ISSUE 014
September 2024
Independence, Missouri

FCS TECH TALK

Your Trusted Technology Partner Since 1989

INSIDE THIS ISSUE:

WHAT IS AI AND HOW DOES IT FUNCTION?

AI (Artificial Intelligence) is one of the most transformative technologies of the 21st century, influencing industries ranging from healthcare and finance to transportation and entertainment. But what exactly is AI, and how does it work? Let's explore the core concepts behind AI and shed some light on how it functions in different applications.

What is AI (Artificial Intelligence)?
At its core, AI (Artificial Intelligence) refers to the ability of machines to mimic human intelligence. AI enables computers and systems to perform tasks that would normally require human intelligence, such as understanding language, recognizing patterns, solving problems, and making decisions.
There are different levels of AI, typically categorized as follows:

- Narrow AI (Weak AI): AI systems designed for a specific task, such as speech recognition, recommendation algorithms, or self-driving cars. These systems are highly specialized and cannot perform tasks outside of their designated functions.
- General AI (Strong AI): A theoretical concept of AI that can understand, learn, and perform any intellectual task that a human being can. General AI does not exist yet, but it is the ultimate goal for many researchers.
- Superintelligence: An advanced form of AI that surpasses human intelligence in all aspects, including creativity, decision-making, and problem-solving. This form of AI remains speculative at this stage.

How AI Functions: Key Components and Techniques
AI is built upon several key technologies and concepts, each contributing to the way it functions. Here's a breakdown of the main elements of AI and how they come together:

1. Machine Learning (ML)
Machine Learning (ML) is a subset of AI that allows systems to learn and improve from experience without being explicitly programmed. Instead of following predetermined rules, ML algorithms use large datasets to identify patterns and make predictions. Machine learning systems are trained on data, learn from it, and can then make decisions or predictions based on what they have learned.
How it works:

- Data is fed into a machine learning model.
- The model uses algorithms to analyze the data, identify patterns, and draw insights.
- Based on these patterns, the model makes predictions or decisions.
- As more data becomes available, the model continues to improve and refine its accuracy.

For example, in email spam filtering, a machine learning model is trained on a dataset of labeled emails (spam or not spam). Over time, it learns to detect patterns associated with spam and non-spam emails, improving its ability to sort incoming messages correctly.

2. Deep Learning
Deep Learning is a specialized branch of machine learning that uses neural networks, which are inspired by the structure of the human brain. Neural networks consist of layers of nodes (neurons) that process data and learn increasingly complex features at each layer. Deep learning has enabled breakthroughs in areas like image recognition, natural language processing, and voice assistants.

How it works:

- A deep learning model, known as a neural network, consists of multiple layers of neurons that process input data.
- Each neuron performs a mathematical calculation on the data it receives from the previous layer, passing its output to the next layer.
- The final layer makes predictions or classifications based on the processed data.

For instance, in facial recognition, a deep learning model is trained on a dataset of faces. The neural network gradually learns to recognize key facial features (like eyes, nose, and mouth), allowing it to identify individuals with high accuracy.

3. Natural Language Processing (NLP)
Natural Language Processing (NLP) is a branch of AI that focuses on enabling computers to understand, interpret, and generate human language. NLP is used in applications like chatbots, virtual assistants, and language translation services.
How it works:

- NLP systems analyze text or speech data using algorithms that break down sentences, detect grammar, and extract meaning.
- These systems can understand context, sentiment, and intent, enabling them to interact with humans in a natural way.

For example, when you use a virtual assistant like Siri or Google Assistant, NLP is at work. The system processes your voice commands, interprets the meaning, and provides a response or action based on your request.

4. Computer Vision
Computer Vision enables machines to interpret and understand visual information from the world, such as images or videos. By using algorithms to analyze pixels and detect patterns, AI systems can "see" and make decisions based on visual input. This technology is crucial for applications like self-driving cars, medical imaging, and security systems.
How it works:

- Computer vision systems analyze visual data (like images or video frames) by breaking it down into pixels.
- Using algorithms and machine learning models, the system detects patterns, objects, or features within the visual data.
- The system then makes decisions or classifications based on what it "sees." For instance, it can identify faces, recognize objects, or detect movement.

A self-driving car, for example, uses computer vision to interpret its surroundings. The AI processes video data from cameras and sensors to detect pedestrians, other vehicles, traffic signals, and road markings, allowing the car to navigate safely.

5. Reinforcement Learning
Reinforcement Learning is an area of AI where systems learn through trial and error. Instead of being provided with a dataset, reinforcement learning agents interact with an environment and learn by receiving rewards or penalties based on their actions. This approach is particularly useful in scenarios where a system must make a series of decisions, such as in robotics, gaming, or automated trading.
How it works:

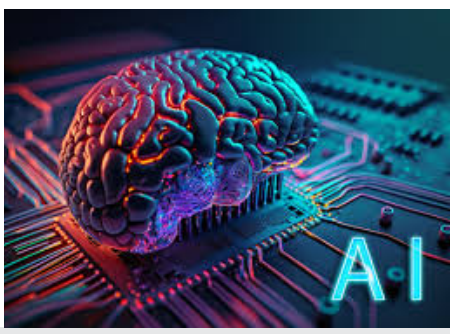
- The AI agent interacts with an environment and makes decisions (actions).
- Based on the outcomes of its actions, the agent receives positive or negative feedback (rewards or penalties).
- Over time, the agent learns to maximize rewards by choosing the best actions, refining its decision-making strategy.

For instance, AI has been used to train robots to navigate obstacle courses. The robot learns through reinforcement learning by trying different paths and learning from successes and failures to optimize its movements.

How AI is Applied in Real Life
AI is already embedded in many aspects of daily life and business, from small tasks to major innovations. Here are some examples:

- Healthcare: AI is used in diagnostic systems to analyze medical images, detect diseases early, and recommend treatment plans.
- Finance: AI algorithms are employed to detect fraudulent transactions, optimize investment portfolios, and predict stock market trends.
- Retail: AI-driven recommendation engines suggest products based on consumer behavior, personalizing shopping experiences.
- Transportation: Autonomous vehicles use AI to interpret surroundings, avoid obstacles, and navigate routes.
- Customer Service: AI chatbots and virtual assistants handle customer inquiries, manage bookings, and provide product support.

Understanding how AI works is crucial, not just for professionals in the tech industry but for anyone looking to stay informed about the future. As AI continues to evolve, it will undoubtedly shape the way we live, work, and interact with the world, making it essential for individuals and businesses to understand its capabilities and potential.



ISSUE 014
September 2024
Independence, Missouri

ESSENTIAL SETTINGS TO MAXIMIZE YOUR MICROSOFT 365 EXPERIENCE

Microsoft 365 is a powerful suite of tools. But to get the most out of it, it's important to optimize the settings. Otherwise, you may only be using a fraction of the power you have.

Here are some tips to get more from your M365 business subscription.

1.Optimize Email with Outlook Features

Set Up Focused Inbox:
This helps you manage your email more efficiently. It separates important emails from the rest.

Organize with Rules:
Create rules to move emails to specific folders or mark them as read to reduce clutter.

2.Enhance Collaboration with Teams

Set Up Channels:
Channels in Teams organize discussions by topic or project. Create channels for different teams or events.

Manage Notifications:
Notifications keep you informed but can be overwhelming. Customize them by going to Settings > Notifications.

Use Tabs for Quick Access:
Tabs in Teams give fast access to important files and apps. Add tabs for frequently used documents, websites, or apps.

3. Customize SharePoint

Organize with Document Libraries:
Document libraries in SharePoint help organize and manage files. Create libraries for different departments or projects.

Use Site Templates:
Use templates for common site types, like team sites or project sites.

4 . Maximize Productivity with OneDrive

Sync Files for Offline Access:
OneDrive allows you to sync files for offline access. This ensures you can access important files without needing an internet connection.

Use Version History:
Version history in One Drive allows you to restore previous versions of files. This is vital for business continuity and ransomware recovery.

5. Leverage Advanced Features

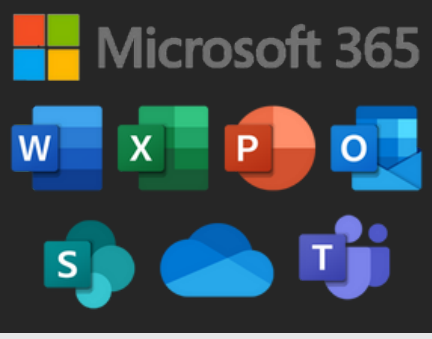
Use Power Automate for Workflow Automation:
Power Automate helps automate repetitive tasks. Go to the Power Automate website and create flows for common workflows.

Analyze Data with Power BI:
Connect Power BI to your Microsoft 365 data sources to create interactive reports and dashboards.

Add Copilot for Microsoft 365:
Copilot is Microsoft's generative AI engine. It can dramatically reduce the time it takes for all types of tasks.

Using these essential settings can maximize your Microsoft 365 experience. This can lead to improved security, efficiency, and collaboration.

If you or anyone at your office needs any help using these features just let us know, we will be happy to help!



HOW TO SPOT A PHISHING EMAIL: KEY WARNING SIGNS

Phishing emails are deceptive messages designed to trick you into revealing sensitive information such as passwords, credit card details, or personal data. Here are some key warning signs to help you identify a phishing email:

1. Generic Greetings

Phishing emails often start with generic greetings like "Dear Customer" or "Dear User" instead of using your actual name. Legitimate companies usually personalize their communications with specific details.

2. Urgent or Threatening Language

Phishers use scare tactics to prompt quick action, such as claims that your account will be suspended or a large payment is due. Be cautious of emails that create a sense of urgency or pressure you to act immediately.

3. Suspicious Sender Addresses

Phishing emails often come from mail addresses that look similar to official ones but contain slight misspellings or extra characters like "support@amaz0n.com" instead of "support@amazon.com". Always double-check the sender's email address.

4. Unexpected Attachments or Links

Phishing emails may include unsolicited attachments or links that lead to malicious websites. Hover over any links to check the URL before clicking. If the link looks suspicious or doesn't match the company's website, don't click it.

5. Requests for Sensitive Information

Legitimate companies will never ask for sensitive information like passwords, Social Security numbers, or credit card details via email. Be skeptical of any email that requests personal or financial information.

6. Poor Grammar and Spelling Errors

Phishing emails often contain spelling mistakes, grammatical errors, or awkward phrasing. Professional organizations typically have well-written communications, so any errors should raise red flags.

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. Closely monitoring links you are sent is crucial to staying secure.

• Malicious Apps
Always research apps before downloading. Don't ever download an app from an unverified site.

• SMS Scams
Be wary of unexpected messages, especially those asking for sensitive info. Any reputable company or site will never message you asking for your personal info without you requesting it beforehand.

• Public Wi-Fi networks
Avoid accessing sensitive information on public Wi-Fi and always make sure that the connection is safe before connecting.

• Fake Apps
Always verify app authenticity. Fake apps can contain malware and infect your phone once you download the app.

• Adware
Less harmful but can be annoying and can expose you to other threats. Some adware may expose your system to more serious malware by directing you to unsafe websites or installing additional unwanted software.

Knowing these common types of mobile malware can save you from falling victim in the future.

WHAT IS GRAYMAIL?

In today's digital age, email clutter is a common problem, with many inboxes flooded by an overwhelming mix of messages.

Among the emails that pile up are those known as graymail. These messages fall into a gray area between useful communication and outright spam.

But what exactly is graymail, and how can you take control of your inbox by managing it more effectively?

What is Graymail?

Graymail refers to emails that are legitimate but unwanted by the recipient. These are emails you subscribed to at some point, such as bulk newsletters, promotional offers, or notifications from businesses, but now no longer find useful.

Unlike spam, graymail isn't harmful or unsolicited; it's simply no longer a priority for the user to read or is not relevant to the user's interests anymore.

Common Types of Graymail:

Newsletters: You signed up for a brand's newsletter but stopped reading them. Now they constantly send you emails that you continue to scroll past every time you access your email.

Promotional Emails: Regular offers or deals from companies where you've previously made a purchase. These are typically emails you scroll past but everyone once in a while you might click on them causing you to feel torn between unsubscribing or continuing to receive emails that clog your inbox.

Notifications: Alerts from services you use, such as social media updates or purchase receipts. These can be useful but the majority of the time you simply scroll right past emails of this nature.

Graymail can clutter your inbox, causing important emails to get buried and making your inbox harder to manage.

This is where having a **Graymail Protection Filter** can vastly improve your experience when checking your inbox.

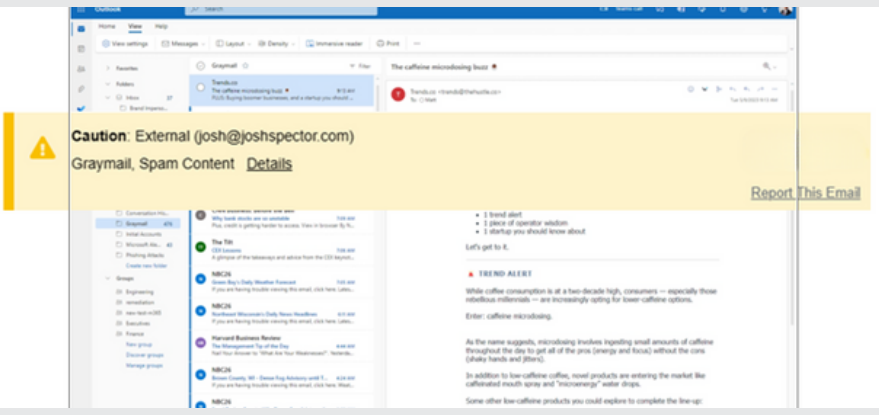
Our Graymail Protection Filter will collect data on all of the emails that your inbox receives and will automatically filter out all the emails that are graymail and drop them into a special graymail folder.

This clears your inbox of messages that simply take up important space in your inbox and potentially lead to missing an important email due to a clogged inbox.

Users who have Graymail Protection Filtering have reported improved productivity, less stress when going through their email inbox and a higher confidence that they will not miss an important email that accidently gets buried in emails we now know are considered graymail.

Clear inboxes can dramatically change the way that you work. Graymail Protection Filtering allows you to have an organized inbox with the ability to still read your graymail emails at your own leisure without the risk of clogging your inbox.

Ask us how to get Graymail Protection Filtering on your inbox today!



ISSUE 014
September 2024
Independence, Missouri

WE LOVE REFERRALS

The greatest gift anyone can give us is a referral to another business in need of IT services. Referrals help us keep costs down so we can pass the savings to our clients.

If your referral ends up becoming a client - we'll gift them their first month of service at no charge AND we'll gift you a $500 Amazon Gift Voucher.

Simply introduce me via email to stan@fcskc.com and I'll take it from there. I personally promise we'll look after your referral's business with a high level of care and attention (just like we do with all our clients).
-Stan

THIS MONTH'S PRODUCT SPOTLIGHT

CLICK HERE FOR MORE INFO!

MANAGED PHONE SERVICES

We Love Feedback

Here at Ferguson Computer Services, we value your feedback greatly. We would appreciate if you took time from your busy schedule to leave us a review. These reviews let us know what we are doing well and what we might be able to improve on in the future.

Leave a Google Review Leave a Facebook Review

TECHNOLOGY TRIVIA TIME

Technology Trivia Question of the Month! Send the correct answer to winner@fcskc.com to be entered to win a $50 gift card to Amazon.

Here is September's question of the month:

What is a key warning sign that an email might be a Phishing email?