

AI AND CYBERSECURITY

How AI is changing the cybersecurity landscape



THIS MONTH'S TOPICS:

AI & Cyber: The Benefits
Detecting and Mitigating Security Risks


AI-Powered Scams
How Hackers Learn About You

Scam of the Month:
Fileless Attacks

How to Recognize AI
Common Signs To Look For

Organizations are using AI to detect threats faster, automate responses, and strengthen digital defenses. At the same time, cybercriminals are harnessing AI to launch more convincing phishing attacks, generate fake content, and evade detection. This dual-use power makes AI one of the most disruptive forces in cybersecurity today.

As technology evolves, so do the methods used to deceive, exploit, and attack. In this issue, we'll explore how AI is shaping the future of cybersecurity, and what you need to watch out for, as understanding the capabilities and limitations of AI is now essential for staying secure in a rapidly changing digital world.



AI & CYBER: THE BENEFITS

01 Threat detection in real time

AI can analyze large volumes of data and network traffic in real time to identify anomalies and potential threats that human analysts might miss or take too long to find.

02 Rapid threat response and mitigation

AI can automatically respond to certain threats the moment they're identified, as well as contain them before they escalate.

03 Predictive capabilities

AI uses historical data to predict future attacks and recommend preventative actions, which helps organizations stay one step ahead of cybercriminals.

04 Reduced false positives

Traditional systems often flag too many false alarms. AI refines detection by learning what normal activity looks like and better distinguishing between legitimate and malicious behavior.

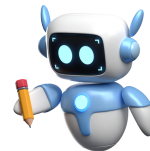
05 Enhanced email and phishing protection

AI scans email content and metadata to detect phishing scams and malicious attachments with greater accuracy than standard filters.





AI-Powered Scams



How Hackers Learn About You

Artificial intelligence isn't just a tool for cybersecurity defenders, it's also becoming a weapon for cybercriminals. Hackers are now using AI to study users, craft convincing scams, and automate attacks at a scale we've never seen before. Here's how it works and what you should watch out for.



Scraping Your Digital Footprint

AI tools can scan social media platforms, public records, and leaked databases to build a detailed profile of you.



Tailored Spear Phishing

AI crafts personalized scam messages using real details about your role, coworkers, or recent activity.



Writing Convincing Messages

Generative AI helps hackers write near-perfect phishing emails, texts, or DMs, without grammar mistakes, awkward language, etc.



Social Engineering

Hackers use AI to automate and personalize manipulation tactics across large groups quickly and convincingly.



Deepfake Voices and Videos

Hackers are now using AI to clone voices or even create realistic videos of someone you trust.



Using Chatbots To Trick You

AI chatbots can simulate real customer service reps, recruiters, or help desk agents.

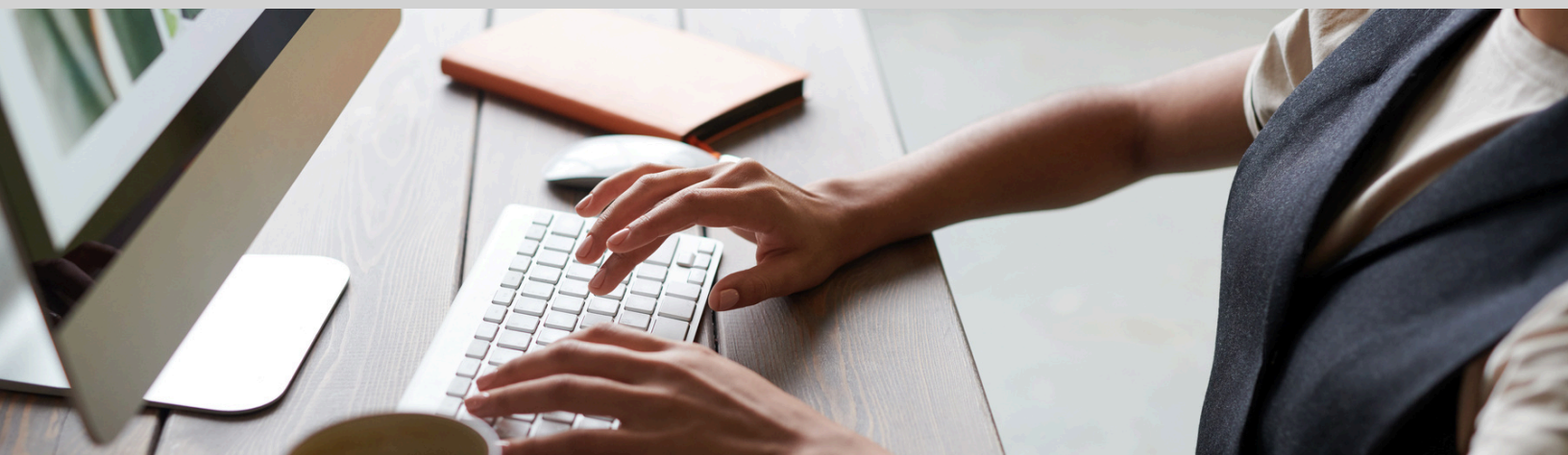


SCAM OF THE MONTH: FILELESS ATTACKS

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

It started like any other day. Linda, who worked in accounts payable at a healthcare clinic, noticed her mouse cursor twitching oddly across the screen. She assumed it was a glitch and went back to work. By lunchtime, several payments had been made to unfamiliar vendors...payments Linda didn't recall approving. The IT team quickly got involved. They ran antivirus scans, checked for malware, and reviewed recent downloads. However, it all came up empty. There were no infected files, no trojans, no digital fingerprints. The culprit? **A fileless attack.**

Days earlier, Linda had clicked a link in what seemed like a routine vendor email. That link launched a malicious PowerShell script that ran entirely in memory. Without installing any files, the attacker gained remote access, mimicked Linda's activity, and redirected payments before vanishing without a trace. The clinic acted fast: PowerShell access was locked down, phishing training was reinforced, and new detection tools were added to monitor suspicious behavior in memory. Linda wasn't at fault, but now she views unexpected emails with a little more caution.



DID YOU SPOT THE RED FLAGS?

- ▶ Unusual behavior, like a moving cursor or unexpected screen activity, can indicate that someone is remotely controlling your computer.
- ▶ When a message appears routine but includes a prompt to click a link or enable something unusual, that's a major red flag.



HOW TO PROTECT YOURSELF



Regularly train yourself and your team to spot suspicious links, even in messages that look legitimate. When in doubt, don't click.



Limit who can run tools like PowerShell, and use security settings to block or log script-based activities.



HOW TO RECOGNIZE AI: COMMON SIGNS

Language that's
"too perfect"

Language that's
loaded with
buzzwords

Repetitive or
generic content

Emotionally
neutral/flat
tone

Images that have
subtle flaws, like
warped body
parts

Voices that sound
flat or have odd
pauses or tone
changes

Overuse of
certain words
or phrases

Hallucinated
information,
sources, or
data

AI-generated content is becoming harder to detect, but there are still signs that can help you tell when something wasn't created by a human. One of the biggest giveaways is tone and structure. AI tends to write with flawless grammar and a formal or overly polished tone. It often lacks the natural flow, emotion, or spontaneity of human communication. Messages may feel generic or impersonal, even if they're loaded with facts or appear personalized. You might also notice repeated phrases, unnatural transitions, or a tendency to over-explain simple points. These are all clues that the message may have been generated by a machine.

Visual and audio content created with AI also leaves subtle hints. AI-generated images might have distorted hands, off-center eyes, strange lighting, or jumbled background text...things that seem "almost right" but feel just a little off. Voice clones and synthetic speech often sound slightly too flat or have awkward pauses and inflections. Social media profiles created by AI may have generic bios, limited or inconsistent activity, and stock-style profile photos. Being able to recognize these signals doesn't require technical training. It just takes a bit of observation and healthy skepticism. In a world where AI can create nearly anything, knowing what to look for is the first step in staying informed and secure.

