STAY SAFE ONLINE WHEN USING AI

01

Mind Your Inputs

AI systems adapt and improve based on user inputs, so it's crucial to avoid sharing anything you want to remain private. This includes both personal details and any sensitive information related to your workplace or company.

TIP: Refrain from inputting confidential data or sensitive information into AI models to ensure your privacy stays intact.

02

Be Privacy Aware

Be mindful of your online presence. Since AI models often pull data from public sources, anything you post could potentially be used or referenced by these tools.

TIP: Before sharing anything publicly, ask yourself if you'd want an AI system to potentially access or store it.

03

AI is a Tool

While AI can help streamline tasks, it's crucial to keep honing your own skills and not depend solely on AI-generated output. Remember, prompting isn't the same as true creation!

TIP: Use AI as a support tool, but don't let it replace your expertise and creativity.

04

How Hackers Use AI

Cybercriminals are now leveraging AI to deceive victims. Tools can replicate a person's voice or create convincing, realistic images and videos—known as "deepfakes." This means a scammer could impersonate someone you trust, making fake calls to steal money or spread false information through altered visuals.

TIP: Stay informed about cybersecurity best practices. As criminals harness AI for scams, it's essential to protect yourself with the "core four" habits: strong passwords, enabling MFA, regular software updates, and promptly reporting phishing attempts.

E-TECH