InnoTek INSIDER

Your monthly newsletter, written for humans not geeks

Technology Update

COMING SOON TO MICROSOFT 365

Faster backup for Microsoft SharePoint, OneDrive and Exchange

Microsoft 365 Backup is said to be a powerful data recovery service, and it's coming soon. It's designed to speedily restore your OneDrive, SharePoint, and Exchange data if you've suffered a breach. It even allows you to restore data within set date ranges.

A public preview is expected later this year. If it gets a positive reaction, we'll be expecting a full rollout next year.

Custom Instructions Come to ChatGPT

OpenAI is rolling out a new feature called Custom Instructions, for ChatGPT Plus subscribers. Through two prompts, you can tell ChatGPT about your specific requirements and preferred response format. Whether you're marketing to prospects, or educating clients, this innovative feature caters to your unique needs.

DID YOU KNOW…

Chrome plans to highlight risky extensions

Google is planning to make extensions safer for everyone, by actively highlighting the ones that have been made unavailable in the Chrome Web Store.

There are three reasons an extension may disappear; the developer has removed it, it breaches Google Web Store policy, or it's malware. This new feature will leave you in no doubt about the potential risk of an extension that's suddenly vanished.

ITS NATIONAL CYBERSECURITY AWARENESS MONTH!

Is AI really for you, *or are you jumping on the bandwagon?*

Do you ever find yourself asking, "What is all this hype about AI?"

If so, you're not alone.

The buzz around artificial intelligence (AI) and its potential to revolutionize every aspect of our lives is inescapable. But how can you navigate through the noise and truly harness the power of AI to meet your business's big goals?

It's a question that keeps many business leaders awake at night.

Imagine being able to predict market trends before they happen, or to streamline your operations with almost exact precision. This isn't some far-off dream; it's the promise of generative AI.

But there's a lot of speculation around AI. Right now, it's uncertain, so... should you simply wait and see what happens?

Of course not!

In fact, now is exactly the time to start exploring generative AI. Sitting back isn't an option when your rivals could be leveraging this technology to gain a competitive edge. Yes, there's a lot to learn and understand, but isn't that part of the thrill of doing business in the 21st century?

But one thing to keep in mind amidst the excitement, is not to lose sight of your core aims, goals, and cultures.

What good is a new AI system if it doesn't align with the way your business behaves?

Whilst the world of AI may seem like uncharted territory, some classic rules still apply.

Although AI offers tremendous growth opportunities for businesses, it comes with its fair share of risks as well. Cybercriminals can manipulate AI to steal identities, spread false information using deep fakes or launch misinformation campaigns.

Boost your business success with AI, but keep yourself updated on everything it encompasses, including its risks. Implementing best practices, such as only using AI tools from trusted sources and reviewing privacy policies, can help you leverage AI's capabilities without compromising your safety.

Will you implement it? Will it generate revenue? Can it reduce your costs? Will it boost productivity? If not, perhaps it's not the right move for your business right now.

So, while the hype around AI is deafening, and the path ahead is not clear at all, the potential rewards are too great to ignore.

Did you catch September's Webinar?

InnoTek
computer consulting, inc.

READY FOR ANYTHING:
PREPARING FOR THE UNEXPECTED

TekCorner
September 2023

From spilled coffee on a laptop, to flooded offices, disasters come in all types and sizes. Make sure you're ready to respond to whatever comes your way by developing a comprehensive disaster preparedness strategy that reduces the likelihood and impact of disasters—both big and small—on your business.

In last month's webinar, we discussed

- Different types of disasters that affect businesses,
- The potential impacts these disasters can have on your business,
- The benefits of disaster preparedness in IT security,
- How you can develop a disaster preparedness plan,
- And finally, some best practices for effective IT disaster preparedness

Collaboration tools are GREAT.
But are they a security risk?

Who doesn't love the convenience of workplace collaboration tools and messaging apps like Slack, Teams, and Zoom?

We can chat with colleagues, share files, hold meetings, and even discuss sensitive topics without leaving our comfy home offices. It's all sunshine and rainbows… until cyber attackers decide to rain on your parade.

You see, whilst these platforms have become a blessing for productivity, they've also opened a Pandora's box of cyber security risks.

Did you know that Slack, despite using encryption, does not feature end-to-end encryption? It's believed this is so clients can maintain visibility into their company's communications.

Or if you use WhatsApp for your business, it has been exploited in a variety of social engineering attacks?

And let's not forget Telegram, which has become a prime target for cyber attackers.

This has given birth to a new attack category –

Business Communication Compromise (BCC), a sinister cousin of the more familiar Business Email Compromise (BEC).

82% of data breaches involve the human element, according to Verizon's 2022 Data Breach Investigation Report. An innocent click on a phishing email, and your communication platforms become a playground for cyber attackers.

Here's how you can stay safe.

- Enforce strict access controls, so only people who are supposed to get into your platform, can do so. Something simple like multi-factor authentication can be a powerful deterrent

- Implement data loss prevention measures. Use a system with encryption and make sure lost or stolen devices can be remotely wiped

- And train your team how to protect sensitive information

If we can help you stay better protected, get in touch.

TekFacts
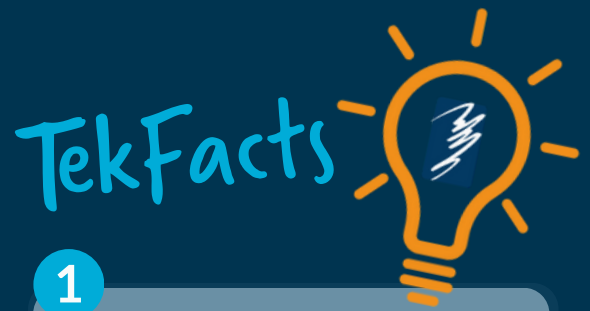
1

The first ever webcam was deployed at **Cambridge University, UK in 1991.** It was designed to monitor a coffee pot, after scientists were fed up finding it empty

2

The first computer to be marketed as a **laptop was the Gavilan SC in May 1983.** It was priced at $4,000, weighed 9 pounds, and was powered by a 5 MHz Intel 8088 chip. Oh, it also ran MS-DOS. Things weren't always better in the past

3

The biggest tech acquisition in history was not, as you might think, Elon Musk's multi-billion dollar takeover of Twitter (now called X) in **2022.** Actually, the record sits with Dell's 2015 acquisition of enterprise storage company EMC for $67 billion in cash and stock

Inspirational Quote of the Month

"There's no shortage of remarkable ideas, what's missing is the will to execute them."

**Seth Godin,
Writer and business genius**

TekQuiz Answers!

1) JumpMan. Nintendo's US office renamed him after their landlord
2) Yet Another Hierarchical Officious Oracle
3) Ctrl+Shift+Escape
4) It's the term used for a product that's been announced but never launched
5) 1,000,000 (but if you ask a developer rather than a hard drive manufacturer, they would say 1,048,576)

How many did you get right?

InnoTek
computer consulting, inc.

24 W Main St, Suite 2
Bloomsburg, PA 17815

101 W Broad St, Suite 405
Hazleton, PA 18201

570-316-0385

consultinnotek.com

Nothing scary in october's TekQuiz!

1. Before becoming widely recognized as the main character of Super Mario Bros, what was Mario called?
2. What does Yahoo stand for?
3. What is the keyboard shortcut to directly open the Windows Task Manager?
4. What does the term "Vaporware" mean?
5. 1024 Gigabytes is equal to 1 Terabyte; 1024 Terabytes is equal to 1 Petabyte. How many Gigabytes are in a Petabyte?

The answers are inside!

Q: How can I tell if my email has been hacked?

A: The most obvious sign is if you can't login. But it's not always that simple. If you suspect something's off, check your sent items and login activity for anything that wasn't you. We can help if you're worried.

Q: Should I allow BYOD (Bring Your Own Device) in my business?

A: If managed correctly, it can be an excellent option for some. However, it does pose a serious security risk if you don't regulate it correctly. Our advice? Seek expert help to get it set up.

Q: Does my business need cyber insurance?

A: If you store or send data, it's a good idea. Every business is vulnerable to an attack or an employee's error which puts you at financial risk, so insurance may remove some of the financial burden in such a situation.