# Beware of QR Code Scams This Holiday Season

November 30, 2024 - As the holiday season approaches, the scam artists are out, targeting our wallets and personal information. This year, scam artists are increasingly turning to Quick Response (QR) codes to deceive shoppers. These seemingly innocuous codes can lead to significant financial and privacy repercussions if you scan the wrong one.

QR codes, those square barcodes you see on everything from restaurant menus to product packaging, are designed to be scanned by smartphones to quickly access information or websites. While they offer convenience, they also provide a new avenue for scammers to exploit.

Scammers typically replace legitimate QR codes with their own malicious codes. These fake codes can be found on flyers, posters, or even pasted over real codes on physical surfaces. When scanned, these codes can redirect you to phishing websites that look strikingly legitimate. Here, you might be prompted to enter personal information, such as login credentials, credit card numbers, or other sensitive data.

One of the most troubling aspects of QR code scams is their appearance of legitimacy. The scam websites are often meticulously crafted to mimic reputable businesses, making it challenging for even the most vigilant consumers to discern the difference. In many cases, the scams are sophisticated enough to include official logos, matching color schemes, and convincing layouts.

Falling victim to a QR code scam can have serious consequences. Financially, consumers may find unauthorized charges on their credit cards or fraudulent transactions in their bank accounts. In some cases, scammers can gain access to entire accounts, draining funds and causing significant monetary loss.

From a privacy perspective, the risks are equally alarming. Personal information entered on phishing websites can be used for identity theft, leading to further financial damage and a long, arduous process of reclaiming one's identity. Scammers can also sell this stolen data on the dark web, making victims susceptible to additional fraudulent activities.

To safeguard against QR code scams, consumers should take the following precautions:

-

Verify the Source: Only scan QR codes from trusted sources. If you receive a QR code via email or text, verify its legitimacy before scanning.

-

Look for Signs of Tampering: Check for stickers or labels that look out of place or have been tampered with. Scammers often use adhesive labels to cover real QR codes with their malicious versions.

-

Use Security Software: Install and update security software on your smartphone. Some security apps can detect and block malicious websites.

-

Be Skeptical: If a QR code prompts you to enter personal information, be cautious. Legitimate businesses typically won't request sensitive data through QR codes.

by Jim Malmberg

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS