Ulliance
Enhancing People Improving Business

Life Advisor
Well-being | Newsletter

LifeAdvisor.com
Employee Monthly Communication

How to Stay Safe in the Digital World

The internet is an extraordinary resource that connects us to knowledge, entertainment, and one another. Yet, like any powerful tool, it carries risks if not used responsibly. Practicing internet safety means safeguarding personal information, avoiding harmful or misleading content, and recognizing potential threats such as scams, cyberbullying, and identity theft. By adopting safe online habits, individuals of all ages can fully enjoy the benefits of the digital world while minimizing exposure to its dangers.

Certain groups are particularly vulnerable to online scams and deceptive practices—most notably children and older adults. To help protect these populations, Ulliance has developed **Safety Tips for Children and Seniors**, offering practical guidance to ensure their online experiences remain safe, secure, and positive.

Internet Safety Tips for Children

- Use Parental Controls: Enable filters on devices and browsers to block inappropriate content.
- Teach Critical Thinking: Help kids recognize scams, fake profiles, and misleading information.
- Limit Screen Time: Set healthy boundaries for device use to avoid overexposure.
- Monitor Social Media: Know which platforms they use and who they interact with.
- Avoid Sharing Personal Info: Teach them never to share their full name, address, school, or photos with strangers.
- Encourage Open Communication: Let them know they can talk to you about anything they see online that makes them uncomfortable.
- Use Strong Passwords: Help them create secure passwords and explain why they shouldn't share them—even with friends.

Internet Safety Tips for Seniors

- Beware of Scams: Educate about phishing emails, fake tech support calls, and fraudulent websites.
- Use Secure Connections: Avoid public Wi-Fi for banking or shopping; consider using a VPN.
- Check Website URLs: Make sure sites begin with "https://" before entering any personal or financial info.
- Update Software Regularly: Keep devices and antivirus programs up to date to prevent vulnerabilities.
- Use Strong, Unique Passwords: Avoid common passwords like "123456" or "password".
- Be Cautious on Social Media: Limit what's shared publicly and be wary of friend requests from strangers.
- Enable Two-Factor Authentication: Adds an extra layer of security to email and banking accounts.

Whether you're guiding a child or empowering a senior, internet safety is a shared responsibility. By fostering awareness, encouraging open conversations, and practicing smart habits, we can all help create a safer digital world for everyone.

Artificial Intelligence (AI)

Another area of the digital world that individuals should be aware of is AI. Artificial intelligence offers enormous benefits, but it also carries significant risks that society must manage carefully.

On the benefits side, AI enhances efficiency by automating repetitive tasks, analyzing massive datasets, and providing real-time insights. It powers innovations like medical diagnostics, self-driving cars, and personalized recommendations, helping industries save costs and improve accuracy. AI also assists in tackling complex global challenges, from climate modeling to drug discovery, and can perform dangerous tasks that reduce human exposure to risk.

However, AI also introduces risks. Bias and discrimination can emerge if systems are trained on flawed or unrepresentative data. Job displacement is a concern as automation replaces certain roles, potentially widening inequality. There are also privacy and security risks, since AI systems often rely on sensitive data.

In short, AI is a double-edged sword: The challenge lies in maximizing its benefits while minimizing its risks.

Here are some General AI Safety Tips:

- **Mind Your Inputs:** Avoid sharing sensitive personal or financial information. If you wouldn't post it publicly, don't feed it to an AI.
- **Be Privacy Aware:** AI systems may learn from public data. Think carefully about what you share, especially in public forums or with generative tools.

- **Watch for Deepfakes & Scams:** Cybercriminals can use AI to mimic voices, faces, or writing styles. Stay alert to suspicious messages or media that seem "off".
- **Use the "Core 4" Cybersecurity Habits:**
    - Strong, unique passwords
    - Multifactor authentication (MFA)
    - Regular software updates
    - Vigilance against phishing attempts
- **Don't Over-Rely on AI:** AI is a tool—not a replacement for your judgment, creativity, or expertise. Always verify facts and cross-check sources.
- **Understand Platform Privacy Settings:** Review and adjust privacy settings on AI platforms to control what data is collected and shared.
- **Teach Kids Responsible Use:** If children are using AI, explain how it works, its limitations, and how to engage safely and critically.

AI is here to stay—and it's evolving fast. By staying informed, practicing smart habits, and teaching others to do the same, we can all enjoy the benefits of AI while minimizing the risks. Safety isn't about fear—it's about confidence, control, and clarity.

For more information, tools, resources, or app information, call your Life Advisor Employee Assistance Program!

Ulliance provides no cost, confidential, short-term counseling for you & your family.

Call us- we're here to help **800.448.8326**