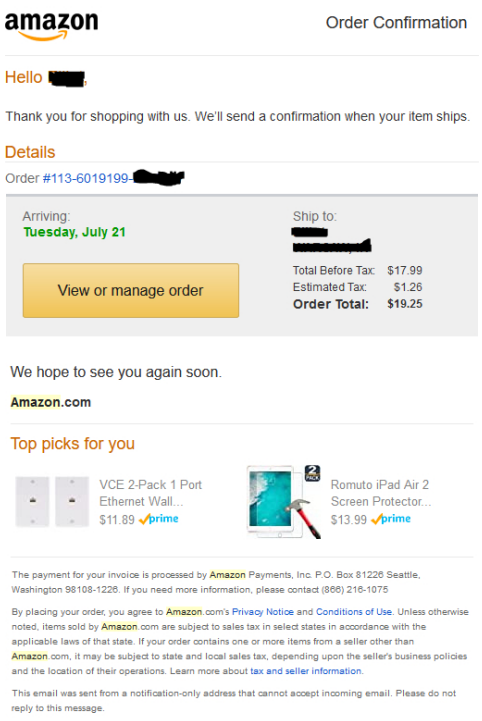
HTML Styling

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.


amazon

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

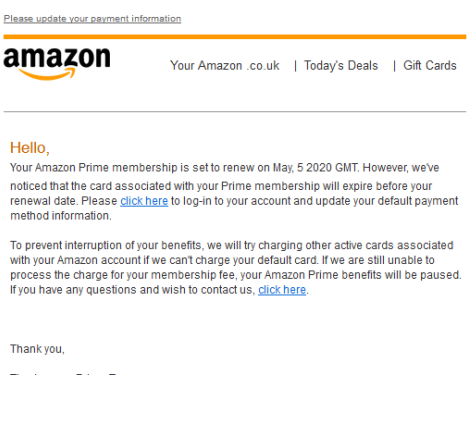
Romuto iPad Air 2 Screen Protector... $13.99 prime

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

amazon

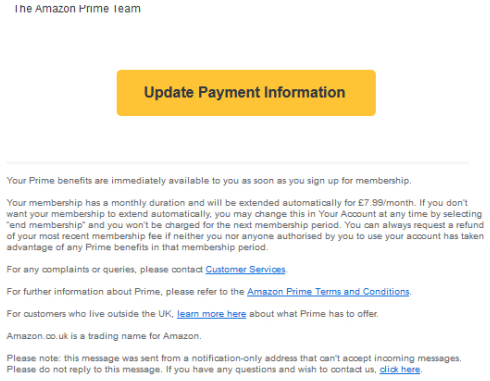
Your Amazon .co.uk | Today's Deals | Gift Cards

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.

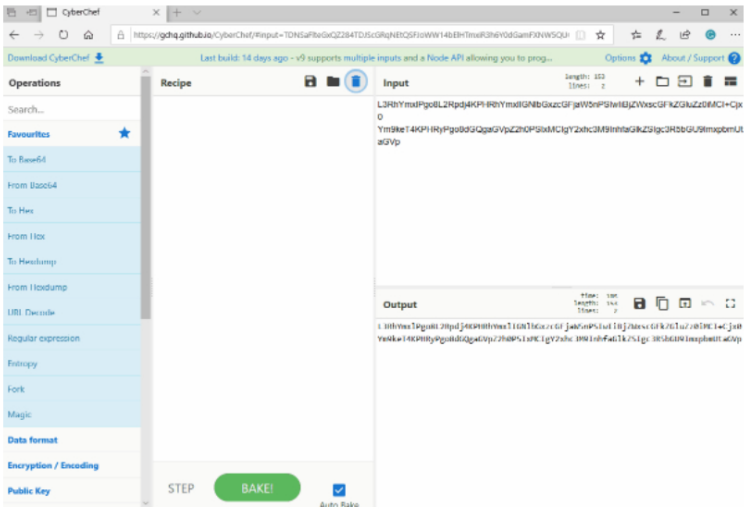
To prevent interruption of your benefits, we will try charging other active cards associated with your Amazon account if we can't charge your default card. If we are still unable to process the charge for your membership fee, your Amazon Prime benefits will be paused. If you have any questions and wish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

Thank you,



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.

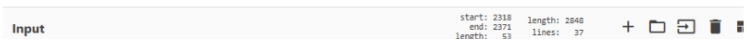
We can use CyberChef, an online tool by GCHQ, to decode it using the "Base64 Decode" recipe. This will transform the encoded text into plaintext that we can read.

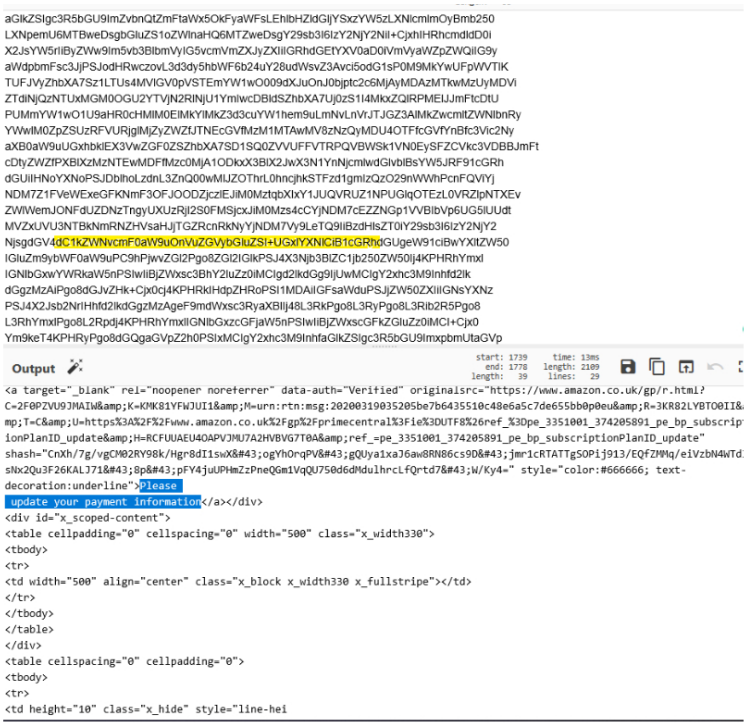


Below is a screenshot of this Amazon credential harvester. In the bottom pane you can see some of the decoded content. Common HTML tags include:

- **<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.





Output

start: 1739 time: 13ms
end: 1778 length: 2109
length: 39 lines: 29

```
<a target="_blank" rel="noopener noreferrer" data-auth="Verified" originalsrc="https://www.amazon.co.uk/gp/r.html?
C=2F0PZVU9JMAIW&amp;K=KMK81YFWJUI1&amp;M=urn:rtn:msg:20200319035205be7b6435510c48e6a5c7de655bb0p0eu&amp;R=3KR82LYBTO0II&
mp;T=C&amp;U=https%3A%2F%2Fwww.amazon.co.uk%2Fgp%2Fprimecentral%3Fie%3DUTF8%26ref_%3Dpe_3351001_374205891_pe_bp_subscrip
ionPlanID_update&amp;H=RCFUUAEU4OAPVJMU7A2HVBVG7T0A&amp;ref_=pe_3351001_374205891_pe_bp_subscriptionPlanID_update"
shash="CnXh/7g/vgCM02RY98k/Hgr8dI1swX&#43;ogYhOrqPV&#43;gQUya1xaJ6aw8RN86cs9D&#43;jmr1cRTATTgSOPij913/EQfZMMq/eiVzbN4WTd
sNx2Qu3F26KALJ71&#43;8p&#43;pFY4juUPHmZzPneQGm1VqQU750d6dMdulhrcLfQrtd7&#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 cellspacing="0" cellpadding="0">
<tbody>
<tr>
<td height="10" class="x_hide" style="line-hei
```


Previous Topic

Back to Lesson

Next Topic