**PHISHING**

1. Phishing is a social engineering technique where an attacker masquerades as a legitimate entity with which the victim might do business in order to prompt the user to reveal some confidential information (very frequently authentication credentials) that can later be used by an attacker. Phishing is essentially a form of information gathering or "fishing" for information [1].
2. (Spear Phishing) An attacker targets a specific user or group with a Phishing attack tailored to a category of users in order to have maximum relevance and deceptive capability. Spear Phishing is an enhanced version of the Phishing attack targeted to a specific user or group. The quality of the targeted email is usually enhanced by appearing to come from a known or trusted entity. If the email account of some trusted entity has been compromised the message may be digitally signed. The message will contain information specific to the targeted users that will enhance the probability that they will follow the URL to the compromised site. For example, the message may indicate knowledge of the targets employment, residence, interests, or other information that suggests familiarity. As soon as the user follows the instructions in the message, the attack proceeds as a standard Phishing attack [2].
3. Phishing is misrepresentation where the criminal uses social engineering to appear as a trusted identity. They leverage the trust to gain valuable information; usually details of accounts, or enough information to open accounts, obtain loans, or buy goods through e-commerce sites [3].

**REFERENCES**

1. <https://capec.mitre.org/data/definitions/98.html>
2. <https://capec.mitre.org/data/definitions/163.html>
3. <https://www.owasp.org/index.php/Phishing>