1991 – 2021
30 YEARS OF EXCELLENCE
Computer Technologies, Inc.

TECHNOLOGY TIMES

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

What's Inside

February 2022

Kim Nielsen
President & Chief Technology Strategist at Computer Technologies Inc.
(248) 362-3800

"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 problems finally and forever!"

Ask These 3 Questions Before Giving An "IT" Expert Access To Your Network

There are seemingly countless IT services providers to choose from these days, and it can be challenging to tell one from another. However, not all IT services providers are created equal. Some offer independent services, while others are part of larger firms. Some are new to the field, while others have been around for years. There are also companies that put out slick marketing to grab your attention but make it hard to tell if they really live up to the hype.

Well, we're here to help you cut through the clutter. You want to hire someone who knows what they're doing and will take care of your business the right way. To do that, there are a few questions you should ask every IT expert before you let them anywhere near your network – to ensure you'll be in good hands.

1. **What's Your IT Experience?** Education, certifications and hands-on experience are all important. You want to know your "expert" is actually an expert. It's all too easy for someone to pass themselves off as an expert when they really have limited experience, so you should never hire an individual or a company without vetting them first. After all, this person (or team) will be handling EXTREMELY sensitive data essential to the operation of your business. This isn't the time to take risks or give someone the benefit of the doubt.

When you work with an IT services company, or MSP, you can generally expect that the people you work with are educated and experienced, but you should **always** ask. It's okay to dive in and ask them about their certifications,

Continued on pg.2

Continued from pg.1

how long they've been doing their job and how familiar they are with your industry. And if you aren't sure what certain certifications are, feel free to ask follow-up questions. There's a very good chance they'll be more than happy to answer all of your questions, especially if they're a true professional who knows what they're doing!

2. **What's Your IT Approach?**
There are different approaches to IT and network security. You have the old-fashioned **break-fix** approach and you have the modern **proactive** approach. The break-fix approach used to be the staple of the IT industry – it was the business model of just about every IT support firm in the 1990s and early 2000s. This approach is pretty straightforward: something breaks, so you hire someone to come in and fix it. If many things break or something complicated breaks, you could be looking at a pretty hefty bill – not to mention the costs associated with downtime.

Today, most MSPs take a proactive approach (and if they don't, look elsewhere). They don't wait for something to break – they're already on it, monitoring your network 24/7, looking for internal issues and outside threats. They use advanced software that can identify trouble *before* it strikes. That way, they can go to work, proactively protecting your business so you avoid those hefty bills and long downtimes. These are companies that are willing to collaborate with you and your business to make sure you're protected, your IT needs are met and you're getting your monies' worth.

"If you're working with an IT company that doesn't have your full confidence, you may need to rethink that relationship."

3. **What's Your GUARANTEED Response Time?**
This question often gets overlooked, but it's one that can make or break your business – and it can make or break your relationship with your IT services provider. You need to know that you won't be left in the dark when something goes wrong within your network. If you're experiencing a power outage or surge or a cyber-attack, has taken out part of your server, the cost to your business can be catastrophic if your IT services provider can't get to you right away. The longer you have to wait, the worse it can get.

You need to work with someone who can give you a guaranteed response time in writing. It should be built into their business model or, better yet, the contract they want you to sign when you hire their services. They should be doing everything they can to instill confidence that they'll be there for you when you need them. If you're working with an IT company that doesn't have your full confidence, you may need to rethink that relationship.

Free Executive Guide: What Every Small-Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems

This guide will outline in plain, nontechnical English the common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills and will provide an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

Download your FREE copy today at
https://www.cti-mi.com/protectdata222/
or call our office at (248) 362-3800

Security Corner

What You Need To Know About Romance Scams

Romance scammers may have a silver tongue, but they're going for your gold. Over $304 million was reported lost to romance scams in 2020 alone. Every year, millions of people turn to online dating apps or social networking sites to meet someone. But instead of finding romance, many find a scammer trying to trick them into sending money.

The Lies Romance Scammers Tell

They'll often say they're living or traveling outside of the United States. We've heard about scammers who say they are: working on an oil rig, in the military, or a doctor with an international organization

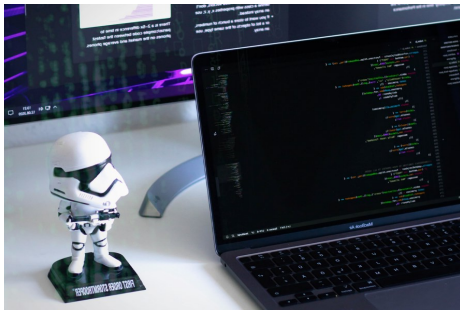
We've heard about romance scammers asking their targets for money to pay for: a plane ticket or other travel expenses, surgery or other medical expenses, customs fees to retrieve something, gambling debts, or a visa or other official travel documents.

Scammers will ask you to pay by wiring money, with reload cards, or with gift cards because they can get cash quickly and remain anonymous. They also know the transactions are almost impossible to reverse.

Here's the bottom line: Never send money or gifts to a sweetheart you haven't met in person.

For more information on how to avoid scams like these, call us at 248-362-3800 or visit us at: https://www.cti-mi.com/

How To Protect Your Business While You're Away



As any seasoned business owner knows, operations can't run one-hundred percent of the time. Whether you only shut down overnight, close on weekends or take regular holidays away, there are going to be times where no one is in the office monitoring the computer systems. When that happens, the risk of a security breach goes way up. Read on to protect your business even when you're shut down or working remotely, and don't become a prime target for cyberthreats.

Where People Go Wrong

There are plenty of reasons why businesses may leave their devices on, even in long periods when people might be out of the office. For instance, the drastic shift toward work from home and remote working opportunities has made it more common for people to remotely log into their work network using dedicated, secure software. This keeps all the company information on its secure server and still gives employees uninterrupted access to the data and applications they need to get their job done.

Consider the holiday season that just passed. How long did you take off for the winter holidays? Did you at least shut down for Christmas and New Years? Did you leave anything running while you were gone, if only to keep track of orders or continue processing requests? Maybe you have a program that logs data 24/7, every day of the week, or you're running constant security scans to protect your confidential files and data.

Keeping your devices running can do more harm than good. Following are a few ways to protect business while you're away.

Shut Down All Devices

It's tempting to keep certain machines running at all times. Sometimes it's as simple as having an old computer that takes awhile to power up, so it's faster to leave it asleep while you're gone overnight. But did you know that this actually presents a security risk that can be deadly for an organization?

Unmonitored equipment can become targets for cybercriminals. Close out of each window, log out and shut down before you leave for the day, and especially over weekends. Machines left running are more susceptible to breaches, and without anyone online or working, it will be too late by the time you log back in and try to edit corrupted or stolen files.

Double-Check Before You Go

This is especially true if you recently made an update or patch. Ethical hacking can check your security posture with penetration tests at entry points into the system and records how deep it can hack. Consider the following scenario:

You manage a company that just released a new version of an online order form for the holidays. You also booked a week-long family vacation for the following week, and gave everyone in your small business the week off to be with loved ones. Just to be safe, you leave your main server turned on over the break so that you can keep processing requests and checking in remotely through the cloud.

Then while everyone's gone, the business becomes a target for a cybercriminal. Without anyone monitoring the network, they're able to break in through a backdoor vulnerability that was left unpatched in the last software update, and quietly steal files to hide behind ransomware. The next morning, you log in through remote access software like TeamViewer to check your email. When you go to send over the requested document though, you notice something very wrong on the internal network.

How can you prevent the same thing from happening next time you want to release a holiday update for your customers? By running a penetration test and vulnerability assessment before each launch, you'll catch potential risks before hackers can exploit them and wreak havoc on your systems.

Conclusion

Between Covid variants and the usual priorities that pull you out of the office from time to time, it's inevitable that your machinery will occasionally be left unattended. Sometimes that will be for more than just overnight between shifts. When shutting down your devices isn't possible, ethical hacking (to catch vulnerabilities before they're ever exploited) and quality cybersecurity can protect you're your most valuable asset, your data.

Cybercriminals don't rest, so your security and precautions shouldn't either. **Consider cyber liability insurance** and upgrading your preventative cybersecurity measures to protect you and your company from the fallout and financial consequences of a breach.

What Is An NFT?

NFT stands for non-fungible tokens. They are the latest cryptocurrency that has exploded to the mainstream. After digital artist Beeple sold his NFT at Christie's action house for $69.3 million, NFTs got thrust to the mainstage of peoples attentions.

So what is a NFT? Basically you can transform anything digital into a one of a kind collectible that can be easily verified and traded in a blockchain. A good example would be if you had one bitcoin and traded it for another bitcoin, you would still have the same thing.

NFTs are totally unique and one of a kind, two will never be the same. Some examples of big NFT sales have been Jack Dorsey's first tweet going for more than 2.5 million and the original Nyan Cat gif went for over $600,000.

So are NFTs worth the money? It's impossible to know at this point in time. In the meantime if you want to check out what NFTs are for sale the most commonly used marketplaces for them are Mintable, Nifty Gateway, OpenSea and Rarible.

How CRM Tools Connect Your Business With Customers

CRM or customer relationship management tools connect you with customers instantly and streamlines your relationship with them. That is why many businesses are shifting to CRM tools to improve consumer interactions' consistency and quality.

With a CRM tool, you can collect information and data about your customers. Understanding your customer will help you provide amazing products or services.

CRM tools also help with customer segmentation. Categorizing your customers will understand the individual needs of customers and target specific audiences based on their liking and preferences. You can develop a better relationship with your customers by relying on customer retention. CRM helps you follow-up with customers on appointments and other activities. When you actively respond to customers, they will know how serious you consider this relationship. With CRM, you will be with your customers when they need you.

Keep Your Customers Happy With A Better User Experience

If your business has a website or an application for your users, you might have heard about user experience. User experience includes elements such as colors, layouts, fonts, and many more.

Improving user experience will elevate engagement on your website, keeping you ahead of competitors. Focusing on user experience will drive more customers. Here are some tips you can implement to improve their overall experience:

- Communicate with your audience and try to understand their behavior.
- Generate valuable insight from your website or application and check your audience's digital footprint.
- With AB testing, you can choose a successful version from two options.
- Keeping fewer elements on your website is better.
- Understand the current marketplace trends.

ELGATO STREAM DECK

If you love automating tasks, the Elgato Stream Deck is the perfect gadget for the job.

Featuring 15 fully-programable LCD keys that you can use to launch a program, adjust audio, switch scenes for streaming and so much more.

The simple drag and drop interface makes changing your key shortcuts a breeze.

You can even turn a key into a folder so that it has other nested functions beneath it. The possibilities are only limited by your imagination.