PDAT 625G
Spring 2026
Jessica Lopez

Model 6: AI Security

Due to the rise of technology use and the increase of cyber attacks and stealing online data collection in the past few years, it's important to navigate security and privacy precisely and carefully. An example of this importance is that the amount of hacking and scamming attempts has increased by 47% (or 50%) percent from 2024 to 2025 (Kindo.ai., Gigamon, Federal News Network).

The most common form of scam is identity theft with data phishing (Top 10 List of Scams of 2026). Next is phone scams, and third most common is debt collection.

Here are ways to protect your computer, device or network:

- Define what data you have and where the data is located on the network or software.
- Decide who in your company or team can access it by level.
- Turn on privacy settings. Select which setting is more protected or best for the situation.
- Be extra careful when buying an item online, making a review, or commenting or sharing information.
- Limit personal information, especially on websites with login information.
- Users of social media should be careful on what information is necessary for upload.
- Turn on the privacy safeguard such as firewalls and VPNs
- Close accounts and social media when you're not using them. Hackers have a harder time gaining access to the account if it is closed and logged out.
- Check the app description twice before downloading it.
- Never download an app or link if it is suspicious or comes from an untrusted website or app.
- Make sure the internet wifi is secure, especially at public places.
- Create a strong password, and use many different passwords when necessary.
- Use password manager to keep passwords safe and secure.
- Use https sites for downloads.
- Make sure to update your virus protection software.
- Back up data regularly.

In comparison to the articles from the assignment, AI platforms like Kindo.ai bring agentic "*execution to security"*. This means security moves seamlessly from workflows to deep infrastructure automation, bridging tools, data and environments within the app and there are no hard-coded secrets, no keys in memory and a full lifestyle control (Meet Kindo AI).

According to the Gigamon AI article, scams can be separated into three categories: phishing and social engineering, malware development and network exploitation. AI cyber attacks are also sorted by data collection, pattern analysis, attack planning and adaptation and evolution. The Gigamon AI Solution Overview also has facts on AI. One fact from this document was that, *"91% of security leaders are recalibrating risk due to the impact of AI."* Another fact is, *"55% say existing tools are ineffective in detecting modern threats, including AI."*

The third article addresses AI cyber attacks through phone devices and calling. Since cyber attacks favor speed, scale and manipulation over technical sophistication, mobile devices are naturally a vector for attack. Also be careful with phones since most devices do not run any form of dedicated mobile security.

As for my personal security, the wifi I use is private with a strong password and I'm using wifi 6 with a firewall on my MacBook Pro. I minimize the risk of scams by staying up to date on the latest version of my apps and software.

Sources

From Instructions
https://www.kindo.ai/blog/the-top-ai-powered-cyber-attacks-in-2025,

https://blog.gigamon.com/2025/07/23/the-alarming-rise-of-ai-powered-cyber-attacks-are-you-seeing-it/

https://federalnewsnetwork.com/commentary/2026/02/ai-powered-mobile-attacks-have-made-device-centric-security-obsolete/

More
https://www.consumerreports.org/money/scams-fraud/texting-and-messaging-scam-attempts-increased-by-50-percent-a1001405682/

https://www.consumerfraudreporting.org/current_top_10_scam_list.php

https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams

https://youtu.be/_V5rd-sG_9E?si=vrF060GKh6zwkmHf

https://www.gigamon.com/content/dam/resource-library/english/solution-brief/sb-gigamon-genai.pdf