TECHMinutes
July 2026
Your Technology Information Source!

This Issue:

Phishing is Getting Sophisticated: The New Threats Businesses Face

Stop Managing Metal, Start Managing People: A Guide to Hybrid IT

Replacing Your Business Computers Actually Protects Your Bottom Line

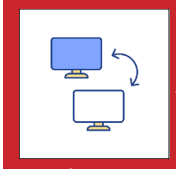
Is Your Business Ready for AI and Machine Learning?

Kill SMS MFA: Securing Your Business with Stronger Authentication

Free AI is Not Free: Why Public Tools Are a Security Risk

Visibility is Key to Success, So Show Yourself Off with a Newsletter

Replacing Your Business Computers Actually Protects Your Bottom Line



How frustrating is it when your computer just doesn't want to cooperate, whether it takes its sweet time starting up in the morning or decides to go on break in the middle of a meeting? How frustrating it is to see it happening to your team members, fully aware that they are feeling the same frustration you would? How much does it cost you, all events...

Read the Rest Online!
https://dti.io/replacetech

About Directive

We are a technology consulting firm specializing in technology implementation and management for businesses. We're known for providing big-business, Enterprise-Level IT services to small and medium-sized businesses.

Visit us **online** at:
newsletter.directive.com

Phishing is Getting Sophisticated: The New Threats Businesses Face

The bad guys have upgraded their toolkits. The days of spotted misspellings, broken English, and obviously fake logos are mostly gone. Phishing has evolved from a numbers game played by solo scammers into a multi-billion-dollar corporate enterprise. To protect a business, it is necessary to understand the specific tactics being used against teams right now.

The New Anatomy of a Phishing Attack

Most automated security advice will state generic information like checking the sender's email address. That is everyday information that anyone can parrot, and it does not help much on a busy Tuesday morning. Sophisticated cybercriminals now rely on targeted, technical strategies to bypass standard human awareness. That said, we still encourage you to follow these basic practices, as it never hurts to check for every sign of phishing.

Artificial Intelligence as a Copywriter

Scammers are using generative AI tools to draft emails, marketing copy, and reports.

(Continued on page 2)

Stop Managing Metal, Start Managing People: A Guide to Hybrid IT

Managing a mix of office servers and cloud services today means you have to stop thinking about the physical pieces of hardware and start thinking about your people. The goal is to get the most out of the technology you already paid for while making sure your team can work from anywhere. When you combine private servers with public cloud services, you are building a network that needs to feel easy for your employees to use while staying locked down tight against an ever-growing series of threats.

Core Management Strategies for Hybrid Environments

Managing a hybrid setup well comes down to three things: who is logging in, how you control the system, and where you put your files. Since your staff works from all over

(Continued on page 3)

Is Your Business Ready for AI and Machine Learning?

Artificial Intelligence and Machine Learning are no longer futuristic concepts reserved for technology giants with limitless budgets. For small and medium-sized businesses, these technologies have become essential tools for staying competitive, efficient, and secure.

However, adopting AI isn't as simple as flipping a switch or signing up for a new app. It requires a solid foundation and a strategic approach. Is your business truly ready to harness these tools, or are you at risk of falling behind?

What Do AI and Machine Learning Actually Mean for You?

At its core, Artificial Intelligence is the ability of a computer system to perform tasks that typically require human intelligence; such as recognizing patterns, making decisions, or understanding language. Machine Learning is a subset of AI where systems "learn" from data to improve their performance over time without...

Read the Rest Online!
https://dti.io/bizready4aiml

Kill SMS MFA: Securing Your Business with Stronger Authentication

Multi-factor authentication (MFA) is necessary for business security. However, relying on text messages to deliver verification codes creates a significant vulnerability that cybercriminals regularly exploit.

To secure business data, organizations must phase out SMS-based authentication and transition to more resilient verification methods.

The Vulnerability of SIM Swapping

Text message authentication codes do not travel through a secure, encrypted data pipeline. Instead, they rely on the cellular network. Cybercriminals exploit this infrastructure through a tactic called SIM swapping.

During a SIM swap attack, a malicious actor obtains personal identification details about a target from existing corporate data breaches. The attacker contacts the mobile carrier pretending to be the account owner, claims their device is lost or damaged, and convinces the customer service representative to route the phone number to a new SIM card.

Once the mobile number is reassigned to the attacker's device, the legitimate user loses cellular service. The attacker then requests password resets for targeted business or financial accounts and receives the SMS verification codes directly.

Secure Alternatives to Text Messages

Upgrading corporate authentication...

Read the Rest Online!
https://dti.io/strongmfa

Phishing is Getting Sophisticated: The New Threats Businesses Face

(Continued from page 1)

This means an attacker can instantly generate flawless, professional, and highly persuasive business prose. They can even feed public blog posts or corporate updates into an AI tool to perfectly mimic an internal tone and communication style. If a corporate culture is casual and uses specific industry shorthand, the phishing email will reflect that. The red flags people used to look for—like weird capitalization or awkward phrasing—have completely vanished.

Deep Context (Spear Phishing)

Bad actors do not just blast out a million identical emails anymore. Instead, they target specific individuals inside an organization, often the accounting department or executive assistants. They map out corporate hierarchies using public platforms like LinkedIn, find out who the vendors are, and intercept existing email threads.

It is alarming how much context attackers can gather just from a public footprint. When an email looks like a direct reply to an actual conversation about an invoice, defenses naturally drop. They might even reference the specific name of a project or a piece of software a team uses daily, making the message look entirely legitimate...

Read the Rest Online!
https://dti.io/smartphish

Stop Managing Metal, Start Managing People: A Guide to Hybrid IT

(Continued from page 1)

the place, your office walls are no longer your main defense. You have to move to a model where the user's login is your new front door. Every single app or database, whether it lives on a server in your closet or in the public cloud, needs to be connected to one main login system.

Do NOT let anyone touch your private business data without Multi-Factor Authentication (MFA). It is also vital to set up common-sense rules for logging in. The system should look at things like where the person is, what computer they are using, and the time of day before letting them in. If someone tries to log in from a weird location or a new device, the system should automatically stop them or ask for extra proof that they are who they say they are.

Trying to manage two different systems often leads to things being missed and higher costs. Using a single management tool allows your...

Read the Rest Online!
https://dti.io/hybridguide

Free AI is Not Free: Why Public Tools Are a Security Risk

During a recent quarterly IT strategy review, a client expressed total confidence that his staff was not utilizing artificial intelligence. However, a review of the company network traffic logs told a different story.

Within minutes, we identified several instances of unauthorized AI use:

- A marketing coordinator used a web-based AI writer for email newsletters.
- An HR manager uploaded confidential resumes to a public PDF summarizer.
- A sales representative used an AI transcription tool to record client calls.

Your high-performing employees are likely already using these tools. Their goal is not to compromise security but to increase their professional efficiency. While their intent is productivity, using unmanaged tools creates a significant data liability for your organization.

Data Security Risks of Public AI

There is a fundamental technical difference between secure enterprise AI and public consumer tools; or, even free open-sourced AI platforms.

Secure Enterprise AI

Business-grade versions of Microsoft Copilot or Google Gemini operate within a closed environment. These systems process your data to provide summaries and insights, but they do not use your inputs to train their global models. Your data remains private and is not shared externally.

Public and Open Source AI

Free versions of AI tools typically require your data as a form of payment. When an employee inputs a vendor contract or proprietary strategy into a public tool, that data is ingested...

Read the Rest Online!
https://dti.io/publicairisks

CYBERSECURITY TIPS

Cryptojacking Prevention

You don't need to be an expert to stop cryptojacking—just a few smart habits and tools can do the trick.

In this Micro Training, learn practical steps to block cryptojacking attempts and what your IT provider can do to help keep your system clean and efficient.

View this tip and others at:
https://dti.io/cryptojacking

Get our Cybersecurity Tips directly to your inbox!

Sign up to receive our **FREE** cybersecurity tips to help you to avoid a data breach or other compromise. These tips can be used to educate yourself and your employees on security best practices.

Sign up today!
https://dti.io/gettips

REVIEW US ON Google

We would ***love*** to hear your feedback, and would be incredibly grateful if you could take a couple of minutes to write a quick Google review for us. This will allow us to improve our service and let others recognize the value we provide.

Thanks in advance!

https://directive.com/review

Marketing Ideas & Tips for Your SMB

Visibility is Key to Success, So Show Yourself Off with a Newsletter

The risk that one of your clients is being actively pitched by a competitor right now is higher than you probably want to admit. Not because your service is lacking… because your competitors are making calls, sending emails, and showing up consistently, silence is an easy opening to walk through.

You don't lose clients to better service as often as you lose them to better presence.

A newsletter is one of the highest-return touchpoints available to a business, because the cost of sending one every month is nothing compared to the cost of losing a client you never saw leave.

Client relationships feel stickier than they are. You can do excellent work for years, deliver in every interaction, and still lose a client to a competitor who simply showed up more often.

Not with better service.

Not with a lower price.

Just more presence.

The Real Cost of Staying Quiet

A marketing touchpoint, in the simplest terms, is any regular, intentional contact...

Read the Rest Online!
https://dti.io/mktingnews

Spotlight: CDO Workforce

The Chenango-Delaware-Otsego Workforce Development Board, Inc., operating as CDO Workforce, connects local employers with qualified job seekers across the region. The organization coordinates employment, training, and education resources that support career growth and strengthen the local workforce.

CDO Workforce offers career counseling, resume support, and interview preparation for individuals at different stages of their job search. Its youth programs provide targeted assistance for job seekers under age twenty-five who are entering the workforce. Local businesses can also access recruitment support and on-the-job training incentives to help meet hiring needs.

Community members can learn more by visiting a regional career center or attending professional development workshops. Businesses can partner with CDO Workforce to find talent and support the local economy. More information is available at:
www.cdoworkforce.org

HAVING AN IT ISSUE?

EMAIL SUPPORT
support@directive.com

CHAT WITH US
chat.directive.com
607-433-2200.

TICKET PORTAL
support.directive.com

MANAGED RESOURCES
Use the icon in your desktop system tray for support options, quick links!

Charlotte & Chris Chase

Tech Trivia

Whatsapp has more than 3.3 billion monthly users.

Directive

330 Pony Farm Road
Suite #3
Oneonta, NY 13820
Toll-Free 888-546-4384
Voice: 607-433-2200

Visit us **online** at:
newsletter.directive.com

newsletter@directive.com
facebook.directive.com
linkedin.directive.com
x.directive.com
blog.directive.com
instagram.directive.com