# CYBERSECURITY

## Awareness & Advice: QR Codes

**QR codes provides a convenient way to access information or services. Here are some key points to consider when it comes to the potential dangers associated with QR codes:**

1. **Malicious codes:** QR codes is a form of hyperlink. it can be used to carry malicious content, such as malware or phishing attacks. Scanning a QR code could lead to unintended consequences, such as, automatic downloading of malware onto your device or being redirected to a malicious website.
2. **Unauthorized app installations:** Scanning a QR code could also trigger automatic installation of an app into your device without your knowledge or consent. This can potentially grant malicious parties access to sensitive data or compromise your security and privacy.
3. **URL obfuscation:** QR codes can conceal the actual URL behind an innocent-looking code. Attackers can use this technique to trick users to malicious websites that appear legitimate.
4. **Social engineering attacks:** Malicious parties can easily replace legitimate QR codes in unsecured physical locations, such as, restaurants or embedded in emails, messages, or advertisements to deceive users. By encouraging users to scan the code, attackers may exploit their curiosity or trust to gain unauthorized access to their devices or personal information.

**To stay safe when using QR codes, please consider the following security practices:**

1. **Be cautious:** Only scan QR codes from trusted sources or known entities. Check for tampered code, such as a sticker placed on top of the original code, especially when you need to enter login, personal or financial information.
2. **Verify the source:** Double-check the source of the QR code before scanning. If you receive an unsolicited QR code via email, message, or advertisement, do not scan unless you can verify its authenticity.
3. **Use QR code scanning apps cautiously:** Use a reputable QR code scanning app from a trusted source. Some scanning apps have built-in security features, such as, link preview, that can help identify potentially malicious codes.
4. **Check the URL:** Before scanning a QR code, pay attention to the URL or web address it is associated with. If possible, manually type the URL into your browser to ensure it leads to a legitimate website. Do not make electronic payment via QR codes.
5. **Keep your software updated:** Regularly update your device's operating system, apps, and security software to minimize vulnerabilities that could be exploited through QR code attacks.
6. **Trust your instincts:** If a QR code appears suspicious or you have doubts about its legitimacy, it is best to err on the side of caution and avoid scanning it.

**By being aware of the potential risks associated with QR codes and implementing these security measures, you can reduce the chances of falling victim to QR code-related attacks.**

**Important Note: This document does not serve as a guarantee these tips will prevent all variants or methodologies.**