Phishing

CONOCE MAS SOBRE EL PHISHING

Qué es el phishing?

Es un método utilizado por ciberdelincuentes para obtener información personal y financiera de las personas, como contraseñas, números de tarjetas de crédito y otra información confidencial.

¿Cómo se realiza un ataque de phishing?

Los atacantes suelen enviar correos electrónicos o mensajes de texto falsos que parecen provenir de fuentes legítimas, como bancos, empresas de servicios públicos o redes sociales. Estos mensajes suelen contener enlaces a sitios web falsos, donde los usuarios son engañados para ingresar su información personal.

¿Cuáles son los riesgos del phishing?

Los riesgos de caer en un ataque de phishing pueden ser graves. Los estafadores pueden utilizar la información robada para realizar compras fraudulentas, vaciar cuentas bancarias, robar identidades y cometer otros delitos financieros.

¿Cómo protegerse del phishing?

Para protegerse del phishing, los socios/clientes deben tomar medidas como verificar la autenticidad de los correos electrónicos y mensajes de texto antes de hacer clic en cualquier enlace, evitando ingresar información personal en sitios web no seguros, y utilizar herramientas de seguridad como antivirus y firewalls. Además, siempre es recomendable mantenerse informado sobre las últimas técnicas de phishing para estar preparado y evitar ser víctima de un ataque.

Es importante recordar que la Cooperativa nunca solicitará información personal o financiera a través de correos electrónicos o mensajes de texto. Si tienes alguna duda sobre la autenticidad de un mensaje, es mejor contactar a la Cooperativa a través de los canales oficiales para obtener más información.

Smishing

CONOCE MAS SOBRE EL SMISHING

¿Qué es el smishing?

Es un método utilizada por ciberdelincuentes para obtener información personal y financiera a través de mensajes de texto fraudulentos.

¿Cómo se realiza un ataque de smishing?

Los atacantes suelen enviar mensajes de texto falsos que parecen provenir de fuentes legítimas, como bancos, empresas de servicios públicos o redes sociales. Estos mensajes suelen contener enlaces a sitios web falsos, donde los usuarios son engañados para ingresar su información personal.

¿Cuáles son los riesgos del smishing?

Los riesgos de caer en un ataque de smishing son similares a los de otros ataques de phishing, incluyendo la posibilidad de que los estafadores utilicen la información robada para realizar compras fraudulentas, vaciar cuentas bancarias, robar identidades y cometer otros delitos financieros.

¿Cómo protegerse del smishing?

Para protegerse del smishing, los socios/clientes deben tomar medidas como verificar la autenticidad de los mensajes de texto antes de hacer clic en cualquier enlace, evitando ingresar información personal en sitios web no seguros, y utilizar herramientas de seguridad como antivirus y firewalls.

Es importante recordar que la Cooperativa nunca solicitará información personal o financiera a través de mensajes de texto. Si tienes alguna duda sobre la autenticidad de un mensaje, es mejor contactar a la Cooperativa a través de los canales oficiales para obtener más información

Vishing

CONOCE MAS SOBRE EL VISHING

¿Qué es el vishing?

Es un método de ingeniería social utilizada por ciberdelincuentes para obtener información personal y financiera de manera fraudulenta. Los atacantes suelen hacerse pasar por representantes de empresas legítimas, como bancos, compañías de tarjetas de crédito o proveedores de servicios, para engañar a los usuarios y obtener su información personal.

¿Cómo se realiza un ataque de vishing?

Los estafadores pueden utilizar técnicas como hacer llamadas telefónicas automatizadas, utilizar números falsificados para que parezca que la llamada proviene de una empresa legítima, y utilizar información personal previamente recopilada para hacer que la llamada parezca más auténtica.

¿Cuáles son los riesgos del vishing?

Los riesgos del vishing son similares a los de otros ataques de phishing, incluyendo la posibilidad de que los estafadores utilicen la información robada para realizar compras fraudulentas, vaciar cuentas bancarias, robar identidades y cometer otros delitos financieros.

¿Cómo protegerse del vishing?

Los socios/clientes de la Cooperativa deben tomar medidas como verificar la autenticidad de las llamadas y los correos electrónicos, no proporcionar información confidencial por teléfono o correo electrónico, y utilizar herramientas de seguridad como antivirus y firewalls.

Es importante recordar que la Cooperativa nunca solicitará información personal o financiera a través de llamadas de teléfono. Si tienes alguna duda sobre la autenticidad de una llamada, es mejor cortar las llamadas que pidan este tipo de datos y contactar a la Cooperativa a través de los canales oficiales para obtener más información.

QRishing

CONOCE MAS SOBRE EL QRISHING

¿Qué es el QRishing?

Es un método de phishing que utiliza códigos QR para engañar a los usuarios y obtener información personal o financiera. Los ciberdelincuentes crean códigos QR que parecen auténticos y los colocan en lugares públicos como carteles, publicaciones en redes sociales o incluso en pegatinas que se colocan en productos.

¿Cómo se realiza un ataque de QRishing?

Cuando se escanea un código QR falso con sus dispositivos móviles, son dirigidos a sitios web fraudulentos que solicitan información personal o financiera, o descargan código maliciosos o virus en sus dispositivos. Los sitios web fraudulentos pueden parecer legítimos, como los sitios web de bancos o tiendas en línea, pero están diseñados para engañar a los usuarios.

¿Cuáles son los riesgos del QRishing?

La exposición de información personal o financiera, el robo de identidad, la realización de transacciones fraudulentas y la infección de dispositivos móviles con código maliciosos o también llamados virus o malware.

¿Cómo protegerse del QRishing?

Se debe verificar la autenticidad de los códigos QR antes de escanearlos, utilizando aplicaciones de escaneo de códigos QR confiables y evitando escanear códigos QR de fuentes no confiables. Además, es importante no proporcionar información personal o financiera a través de sitios web o aplicaciones que no sean de confianza. Finalmente, si se sospecha que se ha sido víctima de un ataque de QRishing, es importante notificar a la Cooperativa y tomar medidas para proteger la información personal o financiera.

Es importante recordar que la Cooperativa nunca solicitará información personal o financiera a través de códigos QR. Si tienes alguna duda sobre la autenticidad de un mensaje, es mejor contactar a la Cooperativa a través de los canales oficiales para obtener más información.