

Blue Team Level 1 Certification
(Standard)

- ☒ 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
- ☐ Activity: Reporting on Tactics Used
- ☐ Activity: End of Section Review: Tactics and Techniques

☒ 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 1 Quiz

☐ TI5) Strategic Threat Intelligence

5 Topics 1 Quiz

☐ TI6) Malware and Global Campaigns

6 Topics 1 Quiz

DIGITAL FORENSICS DOMAIN

☐ DF1) Introduction to Digital Forensics

5 Topics

☐ DF2) Forensics Fundamentals

10 Topics 5 Quizzes

☐ DF3) Digital Evidence Collection

8 Topics 1 Quiz

☐ DF4) Windows Investigations

3 Topics 3 Quizzes

☐ DF5) Linux Investigations

4 Topics 2 Quizzes

☐ DF6) Volatility

3 Topics 1 Quiz

☐ DF7) Autopsy

[Video] Tactics and Techniques & Examples

Blue Team Level 1 Certification (Standard) > PA3) Tactics and Techniques Used > [Video] Tactics and Techniques Used

COMPLETE



Transcript

In this video we're going to take a look at some of the common tactics used by attackers to make emails appear more legitimate to increase the chances of the recipient interacting with the email.

The first email we're looking at is a PayPal credential harvester. You can see right away there is very little styling and brand impersonation other than text, but this email is using a hyperlink to send recipients to the credential harvester site.

The second email has some great styling and an image to make it look legitimate and professional, and is also using hyperlinks to redirect recipients to the site as part of an email marketing campaign.

The third email looks a little strange in outlook, but when we open it in Thunderbird it displays correctly and actually looks like a very effectively styled credential harvester that impersonates Amazon really well. Again this email is utilising hyperlinks to send recipients to the malicious login page.

Finally this email is using an attachment which is likely malicious, but has no real styling or impersonation.

You'll have the chance to test your skills at determining what tactics have been used in malicious emails in the next lesson!

4 Topics1 Quiz

SECURITY INFORMATION AND EVENT
MANAGEMENT DOMAIN

SI1) Introduction to SIEM

7 Topics1 Quiz

< Previous Topic

Back to Lesson

Next Lesson >

Privacy & Cookies Policy

