STOP | THINK | CONNECT™

CONSEJOS PARA PROTEGER LAS COMPRAS EN LÍNEA

Ser un/a comprador/a en línea precavido/a empieza con **PARAR.PENSAR.CONECTAR.**: tomar medidas de precaución, pensar en las posibles consecuencias de los actos personales, y disfrutar de las ventajas tecnológicas con tranquilidad mientras compramos en línea. Recuerde estos consejos al realizar sus compras.

CONSEJOS DE COMPRAS EN LÍNEA

- INVESTIGUE: cuando use una página web nueva para realizar sus compras, lea opiniones de usuarios para ver si otros han tenido experiencias positivas o negativas al usar esa página.
- SI DUDA, TÍRELO: Los enlaces por correo electrónico, tuits, así como artículos y publicidad en línea a menudo contienen la llave de acceso a su computadora para cíber criminales.
- SUS DATOS PERSONALES SON COMO EL DINERO; RECONOZCA SU VALOR, Y PROTÉJALOS: cuando realiza compras en línea, esté alerta para conocer qué tipo de información suya es necesaria para realizar una compra. Asegúrese que la cantidad de información necesaria es razonable. Y recuerde, sólo debe rellenar los campos 'obligatorios' – normalmente marcados en rojo o con asteriscos- cuando llegue a la pantalla de caja.
- USE MÉTODOS DE PAGO SEGUROS: las tarjetas de crédito son normalmente las más seguras porque permiten al consumidor obtener un rembolso de la tarjeta si el producto adquirido no llega o no es lo que ha pedido.
- NO SE DECEPCIONE: lea las políticas de devoluciones/cambios por adelantado para saber a qué atenerse si el producto no es lo que usted deseaba o necesitaba.
- PROTEJA SU DINERO: Cuando maneje sus cuentas o haga compras en línea, compruebe siempre que la seguridad de esa página esta activada. Cuando la página comienza por https:// esa 's' al final indica que la conexión tiene protección adicional. No pague en páginas que no tienen "https".

DE COMPRAS EN TIENDAS REALES

- ESTOY, NO ESTOY: hay tiendas y comerciantes que utilizan seguimiento de Bluetooth y Wi-Fi de la gente para enviar publicidad si el usuario está en su zona. Apague Bluetooth y Wi-Fi cuando no lo esté usando en su teléfono y tableta.
- EVITE LOS 'HOTSPOTS' DE WI-FI: limite lo que hace en Wi-Fis públicos abiertos, y tenga cuidado si necesita entrar en cuentas vitales con contraseña, como por ejemplo su correo electrónico o banca en línea. Ajuste las opciones de seguridad de su teléfono o tableta para protegerlo de ataques ajenos antes de hacerlo.

CONSEJOS BÁSICOS DE SEGURIDAD

- MANTENGA SU EQUIPO LIMPIO: Todos los dispositivos que se conectan a la red –incluyendo PCs, teléfonos y tabletas- se pueden proteger de virus y malware si tiene siempre actualizadas todas las versiones de programas y apps.
- ESTÉ DOS PASOS POR DELANTE: habilite el uso de autentificación bifactorial en aquellas cuentas que lo permiten. Esto le da una capa adicional de protección, más allá del nombre de usuario con contraseña.
- USE MEJORES CONTRASEÑAS: si tiene claves débiles, mejórelas usando frases (sí, frases) con mayúsculas, minúsculas, cifras y símbolos; y utilice contraseñas distintas para cada cuenta.

Traducido del original por Terry Inskip para OAS FCU.