SystemsNet

THE GROWING ROLE OF AI IN SECURITY

THE GOOD, THE BAD AND THE UGLY

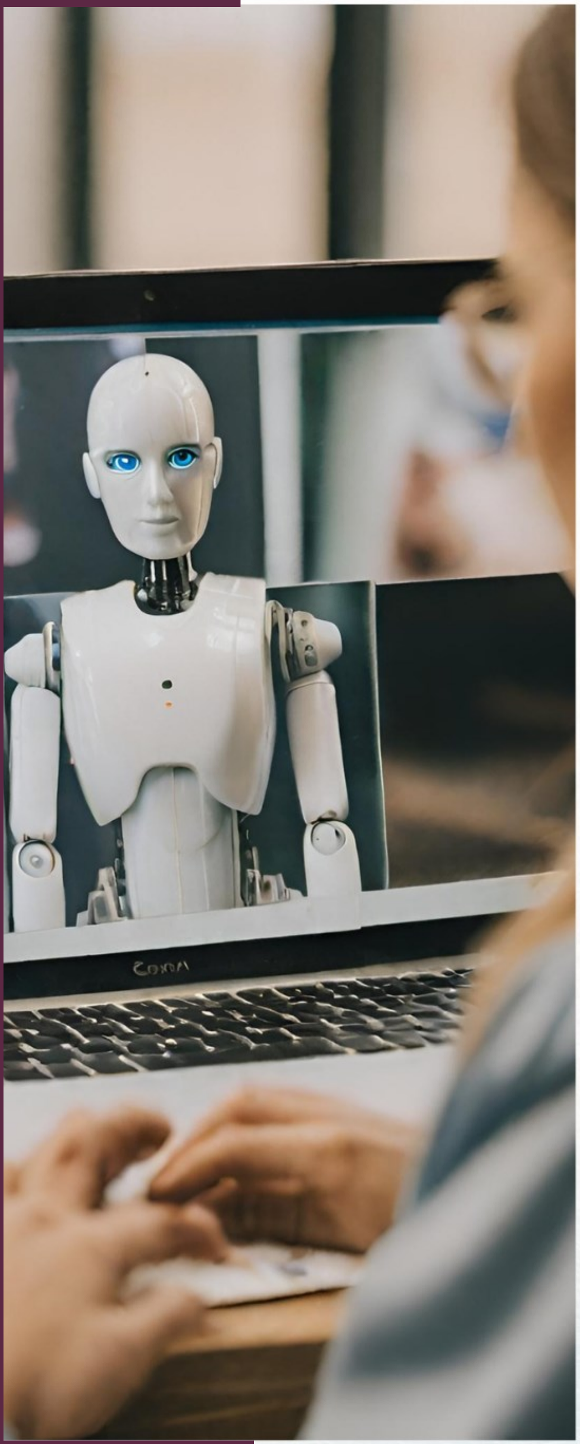
https://systnet.com/

(215) 340-1951

Since it entered mainstream use, AI has attracted opposing reactions, especially regarding its applications in security. On one side, supporters hoped it could provide some answers to all our security problems with its incredible machine learning capabilities. Others point out that AI has its own vulnerabilities, which could expose businesses to more risks.

Both reactions are correct, of course, because AI has a good side and a bad side. But thanks to security solutions experts, it's possible to work around the kinks and make AI really work for system security. The problem lies in how hackers are now leveraging AI to attack businesses with an intensity like never before. And that is the ugly side of AI that business owners must deal with.

It can be scary, but the point of this e-book is not to frighten you. The goal is to spread awareness about these AI-powered cyberattacks and equip businesses with the knowledge and tools to protect their data, which we hope to achieve within the following pages.



THE GOOD

HOW BUSINESSES CAN USE AI TO IMPROVE SECURITY

Protecting against cyberattacks has been one of the primary concerns of business owners for the last couple of years. Businesses have taken many measures to prevent and counter these attacks, from employee training to installing an iron-clad security solution. Still, hackers continue to find ways into our systems. With AI technology, security experts quickly saw a new hope. Here are some ways AI is utilized in business security solutions.

Faster and More Accurate Threat Detection

Identifying potential threats is one of the most crucial steps in ensuring business security. It is difficult with the constantly changing strategies employed by hackers. But with AI's ability to analyze massive amounts of data, your security system can stay on top of even the newest threats. It will detect red flags and unusual behavior, identify unknown threats, and mitigate security risks.

Efficient Incident Response

Much of the damage caused by cyberattacks is due to a delayed or inadequate response. AI allows you to automate several crucial processes in responding to a potential breach, such as temporarily shutting down a compromised network or notifying the IT team. Threats are contained and damage limited or stopped when automation is part of your cybersecurity.

More Secure Authentication

One of the most fundamental ways that AI strengthens your business security system is by adding extra layers of security and protection. In addition to the usual password system, AI now gives organizations more security through authentication tools like facial recognition, voice recognition, fingerprint scanning, and CAPTCHA. These additional layers greatly reduce the risk of fraudulent logins and unauthorized access.

Bot Blocking

Hackers will use bots to carry out their attacks on a large scale. But no matter how fast they move or how widespread their reach is, bots can't do much against an AI-guarded system that can easily block their attempts at creating a security breach.

THE BAD

SECURITY RISKS ASSOCIATED WITH THE USE OF AI SYSTEMS

There is no doubt that AI brings a mountain of benefits to businesses in general and to their security in particular. Its ability to rapidly and accurately analyze large amounts of data makes it a powerful tool for fighting cyberattacks of all kinds. However, highly advanced as it is, the development of AI algorithms is still in the early stages. As such, it still has quite a few vulnerabilities, which is why some businesses are hesitant to rely heavily on an AI system.

Data Poisoning and Adversarial Attacks

Training is a crucial part of the machine learning process, and massive amounts of data are required and for it to work. If this data gets even slightly compromised with false data, the results will be incorrect, leading to distorted AI behavior.

This is very similar to another common concern, which is model fragility. AI models are sensitive, so even tiny manipulations in the training data can produce grossly inaccurate outputs, which can be extremely dangerous in some applications.

Privacy Breaches

The success of most AI systems relies on the use of large amounts of sensitive information. In other words, the system collects and stores a variety of confidential data and personal details to work correctly. In the event of a hacking attack, all this information can be compromised, leading to a breach of privacy and confidentiality.

Lack of Explainability

AI algorithms can produce outputs or make decisions that do not always have a viable explanation. As a complex technology, it's difficult to understand how AI sometimes comes up with the outputs that it does. With this lack of explainability and transparency, businesses that rely on these systems might be inadvertently put at risk.

Transfer Learning Risks

AI models may be used repeatedly for different applications, and this is fundamentally not a problem. But when a model learns to do specific tasks one way, the flaws or biases in the original data might get passed on to the next model. This miscommunication could change how it acts and how well it does its job.

Supply Chain

An AI tool or system is not developed in complete isolation, which would be much easier to ensure the system's security. With many components that work together to build the system, several libraries and frameworks are involved to ensure the system functions properly. As you can imagine, each part of the process presents a set of new risks that can turn into attack entry points. As it goes down the supply chain, the security of an AI system would be very vulnerable.

Over-Reliance on AI

With the rapid growth and impressive features of AI technology, over-reliance on it is becoming a real problem. Businesses are becoming too confident in the power of AI, often forgetting that it is still not perfect and that there are instances where human input is still advisable.

THE UGLY

HOW HACKERS USE AI TO ATTACK BUSINESSES

Cybercriminals seem to find an illicit use for every good thing digital technology offers. Take generative AI, for instance. It is still new, but hackers have already figured out dozens of ways to use it for cyberattacks and are becoming faster, more efficient, and more destructive to businesses.

Launching More Efficient Phishing Campaigns

Phishing is not new, but hackers who use it are becoming more threatening thanks to AI. Just a few years ago, the hackers had people manually write phishing emails, many of which were full of grammatical and spelling errors. They even used generic messages for all potential victims.

With AI, cybercriminals have really stepped up their phishing game. Now, they use chatbots to create highly credible and perfectly written emails, which are more convincing and more likely to get a response. AI tools also give them access to loads of information that allow the creation of personalized messages, such as those they use for executive phishing and CEO fraud.

Using Deepfakes for Deceptive Purposes

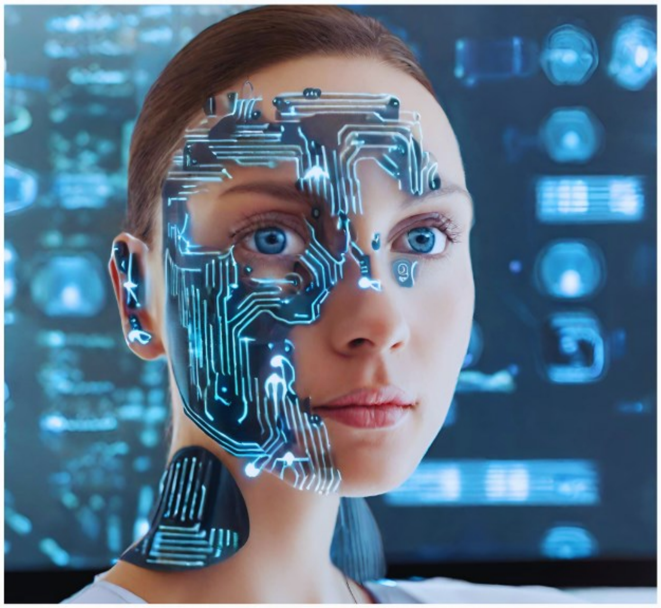
Deepfakes are AI-generated images or videos and are not necessarily a threat as they are generally used for entertainment. However, hackers have a completely different use for deepfake technology, which is to create deceptive content for phishing and other social engineering tactics. As AI continues to improve, deepfakes have become increasingly realistic, and they can gain trust and dupe employees into divulging sensitive information.

Automating Attacks

Automation by means of AI technology is one of the most beneficial uses of AI for cybercriminals. From identifying vulnerabilities in target systems to launching a full-scale attack, these are easily automated using the right AI algorithms. This process results in a higher probability of success for each attempt, and greater damage dealt for each successful attack.

Designing Undetectable Malware

While hackers have been creating malware for the longest time, many top security systems can detect these programs, so they are immediately blocked and do not get the chance to wreak havoc. But with AI, it is now possible to generate code for malware that is virtually undetectable because it can change its behavior to slip through even the most advanced antivirus programs.



Fooling Authentication Systems

Cracking passwords has become substantially easier using AI tools, but hackers can go much further than that. The high-tech AI programs they use are so well-trained in emulating human behavior that they are perfectly capable of bypassing CAPTCHA authentication. Even biometric systems can now be fooled by AI-generated fingerprints, voiceprints, and facial images.

Social Engineering

For social engineers, the arrival of generative AI is like opening a chest full of treasure. AI-powered chatbots are versatile tools that have greatly improved the efficiency of social engineering. The work and preparation that used to take days or even months now only takes a few seconds using AI tools. As new AI technology continues to emerge, it is no surprise that social engineering has suddenly become one of the biggest challenges businesses face today.

HOW TO PROTECT YOUR BUSINESS FROM AI POWERED ATTACKS

1. Know what you are up against

If you barely understand what is currently happening in the world of cybersecurity, then you might as well hand your business over to the hackers. Even if technology is not your focus, it is necessary to have an idea of how cybercriminals are now attacking businesses like yours. Awareness of the risks is the first step towards protecting your business from AI-assisted attacks.

2. Keep your systems updated

Technology changes constantly, so you need to make sure your systems are equipped with the most advanced tools to fight modern threats. Updates and upgrades need to be taken care of frequently, so experts strongly recommend that you delegate the task to a managed service provider rather than handle it yourself so you can focus on running your business.

3. Train your employees

Online threats continually evolve, so your workforce must also be continually trained on how to identify and avoid these threats. AI tools may have made the cybercriminal's job easier, but it doesn't change the fact that social engineering still relies heavily on human behavior. If your staff is watchful and does not engage with these threats, then the security of your business would be in much safer hands.

4. Strengthen your security system.

What you thought to be a robust security system a couple of years ago might be completely useless now, considering the pace at which hackers can create new malware and unleash attacks. So, every time there is a new upgrade available, or a more powerful security tool has been created, consult with your IT expert immediately and make the necessary changes to keep your system resilient amidst new threats.

5. Capitalize on helpful AI tools

Although threat actors are using AI for illegal activities, you can use AI technology to improve your system security. We have mentioned some of the ways to do this in an earlier section of this e-book. But what's even more advisable is to sit down with an IT expert who can design and create an AI-powered security system specifically tailored to the situation and needs of your business.

6. Partner with a reliable MSP

All this talk about AI attacks and AI security can be overwhelming, especially for non-technical business owners. There is no need to fear, because you can always entrust these IT tasks to a managed services provider. With their expertise, a reputable MSP can leverage AI tools to fortify your defenses against online attacks and to improve the different aspects of your business.

Like any other technology, AI can work for you or against you. It depends on what you choose to do about it. But don't take too long to decide – choose correctly so your business will have the best security available.

SystemsNet