# QR Codes

## What are QR Codes?

Quick Response (QR) codes are white squares with unique black markings that can be read by a digital device (usually a smartphone) using the camera lens, functioning much like a traditional barcode.

## What do QR codes do?

QR codes are links with no clicking required. Instead, online pages are quickly opened by scanning them with a smartphone camera. QR codes appear on flyers, magazines, restaurant menus, and even business cards

## How are they used?

They can be used to view a menu on your phone, or to easily display and scan information like boarding passes, proof of vaccination, or concert tickets.


**By scanning a QR code, you may be at risk of...**

Including the device you used to scan the code, your IP address, location, and any other information you enter while using the site.

### Having your information collected

Including your credit card or any other payment information used if you make a purchase on the fraudulent site.

### Having your financial information stolen

### Having website cookies used without your consent


These cookies track and collect your activity online for marketing purposes

### Having your device infected with malware

Downloading a scanner app increases the risk of your device getting infected with malware. Most smartphones have a built-in scanner within the camera.

# 12 STEPS TO USING QR CODES SAFELY

KNOWLEDGEFLOW CYBERSAFETY FOUNDATION

It's important to **be cautious** when encountering and **scanning QR codes**.
If you have doubts about a code's authenticity, **it's best to avoid scanning it**.

## 1 Examine the URL preview before opening

Prior to opening a QR code link on your phone, a URL preview should be visible. Ensure the URL appears genuine and isn't a typo or misspelling of a legitimate website. (e.g., "KnowladgeFlow.org" instead of "KnowledgeFlow.org").

## 2 Safeguard your personalized QR codes

Store QR codes containing your sensitive information in a secure folder on your device.
(e.g., vaccination proof, boarding pass)

## 3 Download apps from reputable app stores

Avoid downloading apps via QR codes.

## 4 Avoid financial transactions that use QR codes

When dealing with your hard-earned money, no convenience is worth the risk.

## 5 Check for tampering

Fraudsters will place a fake QR code on top of a legitimate one. Exercise caution by inspecting QR codes for signs of tampering, such as added stickers, and be wary of webpages that request unnecessary personal information.

**Tip**: Most businesses place QR codes behind glass or have them laminated, and their logo is often incorporated in the middle of the QR code.

## 6 Contact the institution directly

If you receive a suspicious message containing a QR code supposedly sent by a major institution, like a bank, always contact the institution directly to verify the message's authenticity.

- Avoid using a browser search to find a contact number
- Use the phone number provided on a recent bank statement or invoice

## 7 Report!

Report any suspected cases of fraud or cybercrime to your local police and the Canadian Anti-Fraud Centre.

## 8 Provide minimum information

When completing online forms through QR codes, provide the minimum amount of personal information required.

## 9 Be Skeptical

Keep in mind that QR codes are typically used for payments, not for receiving money. Be cautious if someone asks you to scan a code to receive payment; this is likely a scam that could result in unauthorized withdrawals from your bank account.

## 10 Install antivirus software

Enhance your device's security by installing a reputable antivirus software such as Malwarebytes. This will provide you with a higher level of protection in case you scan a malicious QR code.

## 11 Manually find information first

If you encounter an untrusted QR code but want more information about the service or product offered, try to manually find information first to verify its legitimacy. Avoid using the contact information provided with the suspicious QR code.

## 12 Stay skeptical

Stay alert when encountering "too good to be true" messages, like a stranger offering you money or free products if you scan their QR code. Don't hesitate to decline requests from strangers asking you to scan a QR code.

# Common QR Scams

## Why the rise in QR scams?

The convenience and rise in popularity of QR codes make them more appealing to cybercriminals

**Use this QR Code to practice Step 1: Examine the URL Preview**

https://knowledgeflow.org/resources/

## How do QR scams work?

The goal of a QR Code scam is usually to get you to navigate to a fraudulent or malicious page. Once navigated to, cybercriminals will then steal your personal data, money, or both.

## Reported QR Scam Examples

### Fraudulent QR codes placed over legitimate ones

Commonly occurs in locations where you would encounter genuine QR codes such as gas stations, banks, restaurants, bus stations, and community boards.


### Fraudsters disguised as utility company employees

Reported instances include fraudsters knocking on doors stating “overdue payments” which “can be paid” by following the link presented via QR Code.

## Have you been impacted by a QR code scam? Follow these steps.

### Update your passwords

If you used your login credentials on a fraudulent site, change your password as soon as possible. If you haven’t already, set up two-factor authentication for added account security.

### Get in touch with your bank

If you provided your credit card details on a fraudulent website, inform your bank immediately. Freeze your account and collaborate with your bank to implement additional safeguards for your financial security.

### Report scams and fraud

Reporting scams and fraud helps to keep us all safe. Report to the Canadian Anti-Fraud Centre (CAFC) online, or by phone.

**Toll free: 1-888-495-8501**