Incident handler's journal

Date: September 20, 2024	**Entry:** #2
Description	An employee received an email with a password-protected spreadsheet attachment, and the password was included in the email. After downloading the file and entering the password, the employee unknowingly triggered a malicious payload, which was executed on their computer.
Tool(s) used	• VirusTotal • Pyramid of Pain
The 5 W's	• **Who:** A malicious actor • **What:** An unauthorized executable file • **When:** About 1:10 p.m. • **Where**: At a financial services company • **Why**: The employee was tricked into executing a malicious file delivered through a phishing email, leading to a security breach.
Additional notes	- Should the company consider terminating the employee for their involvement in the security breach? - What preventive measures and protocols should the company implement to mitigate the risk of similar attacks in the future?