# FOUNDATION: PHISHING ATTACKS

**What are phishing attacks?**

Phishing has become a common method of attacks on small start-up companies. Phishing preys on the gullible and careless nature of people. Attackers send links and attachments disguised as legitimate emails or messages to entice people to click on certain links or respond to messages sent by the attacker. By responding to certain messages or clicking on sketchy links, employees have given the attacker sensitive information about the company which could include bank account details, personal information or undisclosed plans of the company. (Content+Cloud, 2023)

Firms can fall victim to this in several different ways. they include

* **Bulk Phishing:** This occurs when the attacker sends a bulk of personalised emails to several members of the company. Employees tend to fall victim to this method most of the time. Since the emails are sent to all employees, they believe its legitimate and go on to download unsafe attachments and sketchy links
* **Whaling**: This occurs when the primary victims of the attack are high level officials of the company. This is probably the most effective way in which attackers can steal vital information from the company.
* **Clone phishing:** This is when the attacker disguises sketchy links in emails similar to previous ones received by the employee. Since the original email was legitimate, the employee is immediately assured that the one sent by the attacker is also safe to open.

# REFERENCE LIST

* Content+Cloud (2023). *Defence and Protection from Phishing Attacks*. [online] Content+Cloud. Available at: https://contentandcloud.com/how-to-defend-against-types-of-phishing-attacks/ [Accessed 27 Nov. 2023].