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

October 2024

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!"

Artificial Intelligence 101

Introduction
Do you use AI? Do you understand what it is…or how it works…or *anything* about it beyond the buzz?

Even if you don't seek out artificial intelligence engines, there are more than 4.2B WiFi-connected devices that use AI for their "virtual assistants."

Our society is embracing artificial intelligence in more and more aspects of daily life! It automates menial tasks, answers our toughest questions right on the spot, and even keeps us safer online. Read on to dive into your crash course in everything AI.

What Is AI?
Artificial intelligence (AI) is a field of computer science focused on creating machines that can think and act like humans. This involves things like AI algorithms analyzing massive amounts of information and identifying patterns in it. Think of it like studying for a test, but on a much bigger scale. Then, based on what they've learned, AI systems can make predictions, solve problems, and even take actions. As AI encounters new data or situations, it constantly refines its skills and gets better at what it does. Imagine constantly practicing and perfecting a skill through experience…except unlike the skills we have to internalize, all of *this* is done without having any human input!

Automation like this can be incredibly helpful. Think of the AI engines that can create recipes, write songs, and make art. This can simplify tasks like driving,

Continued from pg.1

translating languages, or providing customer service, therefore freeing up people for more creative and strategic work that requires a human touch. It can also make difficult tasks easier for us, such as analyzing complex data to extract insights that would take us a lot more time and effort to digest. This can help lead to advancements in healthcare, finance, and even scientific research. Sounds great, doesn't it?

The Downsides of Artificial Intelligence

As AI automates more tasks, some jobs may disappear, requiring society to adapt and create new opportunities. This can be frustrating, especially for people who work in very specialized industries or who have particular skillsets that they have fostered throughout their professional career, now rendered obsolete.

Then there is bias to consider. Many people consider machines to be impartial, and therefore free of the unconscious opinions that influence humankind. Unfortunately, that is not strictly true for AI; because these machines learn by studying aggregated data, the data itself was created by people with their own unconscious (or intentional!) biases. Thus, AI may unwittingly reflect the opinions of its source material, and produce offensive, insensitive, or incorrect content.

As AI becomes more sophisticated, questions arise about who's responsible for its decisions and how to ensure it doesn't harm humans. We must consider the integrity of the data being fed to the AI so as to create more impartial technology moving forward.

Conclusion

Artificial intelligence can be used for good or bad, depending on how we develop and implement it. By being aware of both its benefits and dangers, we can ensure that AI benefits all of humanity while minimizing the risks therein.

One thing is for sure: AI isn't going anywhere soon! If we can learn to recognize and avoid its dangers, we can make use of all the good it can do—without risking our digital security.

"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 …

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 e-mail 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/1024-signup/

Security Corner

Real Site or Typosquat? Here's How to Tell

Introduction
What if you click on the link by mistake, or simply because you don't stop to more carefully examine the email? Then, we run into another problem: Typosquatting.

This happens when scammers create lookalike websites so you believe that you are on the legitimate landing page of whatever organization the hacker is trying to emulate.

How It Mimics a URL
The best way to avoid typosquats is to catch the mistake in the URL before you ever follow it to the false website. Hackers will create extremely similar domains to the real address like misspelling *Apple* as *Appie* or *Yahoo* with an extra *O*.

Signs of a Typosquat
Sometimes the scammer successfully pressures or entices you into clicking on their link without careful enough inspection. Since they have already fooled you with the URL in this scenario, it's now time to look at the page where you've been redirected.

- **Evaluate visual design:** Compare the website's design with the legitimate site.
- **Examine content quality:** Typosquatting sites often have poor grammar, spelling errors, or generic content inconsistent with a real company's branding.

Remember, it is ALWAYS best to go through verified websites and portals when you are unsure about a message or request. If you suspect a website is a typosquat, avoid entering any personal information and close the browser window immediately.

For more information about typosquatting, call us at 248-362-3800 or visit: https://tinyurl.com/4ewfvtxf

Why Securing Your Software Supply Chain Is Critical

In today's world, everything's connected. That includes the software your business relies on, whether you've installed that software locally or use it in the cloud.

Protecting the entire process that creates and delivers your software is very important. From the tools developers use to the way updates reach your computer, every step matters. A breach or vulnerability in any part of this chain can have severe consequences.

A recent example is the global IT outage that happened last July. This outage brought down airlines, banks, and many other businesses. The culprit for the outage was an update gone wrong. This update came from a software supplier called CrowdStrike. It turns out that the company was a link in a LOT of software supply chains.

What can you do to avoid a similar supply chain-related issue? Let's talk about why securing your software supply chain is absolutely essential.

Increasing Complexity and Interdependence

- **Many Components.** These include open-source libraries, third-party APIs, and cloud services. Each component introduces potential vulnerabilities.
- **Interconnected Systems.** A vulnerability in one part of the supply chain can affect many systems. The interdependence means that a single weak link can cause widespread issues.

Rise of Cyber Threats

- **Targeted Attacks.** Attackers infiltrate trusted software to gain access to wider networks.
- **Financial and Reputational Damage.** Companies may face regulatory fines, legal costs, and loss of customer trust. Recovering from a breach can be a lengthy and expensive process.

Regulatory Requirements

- **Compliance Standards.** These include regulations like GDPR, HIPAA, and the Cybersecurity Maturity Model Certification (CMMC).
- **Vendor Risk Management.** Companies must ensure that their suppliers adhere to security best practices. A secure supply chain involves verifying that all partners meet compliance standards.
- **Data Protection.** Securing the supply chain helps protect sensitive data from unauthorized access. This is especially important for industries like finance and healthcare.

Ensuring Business Continuity

- **Preventing Disruptions.** A secure supply chain helps prevent disruptions in business operations as cyber-attacks can lead to downtime.
- **Maintaining Trust.** By securing the supply chain, companies can maintain the trust of their stakeholders.

Steps to Secure Your Software Supply Chain

- **Strong Authentication.** Use strong authentication methods for all components of the supply chain. Ensure that only authorized personnel can access critical systems and data.
- **Phased Update Rollouts.** Keep all software components up to date, but don't do all systems at once. If those systems aren't negatively affected, then roll out the update more widely.
- **Security Audits.** Assess the security measures of all vendors and partners. Identify and address any weaknesses or gaps in security practices.
- **Threat Monitoring.** Use tools like intrusion detection systems (IDS) as well as security information and event management (SIEM) systems.
- **Education.** Awareness and training help ensure that everyone understands their role in maintaining security.

A breach or outage can have severe consequences. Securing your software supply chain is no longer optional; investing in this is crucial for the resilience of any business.

7 Strategies For Tackling "Technical Debt" At Your Company

Think of technical debt as the interest you pay on a loan you never intended to take. As your system grows, those hasty decisions can cost you in the long run. Here's how to address it:

1. **Identify and Prioritize.** Focus on the most critical issues that will drive the most value first.
2. **Integrate Debt Management into Your Workflow.** Maintain a balance between new development and debt reduction.
3. **Educate and Train Your Team.** Foster a culture of quality thinking.
4. **Improve Documentation.** It provides a reference for team members.
5. **Regularly Update and Refactor Systems.** This involves making small, manageable changes for quality.
6. **Optimize Security Practices.** Helps maintain system reliability and performance.
7. **Foster a Culture of Continuous Improvement.** Encourage learning, celebrating successes, and regular reflection to drive ongoing enhancement.

4 Tips To Troubleshoot Common Business Network Issues

Get started on keeping your network up and running smoothly:

1. **Inspect Physical Connections.** Quickly rule out or identify simple problems.
2. **Test Network Connectivity.** Simple testing can provide valuable insights.
3. **Monitor Network Performance.** This helps identify ongoing issues and potential bottlenecks.
4. **Ensure Security and Updates.** Regular updates and checks can prevent many common issues.

"It's one of those new Instant Cauldrons. You put a kid in here with some eye of newt and an hour later it's the best thing you've ever eaten."

Common Mobile Malware Traps

Mobile malware is often overlooked. People focus on securing their laptops or desktops without paying close attention to smartphone and tablet security. Mobile malware can arrive in various forms, from sneaky apps to deceptive links. Ignorance is not bliss here. Understanding the common traps is your first line of defense.

- Phishing Attacks. Clicking links or downloading attachments can lead to malware infection.
- Malicious Apps. Always research apps before downloading.
- SMS Scams. Be wary of unexpected messages, especially those asking for sensitive info.
- Public Wi-Fi networks. Avoid accessing sensitive information on public Wi-Fi.
- Fake Apps. Always verify app authenticity