

Blue Team Level 1 Certification
(Standard)

- ✓ Section Introduction: Emails and Phishing
- ✓ How Electronic Mail Works
- ✓ Anatomy of an Email
- ✓ **What is Phishing?**
- ✓ Impact of Phishing
- ✓ Further Reading Material: Phishing Analysis
- ✓ Phishing Analysis Glossary
- 📄 Activity: End of Section Review: Emails and Phishing

✓ PA2) Types of Phishing Emails

10 Topics | 2 Quizzes

✓ 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

What is Phishing?

Blue Team Level 1 Certification (Standard) > PA1) Introduction to Emails and Phishing > What is P...

COMPLETE



In order to correctly identify phishing emails, you need to know exactly what phishing is. There are a number of different descriptions for phishing emails out there, so we have created our own that we believe is appropriate:

- **Phishing is the act of sending an email with malicious intent, to coerce recipients into disclosing information, downloading malicious files, or otherwise completing an action that they would not normally do, by exploiting a human using one or more social-engineering techniques.**

In short, phishing is a type of email-based attack, where malicious actors are actually attacking humans instead of computer systems, in order to get them to do something they normally wouldn't. Examples include giving out their account credentials, downloading malware, transferring money, disclosing information, and more.

While phishing is primarily email-based, there are other attacks that use voice calls (Vishing) and SMS or text messages (SMiShing). We will cover these in a future lesson.

< Previous Topic

Back to Lesson

Next Topic >

Privacy & Cookies Policy

