Tip sheet

Protecting your information while using AI

This tip sheet helps you understand how to keep personal information safe while using AI. It gives simple steps for what to do and why.

Good Things

1 Think before giving personal details

What to avoid: Don't share personal information like your full name, address, phone number, financial details, or personal identification numbers (e.g., Social Security Number) with AI tools or services.
Why: AI tools might save or misuse this information if not properly secured.

2 Use strong, unique passwords

What to do: Create passwords that are hard to guess and use a different password for each account or service.
Why: Strong passwords reduce the risk of unauthorised access to your accounts.

3 Enable Two-Factor Authentication (2FA)

What to do: Use 2FA for your accounts whenever possible. This adds an extra layer of security.
Why: It helps protect your account even if your password is shown.

4 Be wary of phishing scams

What to look for: Be cautious of emails or messages asking for personal information or login details.
Why: Scammers may use AI-generated messages to trick you into giving away your information.

5 Check privacy settings

What to do: Review and adjust the privacy settings on the AI tools and services you use.
Why: This helps control what information is shared and who can see it.

6 Understand the terms and conditions

What to do: Read the terms and conditions or privacy policy of AI services to understand how your information will be used.
Why: It helps you know what you're agreeing to and how your information might be handled.

7 Avoid sharing personal experiences publicly

What to avoid: Don't share personal stories or sensitive experiences in public forums or with AI chatbots.
Why: This information might be stored or misused by others.

8 Keep software and apps updated

What to do: Regularly update your software and apps to ensure you have the latest security features.
Why: Updates often include security patches that protect against new threats.

9 Be careful of free services

What to consider: Be cautious with free AI tools or apps, as they might collect data for advertising or other purposes.
Why: Free services often sell user data, which can compromise your privacy.

10 Report suspicious activity

What to do: If you notice any unusual activity or believe your information might be compromised, report it immediately to the service provider.
Why: Acting quickly can help reduce potential damage and protect your information.

11 Educate yourself about AI tools

What to do: Learn about the AI tools you use and how they work.
Why: Understanding how AI works can help you make informed decisions about your information.

12 Ask for help If needed

What to do: Don't hesitate to ask for help from trusted friends, family, or professionals if you're unsure about how to protect your information.
Why: Getting advice from knowledgeable people can help you stay safe online.