



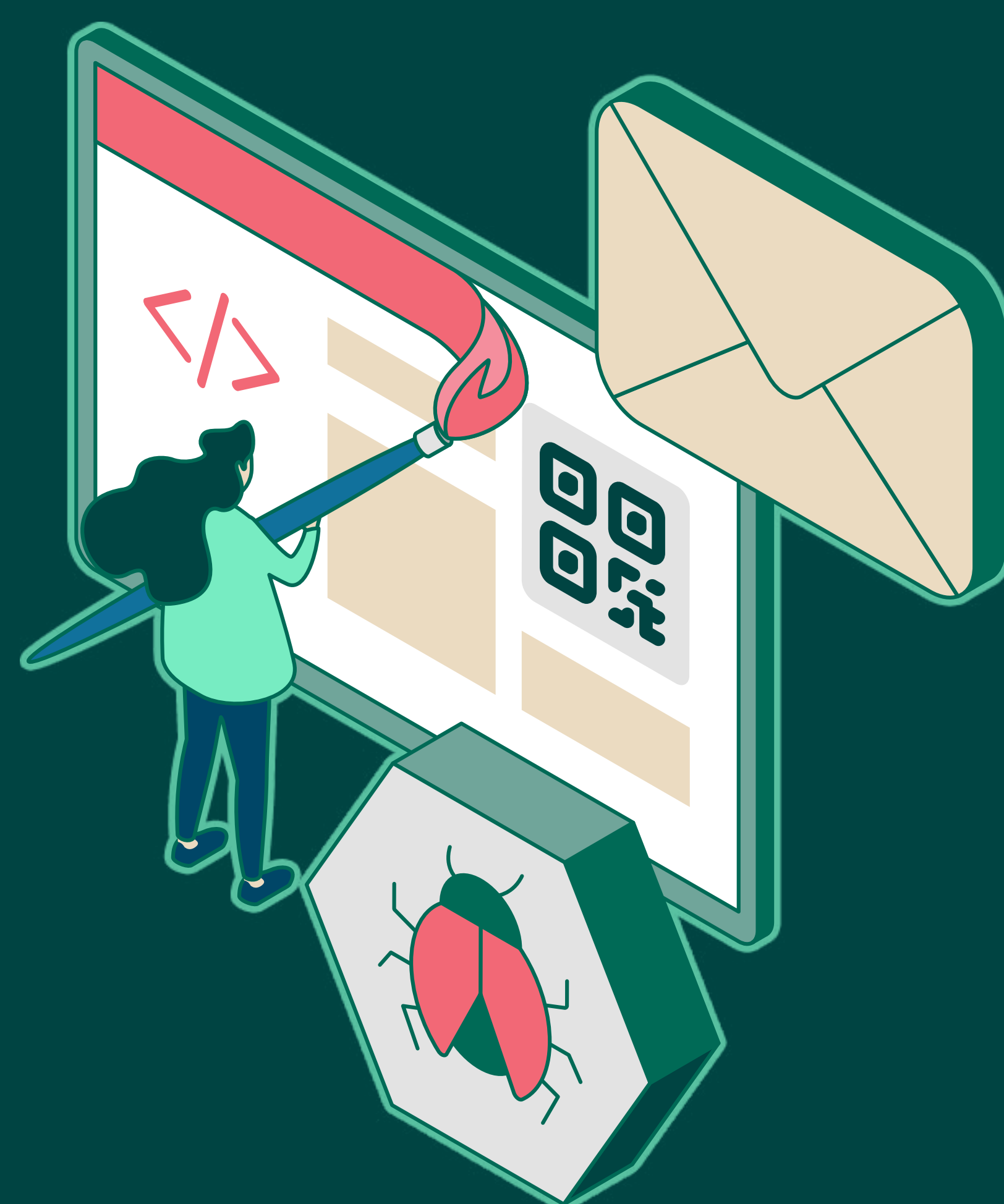
QR CODE PHISHING ATTACKS

Ever notice square bar codes on event flyers, sign-up sheets, or exclusive offers? These are QR codes, and while they seem harmless and offer a quick way to access websites, they can also put your information at risk.

QR code phishing, also known as quishing, is a modern twist on traditional phishing attacks. Instead of clicking a suspicious link in a message, victims are tricked into scanning a QR code that leads to a malicious website. QR codes provide cybercriminals with a convenient and convincing way to trick their targets.

HOW IT WORKS

- Step 1: Fake website creation
 - Attackers build a site that closely mimics a trusted one (e.g., bank, social media, or shopping site), often using a similar domain name.
- Step 2: QR code generation
 - They create a QR code linking to the fake site. These codes hide the full URL, making it hard to spot fraud.
- Step 3: Distribution
 - The QR code is shared via emails, social media, posters, or stickers in public places.
- Step 4: Victim interaction
 - When scanned, the user is taken to the fake site and asked to enter sensitive information like passwords or credit card details.
- Step 5: Data theft or malware
 - The attacker steals the user's data or installs malware on their device.



STAYING SAFE FROM QR CODE PHISHING ATTACKS

Apply these best practices to engage with QR codes safely:

- Do not scan QR codes provided by strangers or displayed in public areas. Always verify the source before engaging with content.
- Before scanning, inspect physical QR codes for overlays, stickers, or signs of tampering. Be skeptical of codes received via SMS or email from unknown senders.
- Scan QR codes using your smartphone's built-in camera or official apps from trusted app stores. Avoid third-party QR scanners.
- Before accessing the site, preview the URL linked to the QR code. Never download apps, files, or enter personal information unless the destination is clearly legitimate and secure.

Always pause and evaluate before scanning a QR code. When unsure about its legitimacy, report it to the appropriate channels (e.g., your IT team, or a manager) to help protect yourself and others from quishing.