Quishing: cómo son las estafas que usan los códigos QR para robar información

10/03/2024

Dentro del mundo de la seguridad informática hay una idea de que, **cuantos más usuarios usen alguna tecnología, más ciberdelincuentes habrá detrás** esperando para aprovecharse. Esto se debe a que no es lo mismo encontrar una falla o un espacio para robar datos en un sistema que tienen miles de usuarios, que hacerlo en uno que tiene **millones o cientos de millones.**

Por este motivo surgió el ***quishing***, una técnica que está siendo cada vez más común y que utiliza los **códigos QR** para robar información a quienes los escaneen; ante esto, es clave saber qué precauciones podemos tomar.

El ***quishing*** tiene como precursor al ***phishing***, una forma de ciberestafa donde se busca robar información al usuario: por lo general se da por medio de correos electrónicos engañosos o

envíos de mensajes que suplantan la identidad de una empresa o persona. El objetivo es robar **datos de tarjetas, cuentas de bancos o contraseñas**.

En en el quishing la estafa tiene el mismo fin, **el engaño**, y comparten una parte de la metodología, pero el ***quishing - o phishing QR-***lo hace a través de un código QR, siendo así más engañoso aún.

El objetivo es que el usuario «caiga en la trampa» y que al ingresar a la pagina donde lo llevó el código QR, la persona -confiada en la confidencialidad del código- brinde datos que luego **los estafadores venderán o usaran para hacer compras en la web**.

El aumento de las estafas con código QR

Los códigos QR tomaron mayor peso en el ultimo tiempo, incluso muchos negocios y servicios pasaron a tener sus **menús en formato digital a través de QR,** además ya ocupan un rol clave en lo que son los **pagos con billeteras virtuales.**

Pero como pasa con todo lo que se hace masivo en el mundo de la tecnología, los estafadores vieron una nueva oportunidad y empezaron a aprovecharse. Ante esto, l**a Comisión Federal de Comercio estadounidense (FTC)** publicó, en diciembre del año pasado, un comunicado donde informaba que **este tipo de estafas estaban en crecimiento**.

“Hay informes de estafadores que encubren los códigos QR de parquímetros con códigos propios. Otros envían un **código QR por mensaje de texto o correo electrónico** e inventan motivos para que los escanees”, explicaron en el informe.

Pago con código QR. Foto: NA

Los expertos de la FTC notaron que **muchos atacantes se hacen**

pasar por empresas de envíos o de correspondencia que argumentan al usuario la necesidad de «actualizar información», o bancos que solicitan la **«confirmación» de datos,** la necesidad de completar registros por algún tipo de «actividad sospechosa» y luego piden el cambio de contraseñas. Es quishing.

Desde la Comisión afirmaron que **"son mentiras que para crear una sensación de urgencia**. **Quieren que escanees el código QR y abras la URL sin pensar".**

Quishing: ¿qué tener en cuenta para evitar este tipo de estafas?

Desde la FTC lanzaron una serie de consejos a tener en cuenta para evitar estafas a la hora de **escanear algún tipo de código QR:**

- Si el código QR está en un lugar extraño o inesperado, es importante **observar bien la URL** para saber a dónde nos envía el código. Si es una pagina que conocemos, hay que **asegurarse de que sea la oficial** (importantísimo) y que no tenga caracteres raros ni especiales.

  Pago online con código QR, economía.

- **No escanear los códigos inesperados que lleguen a través de un correo electrónico o por WhatsApp**, sobre todo si nos piden que lo hagamos de forma rápida, ya que los atacantes siempre **fomentarán y aprovecharán esa «sensación» de urgencia** (ejemplo: es urgente, «tu cuenta se cerrará hoy…») Según el FBI, los correos de **phishing** son el método más popular entre los hackers para enviar ransomware (software malicioso que bloquea el acceso a archivos o sistemas y exige un rescate para restaurar el acceso). Según IBM, el phishing es la c**uarta causa más común y la segunda más costosa de las**

filtraciones de datos, con un costo promedio de 4,65 millones de USD por incidente para las empresas.

Fuente: Canal 26