VOLUME XV ISSUE 3
MARCH 2024
OTTAWA ON

NEOLORE NETWORKS INC.

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

Deepfakes: Unnecessary Panic or Serious Cybersecurity Threat?

The world responded to Taylor Swift's call when her AI-generated explicit pictures began making the rounds on the internet. The need was felt for proper legislation against circulating such content. At last, people started to see that "deepfakes" aren't just an unnecessary panic; this technology has become a significant threat to our security.

In this article, we will discuss the cybersecurity ramifications of deepfakes and how to mitigate this risk in the face of advancements in AI.

The Dangers of Deepfakes

The statistics about deepfakes are nauseatingly reprehensible; they are doubling in number every six months as of November 2023. Five years ago, 96% of deepfakes circulating online were pornographic in nature. But today, deepfakes are used to commit financial fraud, spread political violence, create hoaxes, manipulate elections, and – brace for it – bypass biometric verification.

A hacker can recreate the voice of a CEO to gain access to their company's sensitive information, leading to significant data breaches. What's going to happen when you can't trust if the person speaking to you on the phone isn't just a scammer? Well, it will usher in an era of "truth decay," exemplified by these instances:

A UK energy firm's worker paid £200,000 to a scammer impersonating his boss.

A Chinese bank manager was fooled by AI voice cloning to part with $35 million.

An organization hired a fake employee who was pretending to be someone else to gain access to their data.

This AI-enabled "CEO fraud" should be treated as a cybersecurity nightmare. But here are some ways to thwart the dangers of deepfakes and restore faith in your online interactions.

Dealing with Deepfakes

Even though deepfakes have achieved a level of mimicry previously deemed impossible, there are some ways to tell if a video has been doctored. Online meetings and remote workers have become the "new normal," and sniffing out deepfakes is essential to keep your company's data security intact. Try these simple solutions to deal with deepfakes effectively:

Just as employees are taught not to click on random links, they should be taught to double-check everything and confirm they are talking to the right person.

As deepfakes today have become indistinguishable from genuine content for the naked eye, use deepfake detectors when doing a significant financial transaction.

Look for the telltale signs of a doctored audio or video; some of these audio signs include:

- Choppy sentences
- Awkward phrasing
- Tone inflection varies unnaturally
- Sounds in the background seem kind of suspicious

And some of the video signs include:

- Boxes appear around the speaker's eyes/mouth
- The face gets blurry when it's hidden by an object
- The skin tone changes near the corner of the face
- The speaker blinks bizarrely (or doesn't blink at all)

Hopefully, these recommendations will make deepfakes less of a cybersecurity threat in the future. Just remember that identity theft and false personation existed even before the era of the internet; they are not the products of a tech-dependant world. Deepfakes have become a significant headache for cybersecurity professionals in 2024. Criminals are using doctored content (images & videos) to defraud organizations, gain access to sensitive information, and spread misinformation. We need to go beyond biometrics to fight the onslaught of deepfakes.

Rabbit R1

Do you hate pulling out your phone every time you need to do some boring, mundane thing like DoorDash a hot dog or call an Uber? You might need (or just want) a Rabbit R1, an adorable, pocket-sized AI device. It's about the size of a stack of Post-its with a screen, button, touchscreen, and camera. When you need to run an errand, just push a button, give it a voice command, and send a rabbit to do all the boring stuff that takes up time in your life. Get yours at www.rabbit.tech

VOLUME XV ISSUE 3
MARCH 2024
OTTAWA ON

Demystifying Deep Learning, Reinforcement Learning, and Natural Language Processing in AI

Demystifying Deep Learning

We're living in a world of big data, where 2.5 quintillion bytes worth of information is created daily.

This data is responsible for deep learning, which is basically a neural network with multiple layers. A neural network is the closest we've come to imitating the human brain. Thanks to deep learning, we can teach a computer to think and learn like the human mind does.

Deep Learning also enables computers to recognize patterns, handle vast sets of data, and adapt to their environment. As a critical subset of machine learning, deep learning trains computers to learn by example. Whether you're using Siri, Cortana, or another virtual assistant, they're learning from the data you provide.

Demystifying Reinforcement Learning

The concept of reinforcement is pretty simple. Certain behaviors can be reinforced with trial-and-error mechanisms. For instance, Pavlov trained dogs to salivate upon hearing the ringing of a bell. Children do not pick up bad habits when they are reprimanded but learn to get good grades as they receive praise for this action.

We can train computers to do the same, i.e., maximize the positives and minimize the negatives. Trial and error is the name of the game, and it trains machines to achieve the best results possible.

Reinforcement learning teaches driverless cars to learn from their experiences and avoid repeating the same mistakes twice, making them safer for passengers and pedestrians. This technology has different applications, e.g., gaming, robotics, healthcare, and traffic control.

Demystifying Natural Language Processing

Did you think that ChatGPT was the first AI model you could talk to? You're wrong if you have assumed that; it's just one of the most remarkable examples of what NLP could accomplish if given free rein.

Based on deep learning and natural language processing (NLP), ChatGPT can understand text data and respond in the same manner. It's not easy to teach a computer how to comprehend human speech; there are 7,000+ languages in the world, and a word can have multiple meanings based on context.

Some famous examples of NLP in action include Google search results, email filters, and smart assistants like Siri.

These three disciplines have wide-ranging applications in the modern world. Autonomous vehicles, image processing, digital marketing, and many other fields are progressing far beyond our wildest imaginations.

Serverless Architecture could Reduce Vulnerabilities of Companies using Regular Servers

Cloud computing seems to dominate every industry it touches, and serverless architecture is just one of its many miracles. It's scalable, cost-effective, and offloads security management to cloud providers. So, even if serverless architecture isn't 100% hacker-proof, it still reduces the vulnerabilities rampant in our regular servers.

In 2022, *Orca Security* revealed that average VM and container images had at least 50 vulnerabilities; 78% of hackers exploit these very vulnerabilities to gain access to your system. Serverless architecture still has servers and OS, but cloud providers manage them for you. They deal with security patching and management, making sure your system doesn't have any exploitable vulnerabilities and making sure you have the latest software version installed in every workstation.

Therefore, delayed patching or security misconfiguration isn't a headache for companies using AWS or other cloud providers. Also, a Zero Trust Model goes one step beyond perimeter security and sets up more vigorous security checks to keep hackers at bay in a serverless framework.

Is it Possible to Mimic How the Human Mind Thinks?

The human brain is the most complicated computer known to us, and engineers are trying their hardest to replicate it. Computers can solve complex math problems instantly, but they have to do 10^18 operations every second to mimic the human mind fully. Neuromorphic computing is a much easier way to make tech smarter than man. These computers use artificial neurons and synapses to create a real-life mechanical version of the brain, such as DeepSouth, which will be launched in April this year. It can perform 228 trillion operations in a single second. Our brains are limited by biology, so it won't take neuromorphic engineers more than a few decades to mimic the human mind fully. These artificial brains may even replace our biological ones one day.

6 Things to Look for to Recognize a Phishing Scam

- A poorly-written email with noticeable spelling mistakes or grammatical errors.
- Scammers use link shorteners to disguise fake sites as legitimate ones.
- If an email offers you a too-good-to-be-true offer (consider the Nigerian prince fiasco), never trust it.
- Usually, a scammer's email address doesn't align with the contents of the email
- Something smells "phishy" if the email demands urgent action, such as "Click here immediately or your account will be deactivated."
- A lot of scammers use generic greetings, such as "dear user," "dear customer," or "dear valued member."

How Zero Trust Security Models Actually Work?

"Never trust, always verify" is the motto adopted by the Zero Trust Architecture, a security framework that has successfully curbed the onslaught of data breaches in the world. "Security without perimeters" would be a great way to describe ZTA, as it seeks to verify anyone and everyone trying to gain access to the network, whether from inside or outside.

It's not about mistrusting the employees. 80% of data breaches are caused by careless employees, after all, so ZTA seeks to assume that attackers are everywhere. A Zero Trust Security Model works by giving users the least-privileged access to the network, using 2FA to discourage impersonation, and breaking down security parameters into smaller sections for better risk management. By assuming that every endpoint and connection is hostile, ZTA has successfully brought down the cost of data breaches. Companies are no longer implementing the policy of trusting everyone in the system.

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