Katherine brought their marinated baby beets to New York City's Fancy Food Show, where the response was overwhelmingly positive. Virtually everyone who tasted their beets said they "love beets!"

Not only did the name stick, but Guy and Katherine moved to the United States, looking for opportunities to build their brand and spread the beet love. With the help of family, farmers, and major retailers, the Love Beets brand blossomed and expanded its reach across the country!

Love Beets flourished and grew so much that in 2016 the company invested in its own state-of-the-art production facility in Rochester, New York. Most of the beets come from farms within the United States, most of which are in upstate New York.

Since its launch, Love Beets has been defying preconceived notions of beets with an upbeat, fun, modern brand and tasty products that attract beet lovers and beet newbies alike! Guy and Katherine now have an amazing team to help them spread the beet love.

We love our company and we hope that you will too!

CHOCOLATE BEET BUTTER CUPS W/ RASPBERRY
PREP TIME: 25 MINUTES // COOK TIME: 8 MINUTES

SERVINGS: 12 CUPS

What You'll Need:

Chocolate

16 oz. semi-sweet chocolate, chopped
1 tbsp coconut oil

Cashew Beet Butter
1 cup cashew butter
1 to 2 tbsp Love Beets Beet Powder
1 tsp vanilla extract
1 tbsp maple syrup
¼ tsp sea salt

Raspberry Chia Jam
2 pints raspberries
1 tbsp maple syrup
4 tbsp chia seeds

What To Do:

Line a muffin tin with 12 nonstick muffin liners and set aside. In a double boiler over low to medium heat, add the chopped chocolate and coconut oil and cook until melted and smooth. Remove from heat and set aside.

In a small bowl whisk together the cashew butter, beet powder, vanilla, maple, and salt until smooth. Add the raspberries and maple syrup to a small bowl. Using a fork, mash the raspberries into a chunky puree. Stir in the chia seeds and let bloom for at least 20 minutes to thicken and gel.

Spoon a small amount of melted chocolate into the bottom of the baking papers. Add a dollop of cashew butter to each cup, followed by a dollop of chia jam. Top each cup with more melted chocolate until covered.

Refrigerate or freeze cups until firm. Store in the refrigerator in an airtight container until ready to enjoy.