Límites Inteligentes y Bienestar Digital

Un evento de Alianza por la Seguridad en Internet A.C. **ASI México**

Ponencia en línea

Participación especial de la Guardia Nacional:

Lic. Víctor Agustín Jiménez Juárez

Primer Subinspector

Prevención de delitos electrónicos en Internet

CDMX, Oct 2020

RESUMEN DE CONSEJOS PARA USUARIOS DE INTERNET

Acceso a la ponencia completa en el canal de YouTube de ASI México:

Para contactar a la Guardia Nacional, acceder a la Línea del Centro Nacional de Atención Ciudadana, marcando al **088.**

La Guardia Nacional te puede asesorar antes de hacer una compra en Internet.

Es importante verificar que la página en dónde se vaya a hacer una compra pertenezca a una empresa legítima, y de preferencia, que cuente con el sello de confianza de la Asociación de Internet de México (www.asociacióndeinternet.mx)

Aunque la oferta parezca muy atractiva, y señale que es “sólo por tempo limitado”, es importante saber que en muchos casos se puede tratar de un fraude, por lo que antes de comprar, se puede solicitar asesoría al 088.

Los intentos de fraude más reportados a la Línea de Denuncia de ASI México son:

- Venta de flotillas de autos a precios de remate (suplantando empresas legítimas)
- Ofertas de empleo
- Trámite de pasaportes
- Trámite de documentos ante registro civil (acta de nacimiento, de matrimonio, etc.)

Si una persona es engañada en un sitio web, y a manera de prueba toma un **screenshot** de la página (copia de la pantalla), es recomendable que se haga desde una computadora en lugar de usar una tableta o un celular, ya que así aparece más información en la copia.

Es importante recordar que en los perfiles y contactos de Internet, existe la **suplantación**, una persona que nos contacte puede decir que se llama “Pedro Hernández”, y tratarse de una identidad falsa, con foto, datos y referencias falsas.

La Guardia Nacional puede asesorar a los usuarios sobre los elementos que hacen único a un perfil en una red social, para que pueda aportarlos en su caso a una investigación. (Minuto 13:00)

En caso de perder un dispositivo digital, o que nos sea robado, es importante presentar la denuncia ante el agente del Ministerio Público de nuesrta localidad, para ampararnos por el mas uso que se le llegue a dar, tanto al dispositivo, como a los datos personales o privados que estuvieran almacenados en él.

Es importante proteger el acceso a nuestros dispositivos con claves, NIPs (Número de Identificación Personal), o cuando sea posible, con elementos biométricos como la huella digital o el reconocimiento facial, para impedir que personas no autorizadas tengan acceso a la información que se almacena en ellos.

Si un celular es robado o extraviado, es necesario reportarlo primero a nuestro operador de telefonía, e informarle el número IMEI del teléfono para que sea bloqueado de inmediato.

Para saber el número IMEI de tu teléfono, marca *#06# para que te lo muestre en pantalla, y almacénalo en un lugar seguro.

Guardia Nacional actual en colaboración con las autoridades judiciales y con los proveedores de telefonía y servicios de Internet, para determinar el origen de contenido enviado en la red.

En el caso de una investigación sobre un presunto delito en el que se usaron uno o más dispositivos digitales, se debe contar con la orden de un juez, solicitada por el Agente del Ministerio Público a cargo de dicha investigación, para que se pueda intervenir su contenido.

El Ministerio Público tiene la obligación de recibir todas las denuncias de los ciudadanos, sin importar el monto que impliquen.

En casos de Sexting (intercambio voluntario de fotos intimas que se comparten en forma privada), si una de las personas que almacena esas imágenes, amenaza a la otra con revelarlas, es posible presentar la denuncia por acoso.

A partir del minuto 35:00 se aborda el tema del Sexting, y cómo es atendido por las autoridades, y se aclara que cuando las imágenes de Sexting corresponde a menores de edad, se considera pornografía infantil, y en caso de obtenerse algún tipo de lucro por su distribución, se considera entonces trata de personas.

Se debe tener cuidado al prestar el teléfono a otras personas, pues pueden manipular el contenido del mismo sin nuestro consentimiento. Por ejemplo, pueden publicar una foto que se encuentre en el carrete, o compartirla en grupos de mensajería.

Se recomienda a los usuarios de aplicaciones de redes sociales, que cierren sus sesiones siempre que terminen de usarlas, para evitar lo que se señala en el párrafo anterior.

Antes de seguir a un perfil en redes sociales de una figura pública, como artistas o deportistas, se recomienda asegurarse de que esté verificado por los administradores de las plataformas, lo que usualmente se reconoce por una pequeña palomita azul a la derecha del nombre del perfil, de esta forma se evita el riesgo de entrar en contacto con perfiles falsos que son frecuentemente usados para enganchar a menores de edad hacia actividades ilícitas por medio de falsas promesas o premios.

El **Grooming**, o cortejo, es el proceso paciente y sistemático que llevan a cabo personas mal intencionadas para lograr la atención de niños, niñas y adolescentes, para a través de engaños, ganar su confianza poco a poco hasta lograr convencerlos de salir a un encuentro físico.

Es importante verificar que realmente se conoce a una persona antes de agregarla como seguidor en nuestros perfiles de redes sociales.

Se le recomienda a los padres de familia revisar las aplicaciones que sus hijos instalan en sus dispositivos, para asegurarse que no exponen su privacidad, ni los acercan a la posibilidad de contactar a personas mal intencionadas, o bien, a contenido inapropiado.

La Guardia Nacional recomienda a los padres de familia dialogar con sus hijos sobre los riesgos en Internet, para que siempre estén prevenidos. Por ejemplo, explicarles que en Internet pueden toparse con personas mal intencionadas, posiblemente pederastas, que van a abusar de su exceso de confianza para tratar de engancharlos.

En www.civismodigital.org se pueden encontrar recursos para entender mejor los riesgos y dialogarlos en familia.

Es recomendable supervisar la lista de contactos de los hijos, dialogando con ellos sobre el riesgo que puede surgir en caso de agregar a personas no verificadas.

La Guardia Nacional también puede asistir a las autoridades en casos de ciber-bullying.

La Guardia Nacional recibe capacitación de NCMEC (National Center for Missing and Exploited Children) y del FBI, y participa en operaciones internacionales de investigación de delitos como la pornografía infantil.

La prevención es clave para evitar malas experiencias en Internet, pero si eres víctima de lo que consideras un delito, acércate a la Guardia Nacional para obtener orientación y apoyo, ¡Tu denuncia es importante!

Para más información, visita www.civismodigital.org