T2025_27 Monitor for Signs of Cryptojacking and Unauthorized Cryptomining (October 7th, 2025)

Cryptojacking is a stealthy attack where criminals hijack your computer's CPU/GPU to mine cryptocurrency without your consent, causing slow performance, overheating, higher power bills, and hardware wear. Watch for unexplained high resource use at idle, loud fans, or sluggishness. Check Task Manager (Windows) or Activity Monitor (Mac) for suspicious processes. Protect yourself by using browser anti-mining extensions, keeping antivirus updated, scanning regularly, avoiding untrusted sites/downloads, and (for organisations) monitoring network traffic for connections to mining pools and using endpoint detection to flag abnormal CPU patterns.

References

- Malwarebytes. (n.d.). What is cryptojacking and how to prevent it. Malwarebytes Labs. Retrieved September 29, 2025, from https://www.malwarebytes.com/cryptojacking

- Vectra AI. (n.d.). Cryptomining Attacks and How to Detect Them. Vectra AI. Retrieved September 29, 2025, from https://www.vectra.ai/attack-techniques/cryptomining