Business Email Compromise, also known as “Whaling attack” or “the CEO fraud”

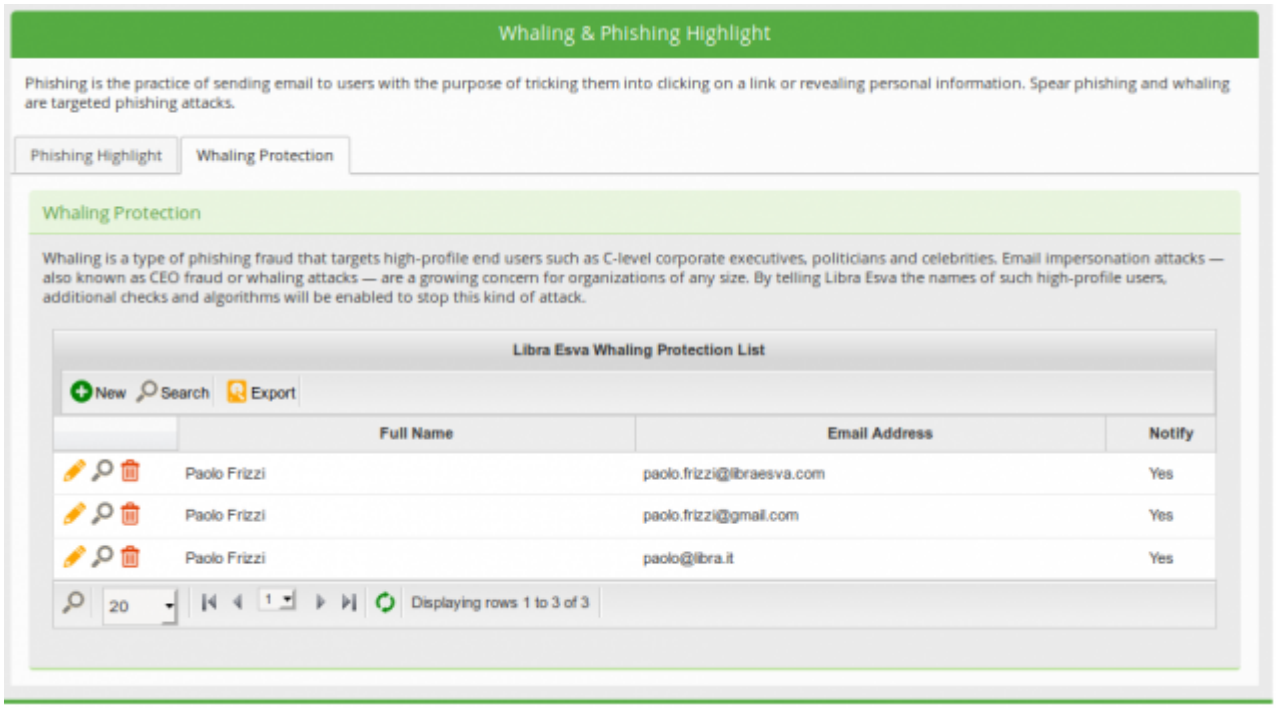
Business email compromise (BEC), Whaling attack, CEO fraud … many different terms to describe a phishing scam where the attacker attempts to impersonate high profile executives.

The attack usually starts with a brief email pretending to come from a C-level executive. “Are you in the office?” is a typical approach.
If the victim replies, then the attacker knows that his email slipped through the defenses and that the victim didn’t spot the scam. The attack can now proceed toward the final target: a wire transfer or divulging sensitive data.

From an email security perspective, this kind of attack is particularly difficult to block because the emails do not have links or attachments, they are brief, the messages use a semantic that is common in business emails.

The number of these attacks is quickly rising and it is reaching companies of all sizes. It is also being semi-automated, at least for the initial email approach. Huge losses have been caused by this type of targeted attacks.

Libraesva designed a specific engine in order to intercept these attacks. The required configuration is minimal: the names and the legit email addresses of the company executives. Email addresses on external email providers are supported as long as the emails are DKIM-signed in order to protect against spoofing.



Impersonation can be performed by leveraging a wide range of techniques, both technical and social. Name similarities, domain similarities and more subtle technical tricks are all checked by our engine. Knowing the legit names and email addresses of the C-level executives, the engine can perform deep content analysis that would not be feasible to be performed on all messages.