ASOCIACIÓN DE BANCOS DE MÉXICO

Recomendaciones de seguridad en compras a través de comercio electrónico

¡Generar una conciencia de prevención, en materia de seguridad de la información es vital hoy en día!

PROTEGE TUS DATOS CUANDO HAGAS TRANSACCIONES EN LÍNEA

- No instales software pirata, de escasa reputación o de fuentes no confiables en los dispositivos donde realices las compras, ¡estos deben ser de tu absoluta confianza!
- Es muy importante actualizar el sistema operativo, tu navegador web y la aplicación de la tienda. De esta manera reparas las posibles debilidades de este software, además de agregarle nuevas funcionalidades que mejoren la experiencia de compra.
- No utilices computadoras de sitios como salas de Internet públicas o de renta. Del mismo modo, no te conectes desde redes públicas o compartidas, ya que la red informática debe ser de plena confianza. Esto ayudará a reducir los riesgos asociados a la intercepción de los datos bancarios sobre la red.
- Si los datos bancarios están en tu dispositivo portátil, asegura que tu dispositivo cuente con mecanismos de autenticación. Debes estar consciente del lugar donde tienes almacenados tus datos bancarios y asegurarte de reducir estos sitios al mínimo necesario.
- Verifica que la URL del comercio sea legítima. También revisa la fecha de creación del sitio web; prefiere aquellos que tengan algún tiempo considerable en el mercado.
- Otra opción interesante es contar con una tarjeta virtual, la cual es una tarjeta de crédito o débito ofrecida por algunos bancos, cuyo CVV (código de verificación) u otro dato bancario,

	cambia en cada transacción, haciéndola temporal y de un solo uso.
Dispositivos Móviles	▪ Nunca lo pierdas de vista y cuida a quien le prestas tu celular. ▪ Realiza una copia de seguridad de los datos del dispositivo. ▪ Activa el acceso a tu dispositivo mediante el PIN (número de identificación personal) o por el medio que lo permita (huella del dedo, foto o Iris del ojo). ▪ Usa una contraseña de acceso segura. ▪ Utiliza la opción de bloqueo automático. ▪ Evita acceder y enviar información a páginas Web no confiables ▪ No enviar información sensible a través de redes Wifi. ▪ Activa las conexiones por Bluetooth, infrarrojos y WiFi solo cuando vayas a utilizarlas. ▪ Asegúrate de que la información transmitida o recibida esté libre de Malware (Programa maligno), instala y mantén a actualizado antivirus y sistemas operativos, navegadores y aplicaciones. ▪ Descarga aplicaciones y software legal solo de sitios de confianza de sitios oficiales. ▪ Desactiva cuando sea posible las funciones de geolocalización. ▪ Tapa la cámara de tus dispositivos cuando no los estés usando. ▪ Cierra todas las sesiones iniciadas al terminar de usarlas. ▪ Protege tus servicios Online con contraseñas robustas. ▪ Utiliza contraseñas diferentes para cada servicio. ▪ En redes sociales, desconfía de perfiles desconocidos.

	▪ No publiques información personal que puedan utilizar en tu contra. ▪ Guarda el número IMEI (La identidad internacional del equipo móvil). ▪ Instala una aplicación de borrado de datos remoto para usarlo en caso de robo o extravío del dispositivo móvil, al bloquear el equipo telefónico mediante el IMEI, el aparato queda inservible.
IDENTIFICA POSIBLES ATAQUES DE PHISHING	▪ Verifica el remitente de los correos. ▪ Comprueba la dirección a la que te dirige un enlace antes de pulsarlo. ▪ Busca posibles errores de ortografía y gramaticales. ▪ Ponte alerta ante requerimientos urgentes. ▪ No descargues archivos adjuntos ni pinches en enlaces si no estás seguro de su origen.
IDENTIFICAR POSIBLES ATAQUES DE INGENIERA SOCIAL	▪ Los ataques de ingeniería social se realizan por diversos canales, sentido común y precaución son los mejores aliados en la defensa contra la ingeniería social: - Por correo electrónico, mediante ataques de tipo phishing - Por teléfono, a través de una técnica conocida como vishing, que consiste en realizar llamadas telefónicas suplantando la identidad de una persona o compañía para conseguir información confidencial de las víctimas - Por mensaje de texto (smishing), ataque en el que también suplantan la identidad de una compañía y con el que los cibercriminales intentan principalmente que las víctimas

	pinchen en un enlace, llamen a un número de teléfono o respondan al mensaje.
GLOSARIO	▪ Spam: Correo basura. ▪ Phishing: Sitios falsos dedicados al robo de credenciales de acceso. ▪ Vishing: (Voice phishing) ocurre cuando un estafador crea un sistema de voz automatizado para hacer llamadas a los usuarios y pedirles información privada. ▪ Smishing: Mensajes de texto dirigidos a los usuarios de telefonía móvil con el fin de que visiten, por ejemplo, una página web fraudulenta. ▪ Spyware: Software malicioso para recabar información del usuario e instalar publicidad molestosa sin consentimiento del usuario. ▪ Malware: Software creado con la intención de robar información o dañar la computadora. ▪ Crackers: Expertos informáticos dedicados a intervenir los sistemas con propósitos malintencionados. ▪ WPS PIN: Mecanismo creado para facilitar la conexión de dispositivos a nuestra WiFi. ▪ IoT: Internet de la Cosas. ▪ Ingeniera Social: Manipular psicológicamente a las víctimas con objeto de que proporcionen la información que los cibercriminales necesitan para realizar accesos ilegítimos a sus equipos.

Asociación de Internet MX.

- Compra en sitios web que sean conocidos y con buena reputación.
- Revisa los comentarios de otros compradores y las calificaciones que otorgan.
- Cuestiona y compara cuando veas precios que son demasiado baratos, sobre todo si son sitios o vendedores poco conocidos o de reputación dudosa.
- Asegúrate que los sitios que visitas cuenten con un certificado de seguridad, éste parece como un candado a un lado de la barra de dirección del sitio y al dar click sobre él puedes ver detalles sobre la seguridad del certificado.
- Revisa que al visitar un sitio estás en la dirección correcta y no en una página que se ve igual, para esto asegura que la dirección está correctamente escrita en tu navegador.
- Si recibes ofertas por correo electrónico o redes sociales que te redireccionan a un sitio, corrobora que la dirección de la página a la que eres redireccionado está correctamente escrita. De preferencia no abras las ligas de los correos y dirígete directamente al sitio donde quieres comprar.
- Mantén actualizado el sistema operativo de tus equipos y dispositivos, así como las aplicaciones que utilizas.
- Es recomendable realizar los pagos a través de medios de pago con altos estándares de seguridad y otras compañías reconocidas para evitar que le proporciones tus datos bancarios a cualquier sitio.
- Protege tus dispositivos y equipos con contraseñas robustas.
- No compartas tus contraseñas con nadie.
- No utilices la misma contraseña en dos servicios o sitios distintos y utiliza un gestor de contraseñas.

- Una contraseña robusta puede generarse de distintas formas, ya sea con caracteres aleatorios o basada en algunas palabras o frases fáciles de recordar para ti, siempre y cuando no sean fáciles de asociar con tu persona o adivinarlos con base en algún dato público como fechas de nacimiento, CURP, nombre de mascotas, etc. o el nombre del servicio que se está protegiendo; puedes intercalar algunos caracteres especiales y mayúsculas con minúsculas para hacerla más robusta.
- Instala y actualiza software de seguridad como antivirus, antimalware y firewalls.
- Realiza copias de seguridad (respaldos) de tu información y realiza pruebas de que funcionan.

ANTAD
Asociación Nacional de Tiendas de Autoservicio y Departamentales, A.C.

AMVO
ASOCIACIÓN MEXICANA DE VENTA ONLINE

RAZONES PARA ADQUIRIR PRODUCTOS EN LÍNEA SON:

1. Comprar el producto que te gusta y recogerlo en tu tienda favorita a la hora que quieres o recibirlo a domicilio
2. Comprar a cualquiera hora del día o de la noche
3. Ahorrar tiempo
4. Realizar compras desde cualquier lugar de la republica
5. Revisar las reseñas de otros compradores
6. Comparar los precios entre las tiendas desde tu casa
7. Encontrar productos que no están siempre disponibles ahora mismo en tu tienda

AMVO
ASOCIACIÓN MEXICANA DE VENTA ONLINE

RAZONES PARA ADQUIRIR PRODUCTOS VÍA ONLINE SON:

1. Recibir las compras a domicilio.
2. Ahorrar tiempo.
3. Más promociones y descuentos que en tienda física.

4. Encontrar productos que en ningún otro lugar.
5. Realizar compras desde cualquier lugar.

Tips para una compra en Línea segura

1. Siempre usa conexiones seguras. Evita las redes abiertas o públicas. Si no conoces la red WiFi a la que te estás conectado, no coloques ningún dato personal o bancario. (Puede ir una señalética de prohibido o un ¡OJO!).
2. Compra solo en páginas con https. Si al e commerce en la que quieres comprar no tiene esto en su URL, NO compres ahí. Esto ayuda a proteger tus datos bancarios y es obligado para tener un procesador de pago.
3. Revisa las reseñas de otros usuarios. Las opiniones positivas y negativas de otros consumidores, nos dan una idea sobre cómo es la experiencia de compra, del estado de los productos o del tiempo de entrega. Un dato importante: si no tiene reseñas, mejor evita comprar ahí.
4. Precios y descuentos razonables. Compara precios en otros lugares: si el precio suena irreal, por ejemplo, un smartphone muy barato, probablemente se trate de una estafa.
5. Verifica sus redes sociales. Son otra fuente de información de la tienda, tanto para conocer productos, sistema de envíos y opiniones de usuarios.

Recomendaciones para comprar en línea.

1. Da clic solo a enlaces que estés seguro a dónde llevan. Lee las políticas de privacidad de la tienda.
2. Antes de comprar, revisa la descripción del producto, condiciones de envío, entrega, devolución y cambio.

	3. Conoce todos los métodos de pago de la tienda: no siempre es necesario tener una tarjeta de crédito o débito. 4. Guarda los comprobantes que se generen de tu compra: número de orden, número de transacción; si tu compra fue con un particular, verifica sus datos personales. 5. Califica tu compra para que otros consumidores conozcan tu experiencia.


¿Cómo comprar en línea de forma segura?
Razones para adquirir productos vía online son:
1 Recibir las compras a domicilio.
2 Ahorrar tiempo.
3 Más promociones y descuentos que en tienda física.
4 Encontrar productos que en ningún otro lugar.
5 Realizar compras desde cualquier lugar.
TIPS para una compra en línea segura
1 Siempre usa conexiones seguras. Evita las redes abiertas o públicas. Si no conoces la red WiFi a la que te estás conectando, no coloques ningún dato personal o bancario.
2 Compra solo en páginas con https. Si en la e commerce en la que quieres comprar no tiene esto en su URL, NO compres ahí. Esto ayuda a proteger tus datos bancarios, y es obligatorio para tener un procesador de pago.
https:// http://
3 Revisa las reseñas de otros usuarios. Las opiniones positivas y negativas de otros consumidores, nos dan una idea sobre cómo es la experiencia de compra, del estado de los productos o del tiempo de entrega. Un dato importante: si no tiene reseñas, mejor evita comprar ahí.
4 Precios y descuentos razonables. Compara precios en otros lugares: si el precio suena irreal, por ejemplo, un smartphone muy barato, probablemente se trate de una estafa.
% $
5 Verifica sus redes sociales. Son otra fuente de información de la tienda, tanto para conocer productos, sistema de envíos y opiniones de usuarios.
Recomendaciones para comprar en línea
1 Da clic a enlaces que estés seguro a dónde llevan. Lee las políticas de privacidad de la tienda.
2 Antes de comprar, revisa la descripción del producto, condiciones de envío, entrega, devolución y cambio.
3 Conoce todos los métodos de pago de la tienda, no siempre es necesario tener una tarjeta de crédito o débito.
4 Guarda los comprobantes que se generen de tu compra: número de orden, número de transacción; si tu compra fue con un particular, verifica sus datos personales.
5 Califica tu compra para que otros consumidores conozcan tu experiencia.
¿Por qué comprar en El Buen Fin vía online?
Según el Reporte de Buen Fin 2018 de la Asociación Mexicana de Venta Online, las tres principales razones son:
Las personas compran en línea porque ofrecen mejores descuentos y ofertas que en las tiendas físicas.
Evitan las aglomeraciones en las tienda física.
Sus compras fueron productos o servicios que no pueden adquirir en tienda física.
Fuente Estudio AMVO ASOCIACIÓN MEXICANA DE VENTA ONLINE
www.amvo.org.mx
/amvomex /company/amvo