

AvTek Chronicle

Insider Tips To Make Your Business Run Faster, Easier and More Profitably

Don't Get Hooked: Understanding and Preventing Phishing Scams

An email from a trusted partner lands in your inbox. Everything seems legitimate. The branding is familiar. The message sounds professional. You click the link, and just like that, you're caught in a phishing trap. AI is helping cybercriminals create polished messages, making scams harder than ever to spot. It's crucial for decision-makers to understand these evolving threats and take steps to protect their data.

Easy-to-spot phishing scams with obvious requests for sensitive information, poor grammar and suspicious links are a thing of the past. Cybercriminals now use AI to create convincing messages that sound like they come from trusted sources.

Even careful, well-trained employees can be tricked by these messages.

COMMON TYPES OF PHISHING SCAMS

Email phishing: Attackers send emails that appear to come from a trusted source.

The messages may contain malicious links or attachments designed to steal information, gain access to accounts or install malware.

AI-powered phishing: Cybercriminals create messages based on online information. They copy someone's writing style, mention real business relationships or use details about an employee to appear legitimate.

Spear phishing: To attack a specific person or business, bad actors research their victim and use relevant details to create a highly personalized message to gain the recipient's trust.

Business email compromise: An attacker impersonates an executive, employee or vendor to request payment, banking details or sensitive information.

Smishing: Hackers use text messages to get recipients to click on a malicious link, share information or call a fraudulent number.

QR-code phishing: Also known as quishing, this uses a QR code to direct someone to a fake website. They often appear in emails, documents, posters or packages.

HOW TO PROTECT YOUR BUSINESS FROM PHISHING ATTACKS

- Train employees to recognize AI-generated emails and other phishing tactics.
- Use advanced email security tools to detect malicious links and attachments.
- Enable multi-factor authentication.
- Verify urgent requests for payments, passwords or sensitive data in a separate channel.
- Limit publicly available employee and business information.
- Keep software, systems and security tools up to date.
- Make it easy for employees to report suspicious messages.

Key Takeaway:

One convincing message can expose sensitive data, so knowing what to watch for is key to staying secure.



Cybersecurity Risk Starts Closer Than You Think

When businesses think about cybersecurity, outside attackers often come to mind first. But cybersecurity risk can also come from everyday activity inside your organization. Employees, vendors and other trusted users have access to systems and sensitive information, and a mistake, compromised account or misuse of that access can expose your business. Managing who has access, educating employees and preparing for incidents can significantly reduce that exposure.

COMMON SOURCES OF INSIDER RISK

Data theft

Sensitive information can be downloaded, copied, shared or removed from the organization without authorization. This can also include the theft of company-owned devices containing business data.

Sabotage

A malicious insider may intentionally delete important files, disrupt operations, infect devices or interfere with critical systems.

Unauthorized access

Employees or other users may gain access to sensitive information they do not need for their role, whether intentionally or by mistake.

Negligence and error

Mishandled data, overlooked security procedures and everyday mistakes can expose sensitive information or create opportunities for an attacker.

Credential sharing

Sharing passwords or login credentials makes it harder to control access and can expose business systems and data to unauthorized users.

Unauthorized AI use

Employees may enter company, customer or other sensitive information into AI tools that have not been approved for business use, creating additional data security and privacy concerns.

SIGNS YOUR BUSINESS SHOULD PAY ATTENTION TO

Security risks are easier to address when unusual activity is identified early. Watch for activity such as:

Unusual access patterns: A user begins accessing sensitive information or systems unrelated to their responsibilities.

Excessive data transfers: Large amounts of business data are downloaded, copied or moved to external storage.

Repeated access requests: A user repeatedly requests access to sensitive systems or information outside their normal responsibilities.

Use of unapproved devices: Sensitive business information is accessed or stored on personal or unauthorized devices.

Disabled security protections: Antivirus, firewall protections or other security controls are turned off or bypassed.

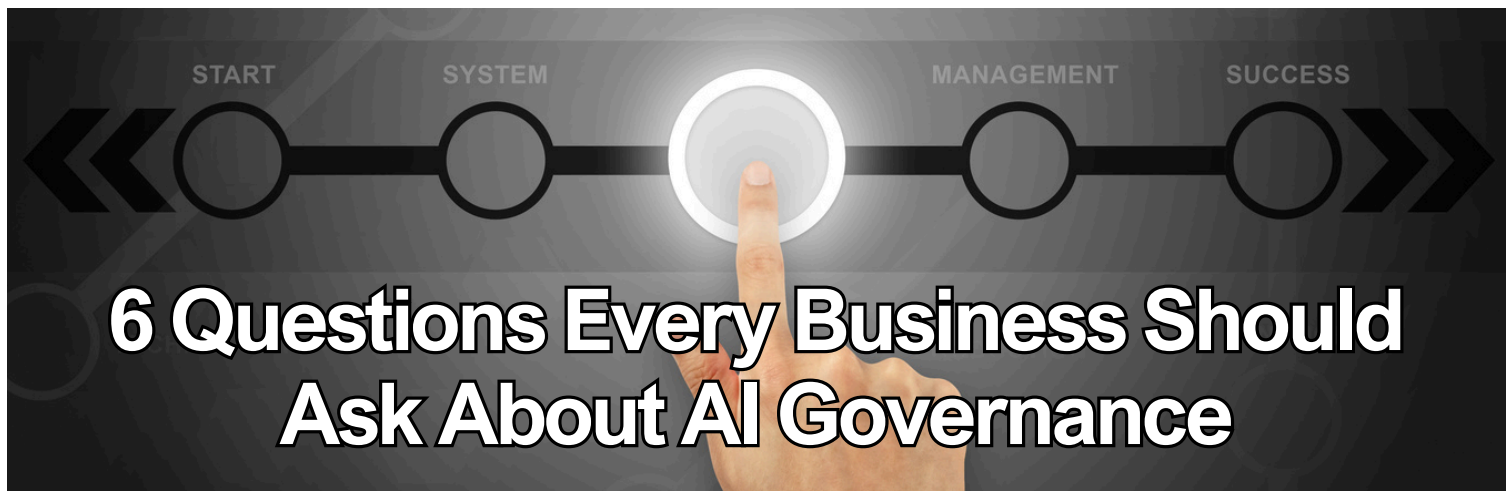
REDUCING INSIDER RISK STARTS WITH THE BASICS

Here are five practical ways to reduce cybersecurity risk inside your organization.

1. Implement a strong password policy and use multi-factor authentication.
2. Ensure your employees access only the data and systems required for their roles. Regularly review and update privileges.
3. Educate and train your employees on insider threats, security best practices and the safe use of AI tools.
4. Back up your important data regularly to be sure you can recover from an incident.
5. Develop a comprehensive incident response plan outlining how your business will address insider threat incidents.

Key Takeaway:

Strong cybersecurity includes managing internal risk. Clear access controls, employee awareness, reliable backups and an incident response plan can help protect sensitive information and keep your business operating when something goes wrong.



AI tools are already changing how employees write, research, summarize information and complete everyday tasks. For business leaders, the bigger question is whether those tools are being used with the right guardrails in place. AI governance helps organizations make clear decisions about which tools are approved, what information can be shared, who is responsible for oversight and how risks are handled.

Here are six questions every organization should be able to answer.

1. WHICH AI TOOLS ARE EMPLOYEES ALREADY USING?

AI adoption can happen quickly, especially when employees find tools that save time.

Start by identifying which AI platforms are currently being used across the organization, including tools for writing, meeting notes, document summaries, research and automation.

If leadership does not know what is being used, it becomes difficult to manage the risk that comes with those tools.

2. WHAT INFORMATION CAN EMPLOYEES SHARE WITH AI?

Employees should not have to guess whether a document, client record or internal file is appropriate to enter into an AI tool.

Define what information is allowed, what is restricted and what should never be shared with an unapproved AI platform.

That may include confidential client information, regulated data, login credentials, financial records, proprietary documents or other sensitive business information.

3. WHO IS RESPONSIBLE FOR APPROVING NEW AI TOOLS?

If there is no clear approval process, different departments may make different decisions about which tools are acceptable.

Assign responsibility for reviewing AI applications and define who should be involved in the decision.

Depending on the organization, that may include IT, security, compliance, legal and business leadership.

4. WHO IS RESPONSIBLE FOR APPROVING NEW AI TOOLS?

Before approving an AI tool, understand

what happens to the information employees enter into it.

Ask how data is stored, retained and processed. Determine whether submitted information may be used to improve or train the provider's models, and review the vendor's privacy and security practices.

A useful tool can still create unnecessary risk if the organization does not understand how its data is being handled.

5. WHEN DOES AI-GENERATED WORK REQUIRE HUMAN REVIEW?

AI can help employees work faster, but its output can still be incomplete, inaccurate or inappropriate for a particular situation.

Define when human review is required before AI-generated content is sent to a client, used in a business decision, submitted to a regulator or relied on in another high-impact situation.

Employees should know when AI can assist and when a person must make the final call.

6. When does AI-generated work require human review?

AI should be included in your existing risk and incident response planning.

Employees should know how to report an accidental disclosure, suspicious AI activity, misuse of a tool or an unexpected issue with an approved platform.

Organizations should also know who investigates the event, how it is documented and whether policies or controls need to change afterward.

AI GOVERNANCE IS AN ONGOING PROCESS

AI governance should not be treated as a one-time policy exercise.

Tools change. Vendors change their services. Employees find new use cases. Regulations and contractual requirements can change as well.

That means organizations need to review AI use regularly and make sure policies, access controls, employee guidance and risk management practices keep pace.

For many businesses, the best place to start is simple: Know what tools are being used. Know what data is involved. Know who owns the decision.

AI Governance Quick Check

CAN YOUR ORGANIZATION ANSWER “YES” TO THESE QUESTIONS?

- Do we know which AI tools employees are using?
- Do we have a written AI Acceptable Use Policy?
- Have we defined what information can and cannot be shared with AI?
- Is there a clear process for approving new AI tools?
- Does someone own AI governance?
- Are AI-related risks included in our incident response process?

If you answered “no” or “not sure” to any of these, your organization may have governance gaps worth reviewing.

A graphic with the text "HAPPY HALLOWEEN" in a stylized, purple, blocky font with a thick black outline. The text is set against an orange background decorated with white spider webs and several small orange bats flying around the letters.