



HTML Styling

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

COMPLETE



HTML styling is where code and images are used to style an email. This is used by legitimate emails to provide a more visually attractive design, making the email appear more professional. This is a screenshot of a legitimate email from Amazon, which uses styling to produce a branded and eye-catching email. We can implement logos, hyperlinks, different colored text, buttons, tables, and more. HTML styling is typically observed with credential harvesters, as they are trying to impersonate an organization, and legitimate emails from these senders use branding and email templates to keep everything neat.



Order Confirmation

Hello [REDACTED]

Thank you for shopping with us. We'll send a confirmation when your item ships.

Details

Order #113-6019199- [REDACTED]

Arriving:
Tuesday, July 21

Ship to:

[REDACTED]

View or manage order

Total Before Tax:	\$17.99
Estimated Tax:	\$1.26
Order Total:	\$19.25

We hope to see you again soon.

Amazon.com

Top picks for you

VCE 2-Pack 1 Port Ethernet Wall...	\$11.89	prime
------------------------------------	---------	-------



Romuto iPad Air 2 Screen Protector...	\$13.99	prime
---------------------------------------	---------	-------

The payment for your invoice is processed by Amazon Payments, Inc. P.O. Box 81226 Seattle, Washington 98108-1226. If you need more information, please contact (866) 216-1075

By placing your order, you agree to Amazon.com's [Privacy Notice](#) and [Conditions of Use](#). Unless otherwise noted, items sold by Amazon.com are subject to sales tax in select states in accordance with the applicable laws of that state. If your order contains one or more items from a seller other than Amazon.com, it may be subject to state and local sales tax, depending upon the seller's business policies and the location of their operations. Learn more about [tax and seller information](#).

This email was sent from a notification-only address that cannot accept incoming email. Please do not reply to this message.

Below is a screenshot of an Amazon credential harvester email, that is using very similar styling to impersonate the brand, and make it look more legitimate to victims. The styling has a huge impact on how believable emails are, and the one below looks pretty damn good.

[Please update your payment information](#)

Your Amazon .co.uk | Today's Deals | Gift Cards

Hello,

Your Amazon Prime membership is set to renew on May 5 2020 GMT. However, we've noticed that the card associated with your Prime membership will expire before your renewal date. Please [click here](#) to log-in to your account and update your default payment method information.

To prevent interruption of your benefits, we will try charging other active cards associated with your Amazon account if we can't charge your default card. If we are still unable to process the charge for your membership fee, your Amazon Prime benefits will be paused. If you have any questions and wish to contact us, [click here](#).

Thank you,

Blue Team Level 1 Certification (Standard)

Introduction to BTL1

Welcome to Blue Team Level 1

4 Topics

Lab and Forum Access

SECURITY FUNDAMENTALS DOMAIN

Introduction to Security Fundamentals

1 Topic

Soft Skills

7 Topics

Security Controls

5 Topics 1 Quiz

Networking 101

6 Topics 1 Quiz

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

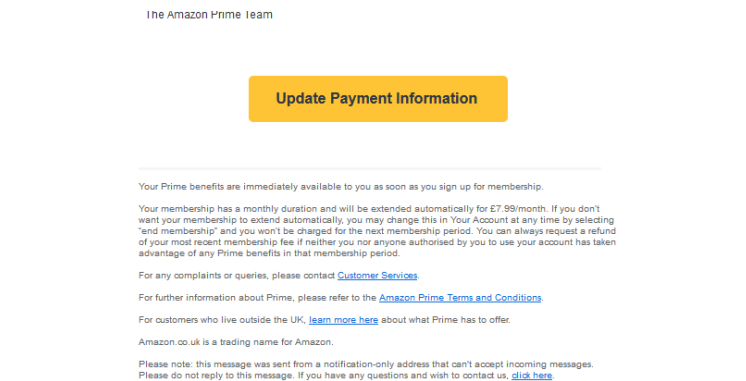
PA8) Phishing Response Challenge

3 Topics 1 Quiz

THREAT INTELLIGENCE DOMAIN

TI1) Introduction to Threat Intelligence

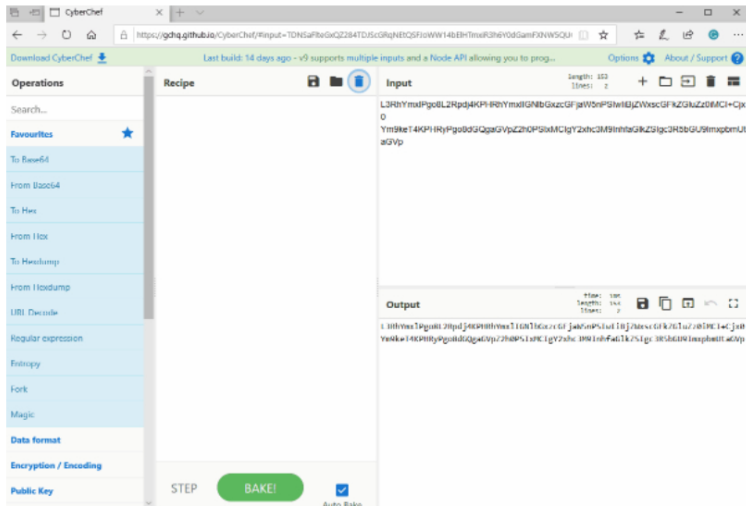
7 Topics
T12) Threat Actors & APTs
6 Topics 2 Quizzes
T13) Operational Threat Intelligence
7 Topics 1 Quiz
T14) Tactical Threat Intelligence
7 Topics 1 Quiz
T15) Strategic Threat Intelligence
5 Topics 1 Quiz
T16) Malware and Global Campaigns
6 Topics 1 Quiz
DIGITAL FORENSICS DOMAIN
DF1) Introduction 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



Now let's take a look at the HTML from the .eml file. We can see on line 146, it tells us that the email is encoded in base64. This is a pretty common practice, especially with legitimate emails, but sometimes emails will be in plaintext and not require decoding.



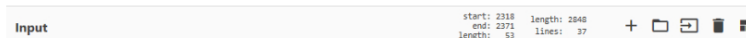
We can use [CyberChef](#), an online tool by GCHQ, to decode it using the "Base64 Decode" recipe. This will transform the encoded text into plaintext that we can read.



Below is a screenshot of this Amazon credential harvester. In the bottom pane you can see some of the decoded content. Common HTML tags include:

- `<a> ` – Anchor tags allow for items (such as text or buttons) to be hyperlinked to a web resource.
- `<table> </table>` – Table tags can be used for spacing or tables that include text or images. These are typically used to structure an email into different sections.
- ` ` – Bold tags can allow text to be **formatted as bold**.
- `<i> </i>` – Italic tags can allow text to be *formatted as italic*.
- `<u> </u>` – Underline tags can allow text to be underlined.

You can view a long list of HTML tags that can be used [here](#).



- Exam Preparation
- Using RDP and SSH
- How to Start Your Exam

aGikZSlgc3R5bGU9ImZbnQZmFtaWx5OkFyaWV5LEhibH2idGjYySxZYW5ZLNXNcmlmOyBmb250
LXNpemU6MTBweDsgbGZS1oZWlnaHQ6MTZweDsgY29sb3I6IzY2NjY2Nii+CjxhIHRhcmddD0I
X2J5YW5rIByZWw9Im5v3BltbmYyIG5vcmVmZkXyZXllGRhdGEtYXV0aD0VmVyaWZpZWQilG9y
aWdpbmFsc3JpPSJodHRwczovL3d3dy5hbWV6b24uY28udWsvZ3Avci5odG1sPOM9MkYwUFPwVTIK
TUFJVyZhbXA7SzlTU54MVGV0pVSTEmYW1wO009dXJuoNuJ0bjptc2c6MjAyMDAzMTkwMzUyMDVI
ZTdlNjQzNTUxMGMOOGU2YTjY2RlNjU1YmIwZDh3b24uY28udWsvZ3Avci5odG1sPOM9MkYwUFPwVTIK
PUMmYW1wO1U5aHR0cHMIM0EIMKYIMKZ3d3cuYW1hem9uLmNvLnVrJTJGZ3A1MkZwcmtZWNBnRy
YWwIM0ZpZSuzRFVURjgIMjYzZWZlJTNEcGVmMzI1MTAwMV8zNzQyMDU0OTF6GVYnBfc3Vic2Ny
aXB0aW9uUgXhbkEX3VwZGF0ZS2hbXA7SD1SQ0ZVVUFFVTRPQVBWSkt1VN0EYsfZCvkc3VDBBBJmFt
cDhYZWZpXW8kbGZlNTEwMDFMzc0MjA1ODIox3B0X2JwX3N1YnNjcmIwZGlvb3B5W5JRf91cGRh
dGUlIHNoYXNoPSJDbolzdnl3ZnQ00wMUZOTnl0hncjksTFzd1gmIzQzO29nWWhPcnFQVYy
NDMTZ1FVeWExeGFKNmF3OFJODZjZjEjM0MzqbXky1JUQVRUZ1NPUGlqOTZlOVRZlpNTXEv
ZWVwemJONF0ZDZnZngyUXUxRjZS0FMScjcxIM0Mz4cCYjNDMT7Yy9LeTQ3IiBzdHsZT0Y29sb3I6IzY2NjY2
MVZxUVU3NTBkNmRnZVsaHjTjZGRcnRkNyYjNDMT7Yy9LeTQ3IiBzdHsZT0Y29sb3I6IzY2NjY2
NjsgdGVydgC1kZWVncmF0aW5uOnlvZGVyGyGZuZSI+UGxYXNlICB1cGRhGUGeV91cBwYXlZW50
IGluZm9ybWwF0aW9uPC9hPjwvZGZlPgo8ZGZlGikPSj4X3Nj3B0ZC1jb250ZW50Ij4KPHRhyxmi
IGNlbGxwYWRkaW5nPSiwiBjZVwsc3BhY2luZ20lMClgd2lkdG9lIjUwMClgY2h3c3M9inhfd2lk
dGZlMzAiPgo8dGVzHk+Cjx0c4KPHRiHdpZHRoPSi1MDAIGFsaWduPSJjZV50ZXllIGNsYXNz
PSJ4X2Jsb2NriHfd2lkdGZlMzAgeF9mdWxsc3RyaXBjIj48L3RkPgo8L3RyPgo8L3RiZHR5Pgo8
L3RhYmxlPgo8L2Rpdj4KPHRhyxmiIGNlbGxzcGFjaW5nPSiwiBjZVwscGFkZGluZ20lMCI+Cjx0
Ym9keT4KPHRyPgo8dGQgaGvpZ2h0PSixMClgY2h3c3M9inhfaGikZSlgc3R5bGU9ImxpbmUtaGVp

```
Output
start: 1739      time: 13ms
end: 1778      length: 2109
length: 29      lines: 29

<a target="_blank" rel="noopener noreferrer" data-auth="Verified" originalsrc="https://www.amazon.co.uk/gp/r.html?
C=2F0PZVU9JHAI&K=KPK81YFWJUI1&M=urn:rtn:msg:20200319035205be7b6435510c48e6a5c7de655bb0p0eu&R=3KR82LYBT00II&
mp;T=C&U=https%3A%2F%2Fwww.amazon.co.uk%2Fgp%2Fprimecentral%3Fie%3DUTF8%26ref_x3Dpe_3351001_374205891_pe_bp_subscrip
ionPlanID_update&H=RCFUUAU40APVJMU7A2HVBVG7T0&ref_pe_3351001_374205891_pe_bp_subscrip
ionPlanID_update&shash="CnXh/7g/vgC02RY98k/Hgr8dI1swX&43;ogYhOrqPV&43;gQYua1xa76aw8RN86cs9D&43;jmr1cRTATTg50PiJ913/EqfZMq/eivzbN4Wtd.
sNx2Qu3F26KAL771&43;8p&43;pF4JulPHmZzPneQgm1VqQU750d6dMduhrcLfQrtd7&43;W/Ky4=" style="color:#666666; text-
decoration:underline">Please
update your payment information</a></div>
<div id="x_scoped-content">
<table cellpadding="0" cellspacing="0" width="500" class="x_width330">
<tbody>
<tr>
<td width="500" align="center" class="x_block x_width330 x_fullstripe"></td>
</tr>
</tbody>
</table>
</div>
<table cellpadding="0" cellspacing="0">
<tbody>
<tr>
<td height="10" class="x_hide" style="line-hei
```

