Incident report analysis

Summary	This morning, an intern reported to the IT department that she was unable to log in to her internal network account. Access logs indicated that her account has been actively accessing records in the customer database, even though she is locked out of that account. The intern indicated that she received an email this morning asking her to go to an external website to log in with her internal network credentials to retrieve a message. A couple of other employees have noticed that several customer records are either missing or contain incorrect data.
Identify	I believe that this was a spear phishing attack as the intern was tricked into entering login credentials into a site from a suspicious link. The intern's login and password were obtained by a malicious attacker and used to access data from our customer database. Upon initial review, it appears that some customer data was also deleted from the database. We then audited the systems, devices, and access policies involved in the attack to identify the security gaps.
Protect	We have implemented new authentication policies to prevent future attacks: multi-factor authentication (MFA), login attempts limited to three tries, and training for all employees on how to protect login credentials. We also implemented a new password policy. Additionally, we will implement a new protective firewall configuration and invest in an IPS.
Detect	To detect new unauthorized access attacks in the future, the team will use a firewall logging tool and an (IDS) to monitor all incoming traffic from and to the internet.

Respond	We immediately disabled the intern's network account. We provided training to interns and employees on how to protect login credentials in the future. We informed upper management of this event and they will contact our customers by mail to inform them about the data breach. Management will also need to inform law enforcement and other organizations as required by local laws to improve collaboration.
Recover	We were able to recover the deleted data by restoring the database from last night's full backup. We have informed staff that any customer information entered or changed this morning would not be recorded on the backup. So, they will need to re-enter that information into the database once it has been restored from last night's backup.