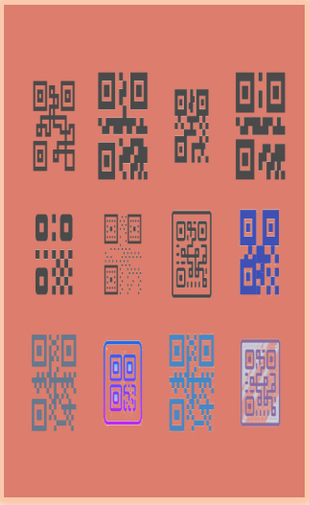
March 20, 2023

CYBERSECURITY AWARENESS

March Monthly Training Bulletin



QR Codes

Quick Response codes (QR codes) are two-dimensional barcodes that can be easily scanned by a smartphone camera to access information. QR codes have become increasingly popular in recent years for various purposes such as marketing, ticketing, and payment transactions. However, QR codes can also be used maliciously by cybercriminals to execute attacks on unsuspecting victims. In this Month's training, we will explore how QR codes can potentially pose a threat and ways to prevent attacks.

Malicious QR codes are those that are designed to trigger an attack on the device scanning them. This can happen when a QR code is used to redirect the user to a website containing malware or phishing pages, or to connect to a malicious Wi-Fi network. In some cases, QR codes can also be used to initiate a call or send a text message to a premium rate number, resulting in unexpected charges on the victim's phone bill.

There are several ways to prevent attacks when scanning QR codes:

Check the source: Always be cautious when scanning QR codes from an unknown source, as they may be used to redirect you to malicious websites or download malware onto your device. It is recommended to scan QR codes from **trusted sources** only, such as those provided by reputable companies or organizations.

Use a QR scanner with built-in security: Use a QR code scanner that has built-in security features, such as anti-malware and anti-phishing protection. This can help to prevent attacks and reduce the risk of being redirected to malicious websites or downloading malware.

Be wary of unusual behavior: Be wary of unusual behavior when scanning QR codes, such as being redirected to a different website than expected or being prompted to download an app or file. If this occurs, do not proceed and exit the page immediately.

Update your device and applications (apps): Keep your device and apps up-to-date with the latest security patches and updates. This will help prevent attacks by fixing known vulnerabilities in the software.

Disable QR code scanning in certain apps: Consider disabling QR code scanning in certain apps, such as social media or messaging apps, to reduce the risk of being targeted by QR code attacks.

QR Codes

In conclusion, while QR codes can be a convenient and efficient way to access information, they can also be used maliciously to execute attacks on unsuspecting victims. To prevent attacks: 1) it is important to be cautious when scanning QR codes from unknown sources, 2) use a QR scanner with built-in security, 3) be wary of unusual behavior, update your device and apps, and 4) consider disabling QR code scanning in certain apps.

By following these tips, you can help to protect yourself from QR code attacks and stay safe online.

Social Media Reporting

As a reminder, you may also submit suspicious social media contacts to phishing@sti-tec.com. Social media is becoming more popular, allowing attackers to take advantage of the platforms and produce a rise in phishing campaigns and other social engineering tactics. Examples of suspicious connections are foreign personnel with little to no information on their profile trying to connect with you on LinkedIn. When reporting these profiles and connections, please include a screenshot and link to the profile as we are keeping track of these contacts and reporting them to the government in support of efforts to shut down these campaigns.

Stay Vigilant, Stay Secure

If you have any questions regarding QR Codes or if you would like to report any unusual activity, please don't hesitate to contact security@sti-tec.com