Evading Modern Defenses when Phishing with Pixels

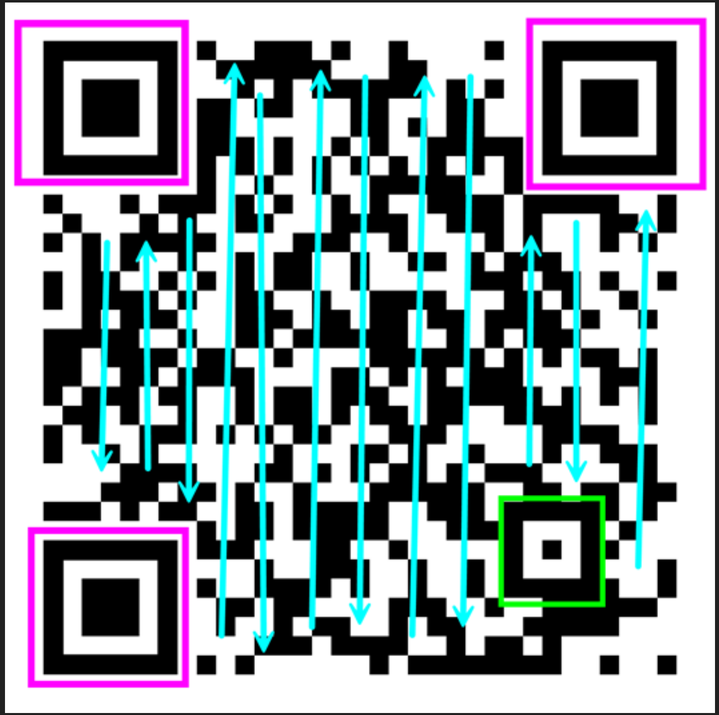
Me, Myself and I

Gameplan

- QR Codes 101
- Phishing with QR Codes
- Detection Engineering
- ***Imageless*** QR Codes (?)
- Profit?
- ***Taking it a step further..***
- QRucible Toolkit

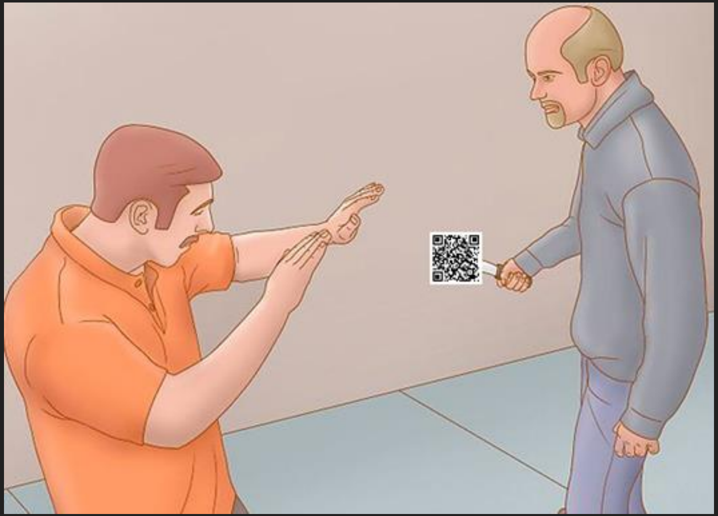
QR Codes 101

- What is a QR (Quick Response) code?
- How does a QR code work?
  - Finder Patterns
  - Alignment Markers
  - Data Modules
  - Error Correction
  - QR Code Versions
- Legitimate use cases of QR Codes

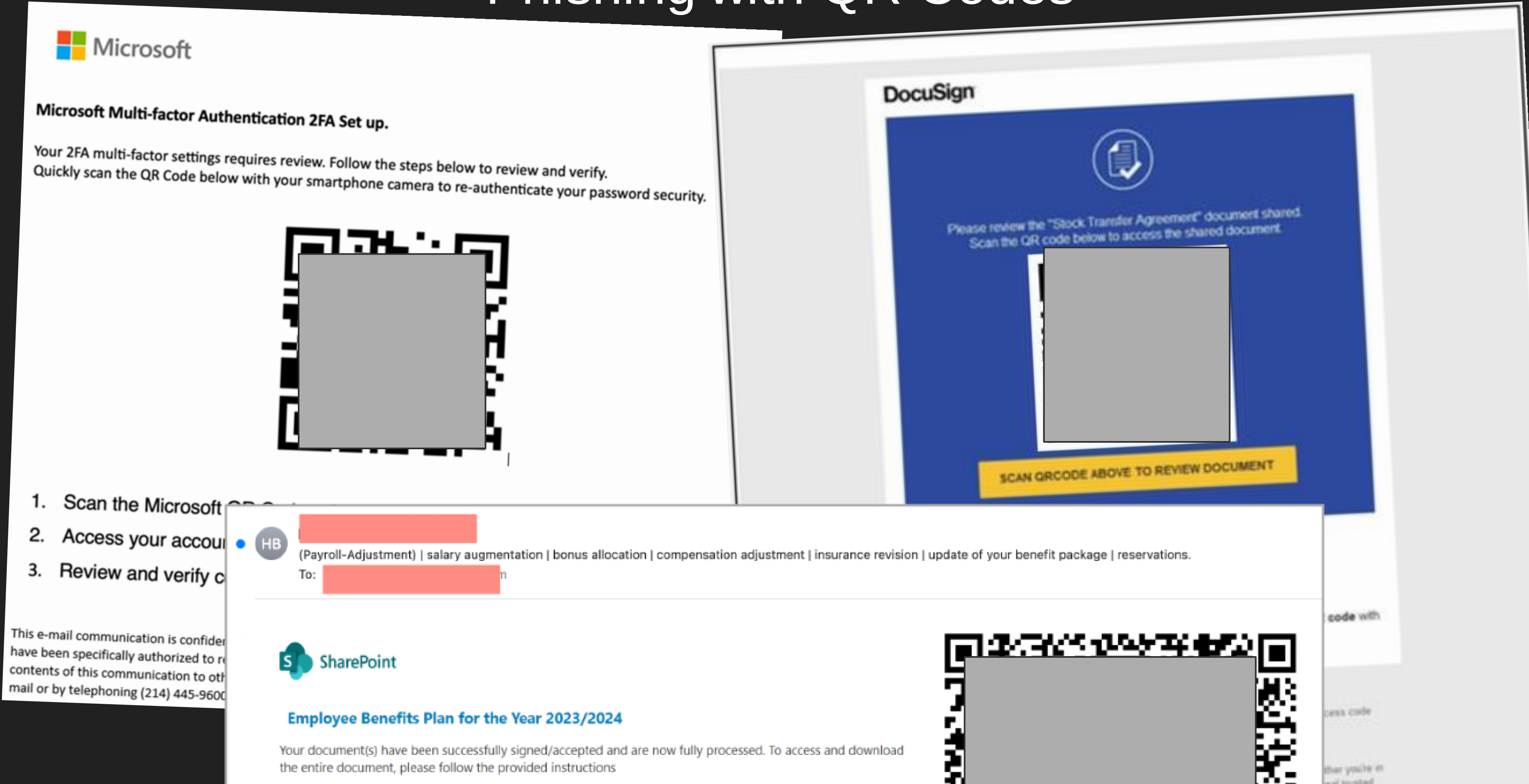


Why do attackers use QR Codes?

- Simple to create and easy to share.
- Not uncommon among non-technical employees
- Evades initial email filters and sandbox solutions
- Conveys a sense of legitimacy to the victim
    - *“Can anyone create an QR code”?*
- Moves the initial landing page onto a mobile device that is commonly less protected



Phishing with QR Codes



Microsoft

Microsoft Multi-factor Authentication 2FA Set up.

Your 2FA multi-factor settings requires review. Follow the steps below to review and verify. Quickly scan the QR Code below with your smartphone camera to re-authenticate your password security.

[redacted]

1. Scan the Microsoft
2. Access your accou
3. Review and verify c

This e-mail communication is confider
have been specifically authorized to r
contents of this communication to oth
mail or by telephoning (214) 445-9600

DocuSign

Please review the "Stock Transfer Agreement" document shared.
Scan the QR code below to access the shared document

[redacted]

code with

cess code

ther you're in
nd trusted

HB [redacted]

(Payroll-Adjustment) | salary augmentation | bonus allocation | compensation adjustment | insurance revision | update of your benefit package | reservations.

To: [redacted]

SharePoint

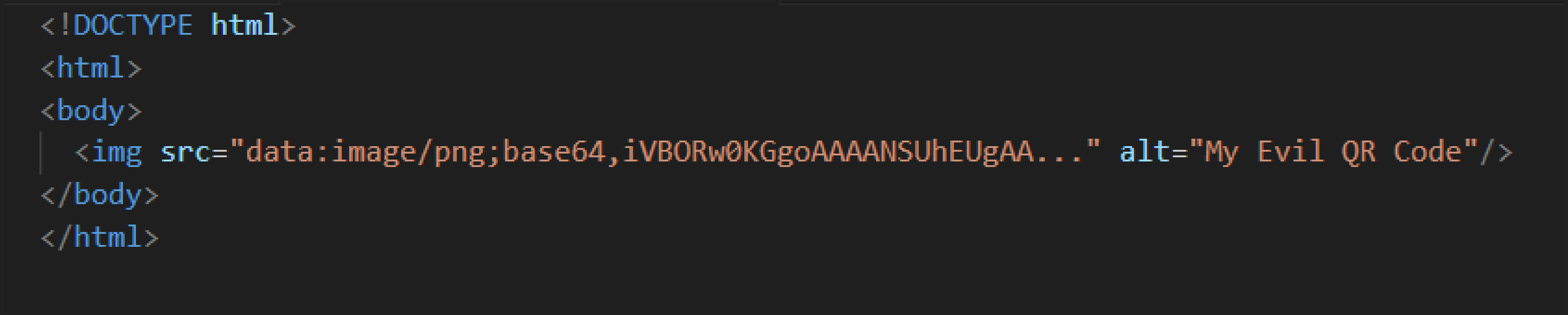
Employee Benefits Plan for the Year 2023/2024

Your document(s) have been successfully signed/accepted and are now fully processed. To access and download the entire document, please follow the provided instructions

[redacted]

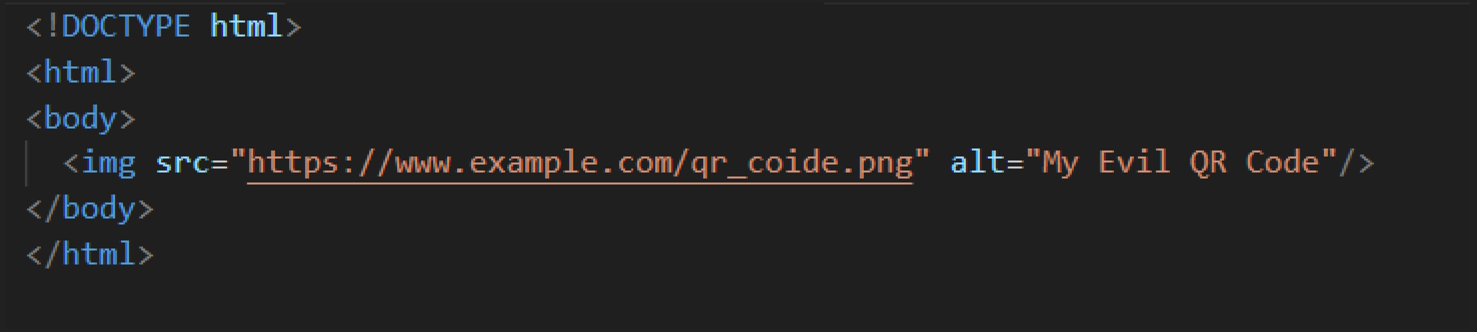
Ways of embedding images

- Base64 Encoded Images



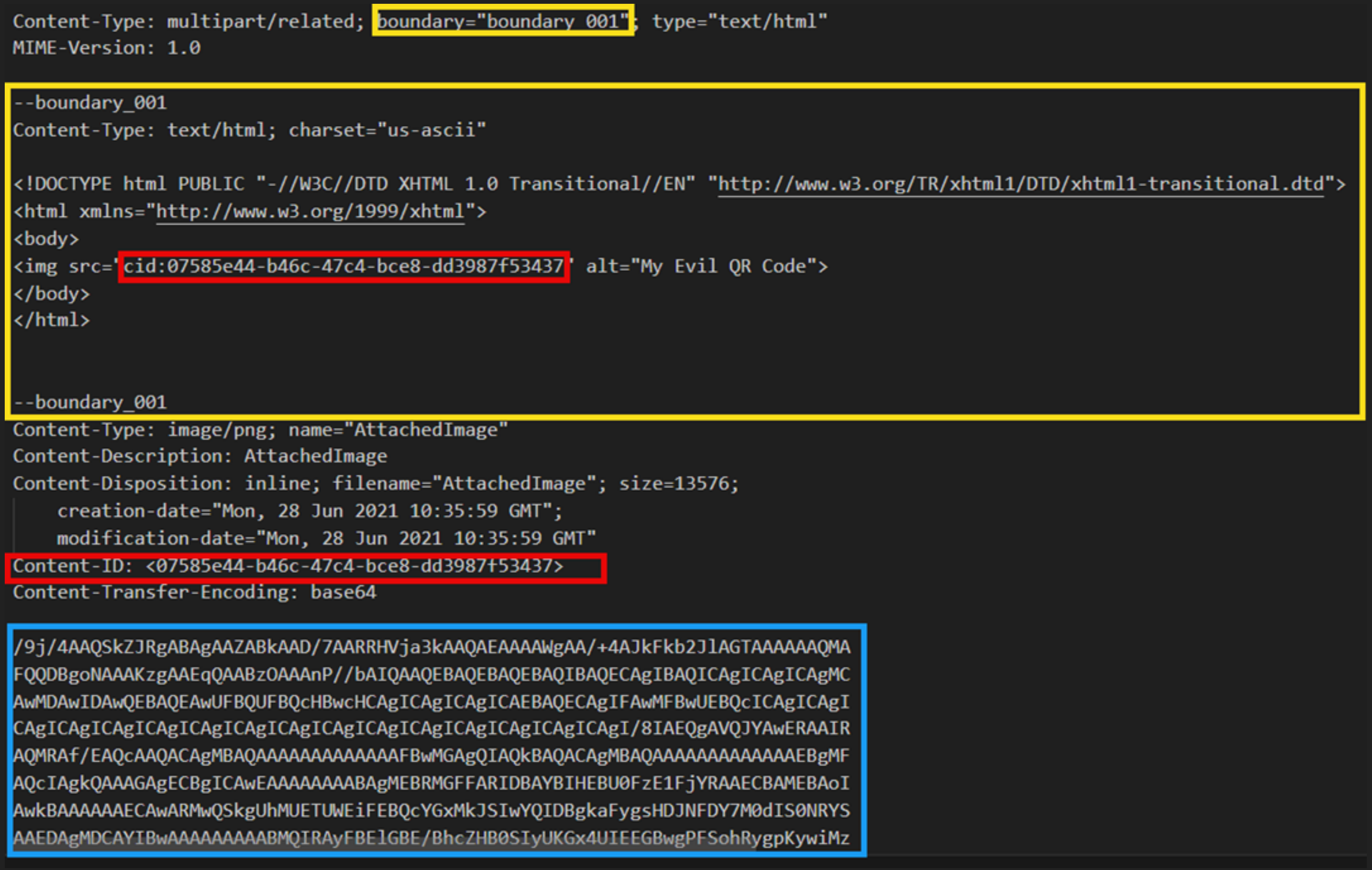
```
<!DOCTYPE html>
<html>
<body>
  <img src="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAA..." alt="My Evil QR Code"/>
</body>
</html>
```

- Link to External Image



```
<!DOCTYPE html>
<html>
<body>
  <img src="https://www.example.com/qr_coide.png" alt="My Evil QR Code"/>
</body>
</html>
```

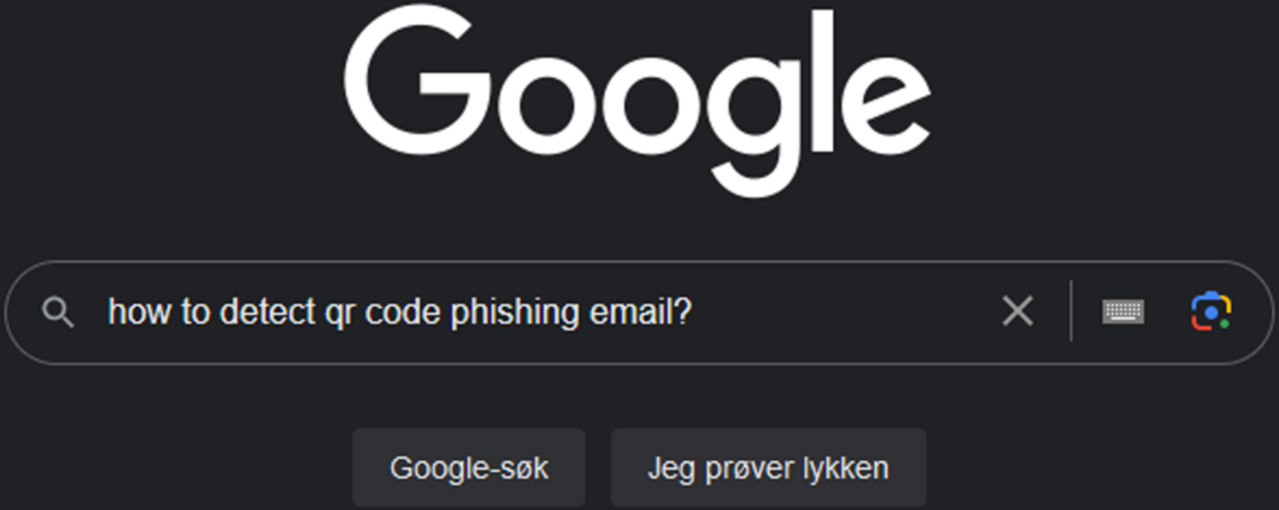
CID (Content-ID) Embedded Images



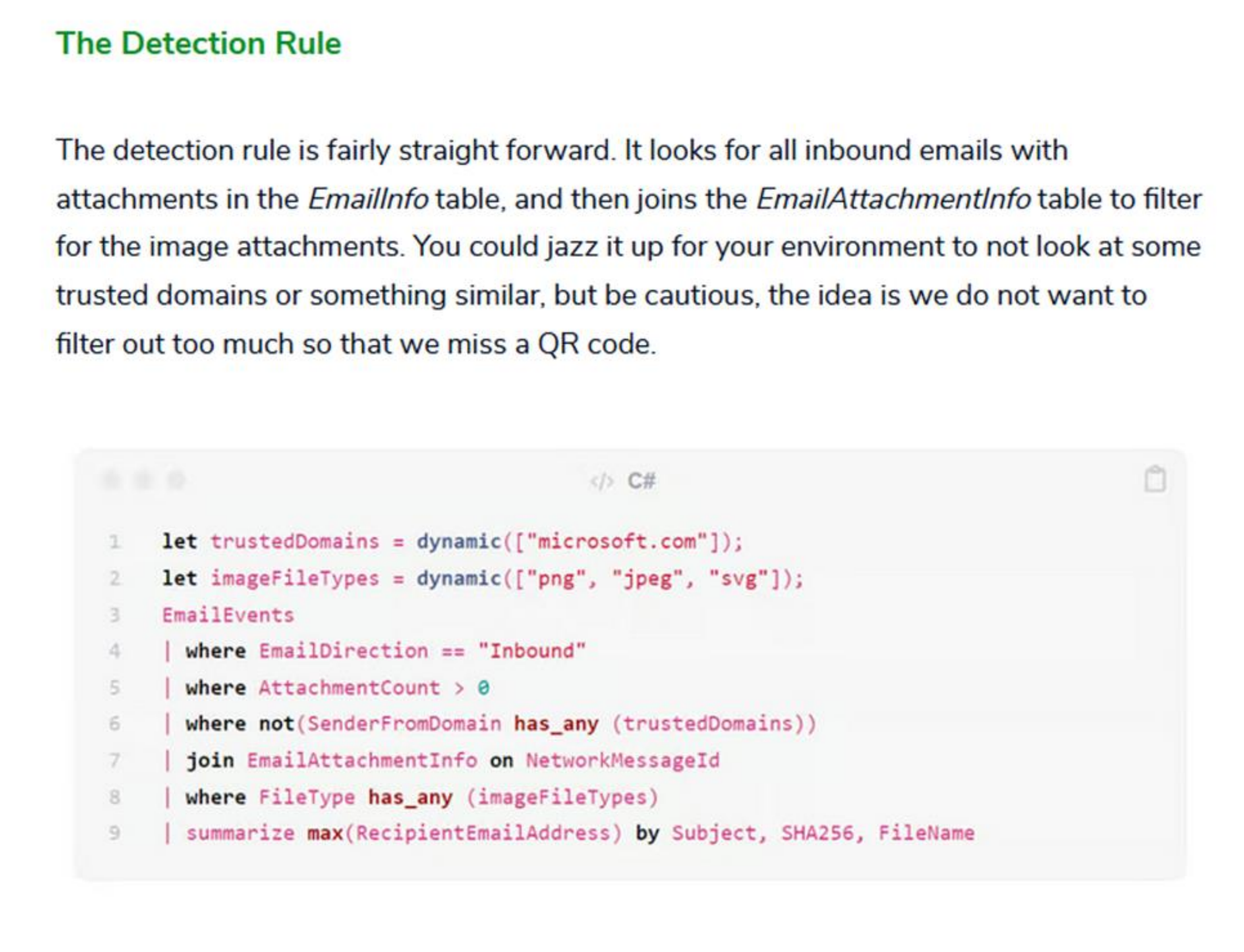
```
Content-Type: multipart/related; boundary="boundary_001"; type="text/html"
MIME-Version: 1.0

--boundary_001
Content-Type: text/html; charset="us-ascii"

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<body>
<img src="cid:07585e44-b46c-47c4-bce8-dd3987f53437" alt="My Evil QR Code">
</body>
</html>


--boundary_001
Content-Type: image/png; name="AttachedImage"
Content-Description: AttachedImage
Content-Disposition: inline; filename="AttachedImage"; size=13576;
    creation-date="Mon, 28 Jun 2021 10:35:59 GMT";
    modification-date="Mon, 28 Jun 2021 10:35:59 GMT"
Content-ID: <07585e44-b46c-47c4-bce8-dd3987f53437>
Content-Transfer-Encoding: base64
```

```
/9j/4AAQSkZJRgABAgAAZABkAAD/7AARRHVja3kAAQAEAAAAWgAA/+4AJkFkb2JlAGTAAAAAAQMA
FQQDBgoNAAAKzgAAEqQAABzOAAAnP//bAIQAAQEBAQEBAQEBAQIBAQECAgIBAQICAgICAgICAgMC
AwMDAwIDAwQEBAQEAwUFBQUFBQcHBwcHCAgICAgICAgICAEBAQECAgIFAwMFBwUEBQcICAgICAgI
CAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgI/8IAEQgAVQJYAwERAAIR
AQMRAf/EAQcAAQACAgMBAQAAAAAAAAAAAAAFBwMGAgQIAQkBAQACAgMBAQAAAAAAAAAAAAAEBgMF
AQcIAgkQAAAGAgECBgICAwEAAAAAAAABAgMEBRMGFFARIDBAYBIHEBU0FzE1FjYRAAECBAMEBAoI
AwkBAAAAAAECAwARMwQSkgUhMUETUWEiFEBQcYGxMkJSIwYQIDBgkaFygsHDJNFDY7M0dIS0NRYS
AAEDAgMDCAYIBwAAAAAAAAABMQIRAyFBElGBE/BhcZHB0SIyUKGx4UIEEGBwgPFSohRygpKywiMz
```

Detection Engineering



how to detect qr code phishing email?

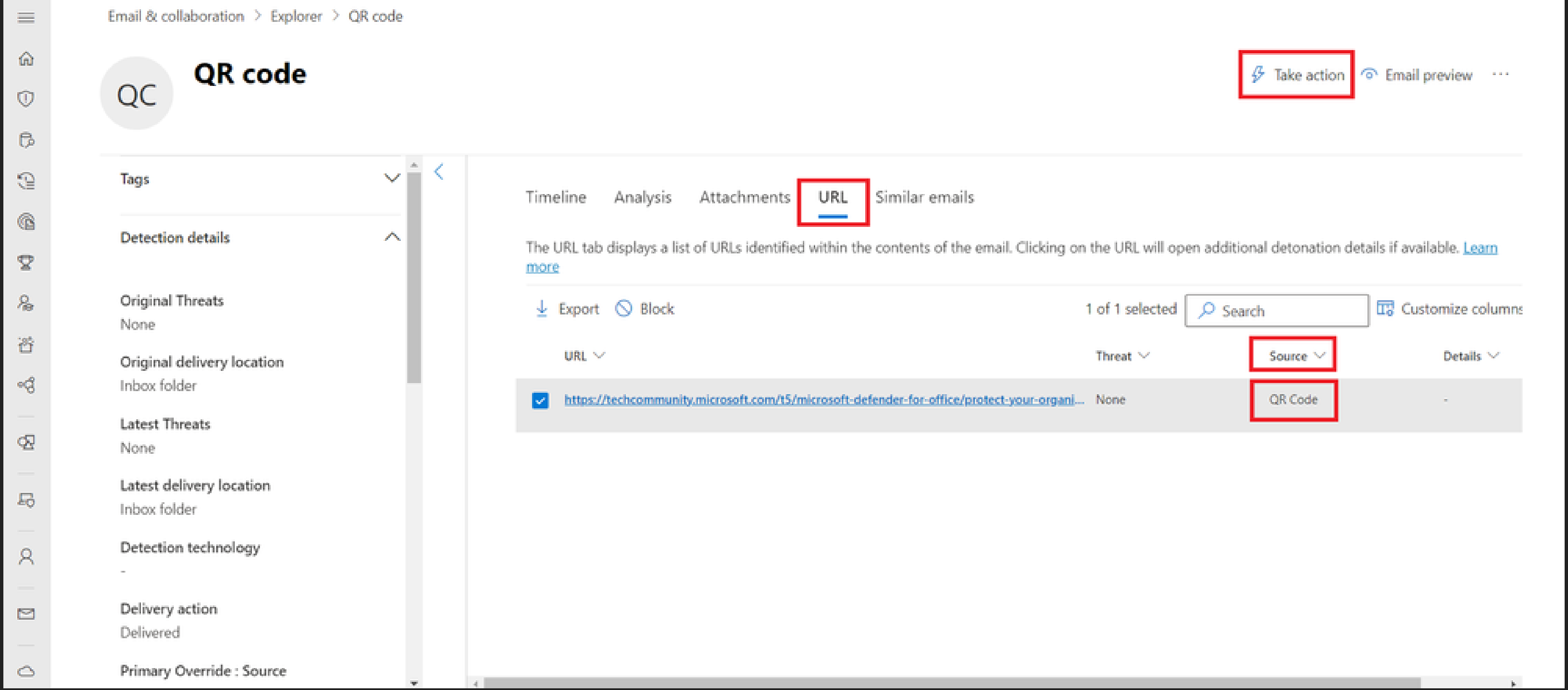


The Detection Rule

The detection rule is fairly straight forward. It looks for all inbound emails with attachments in the *EmailInfo* table, and then joins the *EmailAttachmentInfo* table to filter for the image attachments. You could jazz it up for your environment to not look at some trusted domains or something similar, but be cautious, the idea is we do not want to filter out too much so that we miss a QR code.

```
let trustedDomains = dynamic(["microsoft.com"]);
let imageFileTypes = dynamic(["png", "jpeg", "svg"]);
EmailEvents
| where EmailDirection == "Inbound"
| where AttachmentCount > 0
| where not(SenderFromDomain has_any (trustedDomains))
| join EmailAttachmentInfo on NetworkMessageId
| where FileType has_any (imageFileTypes)
| summarize max(RecipientEmailAddress) by Subject, SHA256, FileName
```

https://stripeolt.com/knowledge-hub/expert-intel/qr-code-phishing-detection/ - Liam Jones



Email & collaboration > Explorer > QR code

QC

QR code

Tags

Detection details

Original Threats
None

Original delivery location
Inbox folder

Latest Threats
None

Latest delivery location
Inbox folder

Detection technology
-

Delivery action
Delivered

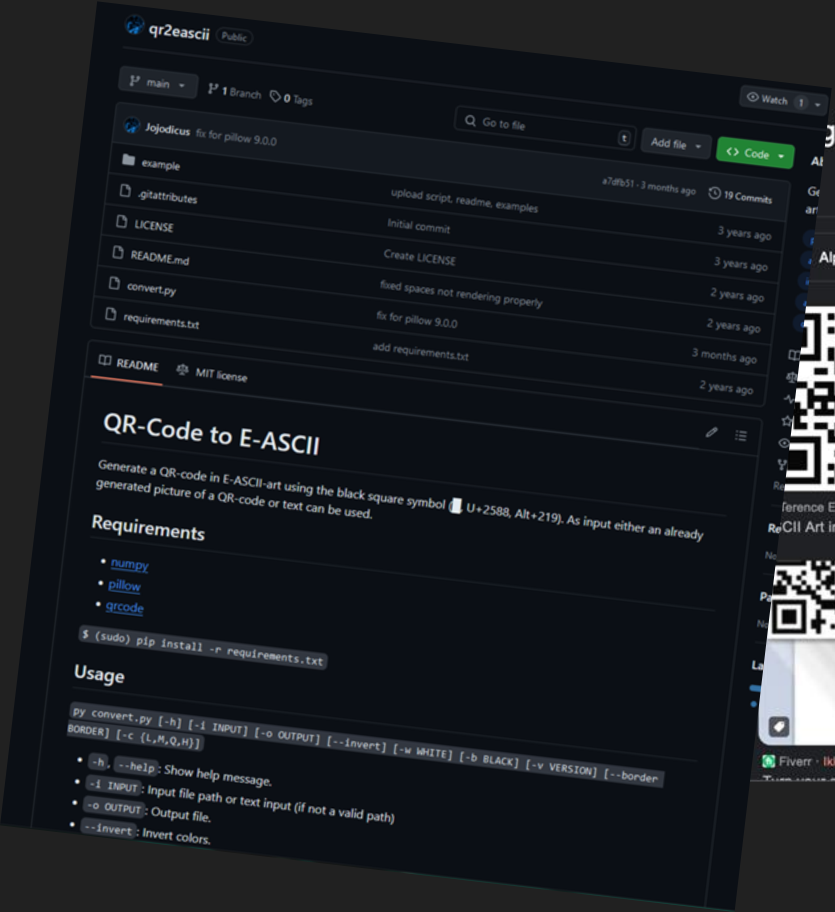
Primary Override : Source

The URL tab displays a list of URLs identified within the contents of the email. Clicking on the URL will open additional detonation details if available. Learn more

	URL	Threat	Source	Details
☑	https://techcommunity.microsoft.com/t5/microsoft-defender-for-office/protect-your-organi...	None	QR Code	-

https://techcommunity.microsoft.com/t5/microsoft-defender-for-office/hunting-and-responding-to-qr-code-based-phishing-attacks-with/ba-p/4074730

imageless QR codes?



Jojodicus fix for pillow 9.0.0 a7dfb51 · 3 months ago 19 Commits

example	upload script, readme, examples	3 years ago
.gitattributes	Initial commit	3 years ago
LICENSE	Create LICENSE	2 years ago
README.md	fixed spaces not rendering properly	2 years ago
convert.py	fix for pillow 9.0.0	3 months ago
requirements.txt	add requirements.txt	2 years ago

QR-Code to E-ASCII

Generate a QR-code in E-ASCII-art using the black square symbol (█ U+2588, Alt+219). As input either an already generated picture of a QR-code or text can be used.

Requirements

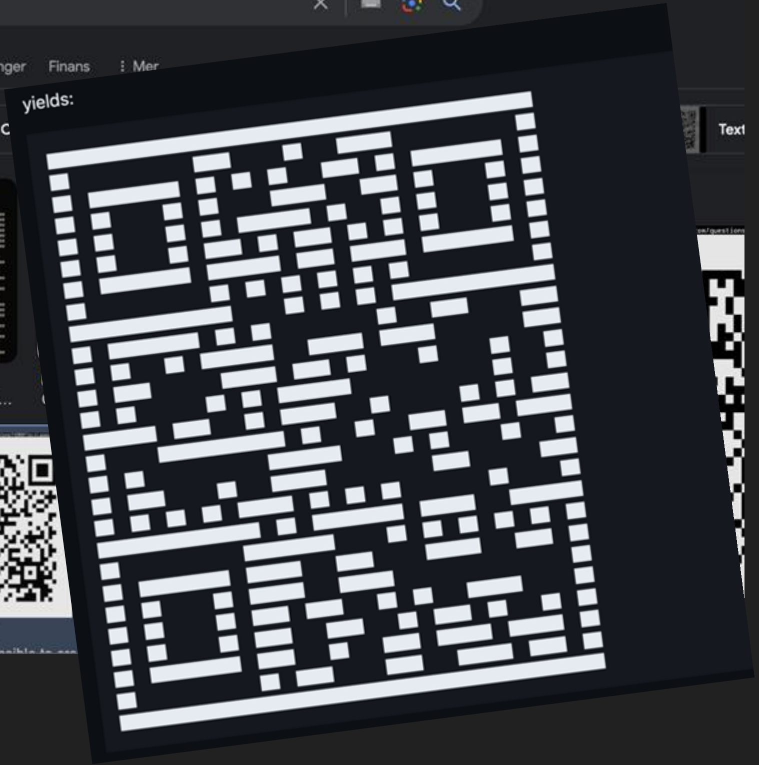
- numpy
- pillow
- qrcode

```
$ (sudo) pip install -r requirements.txt
```

Usage

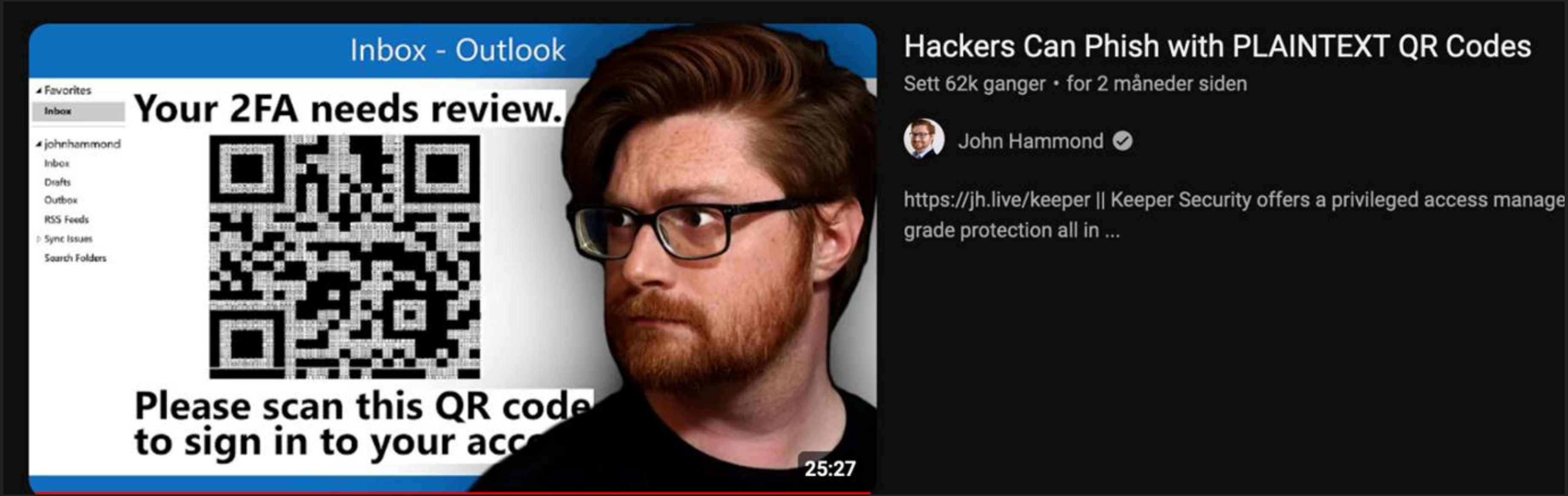
```
py convert.py [-h] [-i INPUT] [-o OUTPUT] [--invert] [-w WHITE] [-b BLACK] [-v VERSION] [--border BORDER] [-c {L,M,Q,H}]
```

- `-h`, `--help`: Show help message.
- `-i INPUT`: Input file path or text input (if not a valid path)
- `-o OUTPUT`: Output file.
- `--invert`: Invert colors.



yields:

It’s well known!



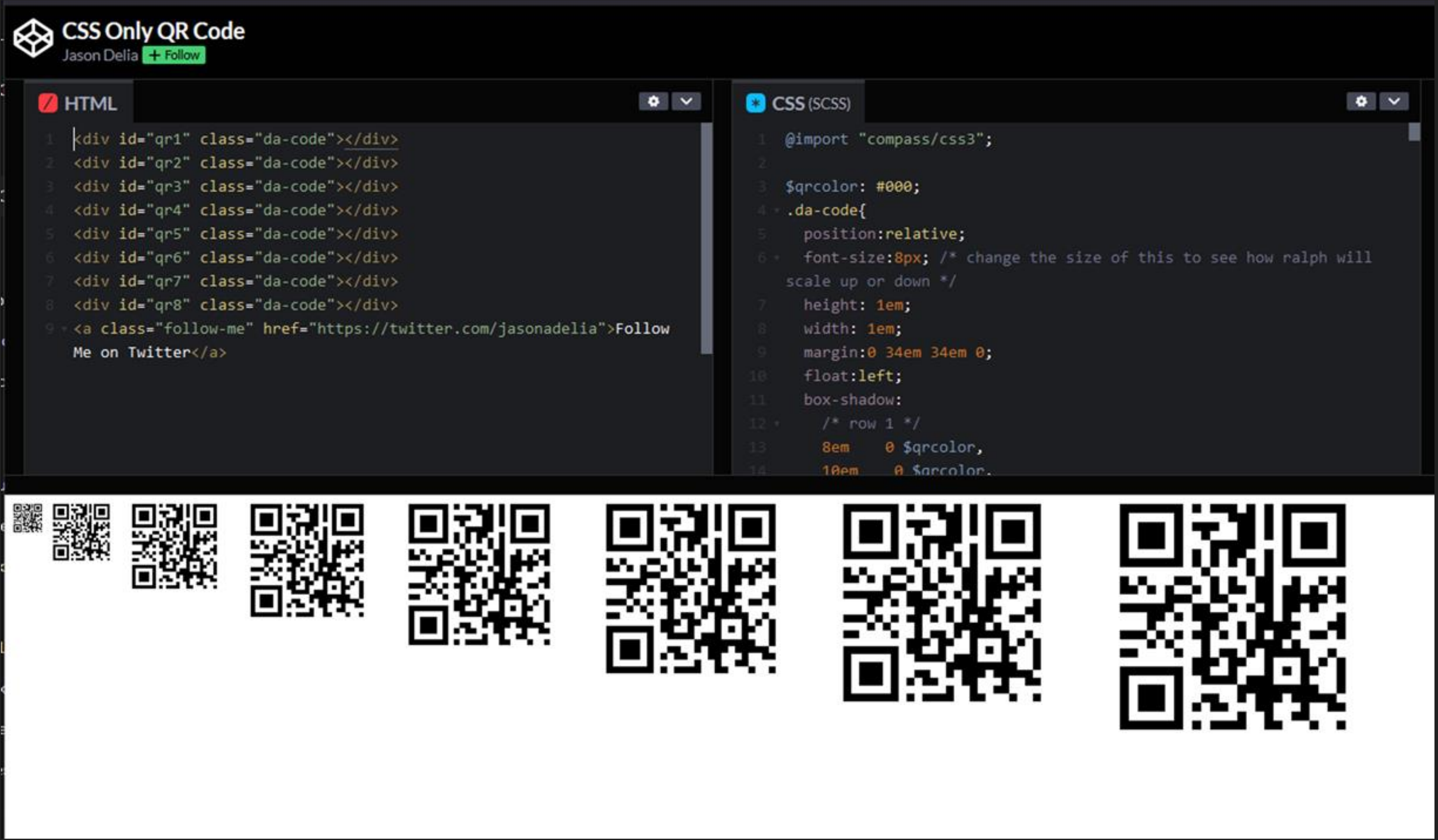
Hackers Can Phish with PLAINTEXT QR Codes

Sett 62k ganger • for 2 måneder siden

John Hammond

https://jh.live/keeper || Keeper Security offers a privileged access manage
grade protection all in ...

https://www.youtube.com/watch?v=cG8Uq2VESfM&pp=ygUPSm9obiBIYW1tb25kIFFS



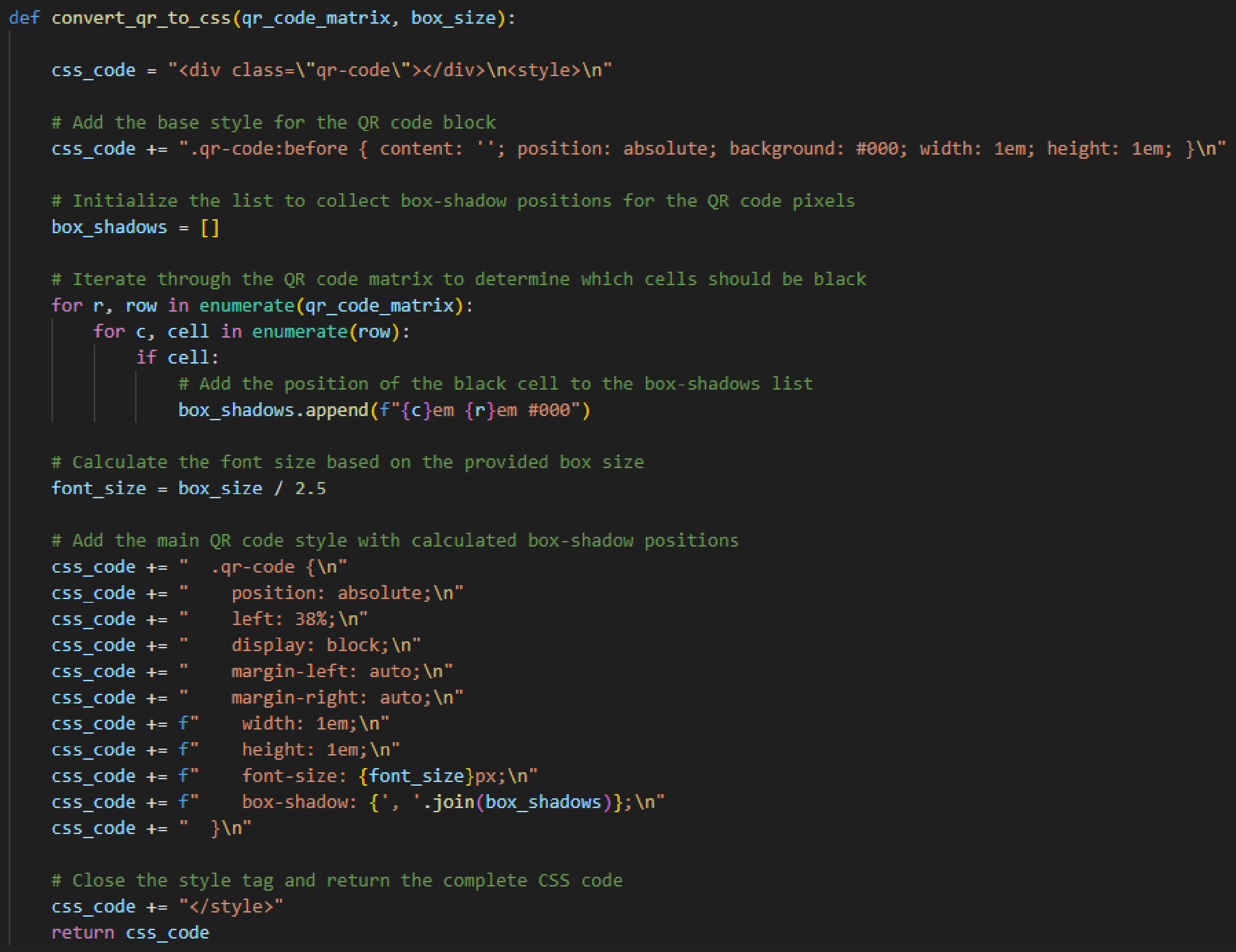
CSS Only QR Code

Jason Delia

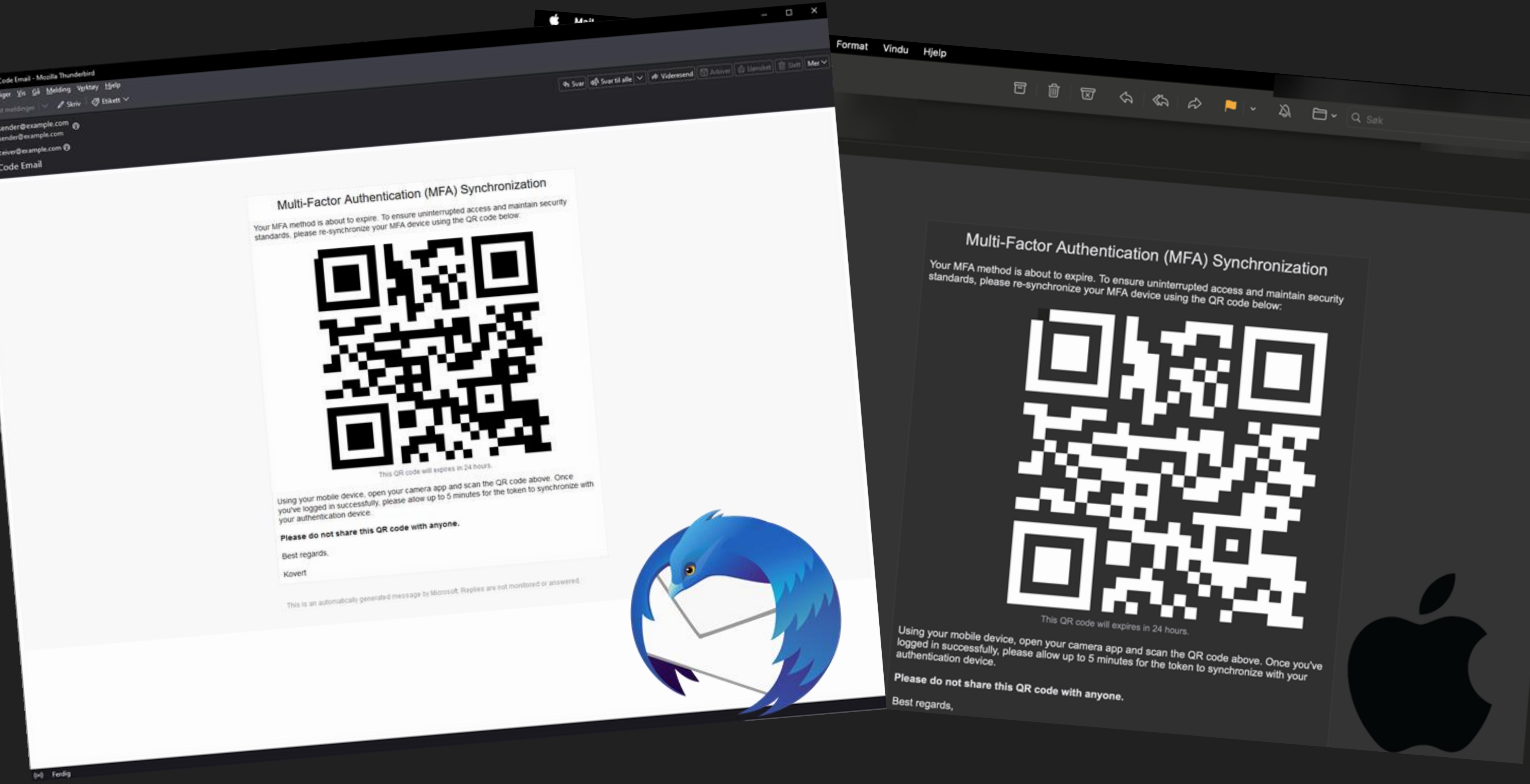
```html
<div id="qr1" class="da-code"></div>
<div id="qr2" class="da-code"></div>
<div id="qr3" class="da-code"></div>
<div id="qr4" class="da-code"></div>
<div id="qr5" class="da-code"></div>
<div id="qr6" class="da-code"></div>
<div id="qr7" class="da-code"></div>
<div id="qr8" class="da-code"></div>
<a class="follow-me" href="https://twitter.com/jasonadelia">Follow Me on Twitter</a>
```

```scss
@import "compass/css3";

$qrcolor: #000;
.da-code{
  position:relative;
  font-size:8px; /* change the size of this to see how ralph will scale up or down */
  height: 1em;
  width: 1em;
  margin:0 34em 34em 0;
  float:left;
  box-shadow:
    /* row 1 */
    8em    0 $qrcolor,
    10em    0 $qrcolor,
```

https://codepen.io/jasonadelia/pen/DwWaNW



```python
def convert_qr_to_css(qr_code_matrix, box_size):

    css_code = "<div class=\"qr-code\"></div>\n<style>\n"

    # Add the base style for the QR code block
    css_code += ".qr-code:before { content: ''; position: absolute; background: #000; width: 1em; height: 1em; }\n"

    # Initialize the list to collect box-shadow positions for the QR code pixels
    box_shadows = []

    # Iterate through the QR code matrix to determine which cells should be black
    for r, row in enumerate(qr_code_matrix):
        for c, cell in enumerate(row):
            if cell:
                # Add the position of the black cell to the box-shadows list
                box_shadows.append(f"{c}em {r}em #000")

    # Calculate the font size based on the provided box size
    font_size = box_size / 2.5

    # Add the main QR code style with calculated box-shadow positions
    css_code += "  .qr-code {\n"
    css_code += "    position: absolute;\n"
    css_code += "    left: 38%;\n"
    css_code += "    display: block;\n"
    css_code += "    margin-left: auto;\n"
    css_code += "    margin-right: auto;\n"
    css_code += f"    width: 1em;\n"
    css_code += f"    height: 1em;\n"
    css_code += f"    font-size: {font_size}px;\n"
    css_code += f"    box-shadow: {', '.join(box_shadows)};\n"
    css_code += "  }\n"

    # Close the style tag and return the complete CSS code
    css_code += "</style>"
    return css_code
```



sender@example.com
sender@example.com
ceiver@example.com

Code Email

Multi-Factor Authentication (MFA) Synchronization

Your MFA method is about to expire. To ensure uninterrupted access and maintain security standards, please re-synchronize your MFA device using the QR code below:

This QR code will expires in 24 hours.

Using your mobile device, open your camera app and scan the QR code above. Once you've logged in successfully, please allow up to 5 minutes for the token to synchronize with your authentication device.

Please do not share this QR code with anyone.

Best regards,

Kovert

This is an automatically generated message by Microsoft. Replies are not monitored or answered.

Multi-Factor Authentication (MFA) Synchronization

Your MFA method is about to expire. To ensure uninterrupted access and maintain security standards, please re-synchronize your MFA device using the QR code below:

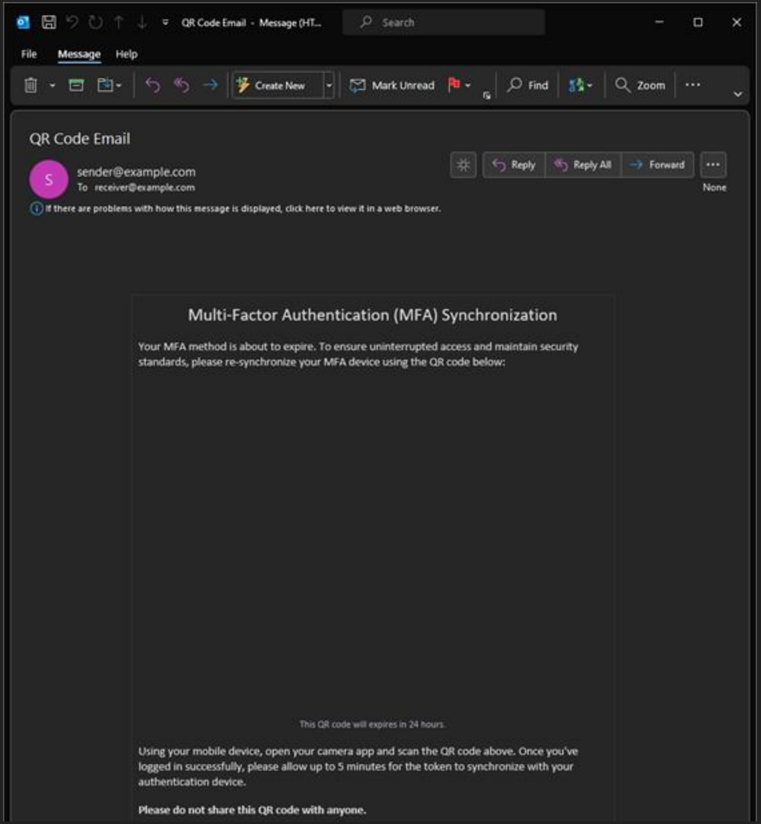
This QR code will expires in 24 hours.

Using your mobile device, open your camera app and scan the QR code above. Once you've logged in successfully, please allow up to 5 minutes for the token to synchronize with your authentication device.

Please do not share this QR code with anyone.

Best regards,

Does not render properly in Outlook Desktop client :(



QR Code Email

sender@example.com
To receiver@example.com

If there are problems with how this message is displayed, click here to view it in a web browser.

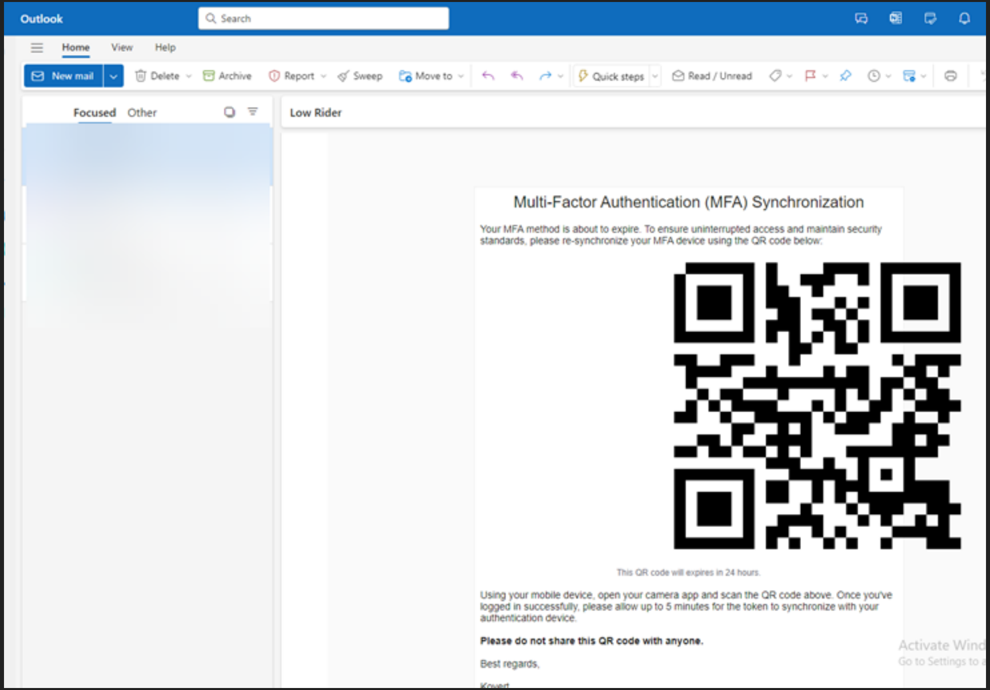
Multi-Factor Authentication (MFA) Synchronization

Your MFA method is about to expire. To ensure uninterrupted access and maintain security standards, please re-synchronize your MFA device using the QR code below:

This QR code will expires in 24 hours.

Using your mobile device, open your camera app and scan the QR code above. Once you've logged in successfully, please allow up to 5 minutes for the token to synchronize with your authentication device.

Please do not share this QR code with anyone.



Multi-Factor Authentication (MFA) Synchronization

Your MFA method is about to expire. To ensure uninterrupted access and maintain security standards, please re-synchronize your MFA device using the QR code below:

This QR code will expires in 24 hours.

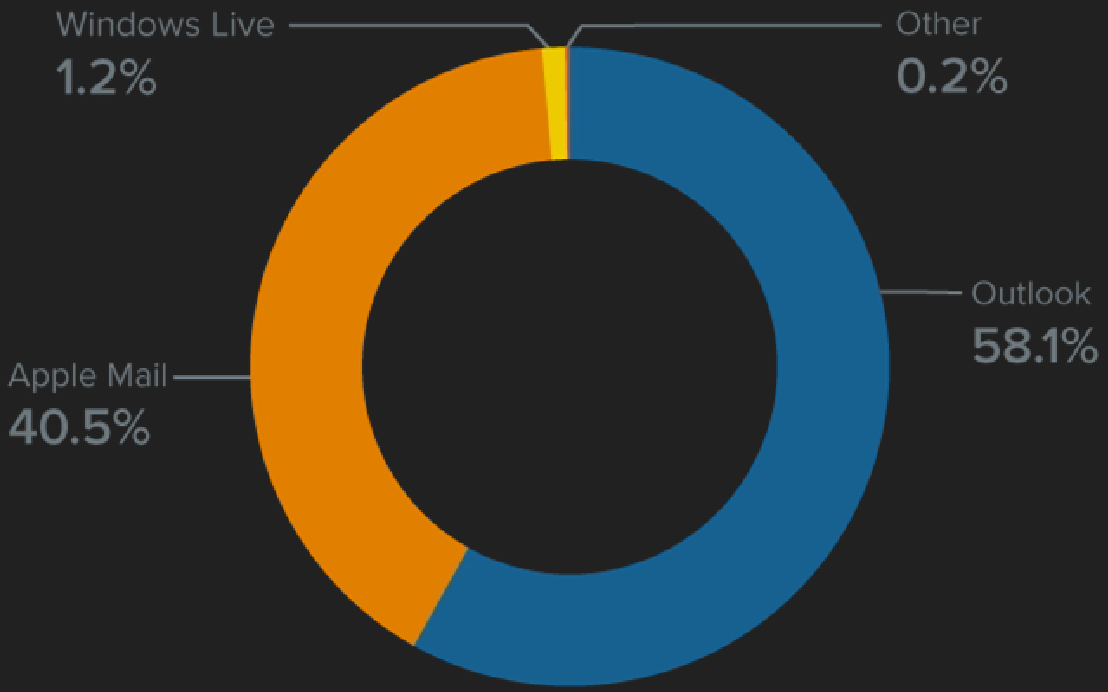
Using your mobile device, open your camera app and scan the QR code above. Once you've logged in successfully, please allow up to 5 minutes for the token to synchronize with your authentication device.

Please do not share this QR code with anyone.

Best regards,

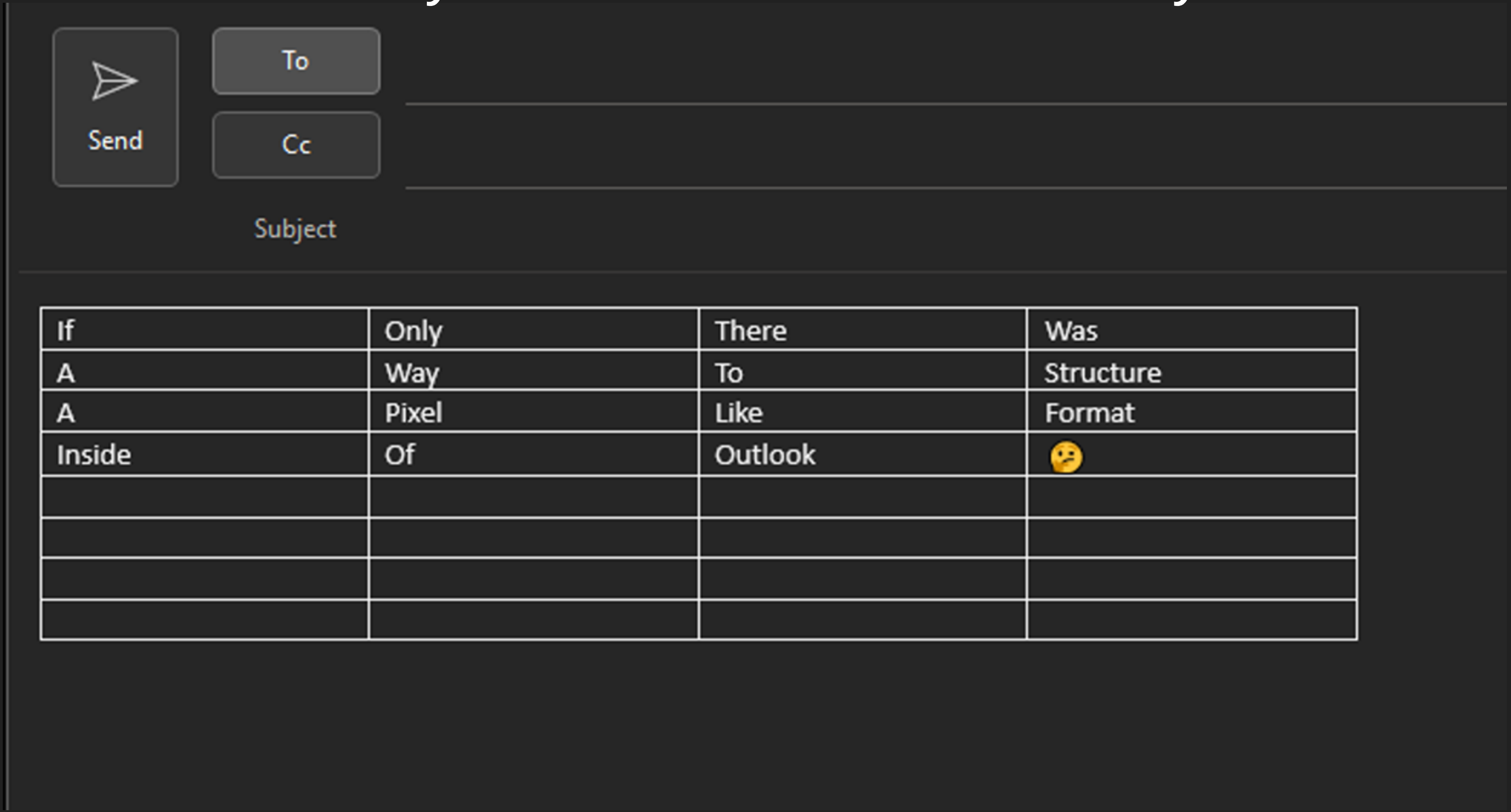
Kovert

Outlook kinda important

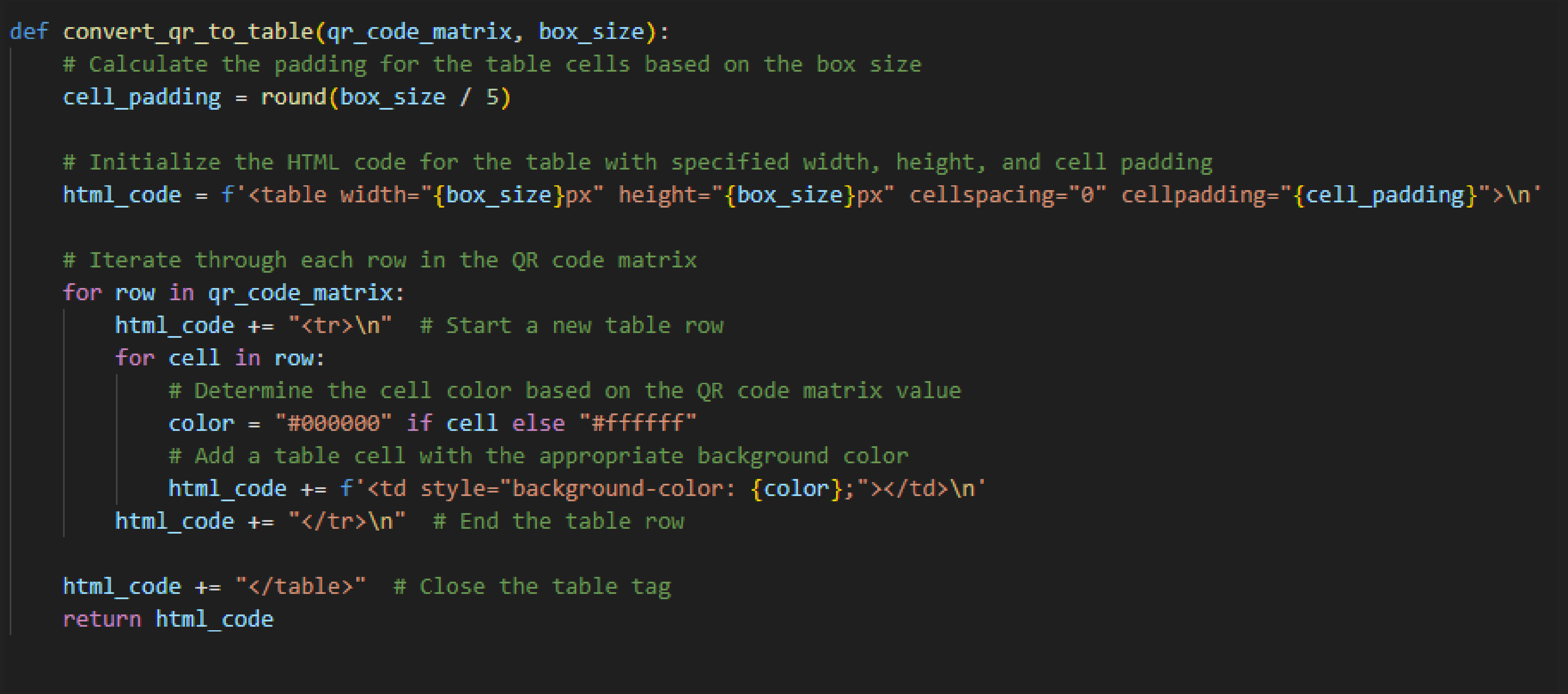


https://www.litmus.com/blog/email-client-market-share-april-2022

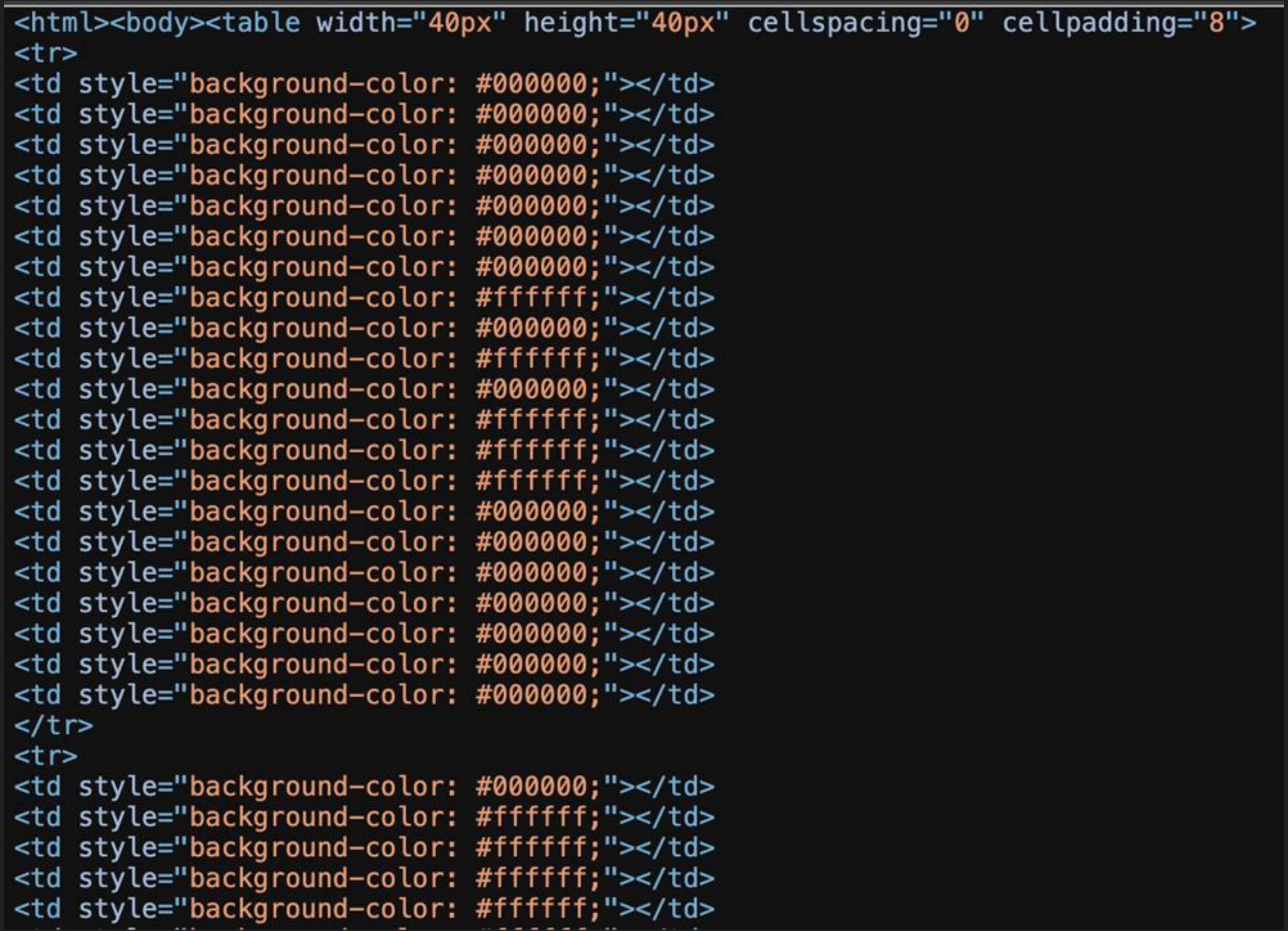
If only there were some other way?



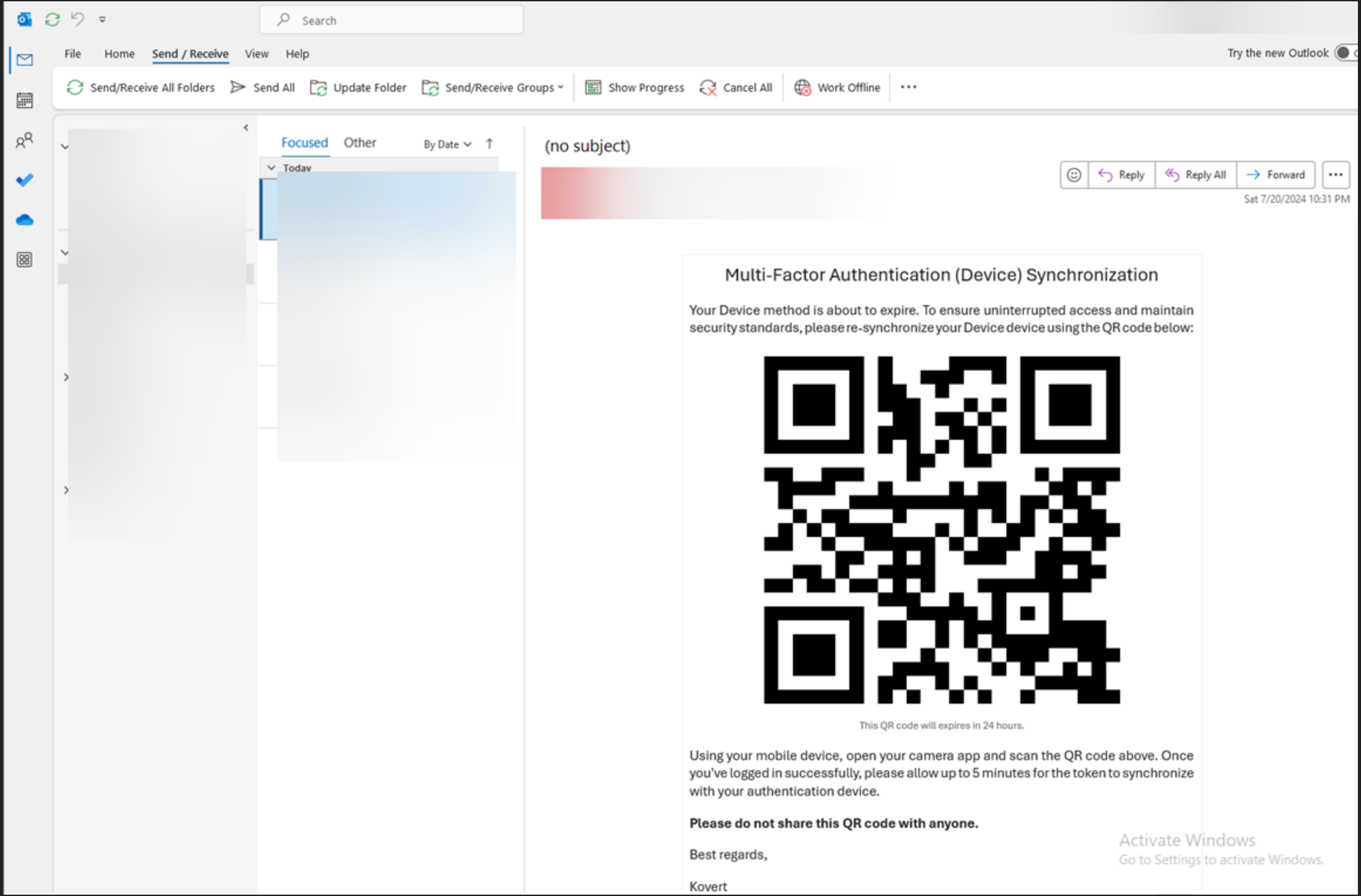
If	Only	There	Was
A	Way	To	Structure
A	Pixel	Like	Format
Inside	Of	Outlook	🤔



```python
def convert_qr_to_table(qr_code_matrix, box_size):
    # Calculate the padding for the table cells based on the box size
    cell_padding = round(box_size / 5)

    # Initialize the HTML code for the table with specified width, height, and cell padding
    html_code = f'<table width="{box_size}px" height="{box_size}px" cellspacing="0" cellpadding="{cell_padding}">\n'

    # Iterate through each row in the QR code matrix
    for row in qr_code_matrix:
        html_code += "<tr>\n"  # Start a new table row
        for cell in row:
            # Determine the cell color based on the QR code matrix value
            color = "#000000" if cell else "#ffffff"
            # Add a table cell with the appropriate background color
            html_code += f'<td style="background-color: {color};"></td>\n'
        html_code += "</tr>\n"  # End the table row

    html_code += "</table>"  # Close the table tag
    return html_code
```



```
<html><body><table width="40px" height="40px" cellspacing="0" cellpadding="8">
<tr>
<td style="background-color: #000000;"></td>
<td style="background-color: #000000;"></td>
<td style="background-color: #000000;"></td>
<td style="background-color: #000000;"></td>
<td style="background-color: #000000;"></td>
<td style="background-color: #000000;"></td>
<td style="background-color: #000000;"></td>
<td style="background-color: #ffffff;"></td>
<td style="background-color: #000000;"></td>
<td style="background-color: #ffffff;"></td>
<td style="background-color: #000000;"></td>
<td style="background-color: #ffffff;"></td>
<td style="background-color: #ffffff;"></td>
<td style="background-color: #ffffff;"></td>
<td style="background-color: #000000;"></td>
<td style="background-color: #000000;"></td>
<td style="background-color: #000000;"></td>
<td style="background-color: #000000;"></td>
<td style="background-color: #000000;"></td>
<td style="background-color: #000000;"></td>
<td style="background-color: #000000;"></td>
</tr>
<tr>
<td style="background-color: #000000;"></td>
<td style="background-color: #ffffff;"></td>
<td style="background-color: #ffffff;"></td>
<td style="background-color: #ffffff;"></td>
<td style="background-color: #ffffff;"></td>
```



(no subject)

[redacted]

Sat 7/20/2024 10:31 PM

Multi-Factor Authentication (Device) Synchronization

Your Device method is about to expire. To ensure uninterrupted access and maintain security standards, please re-synchronize your Device device using the QR code below:

This QR code will expires in 24 hours.

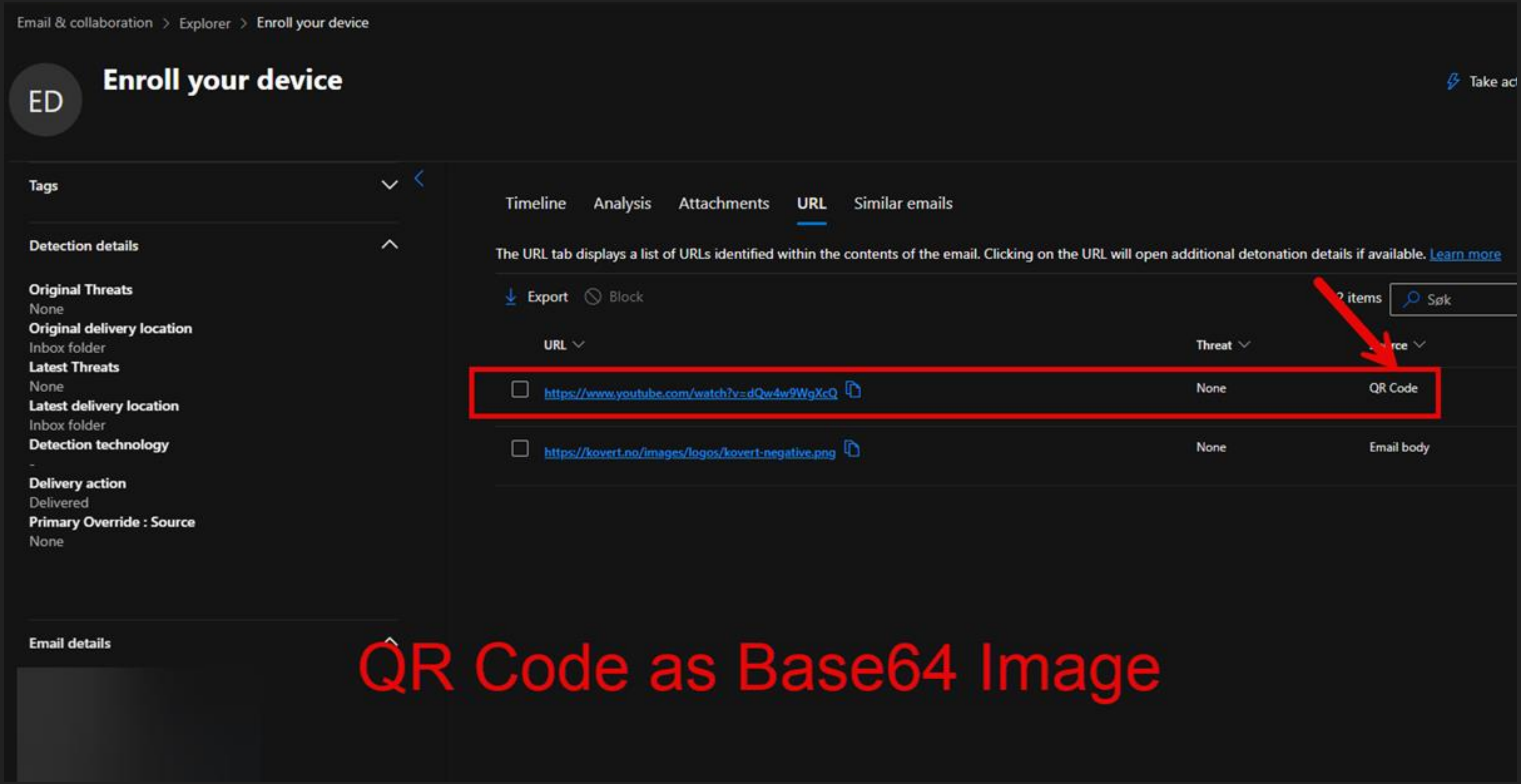
Using your mobile device, open your camera app and scan the QR code above. Once you've logged in successfully, please allow up to 5 minutes for the token to synchronize with your authentication device.

Please do not share this QR code with anyone.

Best regards,

Kovert

Detection?



Email & collaboration > Explorer > Enroll your device

ED **Enroll your device**

Tags

Detection details

Original Threats
None
Original delivery location
Inbox folder
Latest Threats
None
Latest delivery location
Inbox folder
Detection technology
-
Delivery action
Delivered
Primary Override : Source
None

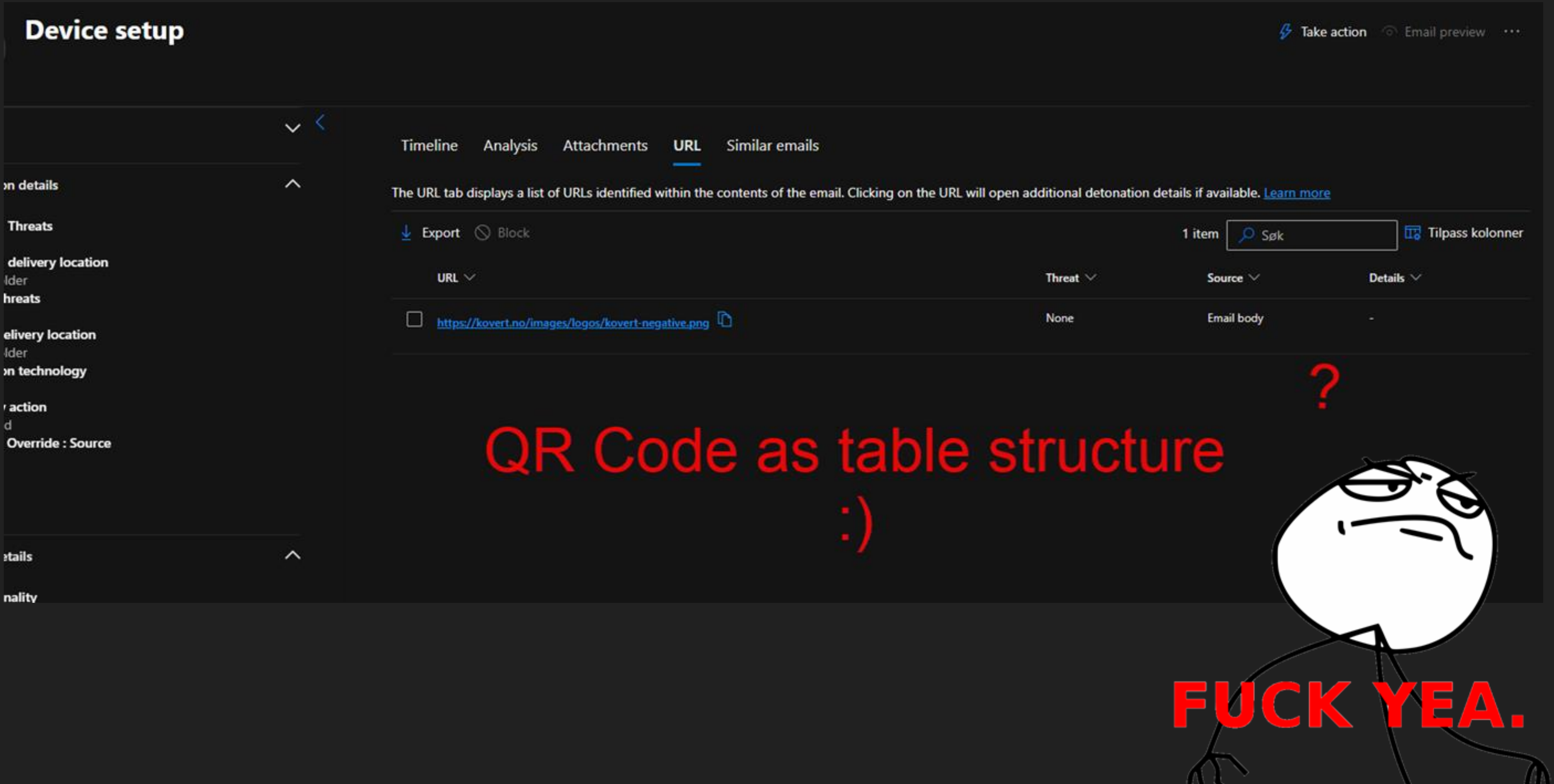
Email details

The URL tab displays a list of URLs identified within the contents of the email. Clicking on the URL will open additional detonation details if available. Learn more

	URL	Threat	rce
□	https://www.youtube.com/watch?v=dQw4w9WgXcQ	None	QR Code
□	https://kovert.no/images/logos/kovert-negative.png	None	Email body

QR Code as Base64 Image

Detection?



Device setup

The URL tab displays a list of URLs identified within the contents of the email. Clicking on the URL will open additional detonation details if available. Learn more

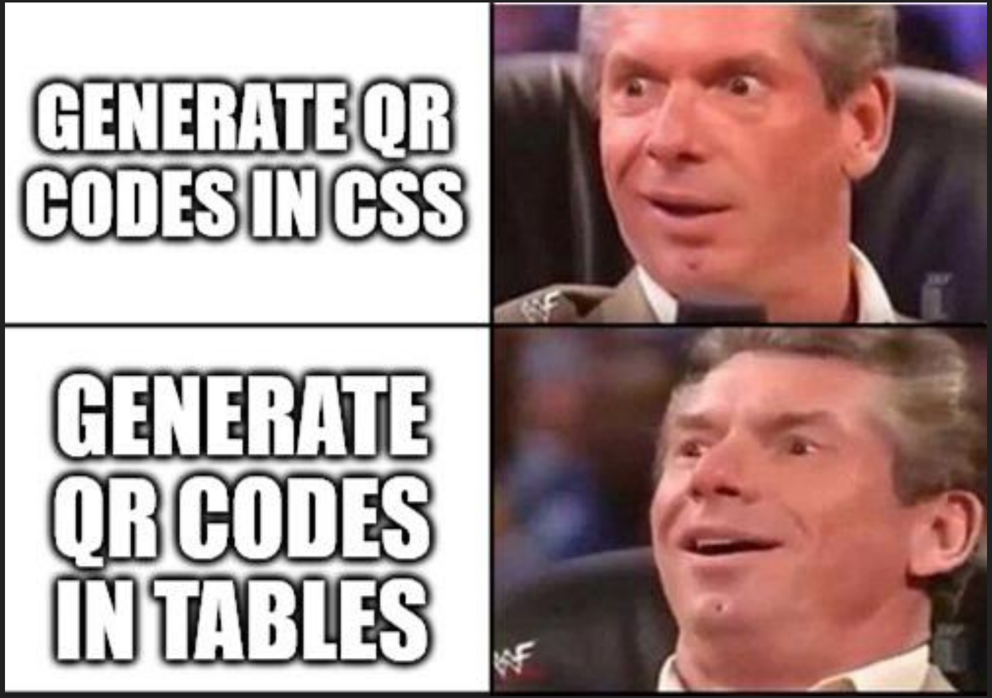
	URL	Threat	Source	Details
□	https://kovert.no/images/logos/kovert-negative.png	None	Email body	-

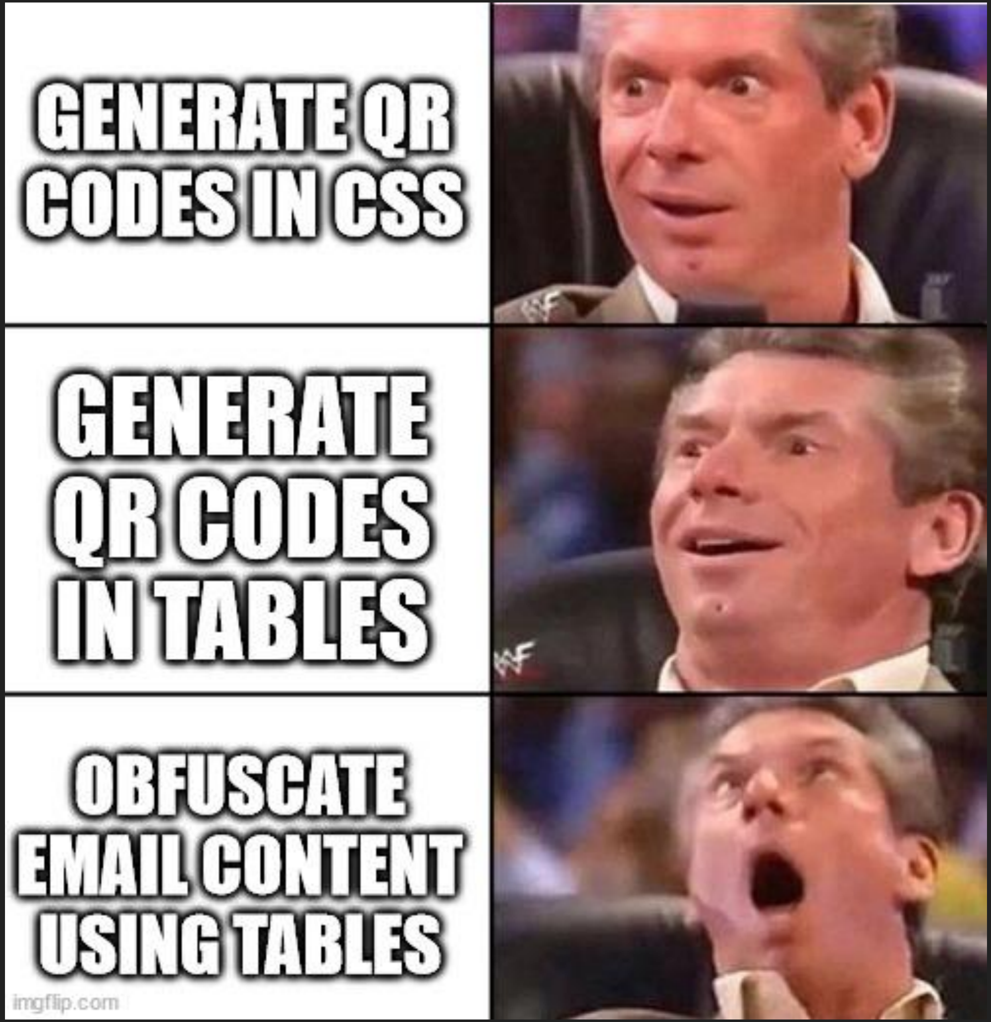
?

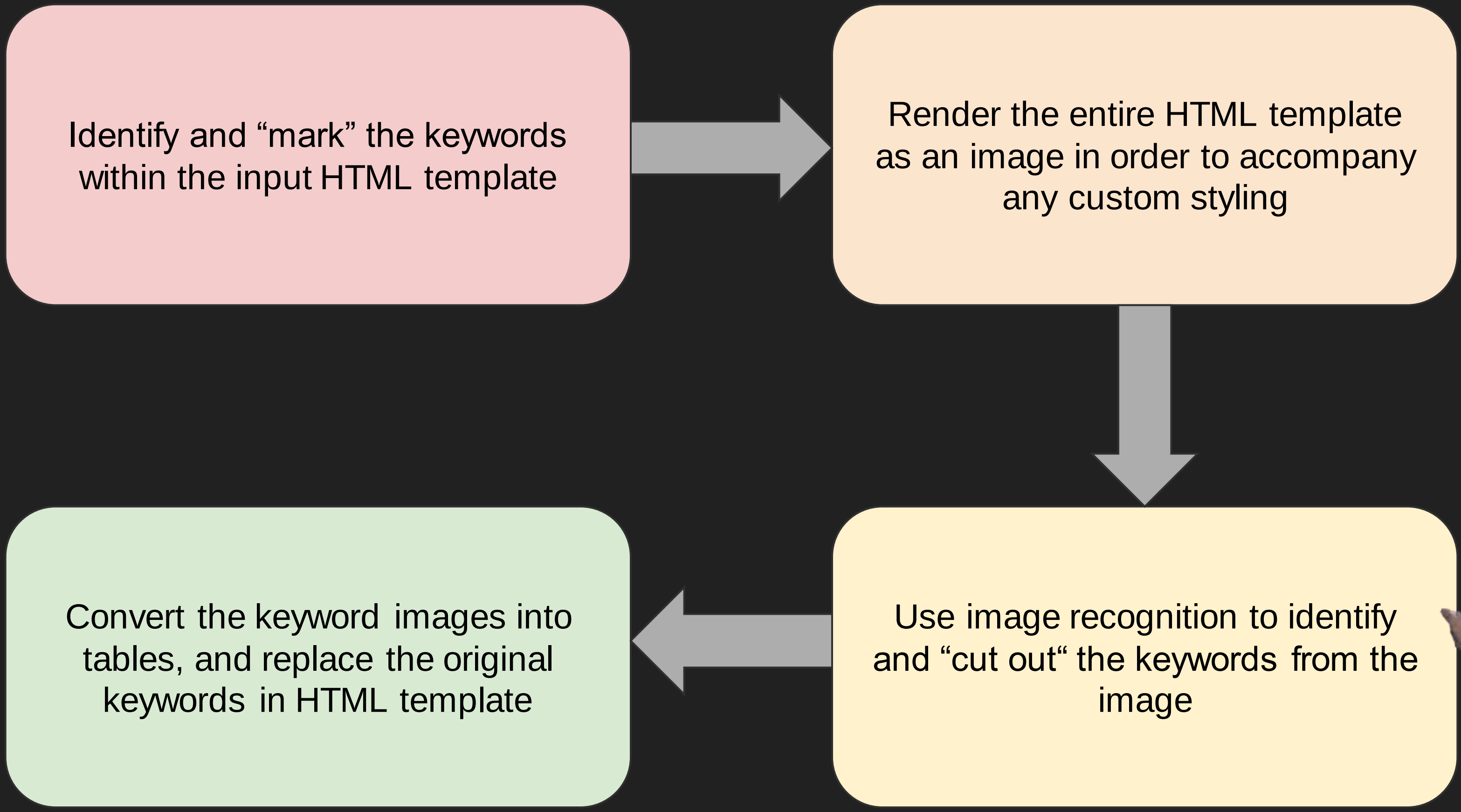
QR Code as table structure

:)

GENERATE QR
CODES IN CSS


GENERATE QR CODES IN CSS
GENERATE QR CODES IN TABLES


GENERATE QR CODES IN CSS
GENERATE QR CODES IN TABLES
OBFUSCATE EMAIL CONTENT USING TABLES
imgflip.com

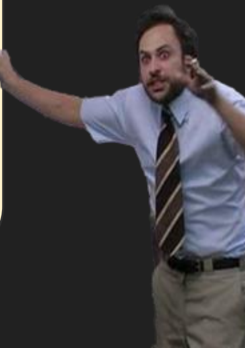


Identify and “mark” the keywords within the input HTML template

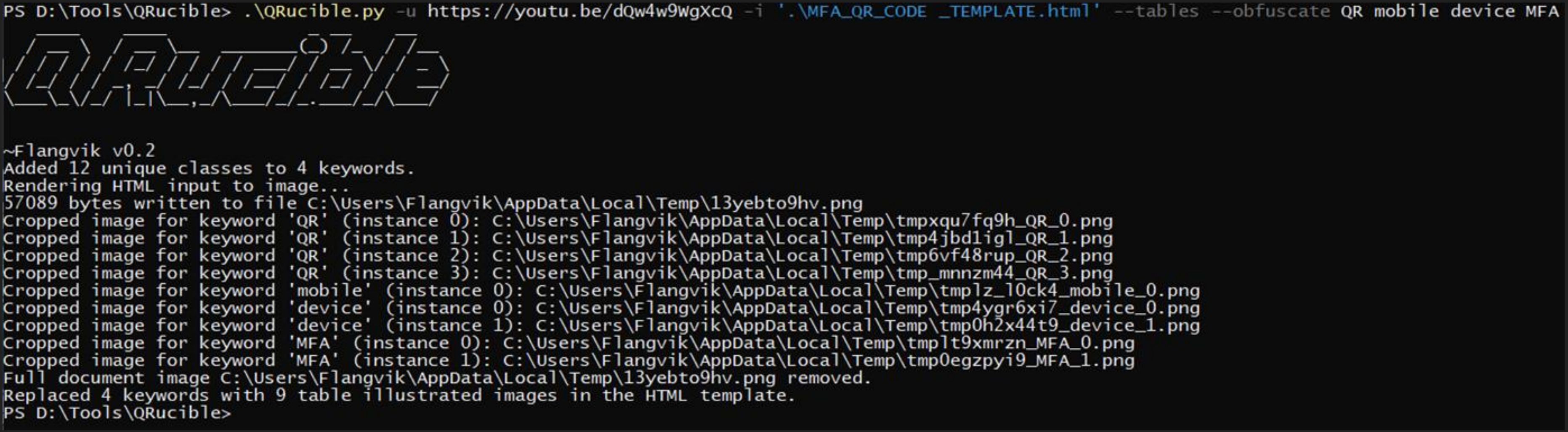
Render the entire HTML template as an image in order to accompany any custom styling

Use image recognition to identify and “cut out“ the keywords from the image

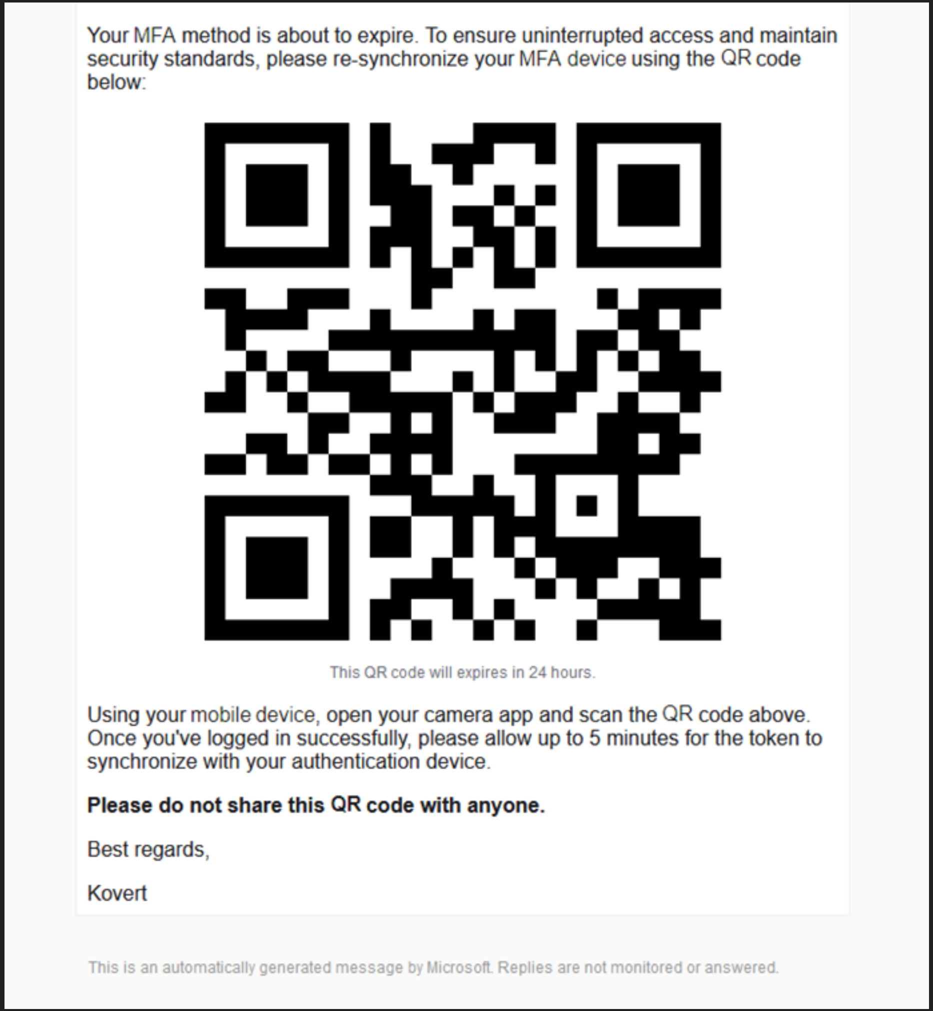
Convert the keyword images into tables, and replace the original keywords in HTML template



BeautifulSoup + Html2Image + pytesseract + ChatGPT



```
PS D:\Tools\QRucible> .\QRucible.py -u https://youtu.be/dQw4w9WgXcQ -i '.\MFA_QR_CODE _TEMPLATE.html' --tables --obfuscate QR mobile device MFA
   ____  ____             _ __    __
  / __ \/ __ \__  _______(_) /_  / /__
 / / / / /_/ / / / / ___/ / __ \/ / _ \
/ /_/ / _, _/ /_/ / /__/ / /_/ / /  __/
\___\_\_/ |_|\__,_/\___/_/_.___/_/\___/


~Flangvik v0.2
Added 12 unique classes to 4 keywords.
Rendering HTML input to image...
57089 bytes written to file C:\Users\Flangvik\AppData\Local\Temp\13yebto9hv.png
Cropped image for keyword 'QR' (instance 0): C:\Users\Flangvik\AppData\Local\Temp\tmpxqu7fq9h_QR_0.png
Cropped image for keyword 'QR' (instance 1): C:\Users\Flangvik\AppData\Local\Temp\tmp4jbd1igl_QR_1.png
Cropped image for keyword 'QR' (instance 2): C:\Users\Flangvik\AppData\Local\Temp\tmp6vf48rup_QR_2.png
Cropped image for keyword 'QR' (instance 3): C:\Users\Flangvik\AppData\Local\Temp\tmp_mnnzm44_QR_3.png
Cropped image for keyword 'mobile' (instance 0): C:\Users\Flangvik\AppData\Local\Temp\tmplz_l0ck4_mobile_0.png
Cropped image for keyword 'device' (instance 0): C:\Users\Flangvik\AppData\Local\Temp\tmp4ygr6xi7_device_0.png
Cropped image for keyword 'device' (instance 1): C:\Users\Flangvik\AppData\Local\Temp\tmp0h2x44t9_device_1.png
Cropped image for keyword 'MFA' (instance 0): C:\Users\Flangvik\AppData\Local\Temp\tmplt9xmrzn_MFA_0.png
Cropped image for keyword 'MFA' (instance 1): C:\Users\Flangvik\AppData\Local\Temp\tmp0egzpyi9_MFA_1.png
Full document image C:\Users\Flangvik\AppData\Local\Temp\13yebto9hv.png removed.
Replaced 4 keywords with 9 table illustrated images in the HTML template.
PS D:\Tools\QRucible>
```



Your MFA method is about to expire. To ensure uninterrupted access and maintain security standards, please re-synchronize your MFA device using the QR code below:

This QR code will expires in 24 hours.

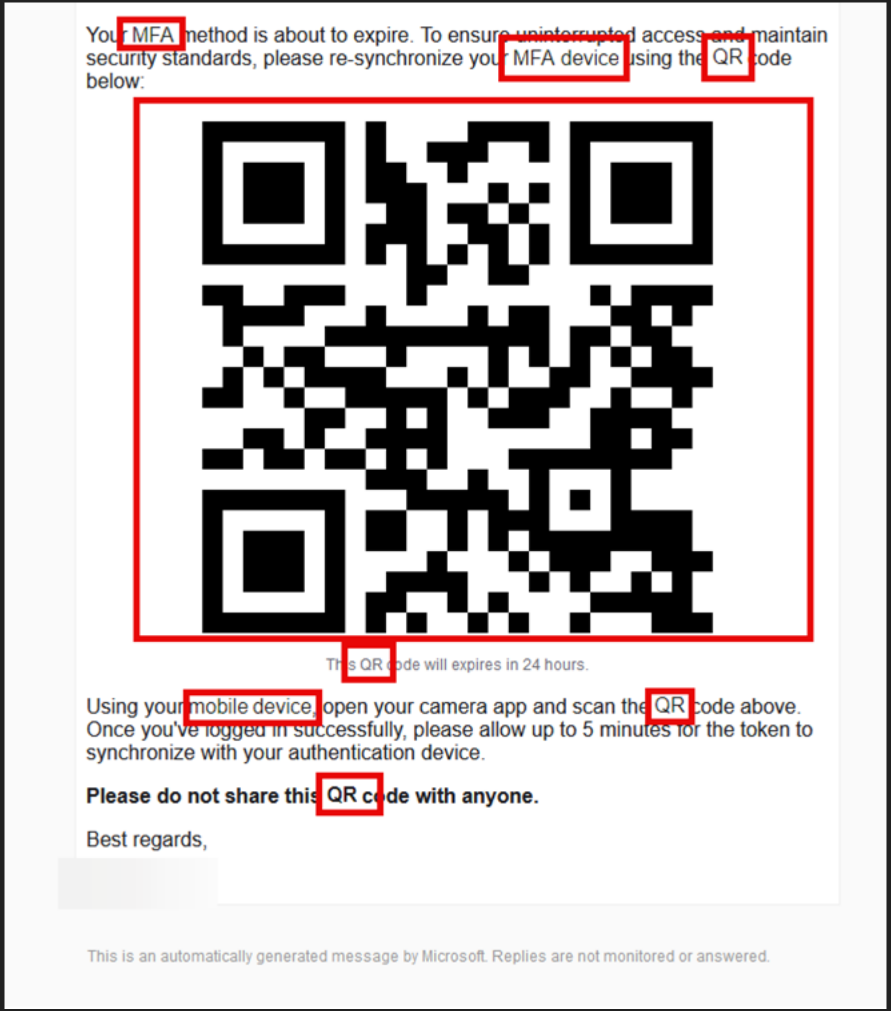
Using your mobile device, open your camera app and scan the QR code above. Once you've logged in successfully, please allow up to 5 minutes for the token to synchronize with your authentication device.

Please do not share this QR code with anyone.

Best regards,

Kovert

This is an automatically generated message by Microsoft. Replies are not monitored or answered.



Your MFA method is about to expire. To ensure uninterrupted access and maintain security standards, please re-synchronize your MFA device using the QR code below:

This QR code will expires in 24 hours.

Using your mobile device, open your camera app and scan the QR code above. Once you've logged in successfully, please allow up to 5 minutes for the token to synchronize with your authentication device.

Please do not share this QR code with anyone.

Best regards,

This is an automatically generated message by Microsoft. Replies are not monitored or answered.

Thank you!

- **Enjoy DEF CON 32!**
- **Thanks to Adversary Village** 💜
- **QRucible can be found at**