Blue Team Level 1 Certification (Standard)
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
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] Types of Phishing Attacks & Examples

Transcript

In this video we're going to take a look at 4 different phishing emails, so you can become more familiar with spotting suspicious indicators and classifying emails properly. The first email that we're looking at is a recon email – we can see that there is no real message in the subject line or the email body text, as this email is simply looking to see if the target mailbox is in use. If the recipient is not a real mailbox, then the attacker will receive an email notification stating that this message was not successfully delivered. Once valid mailboxes have been found, these can be targeted in future phishing attacks.

The second email is a spam email, something that is unsolicited or unwanted and often apart of an email marketing campaign. This specific spam email is themed around bitcoin and how I can apparently make up to £40,000 a month! This spam email is trying to get users to sign up for a bitcoin investment platform. Whilst these emails are often harmless, users should always be careful when clicking links.

The third email is a credential harvester imitating Amazon, claiming that the recipient's Amazon Prime membership is about to expire due to a payment card issue. And it tells the recipient to click the link to update their information. When clicking on the link it presents a fake amazon login portal which will steal any entered information and send it to the attacker.

Finally we have a social engineering email that is trying to convince the recipient to open the attached Microsoft Word file. This file will likely have malicious macros that will download malware to the system once it is opened. These emails can be very damaging

4 Topics | 1 Quiz

SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN

SI1) Introduction to SIEM
7 Topics | 1 Quiz

SI2) Logging
6 Topics | 2 Quizzes

SI3) Aggregation
2 Topics | 1 Quiz

SI4) Correlation
6 Topics | 1 Quiz

depending on what the malware is designed to do, so it is crucial that files from an unknown source are not opened, or should at least be scanned by anti-virus tools or sandboxed.

You'll have the chance to categorize emails in the next lesson!

Previous Topic

Back to Lesson

Next Lesson

Privacy & Cookies Policy

Privacy - Terms