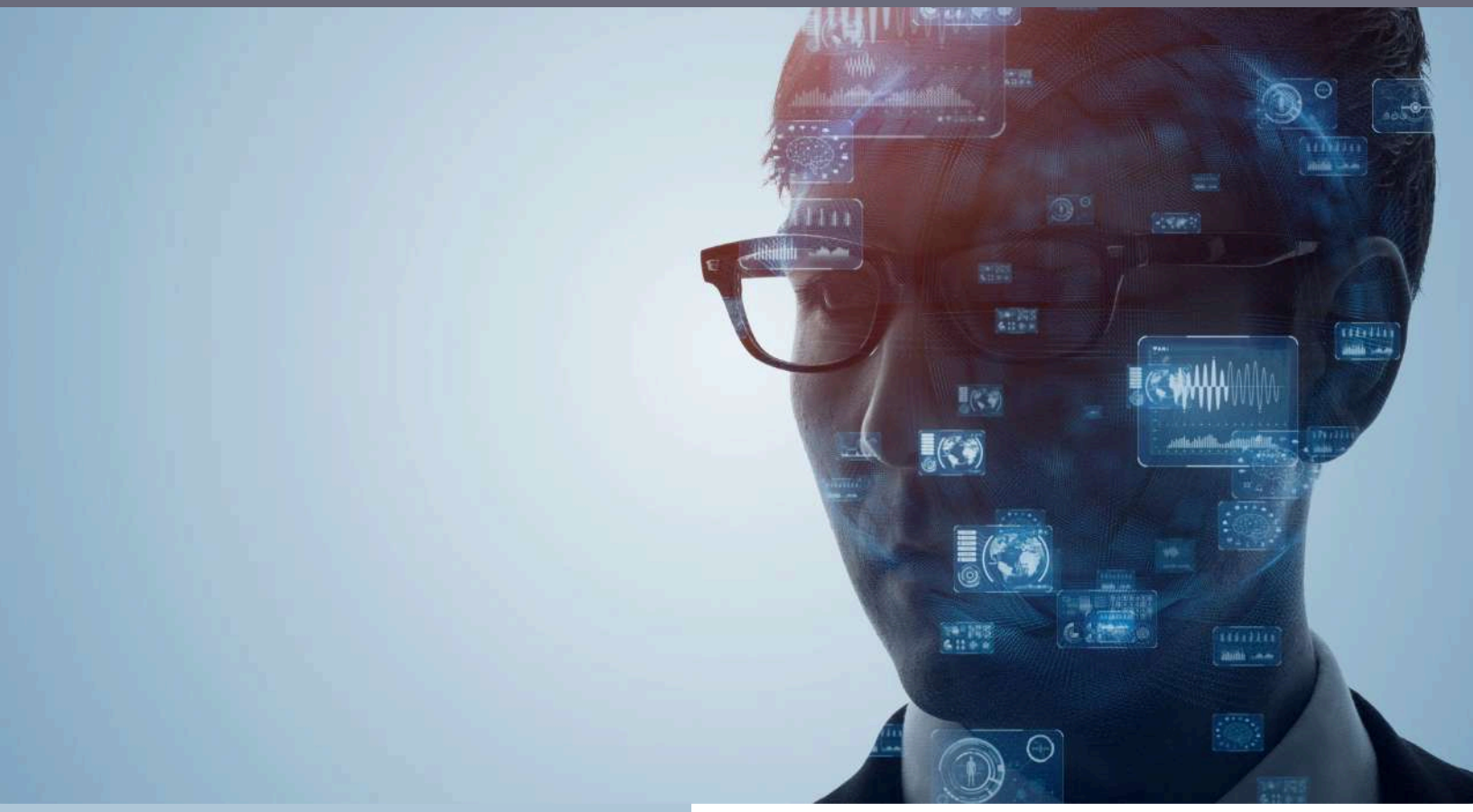
AI IN CYBERSECURITY

The pros and cons of artificial intelligence in cybersecurity



THIS MONTH'S TOPICS:

Artificial intelligence already plays a part in our daily lives. From our smartphones to our navigation systems, it is integrated in many technologies we are already familiar with. AI has allowed for the development of powerful tools to enhance security. But it can also present new challenges as cybercriminals utilize its capabilities as well.

In this month's newsletter, we will demystify how AI is reshaping the cybersecurity landscape. We will explore the benefits AI brings to cybersecurity, the advantages it offers, and the ways in which it is being manipulated by adversaries.

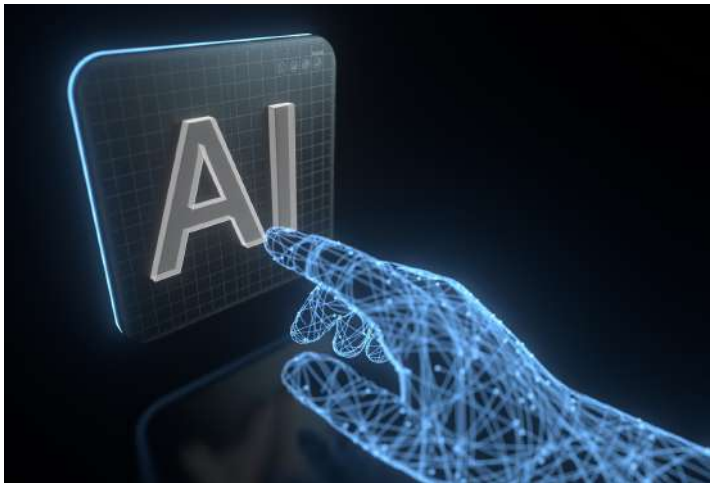
The Pros of Artificial Intelligence

Enhanced Threat Detection

AI dramatically improves the ability to detect emerging threats. Traditional security systems often rely on known threat databases and previously encountered attack patterns. AI, however, utilizes machine learning to analyze patterns and learn from them, enabling it to identify anomalies that could signify new, never-before-seen threats. This proactive approach to threat detection offers unique benefits in a landscape where attackers continually evolve their strategies.

Combatting Security Fatigue

Using artificial intelligence properly can help combat fatigue and increase productivity. This makes us better digital citizens and reduces the risk of falling for threats like phishing emails just because of fatigue.



AI Chatbot Reminders

- Avoid putting sensitive personal or company information into an AI chatbot.
- Don’t blindly trust the chatbot’s outputs. Ask your chatbot to cite its sources and verify the accuracy of its response.

Potential Cybersecurity Threats of Artificial Intelligence

AI in Phishing Attacks

Cybercriminals are using AI to generate phishing messages without errors. Spotting misspelled words or grammar errors is no longer a sure way of determining whether a message is a scam.

By analyzing vast amounts of data with AI, scammers can also create extremely specific spear phishing messages using personal details of the user they are targeting.

Deepfakes and Misinformation

The use of AI deepfakes—highly realistic fake audio and video—is on the rise. These deepfakes can be used to spread misinformation or impersonate individuals to gain unauthorized access to sensitive information. Cybercriminals also use hot topics in their deepfakes to get users to click on malicious links.

Scam Efficiency

Scammers can now operate at a scale previously unimaginable, and they can rapidly adapt their strategies in response to detection efforts. Automated systems help them test different approaches, learn from their failures, and refine their techniques.

Tips

Think twice before trusting a familiar face or voice. Continue using the SLAM method to evaluate the sender, links, attachments, and message of emails, texts, and other online communications.

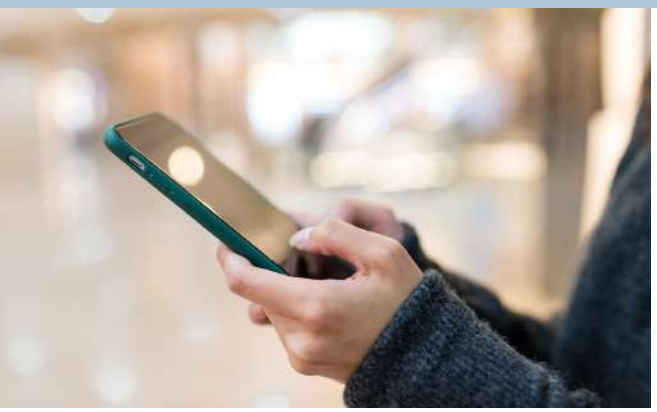
SCAM OF THE MONTH

Each month we highlight a scam that demonstrates tactics criminals are using RIGHT NOW, to better prepare you when the next scam hits.

In the offices of a renowned robotics firm, Lisa, a lead engineer, was designing a new autonomous drone system. Her concentration was broken by an unexpected email from Dr. Morris, a prominent figure in robotics and someone Lisa greatly respected.

The subject of the email read, "Urgent: Proposal for Collaborative Project in Robotics." Intrigued, Lisa opened the email, which articulated a proposal for a joint venture between her firm and the university where Dr. Morris was a lead researcher.

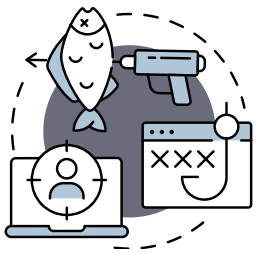
Attached was a document named "Project Specifics.pdf." The email captured the tone Lisa would expect. She was ready to open the attachment when a detail made her pause: the email address looked strange. She found the professor's official university email on the department website and sent an inquiry, attaching the received proposal for reference. Dr. Morris replied, confirming Lisa's suspicions: she had not sent the email and it was likely a scam.



Did you spot the red flags?

- Lisa should not have forwarded the document to Dr. Morris in case the attachment contained malware.
- Lisa should have alerted her IT team and her fellow employees about the message.
- The sender's email address looked suspicious. Always use the SLAM method to evaluate the different parts of a message.

If you are unsure whether an email is legit or not, it is best to research the organization's contact information or verify the message with the sender through another source.



Spear phishing attacks often use specific details about an individual to get them to trust the message. With AI, cybercriminals can generate these messages easier than ever before. Just because a message includes information personalized to you, doesn't mean you can automatically trust it.

CYBER NEWS

JULY
2024

NATURAL DISASTER SCAMS SURGE

As hurricanes and other natural disasters occur, scammers try to capitalize on these emergencies by offering fake services or relief. Always ask for identification if “officials” show up at your door, avoid paying upfront for services, read reviews before working with a company, and rely on official sources for information and updates. Other scammers are using AI deepfakes to pose as celebrities on social media asking for donations. Consider using official charity pages to donate instead of following links on celebrities’ social media pages.

JULY HOLIDAYS

July 29th is Global Tiger Day. Just like the tiger, we should stay strong and stealthy online. Keep your information secret and use strong passwords and security defenses.

AMAZON OTP SCAM CIRCULATING

In a recent scam, users are receiving automated calls claiming to be from Amazon, alerting them to a password change attempt on their accounts. The user is prompted to enter a code sent via text—which, notably, is a legitimate message from Amazon, to verify their identity. What’s really happening is scammers are trying to hijack Amazon accounts by stealing users’ verification codes. It is important not to give away one-time passwords to unsolicited callers, even in supposedly urgent situations.