Whaling

Whaling is a highly-targeted phishing attack that looks to target individuals within management positions in an organization, often C-level executives, due to the wealth of information they have access to, and that stereotypically they are not highly educated around cybersecurity and phishing. Targets often include:

- **Chief Operations Officer (COO)**
- **Chief Executive Officer (CEO)**
- **Chief Finance Officer (CFO)**

These emails will be refined typically using information gained from open-source intelligence sources, making them more believable for the intended target, increasing the chance they will interact with it. Attacks could attempt to entice the target to download a file that will download malware to the system, try to extract their credentials by sending them a link to a credential harvester, or simply work to extract private or confidential information from the individual using social engineering tactics.

Whaling is one of the most difficult types of phishing to detect because they are sent in very small volumes and are tailored to appear legitimate and not generate red flags that could alert the security tools or team. Education and adoption of senior management, marking external emails by appending the subject line or email body text, and implementing policies such as data loss prevention are some of the best methods to mitigate these threats. Often business executives will have a personal assistant who monitors their mailbox for them – these individuals should be trained specially to detect phishing emails, and report them to the security team, ensuring they are not opened by the business executive.