Incident response report

An incident response report for a multimedia company which experienced a Denial of Service Attack.

Summary	At 2:20pm on Monday July 3, 2023, a member of the HR team reported to the IT Support Officer that she has not been able to access her work account. She has been locked out of her account. However, the network logs indicate that her account has been accessing the employees' records in the employees' database. From her report, she received an email from someone purporting to be the HR Manager asking her to click on a link to a fake website, and login to her account to access confidential HR documents which can not be shared through email. We believe that the attacker used this technique to steal the employee's credentials and later impersonated her to gain access to the network and company records. The attacker, after accessing the employee database, manipulated some of the records. We have received complaints from other employees that some of their records have been altered while others have been deleted.
Identify	The incident response team audited the systems, devices, access policies and password policies involved in the attack to identify the gaps in security. It was discovered that the threat actor used the malicious site to trick the employee to release her login credentials and later used such details to access and manipulate the employee database.
Protect	The security team has implemented new authentication policies to prevent future attacks: multi-factor authentication (MFA), limited failed login attempts to three, and trained all employees on how to protect login credentials, and how to identify malicious emails. The team will implement a new protective

	firewall configuration and invest in an intrusion prevention system (IPS).
Detect	To detect new unauthorized access attacks in the future, the team will use a firewall logging tool and an intrusion detection system (IDS) to monitor all incoming traffic from the internet. We will also use Splunk to monitor and analyze the company's logs.
Respond	The security team deactivated the compromised employee account. We updated our access control policy and provided training to all employees on how to secure login credentials, and identify suspicious emails. We informed upper management of this event and they will also need to inform law enforcement and other organizations as required by local laws.
Recover	The team will restore clean data from last night's full database backup. Employees have been informed to re-enter all the data that we added to the database after the last system backup.