



# Recomendaciones de seguridad en compras online

El grupo de trabajo de medios de pago y ciberseguridad de la Cámara de la Economía Digital del Uruguay, integrado por **Bamboo Payment, Datasec, Evertec, OCA, Senpai Academy y VisaNet**, presenta un conjunto de recomendaciones de seguridad para las compras online.



CÁMARA  
DE LA ECONOMÍA  
DIGITAL DEL URUGUAY



Desde CEDU sostenemos que comprar online es seguro, y más seguro es si se toman en cuenta las siguientes recomendaciones:

- Utiliza una conexión a Internet segura y evita redes públicas.
- Revisa las medidas de seguridad en la transacción (cerciórate que el sitio sea seguro [<https://www.>], candado en el navegador, por ejemplo).
- Busca y lee cuidadosamente las políticas de privacidad y los términos y condiciones del sitio en el que realizas la compra electrónica, antes de comprar, o ante dudas, muchas veces las preguntas más frecuentes están incluidas allí.
- Revisa que en el sitio en el que realizas la compra electrónica, se informe su domicilio, números telefónicos u otro medio para acudir al comercio en caso de necesidad.
- Presta atención al sitio antes de aceptar todas las cookies: al hacerlo, si la página no es segura, se aumenta el riesgo de vulnerabilidad por el intercambio de información que se abre al aceptar esto. De acuerdo a la definición que presenta Google en su sitio de privacidad y términos “Una cookie es un pequeño fragmento de texto que los sitios web que visitas envían a tu navegador. Las cookies permiten que los sitios recuerden información sobre tu visita”.
- Si el sitio web te resulta sospechoso o desconocido, antes de comprar chequea referencias o averigua más, por otros medios, de la veracidad del mismo.
- Establece alertas y notificaciones de compra en tiempo real con tus medios de pago (tarjetas, bancos, otros)
- Revisa con periodicidad tus transacciones en los sistemas que proveen los medios de pago (bancos, de tarjetas de crédito, prepagas, otros.)
- Siempre cierra la sesión cuando hayas terminado de realizar tu compra y obtenido los comprobantes de la transacción.
- Nunca envíes por mail u otros medios (teléfono, vía pública, domicilio) tus datos de acceso bancario, ni tu información de inicio de sesión en sitios de compra, o de medios de pago.
- El phishing (suplantación de identidad) es uno de los principales factores de riesgo, por lo que presta atención a la dirección de mail o el nombre de la dirección que aparece en tu navegador (URL) siempre que ingreses información.
- Si el sitio lo permite, verifica la reputación del vendedor.
- Utiliza siempre todas las herramientas o funcionalidades de seguridad que tu medio de pago tenga disponibles.