Incident handler's journal

DATE->(DD/MM/YY)

Date: 17/09/23	**Entry:Number 2** **Ticket ID:A-2703**
Description	-Ticket submission was submitted reporting on a potential download of malware via phishing attempt. Email targeted human resources claiming to be from Clyde West with an interest in a open infrastructure engineer role. -File hash was found to be a match for a trojan virus(TotalVirus)
Tool(s) used	VirusTotal.com was used in determining if file is a known malicious file SHA256sum used to calc the hash of the potential malware file
The 5 W's	Capture the 5 W's of an incident. • **Who ->** File was opened by HR employee, sender is unknown(pseudonym Clyde West) • **What ->** Phishing email was open and attachment was opened, running he virus • **When** ->This occurred on July 20, 2022(date of writing 17/09/23) • **Where** -> Event occurred on the endpoint machine of a HR employee in the Inergy HR department • **Why** -> Event happened due to a phishing email sent to trick the HR employee
Additional notes	Additional training for employees may be needed to ensure that employees can spot a targeted phishing email Updating the firewall to block the IP address/follow up with security manager is needed

Need another journal entry template?

If you want to add more journal entries, please copy one of the tables above and paste it into the template to use for future entries.

Reflections/Notes: Record additional notes.