

AI SAFETY, PRIVACY & SCAM AWARENESS GUIDE

A practical guide to using artificial intelligence with greater confidence while protecting your information, identity, money, and family.

Health Therapies Lifestyle

Building Healthier Lives, Stronger Families, and Lasting Legacies.

Artificial intelligence can be enormously useful for learning, planning, writing, organizing, and everyday problem-solving. But AI can also make convincing false information, manipulated images, cloned voices, and sophisticated scams easier to create. The safest approach is to enjoy the benefits while keeping human judgment firmly in charge.

This guide is designed for everyday users, families, seniors, students, community members, and small-business owners.

1. The Golden Rule: AI Can Sound Certain and Still Be Wrong

AI systems generate responses based on patterns and available information. They can misunderstand a question, use outdated information, or confidently produce an incorrect answer.

- Treat AI as an assistant, not an unquestionable authority.
- Verify important facts using reliable independent sources.
- For medical, legal, financial, tax, or safety decisions, consult an appropriately qualified professional.
- Ask AI to explain uncertainty, assumptions, or what should be independently checked.

2. Protect Personal & Family Information

Think carefully before entering information into any AI service, website, chatbot, form, or unfamiliar app. Information that seems harmless can become sensitive when combined with other details.

- Avoid entering passwords, PINs, security-question answers, Social Security numbers, full banking details, or authentication codes.
- Do not casually upload confidential medical, legal, employment, customer, or family records.
- Remove unnecessary names, addresses, account numbers, dates of birth, signatures, and identifying details before sharing documents.
- Review the privacy and data settings of services you use, especially when handling business or family information.

3. Recognize AI-Enhanced Scams

Scammers can use AI to create polished messages, realistic photographs, fake documents, cloned voices, and even convincing video. Familiarity is no longer proof of authenticity.

- Be suspicious of unexpected urgency: 'act now,' 'don't tell anyone,' or 'send money immediately.'
- Never send money solely because a voice message or video appears to be from someone you know.
- If a relative claims to be in trouble, stop and contact them through a number or method you already trust.
- Be wary of unexpected investment opportunities, prizes, refunds, romance requests, job offers, and account-security warnings.
- Do not share one-time verification codes with someone who contacts you.

4. Create a Family Verification Plan

A simple family system can defeat many impersonation scams. Agree in advance how family members will confirm unusual or urgent requests.

- Choose a private family verification word or question that is not posted publicly.
- For unusual money requests, require a second method of contact before acting.

- Teach children, parents, and grandparents that a familiar voice can now be imitated.
- Keep trusted contact numbers stored rather than relying on numbers supplied in an incoming message.

5. Links, Attachments & QR Codes

AI can make phishing messages look professional and grammatically perfect, so spelling mistakes are no longer a reliable warning sign.

- Avoid clicking unexpected links in texts, emails, social messages, or pop-ups.
- Navigate to important accounts using the official app or a trusted bookmark rather than an incoming link.
- Treat unexpected attachments and QR codes cautiously.
- Check the actual sender and domain carefully; a familiar logo does not prove authenticity.

6. AI, Health & Wellness Information

AI can help people prepare questions, understand general concepts, organize information, and build healthier routines. It should not be treated as a substitute for diagnosis or individualized medical care.

- Do not use an AI answer alone to start, stop, or change prescription medication.
- Seek professional evaluation for concerning or persistent symptoms.
- Be skeptical of claims that a product, scan, supplement, or technology can guarantee a cure.
- Use AI to become better prepared for conversations with qualified healthcare professionals.

7. AI, Money & Investments

Fraudsters frequently combine urgency, exclusivity, impressive-looking websites, testimonials, and AI-generated materials. High-quality presentation does not prove legitimacy.

- Never invest because of pressure, fear of missing out, or a celebrity-style endorsement alone.
- Independently verify the company, person, registration status, fees, withdrawal rules, and custody of funds.
- Do not allow an unknown person remote access to your computer or phone.
- Be especially cautious when payment is requested through cryptocurrency, gift cards, wire transfers, or other difficult-to-reverse methods.

8. Children, Teens & AI

Young people should understand both the possibilities and limitations of AI. Family rules should evolve with age, maturity, school requirements, and the technology being used.

- Teach children not to share identifying information, private photographs, passwords, or family financial details.
- Encourage them to tell a trusted adult when an AI interaction feels threatening, sexual, manipulative, or frightening.

- Discuss academic honesty and when AI assistance is or is not permitted.
- Remind them that generated images, videos, and messages can be fake even when they look convincing.

9. A 30-Second Safety Check

Before acting on an unexpected digital request, use this simple sequence:

- STOP - Do not let urgency control the decision.
- CHECK - Who is actually asking, and can you verify them independently?
- THINK - Does the request involve money, passwords, codes, private information, secrecy, or unusual pressure?
- VERIFY - Contact the person or organization through a trusted channel.
- ACT - Proceed only after you are comfortable that the request is genuine.

Common Warning Signs

Warning sign	Why it matters
Extreme urgency	Scammers try to prevent you from slowing down and checking.
Secrecy	Requests not to tell family, a bank, employer, or authorities are a major warning sign.
Unexpected money request	Verify independently, even when the voice, photo, email, or account looks familiar.
Verification-code request	Legitimate security codes are generally meant for you, not the caller or texter.
Guaranteed returns or cures	Absolute promises deserve skepticism and independent verification.
Remote computer access	Unknown callers may use remote-access software to steal information or money.
Changed payment instructions	Independently confirm banking or payment changes through a trusted contact method.

If You Think You Have Been Scammed

Move quickly, but do not panic. Stop communicating with the suspected scammer. Contact the relevant bank, card issuer, payment provider, employer, or account provider through an official channel. Change compromised passwords, enable multi-factor authentication where available, preserve messages and transaction records, and report suspected identity theft or fraud to the appropriate authorities or service provider.

If someone gained remote access to your device, disconnect it from the internet and seek trusted technical assistance before using it for sensitive activity.

Your Personal AI Safety Promise

I will use AI to help me think, learn, create, and organize - but I will slow down when money, identity, privacy, health, or family safety is involved. I will verify before I trust and confirm before I act.

Health Therapies Lifestyle

Building Healthier Lives, Stronger Families, and Lasting Legacies.

Educational notice: This guide provides general educational information and is not legal, financial, cybersecurity, or medical advice. Technology and scam methods change rapidly. For significant incidents or individualized advice, contact the appropriate qualified professional, financial institution, technology provider, or relevant authority.