

Blue Team Level 1 Certification
(Standard)

✓ 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

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

○ T11) Introduction to Threat Intelligence

7 Topics

○ T12) Threat Actors & APTs

6 Topics 2 Quizzes

○ T13) Operational Threat Intelligence

7 Topics 1 Quiz

○ T14) Tactical Threat Intelligence

7 Topics 1 Quiz

○ T15) Strategic Threat Intelligence

5 Topics 1 Quiz

○ T16) Malware and Global Campaigns

6 Topics 1 Quiz

DIGITAL FORENSICS DOMAIN

Hyperlinks

Blue Team Level 1 Certification (Standard) > PA3) Tactics and Techniques Used > Hyperlinks

COMPLETE

Phishing Analysis
HYPERLINKS

A hyperlink is a webpage URL that is embedded into text, a button, or an image. When clicked, it will open the recipient's default browser, and navigate to the webpage for them. Hyperlinks are used when the attacker wants to direct the target to a web resource, such as a malicious file download, a page with a fake login portal acting as a credential harvester, or other content as part of their phishing attack. Hyperlinks can be coupled with additional techniques such as redirected targets to a typo squatted domain, or use URL shortening services to disguise the true destination of the link. It is important that employees are trained not to click on suspicious links, and security teams should always be cautious when analyzing and handling phishing emails, as one wrong click can lead to an infected system. Later in this domain, we will cover how to protect employees from malicious links, within the **Taking Defensive Measures** section.

But why is something that seems so simple, so effective? This is because almost all emails contain links, so people are used to seeing them, and clicking on them! Attachments are more uncommon which is why they often raise more suspicion. Hovering over text or an image that is hyperlinked will often reveal the URL that will be visited if it is clicked. If not, the email can be opened in a text editor and the URL can be safely retrieved by looking for HTML anchor tags <a> . A friendly reminder that phishing emails should only be analyzed and opened in a virtual machine or on a "dirty" system.



Your account has been limited.

Hello, Customer

We've limited your account

After a recent review of your account activity, we've determined you are in violation of PayPal's Acceptable Use Policy. Please log in to confirm your identity and review all your recent activity

You can find the complete PayPal Acceptable Use Policy by clicking Legal at the bottom of any PayPal page.

Reactive My Account

<https://semangat-gajian.uniformperception.com/QeDdg>Having trouble logging in? [Sign up now](#)

EXAMPLE WALKTHROUGH

Looking at another PayPal-themed phishing email, we can see that the hyperlinked button definitely isn't taking us to PayPal.com.

Payment Receipt.

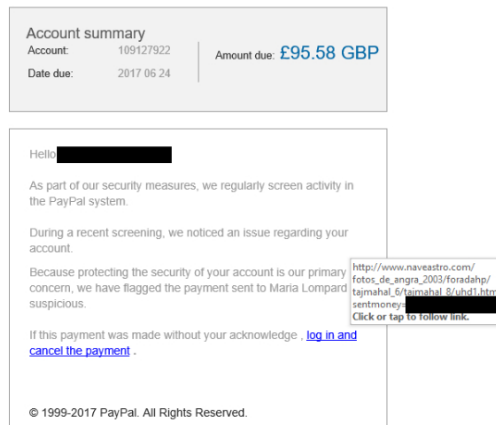
receipt@intl.paypal.com <qgrv@techgenix.com>
To: [REDACTED]

Reply Reply All Forward ...

Sat 24/06/2017 19:34

Payment Receipt

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	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
SI5) Using Splunk	5 Topics 2 Quizzes
INCIDENT RESPONSE DOMAIN	
IR1) Introduction to Incident Response	8 Topics 1 Quiz
IR2) Preparation Phase	10 Topics 2 Quizzes
IR3) Detection and Analysis Phase	7 Topics 4 Quizzes
IR4) Containment, Eradication, and Recovery Phase	5 Topics 1 Quiz
IR5) Lessons Learned and Reporting	7 Topics
IR6) MITRE ATT&CK	13 Topics 2 Quizzes
BTL1 EXAM	
Exam Preparation	
Using RDP and SSH	
How to Start Your Exam	



Opening this email in a text editor, we can find the HTML body content, and identify where the hyperlink is. Below we will explain how hyperlinks actually work using HTML anchor tags.

```
<p style="text-align: left; padding-bottom: 0px; line-height: 19px; padding-left: 0px; padding-right: 0px; font-family: 'Helvetica', 'Arial', sans-serif; color: #999999; font-size: 1em; font-weight: normal; padding-top: 0px; align="left">If this payment was made without your&nbsp;acknowledge , <a href="http://www.naveastro.com/Fotos_de_Angra_2003/foradap/tajmahal_6/tajmahal_8/uhd1.html?sentmoney=30">log in</font> and cancel the payment</a> <strong></strong></p></td></tr><tr>
```

If we wanted to use HTML to hyperlink the word Google to Google.com, we could use the following HTML code:

```
<p> Need to access Google? <a href="https://www.google.com"> Just click this text! </a></p>
```

- **<p>** Paragraph tag declares that we want to print text to the screen.
- **"Need to access Google?"** Non-hyperlinked text.
- **** Anchor tag used to hyperlink anything between the opening anchor tag and the closing tag ****, and states the address to link.
- **"Just click this text!"** Hyperlinked text.
- **** Closes the hyperlink.
- **</p>** Closes the paragraph.

Below we have taken a screenshot of an email we made, and how the HTML looks within a text editor.



< Previous Topic

Back to Lesson

Next Topic >

Privacy & Cookies Policy

