[Video] Tactics and Techniques & Examples

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 Topics | 1 Quiz

SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN

SI1) Introduction to SIEM

7 Topics | 1 Quiz

Previous Topic

Back to Lesson

Next Lesson