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

Who Else Wants To Win A $25 Gift Card?

The Grand Prize Winner of last month's Trivia Challenge Quiz was Lindsey Pacitto from the Town of Hamlin. She was the first person to correctly answer my quiz question from last month.

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.

Who designed the "first" small computer for home use?

A) John Blankenbaker
B) Steve Wozniak
C) Chuck Peddle
D) Steve Leininger

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

Back To Basics

A lot of time is spent staying protected from the newest type of scam or the newest cybercrimes, but as is true with many things, remembering the basics is the entire foundation of making sure you, your company and your clients remain safe.

Everyone in the company or organization should know basic security principles. Security principles and policies should be documented and part of every new employee training. Strong password requirements, Internet usage guidelines and only connecting remotely over VPN are examples of some common security policy items. Strict penalties for violating the security policies should be detailed.

It's not a good habit to save files onto your computer if there is a location on the network or on your server where they can live. They're much less likely to be backed up on your computer, whereas they'll reliably and regularly be backed up if they are saved on the server.

If you use websites or software that do not require regular password changes, set a calendar reminder to change the password yourself every other month. As with other things, a little prevention goes a long way – remembering the security basics, and asking about them if you don't know what they are, is the single best thing you can do to protect yourself and protect the company.

3 E-MAIL PRODUCTIVITY TRICKS YOU NEED TO KNOW

Turn Off Notifications. Every time you get a ping that you have a new e-mail, it pulls your attention away from what you were doing. It's a major distraction. Over the course of a day, you might get several pings, which can equal a lot of time wasted. Set aside a block of time for reading and responding to e-mails instead.

Use Filters. Many e-mail programs can automatically sort incoming e-mails. You define the sources and keywords, and it does the rest. This helps prioritize which e-mails you need to respond to soonest and which are most relevant to you.

Keep It Short. Most of us don't like to read e-mails – and so we don't. Or we quickly scan for relevant information. Your best bet is to just include the relevant information. Keep it concise and your recipients will appreciate it, and as a recipient, you'll appreciate it as well.
Small Business Trends, April 23, 2020

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

WHAT'S NEW

We are excited to welcome Eli Carter to our CE-Tech family!

If you heard an Australian accent when calling for support that is Eli! Some of you have already talked with and met Eli. He joined us back in late February just before quarantine.

Eli says, "I'm from Australia which isn't the closest place to here. I moved to Rochester 2 years ago for my wife and I have loved it ever since even though the winters are just slightly colder than where I moved from."

He has been a wonderful addition to the team. We get constant feedback from our clients about the terrific job he is doing. We are very fortunate to have him.

Eli says, "I love IT because I love helping people but I also love how it's ever-changing and always moving forward in new and different directions. One of my favorite areas of IT is development since its all about solving problems in new and creative ways."

Outside of work, Eli loves hiking and going to the beach.

585-441-0055

Why Your Business Is The PERFECT Target For Hackers ... *And What You Need To Do NOW To Protect Yourself*

Everybody gets hacked, but not everything makes the evening news. We hear about big companies like Target, Home Depot, Capital One, and Facebook getting hacked. What we rarely hear about are the little guys – the small businesses that make up 99.7% of employers in the United States, according to the Small Business Administration. It's these guys who are the biggest targets of cybercriminals.

Basically, if you run a business, that business is a potential target. It doesn't matter what industry you're in, what you sell or how popular you are. Cybercriminals go after everybody. In 2018, a cyber security survey by the Ponemon Institute found that 67% of small and midsize businesses in the U.S. and U.K.were hit by a cyber-attack.

For the cybercriminal, casting a wide net makes the most sense because it gets results. It puts them in a position where they are able to extort money, steal sensitive information and ultimately profit off of destroying the property, prosperity and reputation of others.

Why do cybercriminals love to target small businesses? There are a handful of reasons why small businesses make sense to attack.

1. Small Businesses Are The Most Vulnerable. Business owners, entrepreneurs and executives aren't always up-to-date on network security, current cyberthreats or best practices in IT. They have a business to run and that's usually where their focus is. Unfortunately, that means cyber security

-- Continued on page 2

... continued from cover

can take a back seat to other things, like marketing or customer support. This also means they might not be investing in good network security or any IT security at all. It's just not top-of-mind or they may feel that because it's never happened to them, it never will (which is a dangerous way of thinking).

2. Small Businesses Don't Take IT Security Seriously. Coming off that last point, it's true that many businesses don't properly secure their network because they feel that they aren't vulnerable. They have the mindset of "It hasn't happened to me, so it won't." Along those same lines, they might not even take password security seriously. According to research conducted by *Trace Security*, upward of 80% of ALL breaches come down to one vulnerability: weak passwords! Even in 2020, people are still using passwords like "12345" and "password" to protect sensitive data, such as banking information and customer records. Secure passwords that are changed regularly can protect your business!

> ***"67% of small and medium - sized businesses in the US and UK were hit by a cyber-attack ."***

3. Small Businesses Don't Have The Resources They Need. Generally speaking, medium to large companies have more resources to put into IT security. While this isn't always true (even big companies skimp on cyber security, as the headlines remind us), hackers spend less time focused on big targets because they assume it will take more of their own resources (time and effort) to get what they want (money and sensitive data). Many small businesses lack the resources like capital and personnel to put toward IT security, so hackers are more confident in attacking these businesses.

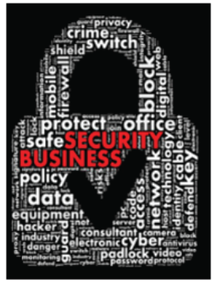
Just because you haven't had any major problems for years – or at all – is a bad excuse for not maintaining your computer systems. Threats are growing in number by the day. While many small businesses might think, "I don't have the time or resources for good security," that's not true! You don't need to hire IT staff to take care of your security needs. You don't need to spend an arm and a leg securing your network. IT security has come a LONG way in just the last five years alone. You can now rely on IT security firms to handle all the heavy lifting. They can monitor your network

24/7. They can provide you with IT support 24/7.

That's the great thing about technology today – while many hackers are doing everything they can to use technology against us, you can use it against them too. Work with a dedicated and experienced IT security firm. Tell them your business's network security needs, and they'll go to work fighting the good fight against the bad guys.

> "Fred and his team have such a thorough knowledge base. Personable, responsive, and quickly solve any issues! Our organization is in good hands with CETech!"
>
> Danell Gaudieri
> BAC Local 3

Free Cyber Security Audit Will Reveal Where Your Computer Network Is Exposed And How To Protect Your Company Now



At no cost or obligation, our highly skilled team of IT pros will come to your office and conduct a comprehensive cyber security audit to uncover loopholes in your company's IT security.

After the audit is done, we'll prepare a customized "Report Of Findings" that will reveal specific vulnerabilities and provide a Prioritized Action Plan for getting these security problems addressed quickly. This report and action plan should be a real eyeopener for you, since almost all of the businesses we've done this for discover they are completely exposed to various threats in a number of areas.

To get started and claim your free assessment now, call our office at 585-441-0055.

CARTOON of the MONTH

CE TECH TIMES September 2020

SHINY NEW GADGET OF THE MONTH

Weber Connect Smart Grilling Hub

Grilling can feel like guesswork. You throw the food on the grill and keep a close eye on it, hoping for the best. Say goodbye to guesswork and overcooked steaks with the Weber Connect Smart Grilling Hub.

The Weber Connect takes the thermometer and timer into the WiFi era. It monitors your food and sends updates to your smartphone. It lets you know when to flip the burgers or steaks – and then notifies you again when it's time to take them off the grill. You can even have the Weber Connect tell you when your meat of choice has reached your ideal level of doneness. It's great for those who are new to grilling or don't grill often, and it works with every grill! See more at **bit.ly/3eTL69Y!**

It's Time For A Smartphone App Permissions Audit

Every smartphone app requests permissions in order to operate. The basic "phone" app needs permission to use the microphone and contacts. This makes sense, and you would never think twice about it.

Other apps can pose problems. Many apps want access to your location, camera or Bluetooth, for example. For some apps, some permissions make sense. For others, they're a red flag. This is why you need to do an app audit.

On an iPhone, check app permissions in Settings > Privacy. You can view the permissions of every app you have installed and change them, if needed.

On Android devices, app permissions are in Settings > Apps & Notifications (it may be under Apps on older devices). Tap on the app for permission details.

CETech's Client Spotlight:

BRIGHTON Volunteer Ambulance

Providing a Continuity of Care

Emergency Medical Services (EMS) is a relatively new industry in comparison to its older siblings the Police and Fire Departments. While its roots go back to Napoleonic times, modern EMS was more formally structured in the 1970s to provide mobile medical care and transportation. EMS has always been at the leading edge of new technology and training. In the beginning it was mobile defibrillators and in-cab radio communications. Today it's accessing patient records via tablets, or live streaming a patient's vital signs directly to the hospital. While all this technology is impressive, it's the people who work and volunteer at BVA that are truly making a difference.

Cody Dean is the Chief of Brighton Volunteer Ambulance and has been with the agency since 2016. Prior to joining BVA he was Chief of Brockport Ambulance for two years. "*BVA is a 501c3 nonprofit, what we call a combination agency, made up of both career and volunteer providers.*" BVA is more than a transportation service, short of X-Rays, Cat Scans and surgery, they do everything in the field that happens in the emergency department and they are standing by ready to go 24x7. BVA is at the forefront of using technology to help save lives and provide a better "continuity of care" for BVA's patients. They use an array of mobile devices and cloud based applications to quickly and securely gather patient data, provide life saving procedures, and inform the hospital of the status of an incoming patient. There is no real down time for BVA according to Cody "*what people don't know about ems is we're essentially very fast-paced. Sometimes it feels like a 'wild west' type business because we can go from one moment where we're having a conversation on a zoom meeting, to the next minute we're going out and responding to all types of emergencies, whether it be taking care of somebody that just simply fell down and needs somebody to help, to standing by with a fire department at a structure fire taking care of family members and firefighters. We have to be very flexible. I have to be able to essentially go from my office, where I am able to manage everything, to really being able to do the same thing out in the field. It's just a vast technological need that I don't think a lot of people expect, we have to go from a to z very quickly but still not drop for the critical parts of the business.*"

Like many small businesses, BVA has faced many challenges during these last few months at the height of covid. While BVA does receive a small piece of their operating budget from the Town of Brighton's Special Ambulance Tax District, much of its revenue comes from billing and services rendered. Call volume was down 35% at the peak of covid, and unlike fire & police departments, the vast majority of BVA's income is tied to calls. BVA is happy to have been able to weather the storm and continue being able to provide the highest level of service to their patients. If your town has a volunteer ambulance service, don't forget to donate, your donation just may save your life.

CETech has been supporting Brighton Volunteer Ambulance for 7 years and absolutely loves having them as our client!