VOLUME XV ISSUE 2
FEBRUARY 2024
OTTAWA ON

TECHLORE

"Insider Tips to Make Your Business Run Faster, Easier and More Profitable"

INSIDE THIS ISSUE:

"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!"
-Ruben Diaz
NeoLore Networks

The Alarming Rise of AI-powered Cybercrime

In the vast and somewhat unregulated realm of Open Source, Artificial Intelligence Large Language Models (LLM) like OpenAI's ChatGPT, cybercrime is on the rise. Hackers are becoming adept at crafting sophisticated phishing scams and cyber attacks that, with the help of AI, now resemble human behavior more closely than ever. This surge in AI-powered cyber sprees is reaching a scale that law enforcement has never encountered before.

Hackers Using AI to Deceive Victims

The recent surge in AI technology advancement over the past year has brought much excitement about the potential efficiency gains in various fields. Unfortunately, it's crucial to recognize that cybercriminals are leveraging AI to amplify their attacks and enhance their ability to evade detection.

With the accessibility of Open-Source AI, individuals can easily train Large Language Models (LLM) on their preferred data. This accessibility has led to a rise in malicious chatbots, designed with the explicit goal of assisting users in executing phishing attacks, coding malware, and creating misleading information to deceive unsuspecting victims.

Most Common AI-Powered Cyber Attacks on Businesses

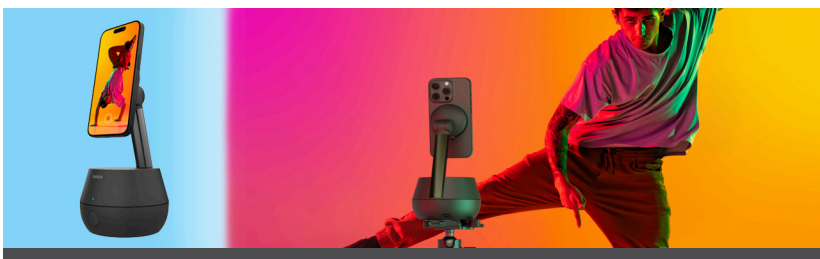
Business Email Compromise (BEC) is a sophisticated form of phishing attack meticulously designed to infiltrate organizations and pilfer critical information or funds. AI algorithms play a pivotal role in this threat, analyzing communication patterns to craft highly convincing phishing emails. These deceptive messages often impersonate high-ranking executives or trusted business partners, aiming to mislead employees into undertaking unauthorized actions such as initiating fraudulent transactions or disclosing sensitive information.

Advanced Persistent Threats (APTs) represent a formidable cybersecurity challenge characterized by their stealthy, prolonged nature. These attacks employ complex techniques to breach business networks, persist undetected, and stealthily extract sensitive information over an extended period. The integration of AI algorithms into APT strategies enhances the attackers' adaptability, enabling them to adjust tactics, bypass security measures, and exploit vulnerabilities within business systems.

Ransomware Attacks pose a significant threat to businesses, employing encryption to lock crucial data and demanding a ransom for decryption keys. AI algorithms are now instrumental in automating and optimizing the distribution of ransomware. Furthermore, these algorithms can selectively target high-value assets, thereby increasing the potential financial gain for cybercriminals orchestrating such attacks.

Fraudulent Transactions
Scammers employ advanced AI algorithms to automate fraudulent transactions, specifically targeting businesses. AI-driven fraud is particularly insidious as it can mimic authentic transaction patterns, thereby eluding traditional fraud detection systems. The use of AI enables cybercriminals to exploit vulnerabilities in payment processes, potentially resulting in financial losses and compromised business integrity.

Payment Gateway Fraud is increasingly being leveraged by cybercriminals to orchestrate complex schemes. This involves automating various aspects of the fraud, making it more intricate and challenging to detect. Fraudsters may use AI to generate realistic synthetic identities, analyze transaction patterns to evade detection systems, or even conduct targeted phishing attacks using AI-generated content.



Belkin Auto-Tracking Stand Pro

The easiest way to FaceTime, create action-packed videos, and go hands-free for livestreaming and video conferencing is here. Our Auto-Tracking Stand Pro follows your face and body movements with 360° rotation and 90° tilt with smooth, quiet motors. Grab and go — the internal battery offers 5 hours of operation on a full charge. Get yours at https://www.belkin.com/

VOLUME XV ISSUE 2
FEBRUARY 2024
OTTAWA ON

The Transformative Role of Generative AI in the Future

Gen AI has its roots in machine learning, dating back to the late 1950s. Early examples include the Markov Chain, a statistical model for generating new data based on input. However, the lack of computational power and data resources hindered its progress.

The real breakthrough happened in the 1990s and 2000s, with the rise of advanced hardware and digital data. Generative AI, as we know it today, took off with the introduction of neural networks—models inspired by the human brain. These networks, especially the Generative Adversarial Network (GAN) proposed in 2014, allow for creative data generation without explicit programming.

Other players like Variational Autoencoders (VAEs) and Recurrent Neural Networks (RNNs) joined the scene around the same time, showcasing the ability to produce novel content.

The Future of Generative AI: Is it Bright?

Recent advancements in technologies like ChatGPT and Stable Diffusion might seem sudden, but they've been years in the making. The potential of generative AI became evident in 2020, with the release of GPT-2 in 2019, showcasing the transformative power of generative language models.

Large Learning Models are Growing

Generative AI, particularly in the form of Large Language Models (LLMs), has been a focal point of technological advancement. Models like ChatGPT are just the beginning, with the next generation of LLMs already in development. Key areas of innovation include:

Self-improving Models: LLMs can generate their training data, continuously refining and improving themselves.

Fact-checking Models: Future LLMs will retrieve data from external sources to enhance accuracy and build trust.

Sparse Expert Models: A new approach, sparse expert models, offers computational efficiency, improved performance, and enhanced interpretability.

Making AI More User-Friendly

Direct Content Creation: Users will have more control over the content they produce, guiding AI to craft tailored results.

Better Visual Content Tools: Generative AI will improve visual content tools, making it easier for users to generate and tweak images.

Simpler User Experience: The goal is to simplify AI use for everyone, regardless of tech skills.

Bias and Ethics Focus: Future generative AI will offer better controls for bias and ethics, allowing users to align AI with their principles for more reliable and user-centric content creation.

The Impact of Artificial Intelligence on the Job Market

Artificial Intelligence (AI) is reshaping the job market, a reality underscored by the World Economic Forum's The Future of Jobs Report 2023. The report predicts that by 2025, AI is poised to replace 85 million jobs globally. However, it also brings a silver lining, foreseeing the creation of around 97 million new roles, resulting in a net positive impact on employment.

The catch, though, lies in the nature of these jobs. The ones AI creates will demand a different skill set compared to the ones it replaces. This creates a challenge for individuals whose current skills might become outdated. The solution? Embrace reskilling and upskilling initiatives to bridge the gap and smoothly transition into new roles.

Yet, amid the changes, it's crucial to recognize that AI isn't just a job taker; it's a job creator too. As AI handles repetitive tasks, it liberates human workers to focus on more strategic and creative endeavors. Jobs that rely on human qualities like creativity, emotional intelligence, and problem-solving are expected to be in high demand, underlining the evolving landscape where humans and machines collaborate to shape the future of work.

What Is The Metaverse (and Why Should You Care)?

The Metaverse is a digital space where you can experience a whole world online, replicating or offering alternatives to real-life activities. It covers everything from social interactions and currency to trade, economy, and property ownership. What makes it special is that it's built on the secure foundation of blockchain technology. In the Metaverse, you can do things that go beyond the limitations of regular online interactions. It's like a virtual realm where collaboration becomes incredibly versatile. Surgeons can work together, designers can sculpt car models in clay, and the potential is vast.

How to Make Your iPhone Battery Last Longer

To boost your iPhone battery life, try lowering the brightness—this simple adjustment can have a significant impact on power consumption.

Additionally, consider activating Low Power Mode for an extra battery-saving boost. Access it in Settings > Battery or add it to Control Center for quick toggling. Manage background app activities to minimize battery drain, as some apps continue running in the background unnecessarily.

Keep an eye on background wireless services like Wi-Fi, Bluetooth, and AirDrop; turning them off when not in use prevents slow battery depletion throughout the day. Implementing these tips can help your iPhone battery last longer and keep you powered up on the go.

DeepFakes: The Good, The Bad and the AI

The Good – Benefits of Deepfake Technology

Cost-Effective Video Campaigns: Deepfake technology has the potential to significantly lower the cost of creating engaging video campaigns, providing a more budget-friendly avenue for marketers.

Enhanced Omnichannel Campaigns: Marketers can leverage deepfake technology to create more impactful omnichannel campaigns, delivering a consistent and compelling message across various platforms.

The Bad – Threats Posed by Deepfakes

False Statements and Announcements: Deepfake manipulation can lead to the creation of videos featuring individuals making false statements or announcements.

Blackmail and Reputation Damage: Cyber attackers could use deepfakes to blackmail companies by threatening to release fabricated videos to the media or on social platforms. This has the potential to damage reputations and create chaos.

Take the NeoLore Cyber Security Survey

Has your company done a Cyber Security Maturity Assessment within the last year? Do you have an IT security policy in place? Do you know if you've been hacked or are leaking data?

If your answer was "no" or "I'm not sure" to any of those questions, your company may be at risk for a devastating cyberattack.

Get the NeoLore Networks Cyber Security eBook for Free!

It Features

- Information on the various threats to your business
- NIST Security Framework
- CIS Controls
- Basic Controls

And More!

https://neolore.com/cybersecurity