Risks and Potential Impacts (In Increasing Order of Risk Level)

* Credential Theft
* Data Breach
* Identity Theft

Investigation Process

From the scenario given, I extracted and noted vital information in this format:

* Case Title: Suspicious Email
* From: Infosec Department
* To: Employees
* CTAs: 1. Click on a Link 2. Change Password

Then, I went on to gather hypothetic findings from the given information.

Hypothesis

It is very likely the sender’s address was spoofed. Using an official or known email address would convince some employees that the mail is actually from the InfoSec department.

Also, the use of a link sent via email rather than official in-house memos instructing employees to change their passwords via their accounts or dashboards themselves indicates the likelihood of a phishing attack.

All these were mere speculations, but after critical analysis of the presented scenario, I arrived at a final conclusion.

Conclusion

The use of the term “allegedly” indicates that the employees were not informed or aware of any existing policy or corporate protocol that involves changing passwords via links sent through emails.

The fact that it seemed suspicious and they went ahead to report, further confirms that it is indeed a phishing email with a spoofed sender’s address.

Recommended Containment Plan

An in-house assessment should be carried out to identify employees who have clicked on the link and inputted their credentials. These set of employees should have their devices contained and isolated from the organization’s network.

Further analysis and investigation could be carried out on this isolated network by taking a sample of the email and analyzing its header.

Email header analysis needs to be carried out in order to get the actual IP address of the sender and block it from gaining access to the organization’s corporate network. i.e. Firewalls, VPNs, Proxy Servers, etc should create an alert when such IP address tries to send an email to anyone on the corporate network.

Recommended Recovery Plan

Send an official in-house memo to all head of departments to instruct their subordinates not to click any link sent via mail without confirmation of authenticity from the InfoSec department via corporate channels.