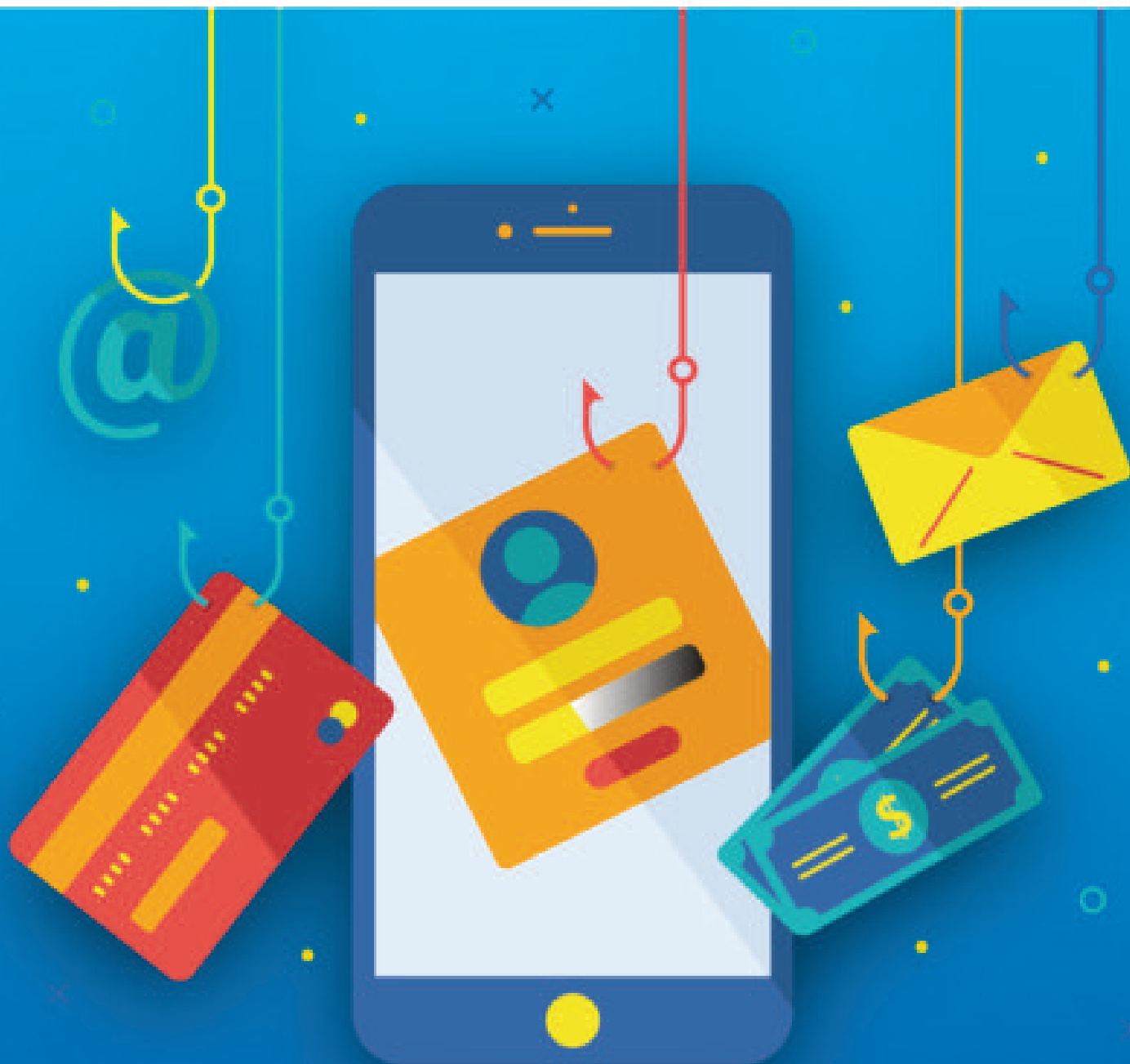


GUIA PRÁCTICA PARA LA PREVENCIÓN DEL PHISHING

Phishing quiere decir suplantación de identidad. Es una técnica de ingeniería social que usan ciberdelincuentes para obtener información confidencial de las tarjetas de crédito y los usuarios de forma fraudulenta



Los ciberdelincuentes envían correos electrónicos falsos como anzuelo para “pescar” contraseñas y datos personales valiosos. Estos mails contienen información falsa y enlaces que redirigen tus respuestas hacia páginas de internet falsas. Desean obtener:

DATOS DE CONTRASEÑAS



Nº DE TARJETAS DE CRÉDITO



DNI

CUIT O CUIL

NOMBRES DE USUARIO



CÓDIGOS PIN

Cuando obtienen estos datos realizan compras, reservas o extracciones de dinero utilizando tu nombre

CONSEJOS PARA EVITAR SER VÍCTIMA DE PHISHING

- Para verificar si fuiste víctima de un ataque de Phishing revisá en forma periódica tus resúmenes bancarios buscando transferencias que no autorizaste.
- No facilites información confidencial por mail ni por teléfono (números de cuenta, clave de la tarjeta de crédito o contraseñas de acceso a redes sociales o cuentas de correo).
- Tené en cuenta que los ciberdelincuentes se hacen pasar por una empresa o servicio conocido y los enlaces presentes en los correos electrónicos te redirigen a páginas fraudulentas que simulan ser las oficiales.
- Si deseas actualizar tus datos en el sitio web oficial de algún organismo u organización escribí vos mismo la dirección web de la organización en el navegador.
- Nunca entres a los links o archivos adjuntos al mensaje.
- Evitá descargar archivos. No te expongas a que se instale en tu computadora un malware (o programa malicioso) y robe tu información personal.
- Corroborá siempre la dirección URL de la página web a la que accedas. No debe tener alteraciones tales como: faltas de ortografía, reemplazo de letras por números, minúsculas por mayúsculas o a la inversa.



¿CÓMO DENUNCIAR?

No contestes, no reenvíes y no borres el correo electrónico o el mensaje de Whatsapp. Es la prueba del delito de estafa (Art. 172 y 173 del Código Penal) y servirá a los expertos en informática del Ministerio Público Fiscal para rastrear y atrapar a los delincuentes.

Comunicate con la Fiscalía de tu jurisdicción y realiza la denuncia. No necesitás abogado: la podés hacer vos mismo de forma presencial o enviar un correo electrónico a las direcciones creadas a tal efecto. Se pueden encontrar en este link: <https://www.mpba.gov.ar/denuncia>

Podés consultar más información sobre Phishing en: <https://www.mpba.gov.ar/phishing>

Fuentes: Ministerio Público de la Provincia de Buenos Aires | Ministerio de Justicia y Derechos Humanos de la Nación