Municipalidad de
San Nicolás
de los Arroyos

CIBERDELITOS

Desde el inicio del Aislamiento Social Preventivo y Obligatorio (ASPO), se vio un notorio aumento de denuncias ante la oficina de información al consumidor por estafas virtuales, por eso compartimos algunos modus operandi más comunes para que estés atento y no te dejes engañar.

Las principales recomendaciones son:

1) PHISHING: Los delincuentes envían un correo electrónico engañoso, buscando obtener datos personales. Son mensajes que en apariencia provienen de un banco o un organismo legítimo. Nos dicen que tenemos un problema con el banco, empresa o institución y que necesitan que hagamos algo de manera urgente o que cambiemos la clave, token o tarjeta de coordenadas.

No ingreses datos personales en sitios utilizando enlaces que llegan por correo electrónico, podrían ser fraudulentos. Tené cuidado con los enlaces sospechosos y asegurate siempre de estar en la página legítima antes de ingresar información de inicio de sesión. Leé con cuidado cada correo electrónico que recibas.

Aprendé a diferenciar un perfil verdadero de uno falso en redes sociales.

Los perfiles legítimos tienen una tilde azul de autenticidad. Los perfiles falsos generalmente solo tienen publicaciones muy recientes y poca cantidad de seguidores.

2) Si te llega un mensaje o un mail: Leé detalladamente toda la información. No brindes datos por mensaje de texto, correo electrónico o whatsapp.- No informes tu usuario, clave, contraseñas, PIN, Clave de la Seguridad Social, Clave Token, DNI original o fotocopia, foto, ni ningún tipo de dato personal.

3) Si es un llamado telefónico: Cortá la comunicación y contactate con el ente oficial que supuestamente está realizando la llamada.- Tené en cuenta estos signos de alarma cuando los estafadores operan por teléfono: principalmente, no quieren darte tiempo para pensar sobre sus argumentos de venta; lo único que les importa es que vos digas que “sí”.

Generalmente, te dicen lo siguiente: Si escuchás algo que suena parecido a las frases de esta lista, decí **“no, gracias”**, colgá.

- Usted ha sido especialmente seleccionado (para esta oferta).
- Si usted compra nuestro producto recibirá una bonificación o premio gratis.
- Usted se ha ganado uno de los cinco valiosos premios.
- Usted se ha ganado una importante cantidad de dinero en un sorteo de lotería extranjera.
- Esta es una inversión de bajo riesgo y le ofrece un rendimiento mas alto que cualquier otra inversión.
- Usted tiene que decidirse inmediatamente.
- ¿Confía en mí, verdad?
- No es necesario que verifique la reputación de nuestra compañía con nadie.
- Aplicaremos los cargos de envío y despacho a su tarjeta de crédito.

Prestá atención y recordá

- No eses redes de WI - FI públicas para acceder a sitios que requieran contraseñas.
- Mantené actualizado tu navegador, el sistema operativo de los equipos y las aplicaciones (se recomienda eliminar las que no se utilizan).
- No uses equipos públicos o de terceras personas para acceder a aplicaciones, redes sociales o cuentas personales.
- Utilizá contraseñas fuertes mezclando mayúsculas, minúsculas y números. Tienen que ser fáciles de recordar, pero difíciles de adivinar por otras personas. No uses la misma clave para distintas aplicaciones, cuentas, plataformas o sitios.
- Nunca acudas a un cajero automático, abras una app o accedas al home banking cuando recibas una llamada supuestamente proveniente de la entidad bancaria. El cliente debe ser el que origina la llamada.
- Tomate un minuto para pensar antes de actuar. Quienes realizan este tipo de estafas apelan a las emociones, descuidos y urgencias.

Si sufriste alguno de estos delitos acercate a la Oficina Municipal de Información al Consumidor (OMIC), en Av. Savio 22 de lunes a viernes de 7:00 a 13:00.

Secretaría de Gobierno
Oficina Municipal de Información al Consumidor
O.M.I.C.