AI Checklist, Do's and Don'ts.

Artificial Intelligence (AI) applications have become increasingly common in business. These AI tools offer numerous benefits, exercise caution when sharing sensitive, personal, company, or private information is crucial. Let's explore the dos and don'ts of disclosing such information to AI applications.

The Do's: Protecting Your Information

Anonymize Data: Whenever possible, anonymize or de-identify sensitive information. It helps protect individual identities and reduces potential risks.

Check Privacy Policies: Familiarize yourself with the AI application's privacy policies and terms of use. Ensure they align with your data security expectations.

Educate Employees: If your employees use AI applications, it's not just a matter of guidelines but a responsibility to educate them on handling sensitive information. Encourage them to follow best practices for data security, making them feel involved in the crucial task of protecting sensitive information.

Legal Agreements: If you share sensitive information with third-party AI providers, consider using legal agreements defining data protection measures and responsibilities.

Limit Information: Share only the information necessary for the task. Avoid providing excessive or sensitive details that aren't relevant.

Monitor Conversation: It's essential to monitor AI interactions, especially those involving sensitive data. This vigilance ensures that the AI is handling information correctly and not sharing it inappropriately, thereby maintaining the integrity of the app you are using or considering using.

Purpose: Understanding the purpose of using an AI application before sharing sensitive information is crucial. This understanding will help you make informed decisions about the necessity and relevance of the information you share.

Secure platforms: Opt for reputable and secure platforms for AI interactions and choose services prioritizing data encryption and following industry-standard security practices. Verify the current security practices and certifications of the platform you use or intend to use, as security measures can change over time.

Strong Passwords: For AI applications that require login credentials, it's essential to use a robust and unique password. Regularly updating these passwords and using a password management app will significantly enhance the security of your AI application usage.

OHIO INSURANCE AGENTS' ASSOCIATION, INC.
175 South 3rd St., Suite 940 · Columbus, Ohio 43215
phone (614) 552-8000 · fax (614) 552-0115 · toll-free (800) 555-1742 · web site: www.ohioinsuranceagents.com

The Don'ts: Avoiding The Pitfalls

Avoid Oversharing: Only disclose what is necessary. Stick to the task and avoid discussing unrelated personal or company matters.

Personal identifiers: Avoid Sharing personal identifiers like social security numbers, passport details, or credit card information with AI applications and should be kept strictly confidential.

Public Channels: Don't use public forums or social media to interact with AI applications for sensitive tasks. Instead, use secure, private channels.

Red Flags: If you notice any suspicious activity or unexpected requests from the AI application, stop the interaction immediately and seek assistance from your IT department

Security Updates: Keep your AI application and related software up to date. Updates often contain crucial security feature patches that protect against vulnerabilities.

Sensitive Data: Avoid Storing sensitive data with AI applications or chat logs. Delete any unnecessary information to reduce the risk of data breaches.

Trade Secrets: Keep your company's trade secrets and proprietary information out of AI conversations. Protect your intellectual property.

Unauthorized Data: Ensure you are authorized to share data, especially if it involves third-party information. Sharing data without consent may lead to legal repercussions.

Unsecured Wi-Fi: When interacting with AI applications, avoid using unsecured public Wi-Fi networks. Instead, use a secure, private network to prevent eavesdropping.

AI applications offer incredible business potential but require responsible handling of sensitive information. Ensure that your interactions with AI remain productive and secure. Protecting your private information is paramount in the digital age, and responsible AI usage is vital to that effort.

OHIO INSURANCE AGENTS' ASSOCIATION, INC.
175 South 3rd St., Suite 940 · Columbus, Ohio 43215
phone (614) 552-8000 · fax (614) 552-0115 · toll-free (800) 555-1742 · web site: www.ohioinsuranceagents.com