FASTREANDO

¡Cuidado con los Códigos QR! ¡El Phishing Ahora también se oculta allí!

Resumen.

Se ha incrementado el uso de códigos QR maliciosos ("Quishing"), donde los atacantes inducen a los colaboradores a escanear un QR para ingresar a supuestos documentos o portales corporativos y así robar sus credenciales. Este tipo de ataque es riesgoso porque el enlace real no es visible antes de escanear.
Si una cuenta corporativa es comprometida, el atacante podría acceder a correo, VPN o incluso a sistemas relacionados con PCI DSS, generando riesgo de exposición de datos de tarjeta.
Para prevenirlo, los colaboradores deben evitar escanear QRs inesperados, verificar siempre el remitente, no ingresar credenciales en sitios dudosos, y reportar cualquier caso. Si ya ingresaron datos, deben cambiar su contraseña de inmediato.

1. Riesgo actual

Durante los últimos meses se ha incrementado el uso de códigos QR maliciosos en correos electrónicos, mensajes de texto, documentos PDF, facturas, órdenes de compra e incluso carteles impresos.

Este ataque se conoce como "Quishing" (QR + phishing). El atacante envía un código QR indicando al usuario que debe escanearlo para:

- Ver un documento.
- Actualizar su contraseña.
- Acceder a una factura.
- Validar su cuenta.
- Ingresar a Microsoft 365, VPN o correo corporativo.

Cuando el colaborador escanea el código desde el celular, es dirigido a una página falsa que aparenta ser legítima. Allí el usuario ingresa sus credenciales y estas quedan en poder del atacante.

Los códigos QR representan un riesgo importante porque el enlace no es visible antes de escanearlo, por lo que muchos filtros de correo y los usuarios no identifican fácilmente la amenaza.

Señales de Alerta

- Correos con mensajes de urgencia como "Su cuenta será suspendida".
- QRs enviados por remitentes desconocidos.

- Documentos que indican "Escanee para descargar" o "Escanee para iniciar sesión".
- Páginas que solicitan usuario, contraseña o código MFA después de escanear.
- Mensajes que insisten en actuar inmediatamente.

Ejemplo de ataque

Un colaborador recibe un correo aparentemente enviado por el área de TI indicando: "Su contraseña expirará hoy. Escanee el siguiente código QR para renovarla." El colaborador escanea el código, ingresa su usuario y contraseña en una página falsa de Microsoft 365 y posteriormente el atacante utiliza esas credenciales para acceder al correo corporativo.

2. ¿Cómo afecta el entorno PCI o los datos de tarjeta?

El compromiso de una cuenta corporativa puede convertirse en la puerta de entrada al entorno PCI DSS.

Con las credenciales robadas, un atacante podría:

- Acceder al correo corporativo.
- Ingresar a la VPN o escritorio remoto.
- Obtener información sobre servidores, aplicaciones o usuarios.
- Enviar correos fraudulentos desde una cuenta legítima.
- Buscar acceso a sistemas que almacenan, procesan o transmiten datos de tarjeta.

Si las credenciales pertenecen a un usuario con acceso al entorno PCI, existe riesgo de exposición de información confidencial y posible incumplimiento de PCI DSS

3. ¿Qué debe hacer el colaborador?

- No escanear códigos QR recibidos en correos o mensajes inesperados.
- Si el mensaje afirma provenir de TI, banco o proveedor, validar primero con el remitente.
- Escribir manualmente la dirección del sitio en el navegador en lugar de escanear.
- Revisar cuidadosamente la dirección web antes de ingresar credenciales.
- No ingresar usuario, contraseña ni código MFA después de abrir un QR sospechoso.
- Reportar inmediatamente el incidente al área de Seguridad o TI.
- Si ya ingresó sus credenciales, cambiar la contraseña inmediatamente

Fuente: https://www.malwarebytes.com/es/cybersecurity/basics/quishing