



JULIO 2023

**MES DE LA
CIBERSEGURIDAD**

JORNADAS DE

**CONCIENTIZACIÓN Y EDUCACIÓN
POR UNA CULTURA DIGITAL SEGURA
PARA TODOS LOS HONDUREÑOS**



AHIBA

ASOCIACIÓN HONDUREÑA
DE INSTITUCIONES BANCARIAS

¿CULTURA DE LA CIBERSEGURIDAD? ¿PARA QUÉ?

Estas Jornadas por la Ciberseguridad, organizadas por la Asociación Hondureña de Instituciones Bancarias, tienen por objetivo colaborar con los usuarios digitales en la prevención de los riesgos asociados al uso de Internet y el mundo digital, aportando consejos y herramientas.

La Educación es una herramienta para prevenir el crimen y la delincuencia organizada. No solo actúa contra conductas delictivas, sino que nos permite concientizar de los impactos negativos que estas pueden tener en nuestras vidas. Al concientizar los riesgos, podemos incorporar hábitos seguros.

La concientización de los usuarios y el trabajo conjunto de todas las instituciones públicas y privadas nos permitirán luchar contra los delitos cibernéticos, y así procurar una sociedad digital segura para poder beneficiarnos de todas las ventajas que nos trae este mundo conectado.

La incorporación de estos hábitos es lo que llamamos Cultura de la Ciberseguridad. Y en esto queremos ayudarlos.



EL BUEN USO DE INTERNET

Nuestra vida diaria y nuestras actividades dependen de las computadoras y dispositivos móviles: Nos permiten comunicarnos, trasladarnos, hacer compras, pagar cuentas, acceder a los sistemas de salud y seguros, acceso a todo tipo de aplicaciones que nos facilitan la vida, pero **-si no tenemos los cuidados adecuados-** nos pueden exponer a riesgos que **solo nosotros podemos evitar. Los beneficios y riesgos del uso de Internet** y todos los desarrollos tecnológicos que día a día nos asombran, **impactan en casi todos los ámbitos de nuestra vida.**

Internet es uno de los grandes inventos del siglo XX, pues permite tantas posibilidades y beneficios para la sociedad que se ha convertido en una cuestión prácticamente indisoluble de nuestro día a día. Ha cambiado incluso la manera de informarse, comunicarse, relacionarse entre las personas y entretenerse. Ser consciente de ello nos permitirá disfrutar de lo que nos brindan todo tipo de dispositivos, las aplicaciones más novedosas y útiles, así como los desarrollos tecnológicos que se vienen.



CÓMO CUIDARNOS EN INTERNET

Internet ofrece enormes ventajas pero también conlleva riesgos que van desde el acceso a contenidos no apropiados para menores (violentos, sexuales, ilegales, etc.); la exposición de nuestra privacidad, o la provisión de información o datos personales de la familia y conocidos.

Es importante estar atentos, ya que los delitos o engaños vinculados a la digitalización de la vida, **llegan a las personas directamente y los llevan a tomar decisiones y realizar acciones que terminan perjudicándolos**. Es por ello que es muy necesario desarrollar **hábitos preventivos** que eviten lamentar las consecuencias que pueden tener estas conductas descuidadas. Para evitar riesgos por un mal uso o un uso descuidado, es necesario tener en cuenta algunos consejos.

Y para que sean de fácil recordación, los hábitos seguros deben implementarse en tres ámbitos del cuidado:

Atención a la información

**Acceso a nuestros
Dispositivos**

Información Personal

ESTAR ATENTOS A LA INFORMACIÓN

Constatar la información encontrada y evitar basar una decisión en falsas promesas. Es importante verificar la información que consiguió en sus búsquedas de Internet o recibida a través de otros canales digitales. No todo lo que se publica es verdad, es importante contrastarla con testimonios de personas reales que permitan verificarla.

- Antes de decidir una compra, revisar los comentarios o calificaciones del producto o servicio. Verifica que el negocio o empresa a la que le estés comprando exista efectivamente y cumpla con lo que ofrecen.
- Prestar atención al link al que estamos accediendo. Verifica que sea el sitio correcto y que además tenga el “candado de seguridad” al inicio de la dirección. Sino, ¡no ingresar! ya que la seguridad de navegación no está garantizada y podemos dejar que un tercero con intenciones maliciosas quiebre nuestra privacidad y seguridad.
- Revisa todas las condiciones de contratación antes de aceptar términos y condiciones. Tomate el tiempo de leer en detalle todo lo que implica la compra o contratación, condiciones y particularmente política de devolución o cambio, para asegurarte que tu dinero está bien invertido.
- Desconfía de ofertas realizadas por teléfono, mail o WA, especialmente si son muy ventajosas o te apuran para tomar la decisión y menos aún si te piden algún desembolso de dinero como garantía o gastos de apertura de una cuenta o una autorización de un crédito.



IMPEDIR EL ACCESO DE TERCERAS PERSONAS A NUESTROS DISPOSITIVOS.

Esta claro que no lo hacemos a propósito, en general esto pasa por usar sitios no seguros o caer en descuidos en nuestra navegación. Para ello es necesario tener en cuenta los siguientes aspectos: riesgos involuntarios.

- **Antivirus:** Proteger nuestros dispositivos contratando y manteniendo actualizados los antivirus y barreras que bloqueen el acceso de terceros no deseados.
- **Cookies:** Ser conscientes de que aceptar las cookies en una web significa dar permiso al sitio para que recopile información de nuestros gustos e intereses, obtenga datos como el idioma de nuestro navegador, la ubicación, o que guarde nuestro usuario, entre otros. No le des automáticamente el Aceptar a las cookies, verifica las opciones para que ellas sean lo menos invasivas posibles. La opción no aceptar en algunos casos está disponible y es la más segura.



Redes de Wifi: Cuando necesiten hacer una gestión que requiere seguridad, no utilizar redes de wifi públicas o abiertas, así nos aseguramos estar conectados a una red que proteja nuestra navegación. Cuidamos así la información privada o confidencial que compartimos y las compras, gestiones o transacciones bancarias que realizamos.

Cierra la sesión de cualquier programa y dispositivo cuando lo termines de usar. Así evitarás que ingresen en ellos.

Apps. Instalar solamente aplicaciones oficiales desde las tiendas de Google Play o Apple Store y App Gallery.

Mensajería Instantánea: Activa la verificación de dos pasos de tus plataformas de WA u otro servicio de mensajería instantánea, evitará que te hackeen tu teléfono por esta vía.

Actualiza tu navegador. Borra contraseñas guardadas, accesos a links, y otros usos del navegador para evitar riesgos



PROTEGER LA INFORMACIÓN PERSONAL

Ella es la llave de acceso a nuestra privacidad y nuestro patrimonio. Es importante tener en cuenta que existen delincuentes reales o producto de la inteligencia artificial, que nos llegan con mensajes falsos o nos invitan a entrar en aplicaciones o links que solo tienen por objetivo cometer un delito. Lo único que nos protege en todos estos casos es no compartirles información que les de acceso a robarnos nuestra privacidad o nuestro dinero. Queda en nuestras manos implementar estos consejos para evitar caer en engaños que nos quitarán valores personales:

- ¿Dónde guardar los datos personales? No guardar en los dispositivos información de claves, usuarios, pins u otros identificadores que habilitan el uso de nuestras aplicaciones o vínculos poniendo. Tampoco guardar las contraseñas en los sitios web o apps donde normalmente hace sus transacciones.
- Crear identificaciones seguras y propias. Que tus contraseñas no contengan datos personales como nombre, apellido, fecha de nacimiento u otros fácilmente adivinables. Además, cámbialas periódicamente y evita usar la misma contraseña para diferentes servicios, así se reducen las posibilidades de que descubran tus claves de protección.
- Contactos y Galería de Fotos u otros contenidos almacenados: Nunca des acceso digital a estos contenidos que son privados y pueden comprometer tu seguridad y la de tus conocidos.

Cuidar tu seguridad es una labor cotidiana que debe ir adaptándose a las nuevas circunstancias y aplicaciones, es vital mantenerse informado. Además, prestar atención, tener una conducta correcta en Internet y ayudar a las personas sirve para fortalecer la Ciberseguridad, si ellas están seguras, aumenta nuestra seguridad, porque vivimos en conexión.

CIBERSEGURIDAD EN EL USO DE LA BANCA

Los Bancos de Honduras están actualizados con las últimas tecnologías que garantizan la seguridad de sus transacciones, con excelentes resultados. Los clientes de los Bancos pueden estar seguros que sus ahorros están muy bien cuidados en su banco de confianza.

Los Cuidados Personales necesarios en el uso de la Banca en Línea, no son diferentes a los que tienen que ver con el uso de Internet en general:

Redes y Dispositivos

Datos y Claves

**Accesos a tus
Productos Bancarios**

Para facilitar su implementación los vamos a resumir en conceptos generales que podrán guiar tus cuidados:

Redes y dispositivos

Para operar con Online Banking o a través de la App, nunca te conectes desde una Red de Wifi pública o abierta o que no sea la de tu casa, trabajo o teléfono celular, es decir una red segura.

No hagas operaciones bancarias por la calle, mientras estás caminando o en lugares donde te pueden sustraer tu teléfono o computadora. Si extravías o te roban el celular, solicita el bloqueo de tu App en el Banco. Y luego comunícate con su servicio de atención al cliente para volver a darla de alta una vez que tengas tu nuevo dispositivo o hayas recuperado el antiguo.

En definitiva, elige un lugar seguro para hacer tus transacciones bancarias.

Datos y Claves

Crea claves seguras y diferentes para cada cuenta bancaria, que no contengan información personal ni números consecutivos o iguales. No recicles las de otras cuentas.

- **Renueva tus contraseñas cada tres meses.**

(link al Banco en cuestión para explicar como generar o cambiar la contraseña)

- **Nunca compartas tus datos:** usuario, contraseña, clave de seguridad, documento, domicilio, así como cualquier otro sistema de identificación y autenticación de su perfil.
- **Guarda tus claves y nombres de usuarios en un lugar seguro, nunca en tu celular o computadora.**

Tampoco compartas tus usuarios y contraseñas por WA, redes sociales o mails. Ni los datos de Token u otras identificaciones enviados de manera segura por tu banco para validar una operación.

En definitiva, tus datos son tuyos, cuédalos y no los compartas con nadie. Tu Banco nunca te pedirá tu usuario, contraseña, código o pin.



ACCESOS A TUS PRODUCTOS BANCARIOS

Para comunicarte con tu banco, utiliza su app oficial o sino escribe el link de acceso a su página en el buscador. Esto es lo seguro, ya que, si haces una búsqueda en Internet, pueden aparecer perfiles falsos. De todas formas, siempre puedes verificar los links seguros que son aquellos que tienen un candado cerrado. Los perfiles falsos son casi iguales a los verdaderos, pequeños cambios en su composición pueden llevarnos a una confusión.

(imagen de la app o página del Banco, imagen de perfil falso)

No permitas que nadie manipule tu app o el acceso a tu cuenta a través del Online Banking.

Al acudir a una sucursal nuestros ejecutivos solo podrán guiarte, pero no pueden operar tu aplicación bancaria u online banking.

No confíes en los correos electrónicos vinculados a tus operaciones de dinero que te mandan un link o para descargar un archivo, lo mismo en mensajes de texto o chats, llamadas telefónicas o perfiles en redes sociales. Menos aún si te piden que ingreses tus datos para validar operaciones, Tu Banco nunca te pedirá esto a través de estos canales. No permitas que usen tu cuenta para fines que no sean tuyos, aunque lo que te ofrezcan a cambio sea muy tentador. **Puede traerte problemas serios con la Justicia.**



No uses WhatsApp para contratar un servicio financiero, ni busques o aceptes préstamos financieros en redes sociales.

Cierra la sesión al terminar tus trámites en el Banco, así estés operando desde tu computadora o la App de tu Banco.

Activa las notificaciones de movimientos para que te informen vía correo electrónico las operaciones que se hacen en tus cuentas. En este mismo sentido, verifica periódicamente tus resúmenes de cuenta y de tarjeta.

Tampoco compartas tus usuarios y contraseñas por WA, redes sociales o mails. Ni los datos de Token u otras identificaciones enviados de manera segura por tu banco para validar una operación.

En definitiva, verifica siempre que estás comunicado con tu Banco y que solo tu puedas realizar tus operaciones bancarias.

¡Conseguir tu dinero te costó mucho esfuerzo y trabajo! Entonces no te apures en tus transacciones online. es mejor consultar con tu banco o una persona de tu confianza, que correr riesgos innecesarios!

Ante cualquier duda, consulta con nuestros canales de información al usuario.

Y NO LO OLVIDES, NUNCA COMPARTAS TUS CLAVES O CONTRASEÑAS, LE ESTARÁS DANDO LA LLAVE DE ACCESO A TU PRIVACIDAD Y PATRIMONIO A LOS CIBERDELINCUENTES.

GLOSARIO

LLAMEMOS A LAS COSAS POR SU NOMBRE

En los medios, redes o también en la información provista por entidades públicas o privadas, puedes encontrarte con conceptos que confunden. A continuación incluimos un detalle de las palabras que hoy están circulando, teniendo en cuenta que la evolución del mundo digital inventará nuevas palabras alrededor de la ciberseguridad.

Pero lo importante es que ante cualquier situación tu tienes que proteger la información que da acceso a tu privacidad y a tu patrimonio. ¡No la compartas con nadie!

**VISHING, PHISHING, SMISHING,
ANGLER PHISING, DOXING, ETC.**

SON DIFERENTES ESTRATEGIAS

PARA ROBARTE TU INFORMACIÓN Y TU DINERO.



No importa el nombre que le pongan, son las nuevas formas de llamar al delito. Se trata de pescarte desprevenido, y para ello utilizan:

- Canales actuales o nuevos (teléfono, mails, mensajes de texto o WA, perfiles falsos en redes sociales, aplicaciones con falsas promesas)
- Formas escritas, audios o videos o inteligencia artificial.
- Información engañosa o mentiras.
- Te empujan a que tomes una decisión rápida.

Suplantación de Identidad:

Como explicábamos en el punto anterior, los delincuentes se hacen pasar por otros para robarte tus datos y así acceder a tus bienes. Verifica que quién te esté contactando, sea efectivamente la persona o entidad verdadera.

SIM Swapping:

El delincuente reportará por el robo de un chip, y pedirá uno nuevo que retirará de tu empresa de telefonía para acceder a tu información. Consulta con tu telefónica, los cuidados a tener para este tipo de situaciones.

Ingeniería Social:

Diferentes técnicas de manipulación que utilizan los ciberdelincuentes para obtener información confidencial de los usuarios.

Red Oscura:

Es un lugar en Internet donde tienen lugar muchos tipos de actividades ilícitas. Parecen la World Wide Web (www) pero tienen nombres extraños que nos confunden respecto de los reales. Para estar seguros, evita visitar sitios no seguros, solo aquellos que tienen el candado cerrado al inicio del link.

Fraudes Cibernéticos:

Son actividades encaminadas a defraudar a través de medios digitales a un cliente para que entregue su dinero o patrimonio o que busca dañar de alguna forma su salud financiera en general por medio de prácticas engañosas e ilegales.

Cuentas Mula:

Los delincuentes te ofrecen dinero o beneficios si les permitas hacer operaciones ilícitas o ilegales a través de tus cuentas, exponiéndote a consecuencias penales que pueden llevarte a la cárcel. No lo permitas.





AHIBA
ASOCIACIÓN HONDUREÑA
DE INSTITUCIONES BANCARIAS

FORTALECIENDO LA CULTURA DIGITAL EN HONDURAS

www.ahiba.hn

Síguenos en:

