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

## May 2025

**Kim Nielsen, CISSP, CCSA**
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!”

## Your Smartphone Could Compromise Your Work Network

Over 7B smartphones are in use today. Over half of the workforce have company programs on their phone, whether it’s for team communication or on-the-go access to the business.

So whether you’re using it to boost productivity (or slack off, although we hope not!) then you need to know: If you connect your smartphone to the company WiFi, then you’re putting your workplace’s network and ALL of its data at risk.

What makes your smartphone such a huge risk to your job’s cybersecurity? How can you keep your personal and company data safe, especially if you need the phone for work?

**Behind Attacks on Your Mobile Device**

Compared to your work computer, your cell phone has a much less complex internal security structure.

It’s true that every OS update and new version of your phone comes with an upgraded cybersecurity structure. New software patches often contain much-needed bug fixes to solve a once-vulnerable part of the network. Nevertheless, your work computer has been personalized with vetted security programs and company-specific firewalls. Meanwhile your phone may not have up-to-date operating software, and you could have downloaded unauthorized and

*Continued on pg.2*

*Continued from pg.1*

insecure applications. A shady program, or one bought from an unofficial app store, could infect your phone with malware or ransomware.

Without proper cyber-defenses to block access to your work data, as soon as you connect to your company's WiFi, that breach could spread to the entire connected network. Likewise, a breach on your work network could compromise your stored personal data!

**Protect Your Work Data and Your Smartphone, Too**

It's not realistic to expect to keep smartphones out of the workplace. People have their phones on them at all times, for work purposes and personal emergencies. In fact, around 80% of companies have some kind of "Bring Your Own Device" policy, which necessitates use of your personal phone, laptop, and other smart devices.

What can we do when our workplace policies allow, or even encourage us to use our phones for job-related tasks?

- Lock your phone with a strong password, PIN or biometric authentication.
- Only install apps from trusted sources and be mindful of the permissions they request.
- Adhere to your company's specific guidelines for using personal devices for work. This is probably outlined in the Acceptable Use Policy.
- Turn on auto-updates for your apps and OS, to stay protected against known cyber-threats.
- Most modern smartphones have built-in encryption features that you can use for your protection. You should also use a company VPN for work.
- Create separate user profiles or workspaces for personal and professional projects. Segmentation supports security!

**Conclusion**

It's impossible to leave your phone at home all day. Most organizations expect you to use personal devices, whether it's to connect with the team, post to the company social media, or for use with multi-factor authentication.

The key to safe smartphone use in the workplace is segmentation and balance. Be careful when you log into your work network from a personal device, but remember that you have proactive defenses in place to protect your data. After all, the best prevention is education and knowledge.

## Free Executive Guide Download: The Business Owner's Guide To IT Support Services And Fees

IT BUYERS GUIDE

What Every Business Owner MUST Know About IT Support Services And Fees

What You Should Expect To Pay For IT Support For Your Business And How To Get Exactly What You Need

You'll learn:

- The three most common ways IT companies charge for their services and the pros and cons of each approach.
- A common billing model that puts ALL THE RISK on you, the customer, when buying IT services; you'll learn what it is and why you need to avoid agreeing to it.
- Exclusions, hidden fees and other "gotcha" clauses IT companies put in their contracts that you DON'T want to agree to.
- How to make sure you know exactly what you're getting to avoid disappointment, frustration and added costs later on that you didn't anticipate.

**Claim your FREE copy today at**
**https://www.cti-mi.com/itbuyersguide-525**

## Security Corner

### How AI Empowers Spear-Phishing

Phishing scams are the most common origin of data breaches. Threat actors convince their victims to send money or private information, usually spurred by false promises, threats, and forming a more personal relationship.

A major targeted and dangerous version of phishing is spear-phishing. Unlike generic phishing, which casts a wide net, spear-phishing targets specific individuals by using personal details to make scam messages more believable. With the advent of AI, these attacks have become even more efficient and dangerous.

Protecting Yourself from Spear-Phishing

1. Be skeptical of unsolicited emails. Always verify the sender's email address and be cautious of unexpected requests for sensitive information.
2. Enable Multi-Factor Authentication (MFA) for an extra layer of security that requires multiple forms of verification before granting access to your accounts.
3. Limit personal information online. Be mindful of the information you share on social media and other public platforms, as this can be used against you in spear-phishing attacks.

By staying vigilant and taking proactive measures, you can significantly reduce the risk of falling victim to spear-phishing attacks.

For more information about spear fishing, call us at 248-362-3800 or visit: https://tinyurl.com/7zyjanpf

## New Gmail Threats Targeting Users In 2025 (And How To Stay Safe)

Cybercriminals target Gmail a lot because it's very popular. It also integrates with many other Google services. As AI-powered hacking attacks become more common, it gets harder for people to distinguish between real and fake emails.

### What Are the New Threats to Gmail in 2025?

Cyber threats are constantly evolving, and some of the most sophisticated attempts have been aimed at Gmail. One major concern is that Artificial Intelligence (AI) is being used to create scam emails that appear very real. The purpose of these emails is to mimic real ones, making them difficult to spot. AI is also being used to create deepfakes and viruses, which complicates security even further.

Gmail is deeply connected to other Google services. This means if someone gains access to a user's Gmail account, they might be able to access all of their digital assets. These include Google Drive, Google Pay, and saved passwords, making it even more critical for people to secure their Gmail accounts.

When hackers use AI in phishing attacks, they can analyze how people communicate. This helps them write emails that look almost exactly like real ones. This level of sophistication has made phishing efforts much more likely to succeed. Now, almost half of all phishing attempts use AI technology.

Gmail continually updates its security, so users need to be adaptable in order to stay safe. Cyber threats are always changing, and Gmail users must stay vigilant to protect themselves.

### What Are Some Other Dangers That Gmail Users Should Know About?

AI-powered hacking isn't the only new threat that Gmail users should be aware of. More zeroday exploits are being used to attack users. They exploit previously unknown security vulnerabilities in Gmail. This allows them to bypass traditional security measures. Attackers can access accounts without permission before Google can address the issue.

Quantum computing is also a huge threat to current encryption methods. As quantum computing advances, it may become possible to break complex passwords and encryption keys. This could make it easier for hackers to access Gmail accounts. Users can implement strong passwords, enable two-factor authentication, and regularly check for suspicious activity.

### Keep Your Gmail Account Safe

Users can protect themselves by staying informed, regularly updating their knowledge, and implementing robust security measures.

Staying up-to-date on the latest security practices and best practices is important to keep your Gmail account safe. In today's cyber world, it's crucial for both individuals and businesses to protect their digital assets. Don't hesitate to reach out if you're concerned about keeping your Gmail account safe or need more help avoiding these threats. You can count on our team to help you stay safe online as the world of hacking

## 10 Tips To Get The Most Out Of Your Microsoft 365 Apps

With its powerful features and cloud-based services, Microsoft 365 gives businesses a way to organize their operations and boost communication:

- Microsoft Teams for communication
- OneDrive for cloud storage
- Power Apps for custom applications.

You can optimize your M365 experience by:

- Embracing collaboration tools like Teams
- Customizing your environment with SharePoint
- Leveraging automation with Power Platform
- Staying up-to-date with training
- Partnering with experts for guidance
- Managing email and time effectively
- Utilizing M365 across devices

## 5 New And Tricky Types Of Malware To Watch Out For

Malware is a huge threat in the digital world. It can cause a lot of damage and cost people a lot of money. As technology advances, so do the tactics used by cybercriminals. Malware keeps getting more complex and harder to detect.

Here are five new and tricky types that you should know about:

- **Polymorphic malware** changes its code.
- **Fileless malware** works in memory without files.
- **Advanced ransomware** targets networks and steals data.
- **Social engineering malware** tricks people.
- **Rootkit malware** hides itself deep in systems.

## 8 Awesome Ways To Customize Your Desktop Layout

Customizing your desktop can make a big difference in how it looks and works, which can help you get more done and make your computer feel more like your own.

Here are 8 easy ways to customize your desktop:

- Change your desktop background.
- Use custom themes to match your desktop to your personal style or work environment.
- Organize icons and folders to reduce stress and improve productivity.
- Add widgets and gadgets.
- Create custom icons to make your desktop more cohesive and visually appealing.
- Set up multiple desktops to help you stay organized and avoid distractions.
- Use keyboard shortcuts to help reduce the need to navigate menus or click through multiple windows.
- Automate tasks to reduce the time spent on routine tasks.

"Where are the neck pillows?"