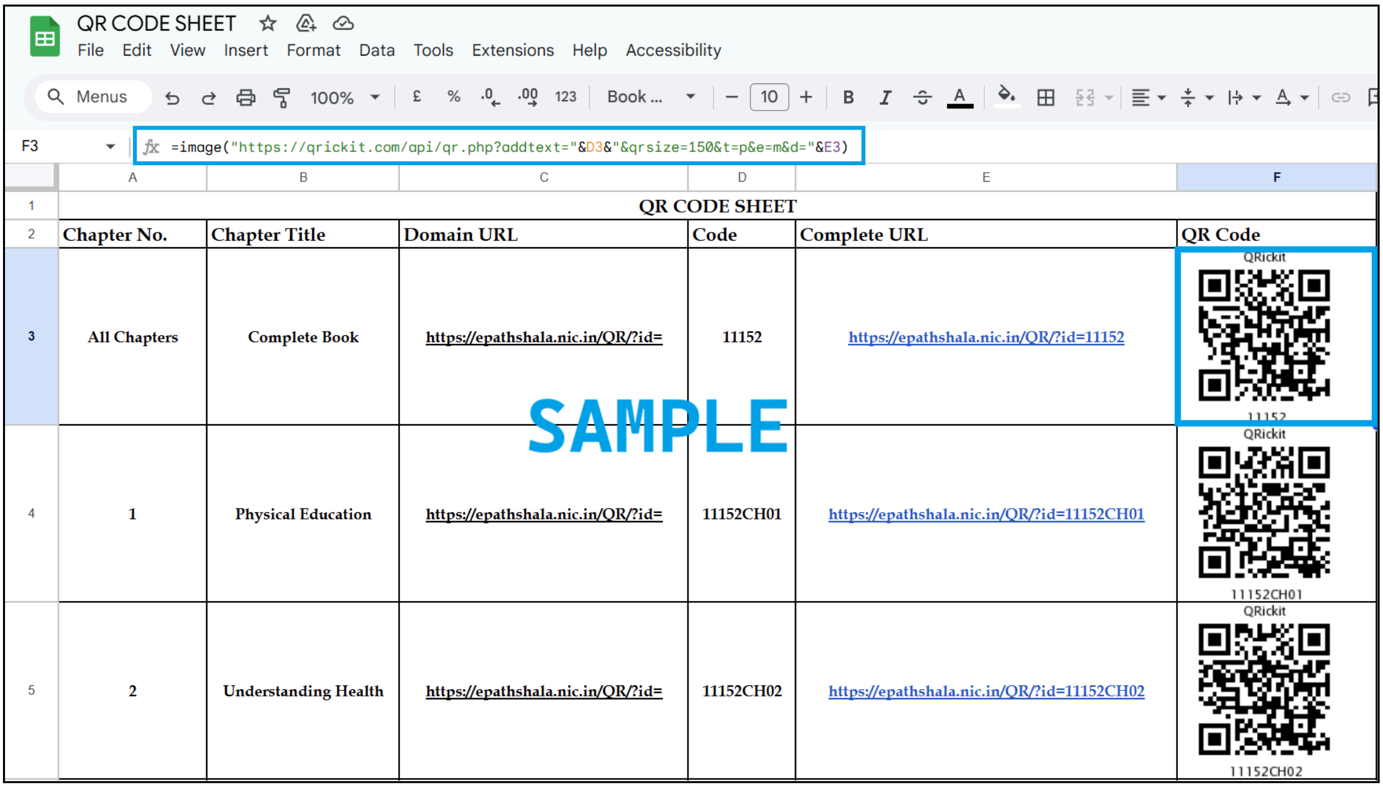
<u>QR Code Safety Concerns</u>

1. Process of generating QR Codes for NCERT Books and Resources

a. Every book have a separate code to identify and every chapter of that book is also denoted by unique code extending the code of the book

b. All the QRs of NCERT books are mapped to online resources at it's official "ePathshala website" with domain URL- "*https://epathshala.nic.in*"

c. After constructing the complete URL, it is passed to the said API shown in the image below to generate QR Codes in bulk within the excel sheet.



```
=image("https://qrickit.com/api/qr.php?addtext="&D3&"&qrsize=150&t=p&e=m&d="&E3)
```

QR CODE SHEET

Chapter No.	Chapter Title	Domain URL	Code	Complete URL	QR Code
All Chapters	Complete Book	https://epathshala.nic.in/QR/?id=	11152	https://epathshala.nic.in/QR/?id=11152	QRickit 11152
1	Physical Education	https://epathshala.nic.in/QR/?id=	11152CH01	https://epathshala.nic.in/QR/?id=11152CH01	QRickit 11152CH01
2	Understanding Health	https://epathshala.nic.in/QR/?id=	11152CH02	https://epathshala.nic.in/QR/?id=11152CH02	QRickit 11152CH02

2. Liabilities related to the process of generating QR using ongoing method

a. These QRs are static only and if printed can't be altered.

b. Some of them doesn't contain the secure URL with SSL (e.g., contains "http")

c. Another liability in this process as we do not have information about how much error correction is implemented in this used API

3. **Measures to be taken in account to make it safer**

    a. Utilize SSL-Secured URLs: Always generate QR codes that redirect to URLs using HTTPS (SSL/TLS encryption). This ensures secure data transmission between the user and the destination, safeguarding against man-in-the-middle attacks.

    b. Consider the Lifetime of QR Codes: The lifespan of QR codes should be carefully determined based on evolving technological trends and security requirements. QR codes should be configured to expire after a set period, limiting exposure to potential vulnerabilities over time.

    c. Ensure using higher correction levels while generating QRs.

4. **Identification by checking QRs before scanning by basic observation.**

    a. Check the source of the QR code

    b. Verify the URL it links to before scanning

    c. Look for any physical tampering

    d. use a QR scanner that previews the URL before launching it

5. **Verification**

    a. Do not scan a code if it is on a sticker, looks like it has been replaced, or is covered up.

    b. After scanning the code, see if the URL you are taken to is a secure one that begins with "https."

    c. Use a QR Code Scanner app that can help you recognize a suspicious code or use the generic app for qr scanning that comes with your device.

6. **How QR Phishing can be prevented**

    a. Implement security measures: Utilize secure QR code generation tools that can include features like dynamic codes or error correction levels.

    b. Use higher error correction limits while generating QRs.

https://ncert.gov.in

Static & No Security

Static & with minimal security

Explanation : Tips to Identify Suspicious QR Codes

1. Be Careful with Unknown Sources:

    a. Unexpected QR codes: If you receive a QR code via text, email, or from unknown sources, be suspicious.

    b. Publicly placed QR codes: Be extra cautious of QR codes placed in public spaces, such as on posters, flyers, or ads. These may have been tampered with to redirect you to malicious sites or download harmful software.

2. Check the URL (via authentic QR Code Scanners):

    a. Verify the URL: If you are scanning a QR code, use a QR code scanner app that shows the destination URL before you open it. If the URL is unfamiliar, overly complex, or doesn't match the business or service it claims to represent, it may be fraudulent. It must contain a SSL (e.g., "https" before all the links embedded in QR)

    b. Be wary of similar-looking domains: Malicious QR codes often lead to URLs that closely resemble legitimate ones (e.g., "g00gle.com" instead of "google.com").

3. Inspect the QR Code's Appearance:

    a. Look for alterations: If the QR code appears to be tampered with, covered up, or it may have been changed as all the shapes should be uniform (all the shapes should be same).

4. Use Trusted Security Software:

    a. Ensure your device has updated security software or apps that can detect and block malicious QR codes or links before they can harm you.

5. Avoid Entering Personal Information:

    a. If the site linked to by the QR code asks for sensitive information like passwords, or bank details, it's likely a phishing attempt. Always be cautious before entering personal data.

    b. Most likely if any qr link asks for special permission is a phishing attempt.

Features in the Dynamic QR application

This Dynamic QR application offers a comprehensive set of advanced features meticulously designed to optimize user experience and security. Below is a detailed explanation of the key features within the application:

1. **Legitimate In-house Generated Code**

   This application is entirely developed by in-house developers, ensuring **complete independence and no reliance on external resources** or any kind of dependencies.

2. **No Duplicacy**

   The system ensures that each QR code generated is **unique, eliminating the risk of duplication**, and guaranteeing that each code points to distinct, dynamic content.

3. **ML Operation for Image Generation**

   Leveraging machine learning, this feature enables the creation of visually appealing, artistic QR codes with gradient designs, enhancing the **aesthetic while maintaining functionality**.

4. **Artistic QRs with gradients**

   QR codes are designed with **artistic gradients**, offering a modern and visually engaging experience that still maintains the code's scannability and effectiveness.

5. **Dynamic Data Collection**

   The application supports **real-time data collection**, allowing CIET-NCERT to track interactions with the QR codes, optimizing user engagement and analytics.

6. **Dynamic Resource Allocation : Secure & Dynamic QR Codes**

   Each QR code generated is both secure and dynamic, meaning it **can be updated in real time without needing to regenerate or redistribute** the code, providing flexibility and security.

7. **Security Features**

Robust security measures are implemented, ensuring that the QR codes are tamper-proof and resistant to unauthorized access or modification, safeguarding sensitive information.

7.1. **Secure URLs :** All URLs embedded in the QR codes are secure, ensuring that the linked content is safe from potential cybersecurity threats.
e.g., http://ncert.nic.in is an unsafe link without SSL/TLS.
URL like https://ncert.nic.in is a safe link with SSL/TLS layer.

7.2. **Masking :** URLs are being masked to not expose the security of data.

7.3. **Hashing :** This feature encrypts the QR code's data using hashing algorithms, adding another layer of security to prevent unauthorized access to the encoded resource URL, and also it functions as the URL **shortening feature to many of our lengthy URLs** such as in DIKSHA portal. e.g., to remove the risk of using ***"bit.ly"*** or ***"shorturl.at"***etc.

7.4. **Claim free as No third party used :** QR code generation process does not rely on third-party services, guaranteeing that the entire operation is handled internally, thus maintaining full control over data and security.

7.5. **High level error correction :** This feature ensures that even if a QR code is damaged or partially obscured, it can still be read and provide the correct information, offering greater reliability in various conditions.

8. **Data analytics Dashboard integrated**

9. **Demographic data collection and mapping can also be integrated further with Machine Learning technologies used in building this Application**

10. Samples of the QR Codes can be generated

STATIC

Simple & Static

Static with logo

Static with colored logo

Coloured, Static with logo

Dynamic

Gradient without logo

Gradient with NCERT logo

Dynamic, with logo, highly secure & Hashed