THE AI THREAT LANDSCAPE

Staying safe in an automated world

Kayvan Yazdi,
CEO of
TruAdvantage

OUR MISSION

Impacting our clients' success through trusting and meaningful partnerships and delivering strategic, secure, white-glove IT.

2025- CALIFORNIA WINNER
MSP 501
Channel Futures.

HIPAA COMPLIANT

SOC 2 TYPE 2

1 Rated IT MSP on CHATGPT
TruAdvantage

250+ Google Reviews

THIS MONTH'S TOPICS:

AI-Powered Attacks
How scammers use AI to scale faster

AI-Generated Phishing
Clues that help employees spot scam emails

Using AI Safely at Work
Simple habits for protecting company data

Scam of the Month:
AI Voice Cloning Scams

Cybercriminals are using AI to make attacks faster, more convincing, and harder to spot. With the help of automation, scammers can create realistic phishing emails, personalize messages, and launch attacks at a much larger scale. As these threats become more polished, employees need to know what to look for.

In this month's newsletter, we explore how cybercriminals use AI to automate attacks, break down the warning signs of AI-generated phishing scams, and share practical tips for using AI securely in the workplace. Understanding how AI can be misused is an important step toward protecting company data, avoiding scams, and reducing risk.

5 WAYS THAT CYBERCRIMINALS USE AI

AI-Written Phishing Emails

Attackers use AI tools to generate professional-looking emails that contain fewer spelling mistakes and can be customized for specific industries or individuals.

Automated Reconnaissance

AI can gather publicly available information from websites, social media profiles, and online databases to help attackers identify potential targets.

AI-Powered Chatbots

Some scams now use AI chatbots that can engage victims in realistic conversations, answer questions, and maintain deception for longer periods.

Malware Development

AI tools can help attackers write scripts, modify malicious code, and test variations to evade detection.

AI-Generated Fake Websites

Cybercriminals can use AI to create websites that mimic legitimate businesses, login portals, or online stores, making it easier to trick users into entering sensitive information.

Recognizing AI-Generated Phishing and Scam Emails

1 Unexpected Urgency

"Your account will be suspended today."

2 Requests for Credentials

Asking you to verify passwords or MFA codes

3 Unusual Requests

Gift card purchases, wire transfers, or confidential information

4 Suspicious Links

URLs that don't match the sender or organization

5 Emotional Pressure

Fear, excitement, or urgency designed to force quick action

Before you click....

✓ Was I expecting this message?

✓ Does the request make sense?

✓ Is the sender who they claim to be?

✓ Can I verify the request through another channel?

USING AI SECURELY AT WORK

1 NEVER ENTER SENSITIVE INFO

Avoid entering customer information, protected health information (PHI), passwords, financial records, and proprietary company data.

2 FOLLOW COMPANY POLICIES

Only use approved AI platforms and follow organizational guidelines regarding data handling and security.

3 VERIFY AI RESPONSES

AI can generate inaccurate information, sometimes called "hallucinations." Always verify facts, calculations, references, and suggestions before using them.

4 REVIEW AI-GENERATED CONTENT

Treat AI output as a draft, not a final product. Review for accuracy, tone, compliance requirements, and confidential information.

5 THINK BEFORE SHARING

Consider where information goes once it's submitted to an AI system and whether it could become accessible beyond your organization.

SCAM OF THE MONTH: AI VOICE CLONING SCAMS

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

Ashley was preparing for a meeting when she received a phone call from someone who sounded exactly like a senior leader at her company. “Ashley, I need your help quickly,” the caller said. “Can you send me the latest employee contact list? I can't access the shared drive right now.”

The request seemed legitimate, and the voice was familiar. Wanting to help, Ashley emailed the file without verifying the request. A few hours later, the real executive contacted her about an unrelated matter. During the conversation, Ashley mentioned sending the contact list. Confused, the executive explained that he had never made such a request. That's when Ashley realized she had been deceived. Cybercriminals had used AI voice cloning technology to impersonate a trusted leader and trick her into disclosing sensitive company information.

DID YOU SPOT THE RED FLAGS?

- Requests with a sense of urgency that involve confidential data should always be verified before taking action.
- Attackers often use excuses about technical problems or lost access to bypass normal security procedures.

HOW TO PROTECT YOURSELF

- If a caller asks for sensitive information, contact the person directly using a trusted phone number or platform before taking action.
- Even if a request appears to come from a trusted leader, follow your organization's established approval and data-sharing processes before complying.