

Blue Team Level 1 Certification
(Standard)

SECURITY FUNDAMENTALS DOMAIN

- ✓ Introduction to Security Fundamentals
 - 1 Topic
- ✓ Soft Skills
 - 7 Topics
- ✓ Security Controls
 - 5 Topics 1 Quiz
- ✓ Networking 101
 - 6 Topics 1 Quiz
- ✓ Management Principles
 - 4 Topics 1 Quiz

PHISHING ANALYSIS DOMAIN

- ✓ PA1) Introduction to Emails and Phishing
 - 7 Topics 1 Quiz
- ✓ PA2) Types of Phishing Emails
 - 10 Topics 2 Quizzes
- ✓ PA3) Tactics and Techniques Used
 - 12 Topics 2 Quizzes
- ✓ Section Introduction, Tactics and Techniques
- ✓ Spear Phishing
- ✓ Impersonation
- ✓ Typosquatting and Homographs
- ✓ Sender Spoofing
- ✓ HTML Styling
- ✓ Attachments
- ✓ Hyperlinks
- ✓ URL Shortening Services
- ✓ Use of Legitimate Services
- ✓ Business Email Compromise
- ✓ [Video] Tactics and Techniques & Examples
- Antibot Detection on Testbed

Section Introduction, Tactics and Techniques

Blue Team Level 1 Certification (Standard) > PA3) Tactics and Techniques Used > Section Introduct... **COMPLETE**

Phishing Analysis SECTION INTRODUCTION



This section of the Phishing Analysis domain will introduce you to the tactics and techniques used by malicious actors to try and make their emails as effective as possible. There are a lot of techniques that can be used to make emails seem legitimate, increase the chances of targets interacting with malicious elements, bypassing security features such as emails scanning, or make it harder for security teams to take defensive measures and stop malicious emails being delivered to employee mailboxes.

LEARNING OBJECTIVES

By the end of this section you will have achieved the following objectives:

- Understand the techniques utilized by malicious actors to make emails more convincing to recipients such as: hyperlinks, attachments, impersonation, typosquatting, and email styling.
- Identify the techniques that have been used in real phishing emails.

[< Previous Lesson](#)[Back to Lesson](#)[Next Topic >](#)