BEWARE OF THE QR CODE!

What is a QR Code?

A QR code (Quick Response Code) codes are barcodes which contain any kind of information that can redirect scanners to online information, such as website URLs, account information, phone numbers or even coupons. To view this information, you can simply scan the code using the camera app on most smartphones. If your phone doesn't have one, you can download it from your device's app store.

A QRL (Quick Response Code Login) is an alternative to password-based authentication. QRL allows users to log into their accounts by scanning a QR code, which is encrypted with the user's login credentials.

How are they used?

QR Codes started becoming popular in 2011 when American mobile users started scanning them to access websites or to download business cards instead of manually inputting information into their mobile devises. Since the pandemic, the use of QR codes has steadily increased and they are now being used in many additional ways. You may find a QR code has replaced the tangible food and beverage menu at a restaurant in order to cut down on printer costs. Perhaps you have even seen them on the side of a water or soda can or beverage cup at a fast-food facility. In business today, you will often encounter them at conventions and expos for an easy and efficient way a company can connect with you or even have you register for prizes. They are still frequently used as a replacement for business cards as a great way to exchange contact information without having to carry around cards.

Dangers of QR Codes

When the victim scans the QR code, they are redirected to the attacker's web server which in turn can give the attacker control of the victim's device. From there, the attacker has multiple attack vectors and numerous ways to exfiltrate the user's data, such as their current GPS location, device type, SIM card data and other sensitive information. With some additional social engineering tricks, the attacker could take things even further. By using on-device spear-phishing, they could spoof the victim's on-device password keeper. After the victim inputs their username and password, the attacker could gain access to the user's full password safe.

Other methods are through "Quishing" and "QRLJacking". Quishing is when the QR code's URL can take you to a phishing website that tries to trick you into entering your username or password for another website. In a QRLJacking attack, threat actors trick unwitting users into scanning specially crafted QRL rather than the legitimate one. Once the victim scans the malicious QRL, the device gets compromised, allowing the attacking to take over complete control over the device.

How to protect yourself

- **Think before you scan!** Scanning QR codes should never be automatic. Ask yourself if you can trust the QR code. Is it on a menu that a server has handed you, or is it suspiciously stuck to the side of a napkin dispenser? If something seems or feels off, don't scan it.
- **Look for signs of tampering.** Inspect the QR code closely before you scan it. If it appears tampered with, such as the placement of a sticker over the original QR code, or if it doesn't seem to fit with its background, don't scan it.
- **Inspect QR Code URLs.** Review the URL that the QR code is directing you to. Does it seem suspicious? Do a quick web search of the URL to determine if it's legitimate. You can also always go to the actual website directly. Legitimate QR codes have an associated URL under it, giving users the option to navigate there directly.
- **Don't download apps from QR Codes.** Stick to the app store. It is always safer to search for and download an app directly from your device operating system's app store.
- **Beware of texted or emailed QR codes.** Verify the request by contacting the sender using a known number.
- **Train your staff!** Train employees to stop and think about codes, images, and stickers before they scan them.

If you are interested in creating your own QR Codes, there are numerous websites that can help you.