Do and Don’ts Checklist

AI and safeguarding your data

The use of Artificial Intelligence (AI) applications like ChatGPT, Google Bard and Microsoft Bing has become increasingly common in the business world.

While these AI tools offer numerous benefits, it's crucial to exercise caution when sharing sensitive, personal, company, or private information.

In this guide, we'll explore the dos and don'ts of disclosing such information to AI applications., we'll explore the dos and don'ts of disclosing such information to AI applications.

AI - dos and don’ts checklist for safeguarding your data

The dos: protecting your information

1. Understand the purpose:

Before sharing any sensitive information, make sure you understand the purpose of using the AI application. Ensure it's necessary and directly related to the task at hand.

2. Use secure platforms:

Opt for reputable and secure platforms for AI interactions and choose services that prioritise data encryption and follow 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.

3. Limit information:

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

4. Anonymise data:

Whenever possible, anonymise or de-identify sensitive information. This helps protect individual identities and reduces potential risks.

5. Use strong passwords:

If the AI application requires login credentials, use strong, unique passwords. Regularly update these passwords to enhance security and use a password management app to manage your credentials.

6. Monitor conversations:

Keep an eye on AI interactions, especially if they involve sensitive data. Ensure that the AI is handling information correctly and not sharing it inappropriately. This 13-point checklist will help you to understand the integrity, or otherwise, of the app you are using, or considering using.

7. Educate Employees:
If your employees use AI applications, provide them with guidelines on handling sensitive information. Encourage them to follow best practices for data security.

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

9. Use legal agreements:
If you're sharing sensitive information with third-party AI providers, consider using legal agreements that define data protection measures and responsibilities.

The don'ts: avoiding the pitfalls

1. Don't share personal identifiers:
Avoid sharing personal identifiers like Social Security numbers, passport details, or credit card information with AI applications. These should be kept strictly confidential.

2. Don't share trade secrets:
Keep your company's trade secrets and proprietary information out of AI conversations. Protect your intellectual property.

3. Avoid over-sharing:
Don't disclose more information than necessary. Stick to the task at hand and avoid discussing unrelated personal or company matters.

4. Don't share unauthorised data:
Ensure you have proper authorisation to share data, especially if it involves third-party information. Sharing data without consent may lead to legal repercussions.

AI - dos and don’ts checklist for safeguarding your data

5. Avoid public channels:
Don't use public forums or social media to interact with AI applications for sensitive tasks. Use secure, private channels instead.

6. Don't ignore security updates:
Keep your AI application and related software up-to-date. Updates often contain crucial security patches that protect against vulnerabilities.

7. Avoid unsecured Wi-Fi:
Refrain from using unsecured public Wi-Fi networks when interacting with AI applications. Use a secure, private network to prevent eavesdropping.

8. Don't store sensitive data:
Avoid storing sensitive data within AI applications or chat logs. Delete any unnecessary information to reduce the risk of data breaches.

9. Don't ignore 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.

AI applications offer incredible potential for businesses, but they also require responsible handling of sensitive information. By following these dos and don'ts, you can ensure that your interactions with AI remain productive and secure. Protecting your secrets is paramount in the digital age, and responsible AI usage is a key part of that effort.

Contact us:
support@itg.uk.com
01625 613 633
www.itg.uk.com