UNDERSTANDING QR CODE FRAUD

EMPOWERING SAFER SCANNING

The use of Quick Response (QR) codes has become a popular way to quickly access websites, pay for parking tickets, or view a restaurant menu. While QR codes have simplified online navigation for consumers, they have also made it easier for scammers to access your personal information. Indicators of potential fraud include:

- **Stickers on top of ads.** Scammers will often place a sticker with a malicious QR code over a legitimate code. Ensure that the code you are scanning is part of the original ad, poster, or sign.
- **Short links.** While many legitimate organizations use short links for URLs, they can also be used to hide a malicious URL. Because these links are shortened, you cannot be certain where the link will direct you once scanned.
- **Requests for money over QR code.** A common scammer tactic is to request money through a QR code for a payment that previously did not go through. These codes may direct you to a spoof site that then collects your payment information.
- **Receiving a surprise package with a QR code inside.** Be wary of any unexpected packages you receive that require you to scan a QR code. By scanning the QR code inside the package, you may be granting access to any personal data or information held on your device.
- **Tampering of codes.** Scammers may create QR codes that look nearly identical to legitimate codes. Look out for slight misspellings in the URL or unusual colors in the QR code before accessing the link.

DO'S

When accessing websites using QR codes be sure to take these steps to protect yourself from scammers:

- **Go directly to webpage instead of using the QR code.** If you know what website the QR code is linked to, you can type in the URL instead. This is particularly important if the site you are navigating to requires personal or banking information.
- **Verify the sender.** If you receive a QR code from an organization or person you know, call to confirm that the code is legitimate. Scammers will often pose as businesses or acquaintances in order to gain your trust.
- **Keep your phone up to date with the latest operating system.** Strong passwords, multifactor authentication, and updated software protect your device and accounts from hackers.
- **Pay using a credit card when using a QR code.** While many forms of payment are taken using a QR code, disputes can more easily be made with credit card companies if fraud is detected.

DON'TS

Scammers will attempt to take advantage of your trust. When it comes to QR codes, consider the following tips:

- **Do not scan unsolicited QR codes in email or text messages.** If you do not know who a code is from or you did not request information from that sender, it is best to leave it alone. Otherwise, you risk granting access to the personal information stored on your device.
- **Do not act out of urgency.** Scammers often urge you to act immediately hoping you will miss the warning signs of a malicious QR code. Always inspect codes and verify senders, especially if money or personal information is requested.
- **Do not download an app from a QR code.** To safely download apps, use your phone's app store, verify the logo, and confirm the correct name. This will ensure you are not downloading a spoof app.
- **Do not download a QR scanner app.** While well intentioned, some scanner apps increase your risk of downloading malware onto your device. Most phones have a built-in scanner through the camera app that is safe to use.

For suspected fraud or scams:

- **Call the VSAFE Fraud Hotline: 1-833-38V-SAFE**
- **Visit VSAFE online: www.VSAFE.gov**

VA | U.S. Department of Veterans Affairs