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

November 2022

Kim Nielsen, CISSP
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!"

The Cloud: Everything You Need to Know About the Invisible Server

Data storage is the foundation of your overall security structure. If your files can be stolen, changed or corrupted very easily, then everything you do online can be erased in the blink of an eye. All that effort you poured into your latest project will be gone, and all that time wasted!

When the world went digital, most data storage did too. Using something besides a physical server that sits in a "server room" reduces the risk of theft in the unfortunate event of a break-in. Off-site storage also protects your data from the negative impacts of a natural disaster.

Over time, more and more people are opting to keep their data in the Cloud instead of (or in addition to) local networks. There are pros and cons of both, but the trend itself mirrors the shift from physical to digital storage. What's more secure than storing files on your local system?

Creating backup files in a remote location, with more resources to protect your data, is safer than your private network that a hacker can take down with a few well-placed spear-phishing emails.

With that in mind, here's everything you need to know about data security in the Cloud.

What is Cloud Security?

People talk a lot about "saving to the Cloud," but what does it actually mean? Where does all that data go? The Cloud refers to a collection of many people's information, all amassed and stored on remote servers somewhere in the hub of your chosen provider. These servers are encrypted and safeguarded with

Continued on pg.2

Continued from pg.1

more powerful defense mechanisms than most small businesses can manage on their own. They store all of this data in a massive library that knows just where to pull your files when you need them.

When you want to retrieve data from your Cloud – let's say, a JPG image – then you would search on whatever browser or app you saved it on for the name of that file. As long as you're connected to the Internet, the remote server can find and deliver your desired file – or in other words, they search your section of the library for the file name and open up that JPG.

The benefits of this are that you, and others, can access that information from many different devices and you don't have to be connected to your home network to do so. If you want to collaborate on Microsoft 365 with a colleague, you can both log in and make edits at the same time. Even if you made that JPG at three in the afternoon from your home office, you can access it from the other side of the planet on your smart phone. This has obvious benefits in today's modern world!

The benefits of Cloud include: convenience, lower costs, and faster service

Is the Cloud as Safe as They Say?

The convenience is the main selling point of the Cloud. However, some people stubbornly stick to their tried-and-true physical storage devices. They've worked for twenty years; why give them up now? In addition to collaboration and worldwide connection (as long as you have Internet), it's typically less expensive to use someone else's storage and safety measures while simultaneously knowing that an expert is managing your cybersecurity overall.

So why do some people stay with what they know

- Reliance on the Internet means a slowdown in your day if the power goes out
- It can be difficult to trace who has your data and where else it may be being sold or accessed
- Conversion can be difficult; whether you're switching Cloud providers or simply trying to open a file in an unsupported format, workarounds are time-consuming and hard to come by
- You must rely on someone else to prevent hiccups and combat breaches

Conclusion

Despite some of the drawbacks, Cloud services have revolutionized digital storage systems around the globe. Convenience, lower costs and faster service have made meeting your personal and professional goals so much simpler, without worrying so much about data loss or theft by cybercriminals.

Where do *you* store your data? Maybe it's time to make the switch to a secure Cloud server instead.

"I DIDN'T KNOW"

Unfortunately, That Excuse Doesn't Replenish Your Bank Account, Resolve A Data Breach Or Erase Any Fines And Lawsuits.

It's coming ...

- That day a hacker steals critical data, rendering your office useless ...
- That day when your bank account or credit card is compromised …
- Or that day when your customers' private lives are uprooted …

Cybercriminals and hackers are constantly inventing NEW ways to infiltrate your company, steal your assets and disrupt your life. The ONLY way to STOP THEM is by CONSTANTLY EDUCATING yourself and your staff on how to PROTECT what's yours!

Now, for a limited time, we have the perfect way to help reduce your risk and keep you safe! Simply sign up to receive our FREE "Cyber Security Tip of the Week." We'll send these byte-sized quick-read tips to your email in-box. Every tip is packed with a unique and up-to-date real-world solution that keeps you one step ahead of the bad guys. And because so few people know about these security secrets, every week you'll learn something new!

Get your FREE "Cyber Security Tip of the Week"
at: https://www.cti-mi.com/1122-signup/

Security Corner

Watch Your Webcam: What Hackers Are Doing With Your Camera

Threat actors can, and do, hack into webcams for nefarious purposes. Hackers may have any number of reasons to illegally access your webcam: Blackmail, gleaning information about you, or for their own perverse entertainment.

Unfortunately, the Internet of Things (IoT) has made their jobs easier in some ways. IoT devices connect to the local network but typically have far fewer defenses against cyber-attacks than your computer, so hackers can (and often do!) target those first to break into the network.

Here are a few simple steps you can take to prevent your webcam from becoming a weapon against you.

- Cover your webcam! You can buy stickers that easily slide over when you need to show your face in a meeting
- Antivirus software automatically scans and detects unauthorized behavior and malware on your computer
- Don't click on links in any suspicious or unexpected messages
- Unplug externally connected webcams unless you're actively using them
- Password protect IoT devices connected to your local network
- Download software updates ASAP for both your computer and its programs
- Password protect IoT devices connected to your local network

For more information about email security, call us at 248-362-3800 or visit: https://bit.ly/3fF5ukw

Avoiding Business Identity Compromise

You may have heard about Business Email Compromise (BEC) scams before, which are a type of phishing threat meant to trick you into giving up private company information by posing as a professional associate. In other words, someone pretending to be your supervisor asks for an end-of-day report. These scams have long posed a risk to organizations of all sizes. Recently, though, the FBI released a warning that cybercriminals are engaging more and more often in what's known as **Business Identity Compromise**.

Business Identity Compromise, or BIC, is a cyber-scam that steals the identifying information of a company, usually a smaller business but not exclusively, to defraud the organization and the people inside it.

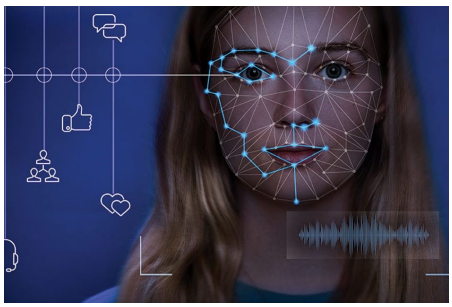
Types of BIC

Over the past several years, and especially after the onset of the pandemic, these BIC scams have reached record highs according to the National Cybersecurity Society. More people working remote at least some of the time means more virtual meetings with your coworkers, which has added a new avenue for cyber-threats in many companies that weren't virtual at all before.

So you might be a target for hackers to break into the local network; that's been true for as long as WiFi has existed, and the reason to closely guard your work accounts. However, employees can also be affected in data breaches of the company as surely as its shareholders. Not only does your employer have private data on you, like your Social Security number and bank information, but they have also assigned you an employment identification number (EIN) which can be stolen too. That would equal a lot of one-on-one time with the IRS to try and sort out your stolen identity!

How BIC Scammers Trick You

The question thus becomes: *How* do cybercriminals launch BIC attacks, and what can we do to protect ourselves?
Within that recent warning about the rise in BIC attacks, the FBI also noted that **deep faking** is a common strategy for cybercriminals. This has been made possible by the advancements in AI created over the past decade, and as a result, they've made



social engineering attacks even more captivating and, hence, dangerous.

Do you remember how novel it was when Facebook started *suggesting* who to tag in your photos? Since then, technology has come a remarkably long way. Now, it can generate a person's face for pictures and even include a digital recreation of their voice, on video calls. AI can now learn enough about your voice and image to recreate it. This is called deep faking. How does this work in real life? Say someone had the means and motive to pretend they were your boss on a video call, or a potential investor at a virtual conference. You'd be much more likely to spill the company's, or your own, confidential information without even thinking about it.

Protecting Yourself from Deepfakes

Avoid becoming a victim of BIC scams with many of the same tactics that you use to stave off any other social engineering attack. Deepfakes can sometimes be identified by blurry or pixelated edges around the person onscreen, as well as unusual requests or if they seem to be fishing (pun intended) for information that seems out of their security clearance.

Conclusion

Cybercriminals are constantly adapting their devious ways to trick us into handing over our credentials and private information. Don't put your company's or your own data at risk! Learn how to recognize deepfakes to help protect your systems from Business Identity Compromise, and any other threat that might approach.

Digital criminals don't take a break, and your security awareness shouldn't either!

Security Tips For Online Holiday Shopping

The holiday shopping season is taking off. This means that scammers have also revved up their engines. They're primed and ready to take advantage of all those online transactions.

Here are some of the most critical safety tips to improve your online holiday shopping.
• Check for Device Updates Before You Shop
• Don't Go to Websites from Email Links
• Use a Wallet App If Possible
• Remove Any Saved Payment Methods/Cards

After Checking Out
• Make Sure the Site Uses HTTPS (Emphasis on "S")
• Double Check the Site URL
• Never Shop Online When on Public Wi-Fi
• Be On High Alert for Brand Impersonation Emails & Texts
• Enable Banking Alerts & Check Your Account

Checklist For Offboarding Employees

When an employee leaves a company, there is a process that needs to happen.

This process of "decoupling" the employee from the company's technology assets is vital to cybersecurity and should include:
• Knowledge Transfer
• Address Social Media Connections to the Company
• Identify All Apps & Logins the Person Has Been Using for Work
• Change Email Password
• Change Employee Passwords for Cloud Business Apps
• Recover Any Company Provided Devices
• Recover Data on Employee Personal Devices
• Transfer Data Ownership & Close Employee Accounts
• Revoke Access to Your Apps & Network
• Change Any Building Digital Passcodes

"Next time you get a strange email with a paperclip, don't click on it!"

CartoonStock.com

What Are The Most Helpful VOIP Features For Small Businesses?

During the pandemic, VoIP and video conferencing have skyrocketed by over 210% due to the move to remote work and hybrid offices. Sixty-seven percent of surveyed companies say switching to VoIP helps improves call handling.

The technology is much cheaper to use than a traditional landline based system. Calling plans are also often less expensive, and a company can add new numbers for very little cost.

VoIP has several helpful features for small businesses, but *what are the best features to drive efficiency, productivity, and positive caller experience?*

1. Voicemail Transcription to Email
2. Local Support
3. Ring Groups
4. Find Me/Follow Me
5. Hold Music
6. Automated Attendant
6. Call Reporting