Blue Team Level 1 Certification (Standard)

- ~~Spam~~
- ~~False Positives~~
- ~~Credential Harvester~~
- ~~Social Engineering~~
- ~~Vishing, Smishing~~
- ~~Whaling~~
- ~~Malicious Files~~
- ~~[Video] Types of Phishing Attacks & Examples~~
- ~~Lab) Categorizing Phishing Emails~~
- ~~Activity) End of Section Review, Phishing Emails~~

~~PA3) Tactics and Techniques Used~~
12 Topics | 2 Quizzes

~~PA4) Investigating a Phishing Email~~
8 Topics | 2 Quizzes

PA5) Analysing URLs, Attachments, and Artifacts
8 Topics | 1 Quiz

PA6) Taking Defensive Actions
12 Topics | 1 Quiz

PA7) Report Writing
7 Topics | 1 Quiz

PA8) Phishing Response Challenge
3 Topics | 1 Quiz

THREAT INTELLIGENCE DOMAIN

TI1) Introduction to Threat Intelligence
7 Topics

TI2) Threat Actors & APTs
6 Topics | 2 Quizzes

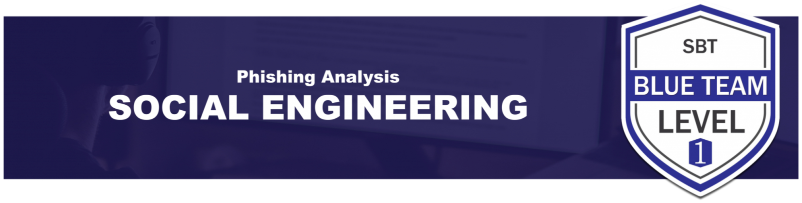
TI3) Operational Threat Intelligence
7 Topics | 1 Quiz

TI4) Tactical Threat Intelligence
7 Topics | 2 Quizzes

TI5) Strategic Threat Intelligence

Social Engineering

Blue Team Level 1 Certification (Standard) > PA2) Types of Phishing Emails > Social Engineering COMPLETE



Social engineering is the practice of exploiting a human as opposed to a system, using psychological methods in order to get them to complete actions that they wouldn't normally do, such as disclosing confidential information, allowing someone into a restricted area without proper authorization, or transferring money to an unverified account. This is no different with phishing. Malicious actors can convince employees that they are someone they know, or even someone in a higher position that has more power than them, and use this deception to get them to complete certain tasks. **Phishing is a social engineering attack.**

Commonly used social engineering tactics in phishing emails include:

- Convincing the recipient to reply to an attacker's initial email (recon emails).
- Convincing the recipient to transfer money by posing as the CEO, CTO, CFO, or another employee on the executive board.
- Convincing the recipient to provide the attackers with information that is confidential or private by posing as the data subject or someone in a higher position within the company.

Essentially all phishing emails will utilise some social engineering techniques, because phishing attacks aren't trying to exploit or hack technical systems, they're going after the human behind the screen that is opening the email. Whether the malicious actor is trying to pressure the target into completing an action by creating a sense or authority or urgency, or impersonating someone the target knows, playing on principles of trust, effective social engineers can make people do unexpected things.

We have also linked this video in the Vishing and Smishing lesson later in this section, but we believe it really reinforces what social engineering is. We highly recommend you watch it! View the video on YouTube.

Previous Topic | Back to Lesson | Next Topic