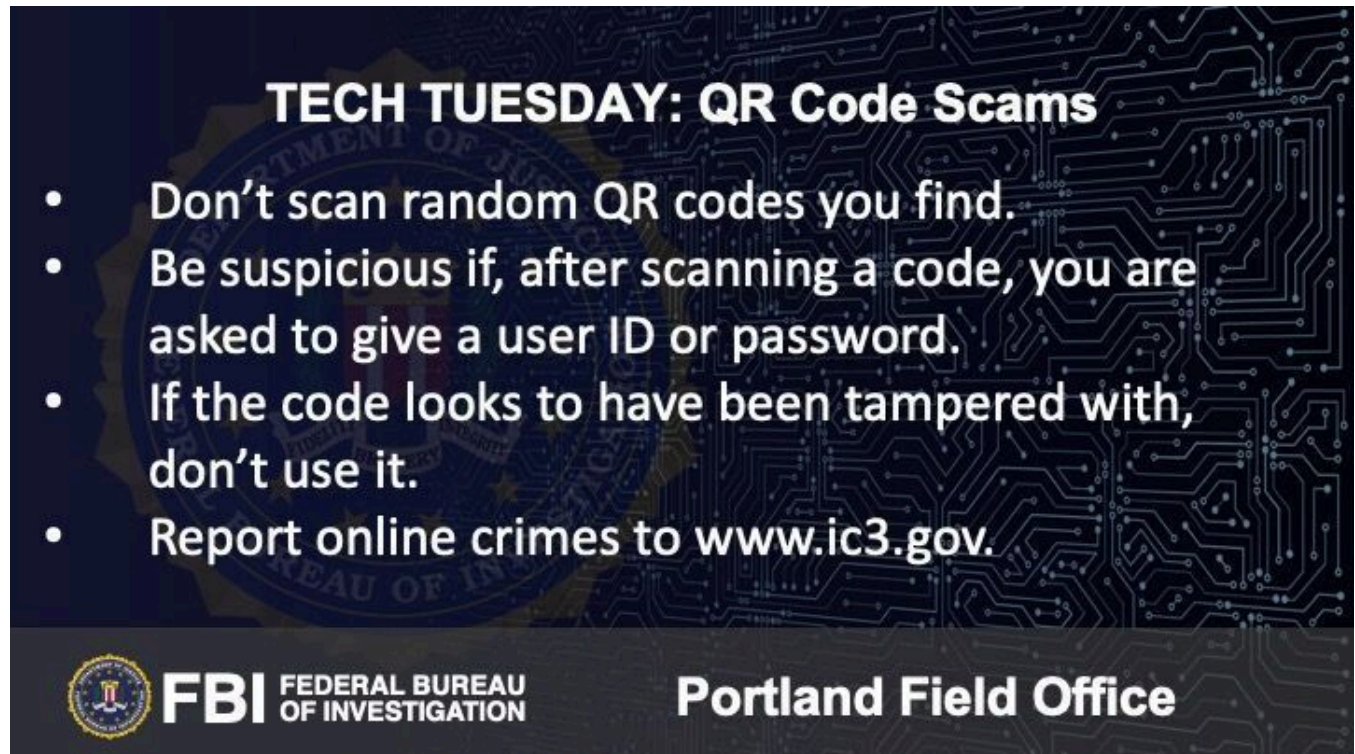


Tech Tuesday: Building a Digital Defense Against QR Code Scams

October 19, 2021

A graphic with a dark blue background featuring a circuit board pattern. In the center is a large, faint circular seal of the Federal Bureau of Investigation. Overlaid on this is the text "TECH TUESDAY: QR Code Scams" in bold white letters. Below this title is a bulleted list of four items. At the bottom left is the FBI logo and the text "FBI FEDERAL BUREAU OF INVESTIGATION". At the bottom right is the text "Portland Field Office" in bold white letters.

TECH TUESDAY: QR Code Scams

- Don't scan random QR codes you find.
- Be suspicious if, after scanning a code, you are asked to give a user ID or password.
- If the code looks to have been tampered with, don't use it.
- Report online crimes to www.ic3.gov.

 **FBI** FEDERAL BUREAU OF INVESTIGATION

Portland Field Office

October is **#CybersecurityAwareness Month**. During this time, the FBI reminds everyone to **#BeCyberAware!** In honor of this recognition, today's Tech Tuesday report will focus on a new scam that is cropping up at restaurants, at stores, and in ads across the country.

Welcome to the Oregon FBI's Tech Tuesday segment. Today: Building a digital defense against QR code scams.

Let's start with basics. "QR" stands for "quick response." The QR code is a square image that you can scan with your phone – usually by just pointing your camera at it. The image itself is filled with data that can do lots of helpful things, such as send you to a particular website or payment portal.

QR codes have become much more common in these COVID times. They allow restaurants to use virtual menus and vendors to accept cashless payments easily. You may find codes physically pasted about or virtually embedded into ads, emails, or online. They are easy to create and, unfortunately, easy to hack.

The FBI is starting to get reports of people who are falling victim to QR code scams, including some who are losing money. One area of particular concern – frauds involving cryptocurrency. Crypto transactions are often made through QR codes associated with crypto accounts... making these transactions easy marks.

If you happen to scan a scammer's bad code, you could end up giving him access to your device. He can access your contacts, download malware, or send you to a fake payment portal. Once there, you can inadvertently give him access to your banking and credit card accounts. If you make a payment through a bad QR code, it's difficult if not impossible to get those funds back. Here's how to protect yourself:

Do not scan a randomly found QR code.

Be suspicious if, after scanning a QR code, the site asks for password or login info.

Do not scan QR codes received in emails unless you know they are legitimate. Call the sender to confirm.

Some scammers are physically pasting bogus codes over legitimate ones. If it looks as though a code has been tampered with at your local bar or restaurant, don't use it. Same thing with legitimate ads you pick up or get in the mail.

Finally, consider using antivirus software that offers QR readers with added security that can check the safety of a code before you open the link.

If you are the victim of any other online fraud, you should report the incident to the FBI's Internet Crime Complaint Center at [www.ic3.gov]www.ic3.gov or call your FBI local office.