

(970) 372-4940 | [TechFramework.com](https://www.TechFramework.com)

Artificial Intelligence IN BUSINESS

- The AI Revolution in Today's Job Market
- AI-Powered Security tools: SentinelOne
- Microsoft's New AI Assistant Can Go to Meetings for You
- Report Links ChatGPT to 1265% Rise in Phishing Emails

Artificial Intelligence AT HOME

- AI-Powered Solution Identifies Energy-Inefficient Homes
- Google Pixel's Face-Altering Photo Tool Sparks AI Manipulation Debate
- How to Use Google Bard to Find Your Stuff in Gmail and Docs

AI IN BUSINESS: The AI Revolution in Today's Job Market

The landscape of employment is transforming rapidly with the advent of artificial intelligence (AI), impacting jobs across various sectors. This change is not just about job displacement but also about the creation of new opportunities and roles.

AI, as a disruptive yet innovative force, is automating repetitive tasks, leading to concerns among workers in such roles. However, it also opens doors to new vocations, solving

However, jobs like teaching, law, management, HR, mental health care, surgery, and creative professions are less likely to be replaced due to their complex human interactions and decision-making requirements.

The key to thriving in this AI-driven era is adaptability, continuous learning, and skill development. Specializing in AI and related fields can offer a competitive edge.

complex problems, and making daily life more convenient.

A key insight from McKinsey Global Institute suggests that AI could contribute significantly to global GDP by 2030, primarily through labor automation and innovation in products and services. This economic growth points to a dual effect: while some jobs are automated, new ones emerge, leading to a dynamic job market.

The types of jobs most likely to be automated include customer service representatives, receptionists, accountants, salespeople, data analysts, warehouse workers, insurance underwriters, and retail staff.

Educational institutions like Nexford University are offering specialized programs in AI to prepare the workforce for this shift.

In conclusion, while AI presents challenges, it also offers immense potential for economic growth and new career paths. Embracing AI with the right skills and mindset can lead to a prosperous future in an evolving job market.

For a detailed analysis, read the full article on Nexford University's insights page below.

[More on this topic here...](#)



AI Tool of the Month: Murf

Discover Murf, your go-to AI Voice Generator. Murf converts text to speech and generates voices in up to 20 languages. It's designed for podcasters, video producers, and social media managers who need to quickly create high volumes of content.

Murf also offers transcription services and includes soundtracks and royalty-free music in its paid plans.

It's praised for enhancing results with quick edits, like voice modifications on pitch, style, speed, and emphasis.

[More about Murf and its capabilities](#)

AI AT HOME: AI-Powered Solution Identifies Energy-Inefficient Homes

Researchers at Cambridge University are making significant strides in promoting energy efficiency and reducing carbon emissions by developing an artificial intelligence (AI) model that can identify homes requiring the most attention for energy-efficient improvements.

This groundbreaking tool, trained on a comprehensive dataset of open-source data, including energy performance certificates, street view images, aerial views, and land-surface temperature measurements, can accurately pinpoint specific areas within buildings that contribute to heat loss. This capability enables targeted interventions and streamlines efforts to achieve a more sustainable future.

The AI model boasts an impressive 90% accuracy in classifying houses, allowing for the identification of approximately 700 "hard to decarbonize" houses in Cambridge alone.

This remarkable precision highlights the potential impact of this innovative approach.

By pinpointing specific areas of heat loss, such as doors and windows, and discerning between old and new properties, the model provides invaluable guidance for energy-efficiency efforts.

This detailed information empowers local authorities and other relevant bodies to prioritize interventions, ensuring that resources are directed towards the properties that will yield the greatest environmental benefits.

The significance of this AI-powered solution extends beyond its immediate impact on energy efficiency.

[More on this topic here...](#)

AI IN BUSINESS: AI-Powered Security tools: SentinelOne

SentinelOne is an AI-powered security platform that uses machine learning to protect endpoints from malware infections and other cyberattacks. SentinelOne's AI algorithms are trained on a massive dataset of malware samples, which allows it to identify new and emerging malware strains.

SentinelOne can prevent malware infections by detecting and blocking malicious behavior at the endpoint level. SentinelOne can also detect and remove malware infections that have already occurred. SentinelOne can also provide security teams with insights into malware infections, such as the source of the infection and the attacker's goals.

SentinelOne is used by a wide range of organizations, including Fortune 500 companies, government agencies, and healthcare organizations. SentinelOne has been credited with helping organizations to prevent and detect a number of high-profile cyberattacks.

AI-powered security tools are a valuable addition to any organization's security arsenal. As AI technology continues to advance, we can expect to see even more innovative and

AI-powered security tools offer a number of advantages over traditional security tools, including:

- **Real-time detection and response:** AI-powered security tools can detect and respond to cyberattacks in real time, which can help organizations to prevent attacks from causing damage.
- **Ability to detect new and emerging threats:** AI-powered security tools can detect new and emerging threats that are not easily detectable by traditional security tools.
- **Ability to provide insights into attacks:** AI-powered security tools can provide security teams with insights into

effective AI-powered security tools emerge in the years to come.

attacks, such as the attacker's identity and their goals.

AI AT HOME: Google Pixel's Face-Altering Photo Tool Sparks AI Manipulation Debate

Google's recent Pixel phone release features Best Take, an AI-based photo editing tool capable of altering facial expressions, such as turning frowns into smiles.

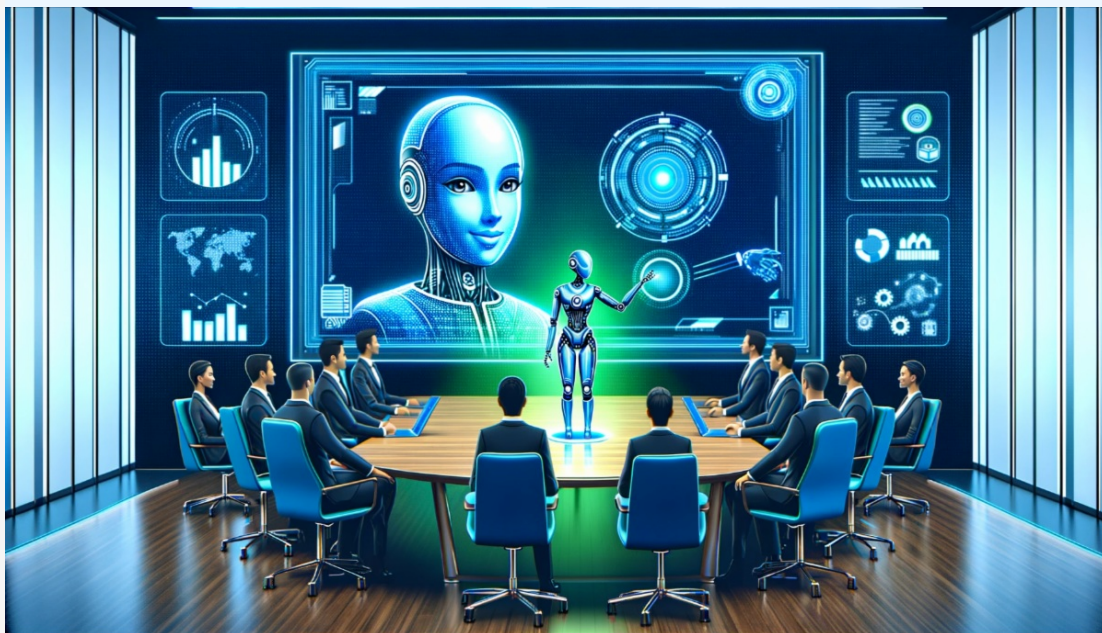
This tool has received mixed reviews, with some appreciating its utility for enhancing photos, while others are concerned about its potential misuse for creating deceptive images or harassment.

Google maintains that Best Take is meant for light-hearted purposes like

improving group photos and requires user consent for sharing edited images. However, the risk of abuse remains a concern. Andrew Pearsall, a professional photographer and university lecturer, cautions against the ethical implications of such manipulations.

The advancement of AI in photo editing not only brings new capabilities but also necessitates a serious conversation on its ethical usage and the need for protective measures against its detrimental use.

[More on this topic here...](#)



AI IN BUSINESS: Microsoft's New AI Assistant Can Go to Meetings for You

Microsoft is introducing a new AI assistant that can attend meetings for you and take notes. This virtual assistant uses voice recognition to listen in on meetings, capture the main discussion points, and save a summary for you. This could be a

Microsoft says that Copilot is designed to save people time and make them more productive. The company hopes that the AI assistant will help people to be more efficient and to get more done.

valuable tool for people who are often overbooked or who want to make sure they don't miss anything important.

The AI assistant is called Microsoft 365 Copilot. It is currently available in beta for Microsoft 365 subscribers. Copilot can be used to attend meetings on Microsoft Teams, the company's video conferencing platform. Once a meeting is over, Copilot will generate a transcript, summary, and notes. The notes can be exported to OneNote or saved as a PDF file.

In addition to attending meetings, Copilot can also be used to draft emails, create word documents, spreadsheet graphs, and PowerPoint presentations. The AI assistant can also be used to answer questions about your work. For example, if you are working on a presentation, you can ask Copilot to provide information on a particular topic.

Some people have expressed concerns about the potential for Copilot to replace workers. However, Microsoft says that the AI assistant is not intended to replace humans. Instead, Copilot is designed to augment human workers and to make them more effective.

Microsoft is also working on features that will make Copilot more transparent. For example, the company is working on a feature that will allow users to see when Copilot has generated content. This will help to ensure that people are aware that they are interacting with AI.

Overall, Microsoft's new AI assistant is a promising tool that could have a significant impact on the way we work. Copilot has the potential to save people time, make them more productive, and help them to get more done. However, it is important to be aware of the potential risks associated with using AI, such as the potential for job displacement.

AI AT HOME: How to Use Google Bard to Find Your Stuff in Gmail and Docs

Google recently updated its AI chatbot, Bard, with extensions that connect it to Gmail, Docs, and YouTube. While the extensions have some potential, they are still experimental and may not always be accurate.

Enabling the Extensions

To use the extensions, you'll need to create a Google account and visit the Bard website. Once you're logged in, you can enable the extensions you want to use, including the Workspace extension for Gmail, Docs, and Drive.

Using the Extensions

To use the extensions, you'll need to tag your prompts with the appropriate service, such as @gmail, @drive, or @docs. For example, to ask Bard to summarize unread emails from today, you would say "Please check my @gmail and summarize the unread emails from today."

Limitations of the Extensions

While the extensions can be helpful for finding specific emails or documents, they are not without limitations. For instance, Bard may prioritize recent emails over older ones, and it may not always accurately understand the context of information it pulls from your files.

Potential Uses for the Extensions

Despite their limitations, the Bard extensions can be useful in certain situations. For example, they can be helpful for finding emails or documents when you remember the topic but not the specifics.

Additionally, Bard can provide feedback on your writing, although it may not be as nuanced as a human editor.

AI IN BUSINESS: Report Links ChatGPT to 1265%

Rise in Phishing Emails

Phishing emails have surged by 1265% since Q4 2022, coinciding with the growing adoption of generative AI tools like ChatGPT. These tools are being exploited by threat actors to craft highly personalized and convincing phishing messages.

The SlashNext State of Phishing Report 2023 also highlights a 967% increase in credential phishing attacks. Patrick Harr, CEO of SlashNext, attributes this dramatic increase to the growing sophistication of AI-powered tools.

The report also reveals a concerning trend in mobile-based phishing attacks, with 39% classified as SMS phishing (Smishing).

The evolving threat landscape calls for a comprehensive approach to cybersecurity, including an increasing reliance on AI-driven solutions to counter AI-fueled cyber threats.

Despite the daunting challenges, there is hope. AI can also be used to defend against sophisticated attacks. Effective training can help protect against AI-generated threats.

The cybersecurity community must adapt to this rapidly evolving threat landscape. By embracing AI-driven solutions and implementing comprehensive protective measures, organizations can safeguard their data, systems, and reputation.