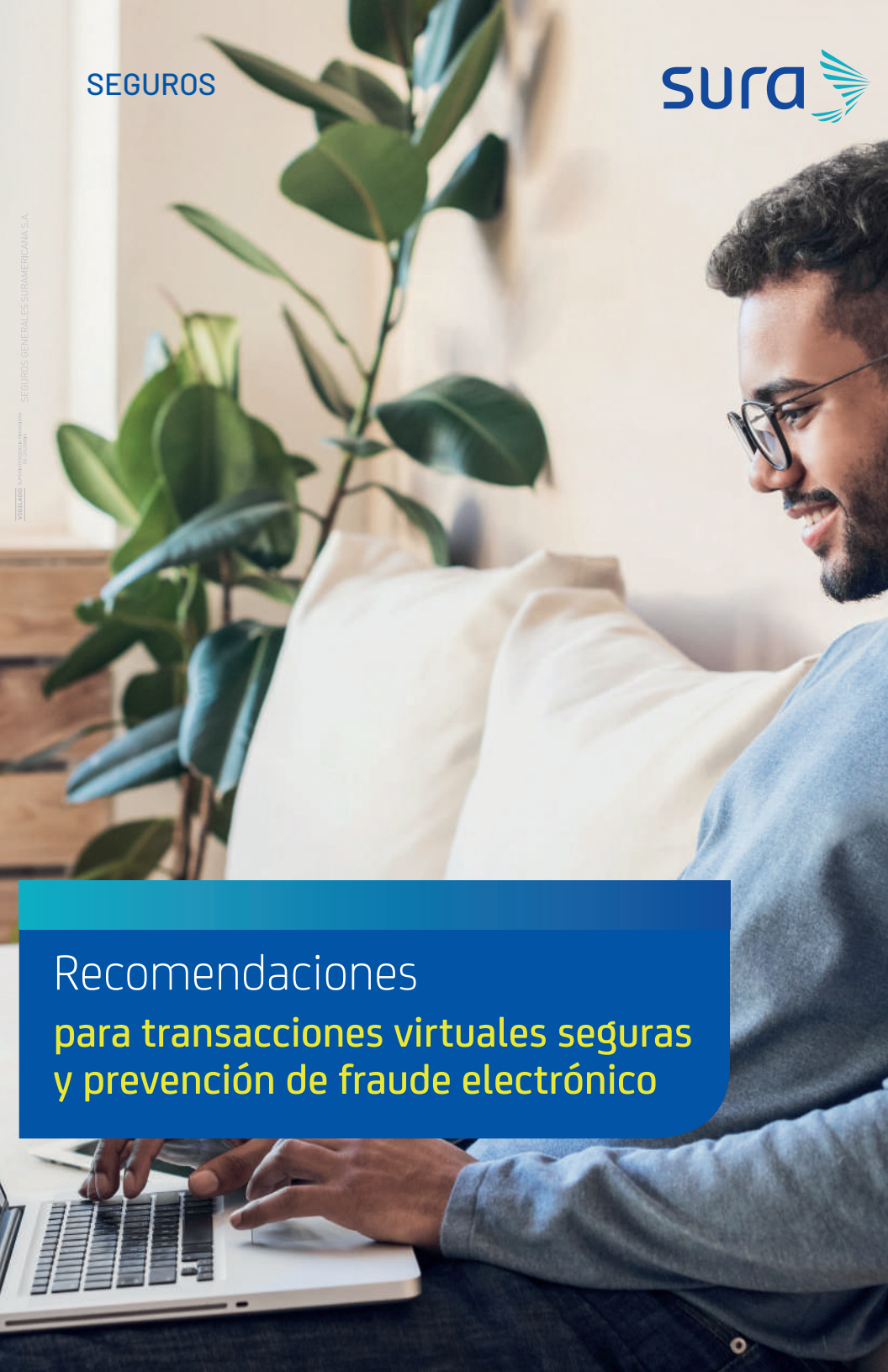
SEGUROS



Recomendaciones

para transacciones virtuales seguras y prevención de fraude electrónico

Recomendaciones para transacciones virtuales seguras y prevención de fraude electrónico

1. **Cuando vayas a realizar transacciones virtuales,** asegúrate de utilizar una red Wifi privada o de disponer de mecanismos de navegación segura como una VPN (Virtual Private Network) para cifrar todos los datos que se usan en esos momentos. Las redes Wifi abiertas suelen contar con pocos o nulos filtros de seguridad, exponiéndote a riesgos cibernéticos en mayor grado.

2. **Evita utilizar equipos de terceros para realizar las transacciones en línea** ya que te expondrás a que puedan estar intervenidos físicamente para robo de datos o información. Incluso, por un olvido en cierre de sesión, podrás dejar expuesta tu información o dejarla en los historiales de navegación de dichos equipos.

3. **Realiza tus transacciones en sitios web de confianza:**
Verifica que el nombre de la página web esté escrito correctamente, de esta manera te aseguras de estar conectado al sitio deseado.

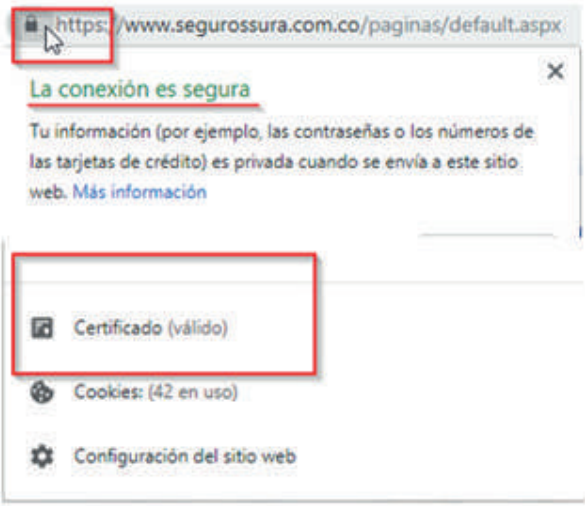
I

II Verifica que la url tenga https:

Al navegar por páginas https garantizas que la información viajará en la red de forma segura y no será fácil que un cibercriminal la intercepte.

III Verifica que el candado que se ve al lado izquierdo de la dirección url aparezca cerrado.

IV Ahora valida que el certificado de seguridad sea real, dándole clic en el candado de la esquina superior izquierda de la url:



Cuando el certificado digital es válido, el sitio está acreditado por entidades reguladoras a nivel internacional, asegurando la identidad del titular y asociando dos claves: una pública y otra privada en poder del titular del certificado.

4. **Desconfía de promociones muy atractivas**, probablemente estas ofertas te lleven a una red fraudulenta y termines perdiendo tu dinero. **Como recomendación: referénciate del vendedor y valida el precio del producto en otros establecimientos.**

5. **Conoce la opinión que tienen otras personas frente a los productos que quieres adquirir y sobre el sitio en el que lo quieres comprar.** Es importante referenciarte en las secciones de "Reviews" y opiniones, publicadas por otros usuarios para identificar si las tiendas online ofrecen una buena experiencia al cliente.

6. **Evita ingresar a las páginas web desde enlaces recibidos a través de correo electrónico.** Estos correos normalmente llegan con los siguientes asuntos:

- Pérdida de cuentas.
- Bloqueo de cuentas debito o crédito.
- Deudas en la DIAN odeclaración de renta.
- Retrasos en el pago cesantías o pensiones.
- Pago de comparendos.
- Citación a juzgados o fiscalías.
- Elegido para recibir una herencia.
- Hoja de vida o CV (Curriculum Vitae)
- Vacuna del coronavirus

En caso de recibir un correo electrónico de un destinatario NO esperado, se recomienda no abrirlo y comunicarse directamente con la entidad que te está "reportando" el acontecimiento. Este es el modo de operación denominado phishing, mediante el cual se realizan robos de información.

7. **Recuerda tener el equipo personal con el sistema operativo actualizado** para disminuir brechas de seguridad, además de contar con un antivirus activo.

8. **Recuerda activar en tu banco de confianza tu tarjeta virtual:** e-Prepago, Ecard o tarjeta Online (El nombre puede cambiar según el banco). Esta tarjeta virtual permite hacer compras o pagos por internet sin exponer los datos de tu tarjeta física como son: nombre del titular, numero de la tarjeta, fecha de vencimiento de la tarjeta y el número de seguridad CVV. Esto disminuye la probabilidad de fraude financiero. Para obtener más información sobre la tarjeta virtual, te sugerimos preguntar en tu banco de confianza.

9. **Revisa frecuentemente los movimientos y extractos de tus tarjetas de crédito y débito, con el fin de monitorear periódicamente posibles anomalías, fraudes o robos de identidad.**

10. **Recuerda activar o añadir una contraseña a tu tarjeta de crédito.** Puedes activar esta opción para tu tarjeta de crédito de acuerdo con la franquicia:

A. Visa: Verified by Visa.
B. Mastercard: Mastercard Secure Code.
C. American Express: American Verify Card Safe Key.

Mediante la activación de este sistema, recibirás un código que puede llegar vía mansaje de texto o correo electrónico. Este código debes ingresarlo en el momento de la compra.

11. **Recuerda activar los mecanismos de protección para la seguridad de tu información y tus transacciones, como lo son:** alertas y notificaciones, primera y segunda clave, identidad protegida (usuario), topes en los valores de las transacciones, entre otros. Haz uso de ellos, así disminuirás el riesgo de ser víctima de fraude. Para más información ponte en contacto con tu banco de confianza.

12. **Las entidades financieras nunca te solicitarán tus datos financieros como usuarios, claves, números de tarjetas de crédito con sus códigos de seguridad y fechas de vencimiento mediante vínculos de correo electrónico.** En caso de recibir un correo que te estén solicitando esta información, ponte en contacto inmediatamente con la entidad y evita ser víctima de robo de información o transacciones fraudulentas.

13. **Evita almacenar páginas de entidades financieras o pasarelas de pago en favoritos.** Digita siempre la dirección de la página de la entidad a visitar en la barra del navegador. Esto disminuye el riesgo de ingreso a una página que migro o cambio su dominio, evitando ser víctima de un phishing.

14. **No descargues archivos o instales programas de fuentes desconocidas;** estos pueden contener programas maliciosos escondidos o virus que pueden comprometer tu información, dándole acceso a los cibercriminales.

15. **Si recibes llamadas telefónicas solicitando tu información financiera** para recibir supuestos premios, o si te piden consignar alguna cantidad de dinero para recibirlo, haz caso omiso y contáctate con tu entidad financiera para validarlo y denunciar en caso de resultar un intento de fraude. Este es el modo de operación del Vishing, modalidad de fraude electrónico muy utilizada.

16. **Cambia tus claves frecuentemente y memorizalas, no la escribas en documentos o papeles de fácil acceso.** Te recomendamos usar administradores de contraseñas que faciliten su uso mediante una clave maestra que te dará acceso a las demás. Recuerda, es ideal que tu clave no sea la misma para los diferentes aplicativos.

17. **Cuando vayas a crear un usuario y clave**, recuerda NO asociarlos a tus nombres, el de tus seres cercanos, fechas de nacimiento, números telefónicos o cédulas. Al realizar esta práctica, le estarás facilitando a los ciberdelincuentes la identificación de esta información. Te invitamos a consultar nuestra ***Guía para construcción y administración segura de contraseñas.***

18. **Cuando te ofrezcan vía telefónica cambiar el plástico de tu tarjeta débito o crédito,** nunca entregues la información de tu tarjeta anterior. Incluso puede que estas personas que te llamaron vayan físicamente hasta tu domicilio; de igual manera nunca entregues tu tarjeta así ellos se ofrezcan a romperla o llevarla a otro lugar para tener registro de esta. No permitas que por ningún motivo se lleven tu tarjeta, así esté rota o dañada.

19. **Cuando te tomes fotografías y las quieras publicar en redes sociales**, ten cuidado de no mostrar tu información financiera o transaccional (tarjetas de crédito, débito, extractos, facturas, entre otras).

20. **Cuando te lleguen a tu correo electrónico, formatos o extensiones de documentos no conocidos, no los abras** y mucho menos si el destinatario es una dirección desconocida. Recuerda algunos formatos bien conocidos y de uso frecuente: doc – pdf – xlsx, aunque es importante desconfiar si al abrir estos formatos te solicita habilitar "Macros". Adicionalmente algunos formatos que nunca debes abrir si te llegan adjuntos de destinatarios desconocidos son: **exe – py – sh – js – zip.**

21. **Analiza siempre todos los adjuntos con un antivirus,** siendo precavido, porque existe la posibilidad de que algún miembro de nuestra familia o conocido, sin saberlo, esté reenviando correos maliciosos.

22. **Las pasarelas de pago son entidades tercerizadas por alguna empresa que ofrece sus productos en internet y ayudan en la intermediación de la compra del producto.** Estas compras tienen tres modalidades de pago:

A. Tarjetas crédito.
B. Tarjetas debito.
C. Emitir una factura de compra para pagar en puntos de atención física.

Estas pasarelas de pago brindan un escalón adicional de seguridad frente a las compras directas en tiendas virtuales en las que te solicitan pagos directos a cuentas de ahorros o corrientes.