A Safer Naper
April 2026 – Online Personal Safety

These days, it's common to spend a considerable amount of time online looking for deals, keeping up with friends and family, and seeing what's going on in the world. But not everything online is what it seems, and criminals routinely use the anonymity of the internet to prey on unsuspecting victims. This month, the Naperville Police Department aims to make our community "A Safer Naper" by reminding everyone of the importance of online personal safety, particularly surrounding the use of artificial intelligence (AI).

Follow these internet safety tips to help you avoid getting into trouble online (and offline):

- **Keep Personal Information Professional and Limited:** You wouldn't stand on a street corner giving out your personal information to the strangers who walk by you, right? Then why would you do that online where millions of strangers can see what you posted?
- **Keep Your Privacy Settings On:** Both web browsers and mobile operating systems have settings available to protect your privacy online. These settings are sometimes hard to find, but make sure you enable these privacy safeguards and keep them enabled.
- **Practice Safe Browsing:** The Internet has hard-to-see pitfalls, where one careless click could expose personal data or infect your device with malware. By resisting the urge to click, you don't even give the hackers a chance.
- **Make Sure Your Internet Connection is Secure. Use a Secure VPN Connection:** When you go online using a public Wi-Fi connection, you have no direct control over its security. Make sure your device is secure, and when in doubt, wait for a better time (i.e., until you're able to connect to a secure Wi-Fi network) before inputting information such as your bank account number. To further improve your Internet browsing safety, use a secure VPN (virtual private network) connection. VPN enables you to have a secure connection between your device and an Internet server so that no one can monitor or access the data that you're exchanging.
- **Be Careful What You Download:** A goal of cybercriminals is to trick you into downloading malware programs or apps that carry malware or try to steal information. This malware can be disguised as an app: anything from a popular game to something that checks traffic or the weather. Don't download apps that look suspicious or come from a site you don't trust.
- **Choose Strong Passwords:** Passwords are one of the biggest weak spots in the whole Internet security structure, but there's currently no way around them. Select strong passwords that are hard for cybercriminals to decipher. Password manager software can help you to manage multiple passwords so that you don't forget them.
- **Make Online Purchases from Secure Sites:** Cybercriminals are eager to get their hands on the credit card or bank account information you provide when making an online purchase. Only supply this information to sites that provide secure, encrypted connections. You can identify secure sites by looking for an address that starts with https: (the S stands for secure) rather than simply http: They may also be marked by a padlock icon next to the address bar.
- **Be Careful What You Post:** The Internet does not have a delete key. Any comment or image you post online may stay online forever because removing the original does not remove any copies that other people made. There is no way for you to "take back" a remark you wish you hadn't made or get rid of

that embarrassing selfie you took at a party. Don't put anything online that you wouldn't want your mom or a prospective employer to see.

- **Be Careful Who You Meet Online:** People you meet online are not always who they claim to be. Indeed, they may not even be real. Fake social media profiles are a popular way for hackers to cozy up to unwary web users and pick their cyber pockets. Be as cautious and sensible in your online social life as you are in your in-person social life.
- **Keep Your Antivirus Program Up to Date:** Internet security software cannot protect against every threat, but it will detect and remove most malware … as long as it's up to date. Be sure to stay current with updates for your operating system and any applications you use. They provide a vital layer of security.

Artificial intelligence (AI) is not new (it has been around for roughly 70 years), but it has experienced explosive growth in the last few years. Today, generative AI is available to the general public to create new content such as audio, images, and text. AI can enhance our lives, but it can also be dangerous and provide another route for cybercriminals to deceive and exploit people. Here are some safety tips.

- **Data Privacy – Personal Information:** Avoid putting passwords, confidential work documents, or sensitive details about yourself into AI chatbots or tools unless you trust the platform and know how they handle this information.
- **Understand Privacy Settings:** Take the time to review and adjust privacy settings on AI platforms according to your comfort level.
- **Check Permissions and Security:** Before downloading AI apps, review their permissions and privacy policies. Evaluate the tool's security settings, including options to disable the tool's ability to reuse your data to train its AI.
- **Be Skeptical of Content:** Assume that not everything generated or presented by AI is true. Malicious actors exploit AI technologies to spread misinformation and disinformation, influencing and manipulating people's decisions and actions. AI can generate deepfakes, which are images or videos altered to misrepresent someone as saying or doing something they did not do.
- **Verify Information (Fact-Check):** AI systems are not perfect and can make mistakes. It can produce false, misleading, or "hallucinated" information. Always cross-reference AI-generated content before reaching conclusions or making decisions based solely on AI-generated output.
- **Be Aware of Cybersecurity Threats:** Bad actors can exploit AI to launch cyberattacks. They manipulate AI tools to clone voices, generate fake identities and send convincing phishing emails—all with the intent to scam, hack, steal a person's identity or compromise their privacy and security.
- **Understand Limitations (Critical Thinking):** Avoid being overly reliant on AI for critical decision-making. Maintain human oversight.
- **Be Aware of Bias:** Humans are innately biased and the AI that we develop can reflect our biases. Review the data sources and generated results for bias to ensure transparency, accountability, fairness and respect for privacy.
- **Use Secure Connections:** Avoid accessing sensitive AI tools on public Wi-Fi.
- **Verify Legitimacy:** Be cautious of new or unknown AI tools, as hackers may use them to steal data.
- **Stay Updated:** Keep up with the latest advancements and developments in AI technology to better understand AI systems' capabilities, limitations and potential risks.

- **Report Inappropriate Contant:** Report inappropriate or harmful AI-generated content or inappropriate interactions. You need to report them to the platform, service provider or a trusted adult if you are a child.