LA CIBERSEGURIDAD ENTRE TODOS

BANCA ELECTRÓNICA

5 Consejos
para un manejo responsable y seguro

Identifique los mensajes sospechosos:

Los mensajes fraudulentos pueden llegar a través de un correo electrónico, un mensaje de texto (SMS) o incluso por sus redes sociales (WhatsApp, Facebook, Instagram, etc.)

¿Cómo sé que es un mensaje sospechoso?
Hágase las siguientes preguntas:

¿Lo esperaba? Esto debe hacerle sospechar inmediatamente. **Si usted recibe un mail de un banco con el cual no opera, elimínelo**.

¿Reconoce a quién le envía el mensaje? Verifique que el dominio del correo recibido corresponda a la entidad bancaria que dice haberlo enviado. Ejemplo: servicioalcliente@**scotiabank.com.uy**.
Recuerde: los bancos no usan cuentas de Hotmail o Gmail.

¿Le pide que haga algo? En los phishing suelen pedir que realice alguna acción como clickear en enlaces, descargar archivos o responder con información sensible.

Antes de hacer clic:

- Si no está seguro del mensaje que recibe, confirme desde un canal de confianza. Por ejemplo, si tiene dudas de una comunicación del banco, ingrese en el área de cliente y revise si tiene notificaciones pendientes. También puede llamar al banco para verificar si ellos enviaron ese email. **Recuerde, si sospecha, repórtelo**
- En caso de que el correo proceda de una entidad bancaria legítima, nunca contendrá enlaces a su página de inicio de sesión o documentos adjuntos
- No contestar en ningún caso a estos correos
- Tener precaución al seguir enlaces o descargar archivos adjuntos en correos electrónicos, SMS, mensajes en WhatsApp o redes sociales, aunque sean de contactos conocidos

Unidad de Ciberdefensa del Ejército
Contacto: ucibere@ejercito.mil.uy
Reportar un incidente: ecsirt@ejercito.mil.uy
2208 1542 Int. 12024