Incident handler's journal

Date: 18/07/2024	**Entry: 1**
Description	Investigated a phishing alert with a malicious attachment..
Tool(s) used	Email analysis tools, Hash verification tool
The 5 W's	**Who caused the incident?** Def Communications <76tguyhh6tgftrt7tg.su> **What happened?** A phishing email with a malicious attachment was received. **When did the incident occur?** July 20, 2022, at 09:30:14 AM. **Where did the incident happen?** On the recipient's computer system. **Why did the incident happen?** The email aimed to trick the recipient into downloading a malicious attachment.
Additional notes	The email contained grammatical errors and an unusual attachment name. The attachment hash was confirmed malicious.