


# SAFE | Security Awareness for Everyone

TIP SHEET - AUGUST 2025

## Stay Safe Online While Using AI



What can AI do for you personally? Increase productivity through task automation, enhance decision-making, provide data-driven insights, access to creative tools, and reduce human error. More than you can think of, and many can be listed here, with more uses continually being created.

While AI might offer valuable capabilities, always remember to stay proactive and educated about the risks. Here are essential tips to ensure you stay secure while using generative AI.

### 1. Mind Your Inputs

AI systems learn from user inputs, so refrain from sharing anything you want to keep private, like your workplace's company data or your personal details.

**TIP:** Avoid sharing sensitive or confidential information with AI models – if you wouldn't post it on social media, don't share it with AI. Read what you are agreeing to before using any of these tools. It should also go without saying that strong, unique passwords with MFA enabled can prevent unauthorized access to your account and information, thereby protecting against malicious actors who aim to cause mischief or harm.

### 2. Be Privacy Aware

Since AI models often scrape data from the web, what you share publicly online may be copied, in whole or in part, by AI tools. Anything you input into them can also be used for training purposes, exposing any sensitive or private data you enter.

**TIP:** Think about what you share with a broad audience – would you want an AI to have it? Information includes any data you share on other, like about family or friends, or any company

internal company information. Please read the privacy policy or terms of use for how it handles and stores your data.

### 3. How Hackers Use AI

Cybercriminals may use AI to fool you. Public tools can mimic a person's voice or image (sometimes referred to as a "deepfake"). Which does sound fun to try, but criminals can make a voice call to mimic a trusted person and steal money, or to harass people by posting fake or modified images and videos. Look for unnatural movements, distortions, or robotic-sounding voices.

**TIP:** Stay updated on cybersecurity best practices. Criminals using AI as a tool make it more critical that everyone protect themselves by adopting the core four behaviors: using strong passwords, enabling MFA, keeping software up to date, and reporting phishing.

### 4. AI is a (powerful) Tool

While AI can assist with tasks, it's essential to maintain your expertise and not rely solely on AI-generated content. Prompting isn't the same as creating! Powerful isn't always perfect, so be sure to review the output for accuracy and your 'voice.'

**TIP:** Treat AI as a helpful tool rather than a replacement for your skills. Increased dependency can reduce critical thinking and expose you to biases and misinformation in the output. If you don't use your own critical thinking skills, you may lose them.

**Stay informed of current AI security best practices, keep all software and device security patches up to date, and find out all the good things that those powerful AI tools can do for you.**