**Incident report analysis Brenner Financial Services**

|  |  |
| --- | --- |
| **Summary** | Employees received emails purportedly from a trusted financial institution, requesting them to update their login credentials.  Some employees unknowingly provided their credentials by clicking on the links provided in the emails. |
| Identify | The incident management team instantly started evaluating what employees sent their credentials to the unknown source. Identify which internal or external teams were involved in the initial response. |
| Protect | To protect against similar incidents in the future, especially in the context of a phishing attack, it's important to implement a combination of technical controls, user awareness training, and organizational policies. Multi Factor Password authentication will be required for all employees in the future. |
| Detect | To detect something like this in the future, the team will be implementing a firewall to detect unwanted requests from outside sources. |
| Respond | The team went ahead and disabled the accounts associated with the employees who gave out their credentials. They do this so they can get to the bottom of this before giving them access again. Changing of credentials is going to be required for the employees, as well as a multi factor authentication. |
| Recover | The team will recover any of the data that had been breached due to the credentials being given to an outside source. Once this has been achieved things should go back to normal. |