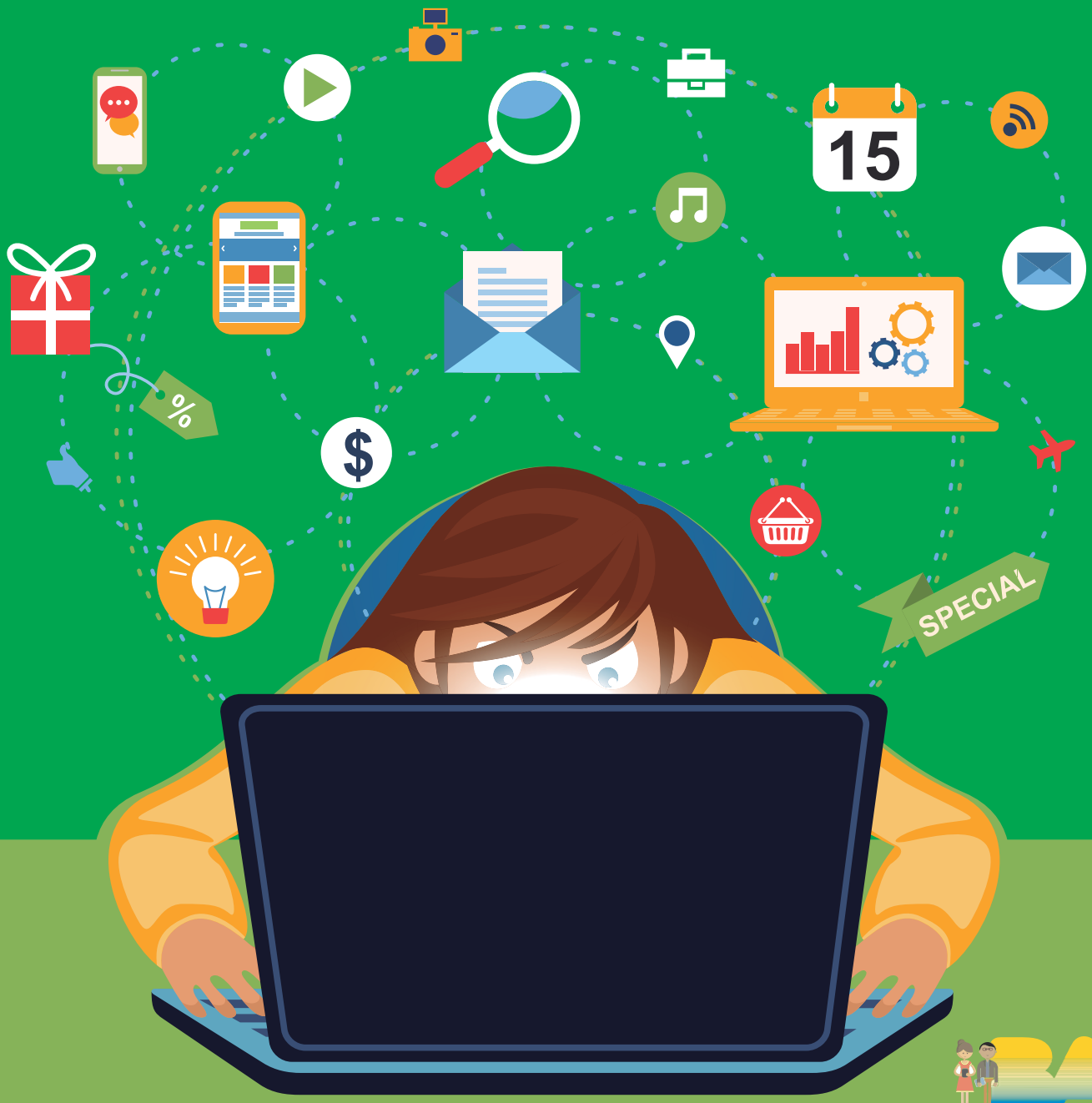
GUIA PRACTICA PARA PADRES, NIÑOS Y DOCENTES

PELIGROS *en Internet*



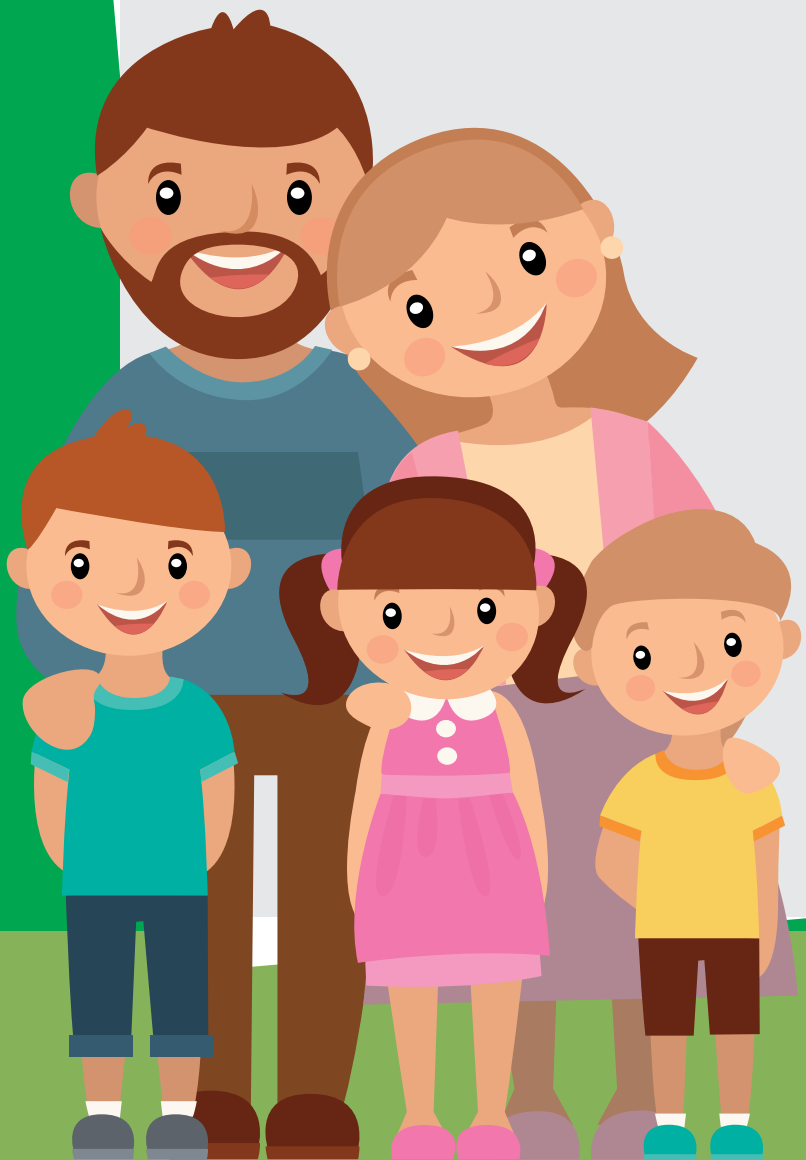
Vamos Buenos Aires
CSIRT Centro de Ciberseguridad

El Rol de la Familia

La familia cumple un rol fundamental sobre la información y prevención de los peligros que habitan en internet. Muchos de ellos, atentan sobre los más chicos.

Proteger todos los dispositivos digitales que se encuentran en el hogar es una tarea indispensable.

Una de las maneras de crear un entorno informático seguro es mediante el dialogo con nuestro hijos y de una actitud proactiva permanente.



Como padres, deberíamos preguntarnos si nos estamos comunicando correctamente con nuestros hijos y si realmente estamos interiorizados en todas las actividades que realizan.

Si conocemos a sus amistades y lo más importante, si consideramos que estamos protegiéndolos de forma adecuada frente a los riesgos que se encuentran en la red.

Se pueden evitar problemas y para ello, debemos interactuar con nuestros hijos, entender cuales son sus inquietudes sus miedos y establecer reglas claras sobre el uso de internet. Explicarles cuales son los riesgos y amenazas más frecuentes y como actuar en estos casos.

Aconsejarlos y demostrarles que cuentan con nuestro apoyo, para que se sientan contenidos y protegidos.

La Escuela

Más allá que dichos peligros se desarrollen en el contexto escolar o no, las entidades educativas deben estar al tanto acerca de la metodología de detección, como afrontarlos y combatirlos, para asegurar un desarrollo educativo favorable en los estudiantes.

La problemática es cada vez mayor por lo que requiere máxima atención por parte de formadores y equipos académicos.

Esto se debe a las características de las nuevas tecnologías como inmendiatez, anonimato, réplica, etc.

Cyberbullying

Riesgos en Redes Sociales e Internet

Son actitudes intimidatorias, agresivas, intencionadas y repetidas -sin motivación evidente- utilizando redes sociales, mensajes de texto o correo electrónico.

Se busca humillar a la persona y para lograr ese cometido, se utilizan diversas técnicas para agredir a la víctima.
El agresor puede ser visible o anónimo.

Puede atacar mediante videos, fotos intimidatorias, mentiras, etc. En alguno casos, se crean perfiles falsos para mantenerse en el anonimato y no dejar rastros de las acciones.

Sabemos que todo lo que forma parte de la web se viraliza facilmente y los agresores son conscientes de ello, por lo cual, mientras la información permanezca en internet, las víctimas padecerán los agravios a lo largo del tiempo.

Recomendaciones

Controlar el acceso de los niños a Internet; vigilando que los menores no publiquen información personal y privada como direcciones, teléfono, colegio, etc., ni tampoco posean contactos desconocidos.

Concientizar a los menores sobre los peligros de la red; para que los niños conozcan los riesgos a los cuales pueden verse enfrentados.

Mantener un diálogo abierto entre padres e hijos; porque el bullying es la mayor causa de depresión entre adolescentes.

Las relaciones libres y fluidas entre padres e hijos, contribuyen a que los niños se sientan con confianza para recurrir a un adulto de ser necesario.

Instalar un antivirus; con el objetivo de proteger la computadora de malware y ciberdelitos.

Instalar software de control parental; para permitir filtrar sitios y contenidos potencialmente peligrosos para los menores de edad.

Cybergrooming

Riesgos en Redes Sociales e Internet

Son acciones realizadas deliberadamente con el fin de establecer una relación y un control emocional sobre un niño o niña. Es un recurso muy empleado por pedófilos y pederastas para captar nuevas víctimas.

Recomendaciones Preventivas

No proporcionar imágenes o información comprometedora a nadie. Algo sin importancia en un determinado ámbito o momento puede cobrarla en otro contexto.

Evitar el robo del "elemento de fuerza". Para ello preservar la seguridad del equipo informático y la confidencialidad de las contraseñas.

Mantener una actitud proactiva respecto a la privacidad, lo que implica prestar atención al manejo que hago de mis imágenes e información personal.

Recomendaciones Correctivas

Cuando se comienzan a recibir amenazas e intimidaciones es importante tomar conciencia de la realidad de la situación.

No ceder al chantaje en ningún caso. Brindarle más elementos al depredador implica darle más poder.

Pedir ayuda. Contar con el apoyo de una persona adulta de confianza es fundamental. Aportará serenidad y una perspectiva distinta.

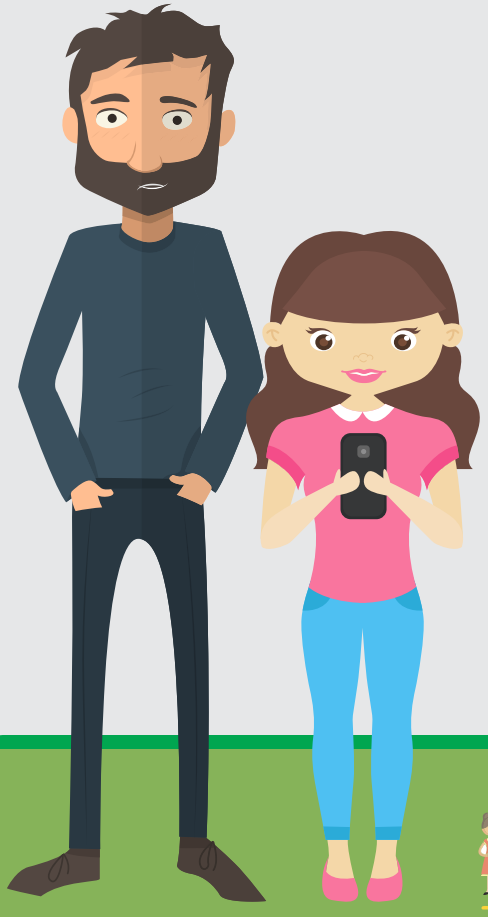
Evaluar la certeza de la posesión por parte del depredador, de los elementos con los que formula la amenaza, las posibilidades reales de que ésta se materialice y las consecuencias. Mantener la cabeza fría.

Limitar la capacidad de acción del acosador. Puede que haya conseguido acceso al equipo o posea las claves personales. En previsión de ello:

Realizar una revisión total del malware del equipo y cambiar las claves de acceso.

Reducir las listas de contactos y la configuración de privacidad en redes sociales.

Cambiar de perfil o incluso de ámbito de relación en la red (correo electrónico, red social, juego online multijugador, etc.).



Vamos Buenos Aires
CSIRT Centro de Ciberseguridad

Sexting

Es una peligrosa moda de tomarse fotos eróticas y compartirlas en redes sociales. Un juego que puede resultar peligroso para los menores y atractivo para los pederastas.

El sexting se trata de contenidos íntimos, generados por los propios usuarios, mediante fotos explícitas o vídeos propios en situaciones de carácter sexual, tanto desnudos como semidesnudos, normalmente con destino a una pareja sexual u ocasional, aunque también en algunas ocasiones a otros amigos, a modo de juego.

Esto expone al creador o creadora de dichos contenidos a innumerables riesgos y por ende, a graves consecuencias.

Recomendaciones

No compartir información o fotografías comprometedoras. Nunca enviar ni tomarse fotografías que pudieran afectar la reputación.

Tomar conciencia de que las fotografías siempre pueden ser interceptadas por terceros.

Evitar contactar con desconocidos.
No acceder a chantajes o amenazas.

Si una imagen ya fue enviada, no volver a hacerlo.

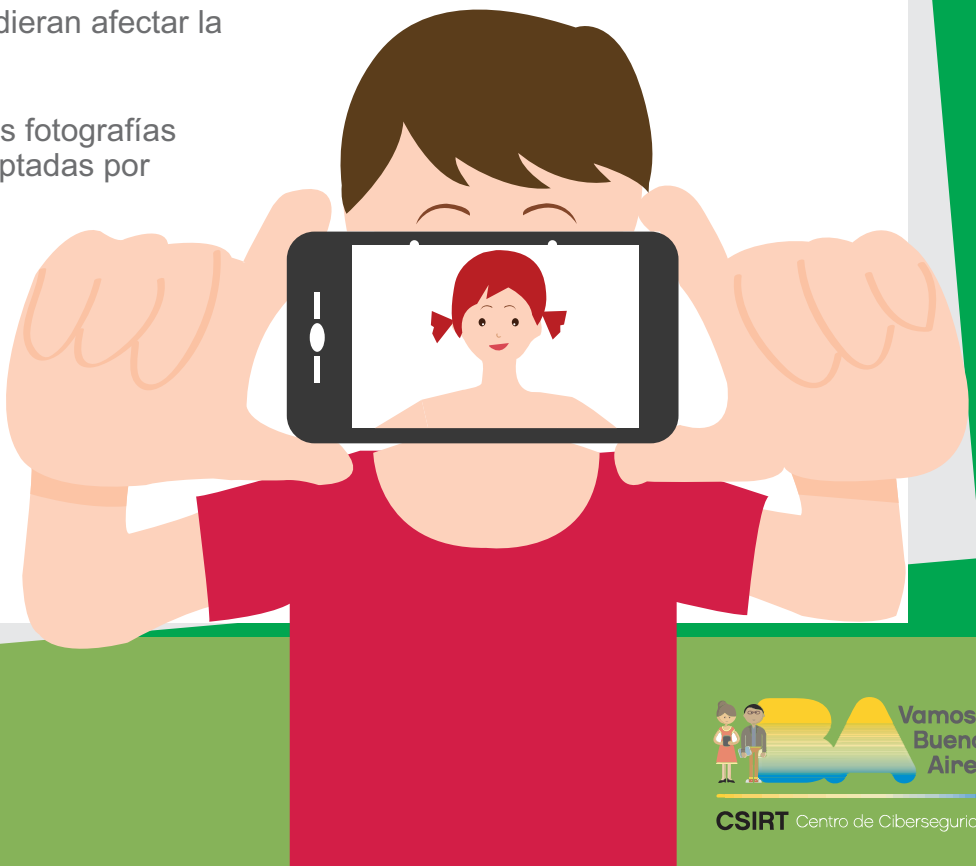
Quitar las fotografías comprometedoras de las redes sociales y sitios públicos, de forma inmediata

Si se conoce a alguien que está enviando o recibiendo fotografías, explicarle el peligro, a fin de evitar que se propague esta práctica.

Está comprobado que el sexting no es sólo un fenómeno exclusivo de los jovenes.

Los adultos suelen difundir fotografías propias de carácter sexual tomadas con un dispositivo móvil.

De hecho, estadísticas oficiales revelan que la incidencia del sexting entre los adultos es superior a la detectada entre los propios jovenes.



Robo de Identidad

Riesgos en Redes Sociales e Internet

Sin dudas, nuestra manera de comunicarnos con el medio que nos rodea ha sido revolucionado por internet.

Constantemente, se generan nuevos vínculos profesionales o sin ir más lejos, conectamos con personas con las que compartimos gustos, preferencias e inquietudes.

Estas nuevas plataformas tecnológicas, como lo son las redes sociales, nos permiten compartir información personal con nuestros contactos.

Dicha información esta librada a las malas intenciones por parte de personas que intentarán suplantar nuestra identidad, mediante el robo de datos.

Recomendaciones

No brindar datos personales a desconocidos. El DNI es el dato más importante asociado a la información financiera personal.

Un ladrón podría utilizarlo en nombre de otro para abrir cuentas bancarias, obtener tarjetas de crédito u obtener préstamos.

Evitar abrir correos electrónicos de remitentes desconocidos.

Evitar hacer clic en enlaces que se reciban de correos electrónicos.

Para acceder a un sitio, teclea la dirección directamente en el navegador.

Evitar usar computadoras de uso público para acceder a cuentas bancarias.

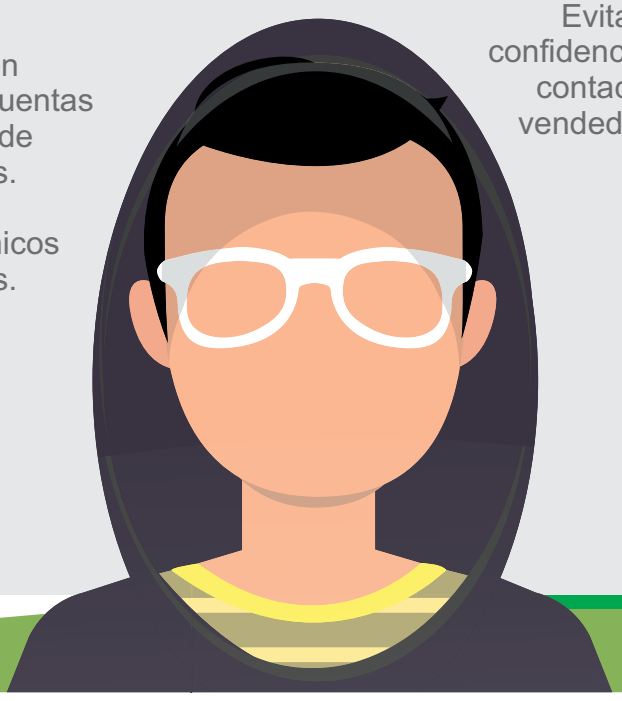
Usar contraseñas fuertes compuestas por mayúsculas, minúsculas y números.
Las contraseñas fuertes son más difíciles de descifrar por los atacantes.

Jamás enviar información personal por correo electrónico. Bajo ninguna circunstancia, enviar contraseñas por correo electrónico o mensajería instantánea.

Destruir físicamente documentos con información confidencial (resúmenes de cuenta, boletas de servicios, etc.), antes de tirarlos a la basura.

Destruir tarjetas de crédito y débito que ya expiraron, no tirarlas a la basura de forma descuidada.

Evitar dar información confidencial (DNI, datos de contacto) por teléfono a vendedores que soliciten esta información.



Vamos Buenos Aires

CSIRT Centro de Ciberseguridad

Malware

Es el término general que se le da a todo software que tiene como propósito infiltrarse o dañar el equipo.

El perfil de los individuos que logran beneficiarse con la creación e implementación de este tipo de programas, varia entre usuarios particulares, organismos gubernamentales y grupos criminales.

La creación de software malicioso implica una labor de tiempo completo.

La manera más efectiva de estar protegido contra el malware es manteniendo actualizado todos nuestros dispositivos, y asegurándonos contar con una versión actualizada del antivirus.

Recomendaciones

No descargar archivos de sitios no confiables o de dudosa reputación. Mantener programas, sistema operativo y antivirus actualizados.

No confiar en correos con programas adjuntos y mucho menos si dicen ser una actualización de un producto determinado. Las empresas nunca envían adjuntos con actualizaciones, sólo informan de la misma.

Evitar los programas ilegales ya que los mismos suelen contener troyanos, keyloggers, etc.
Si se desea utilizar programas libres o gratuitos, recurrir a las soluciones OpenSource.

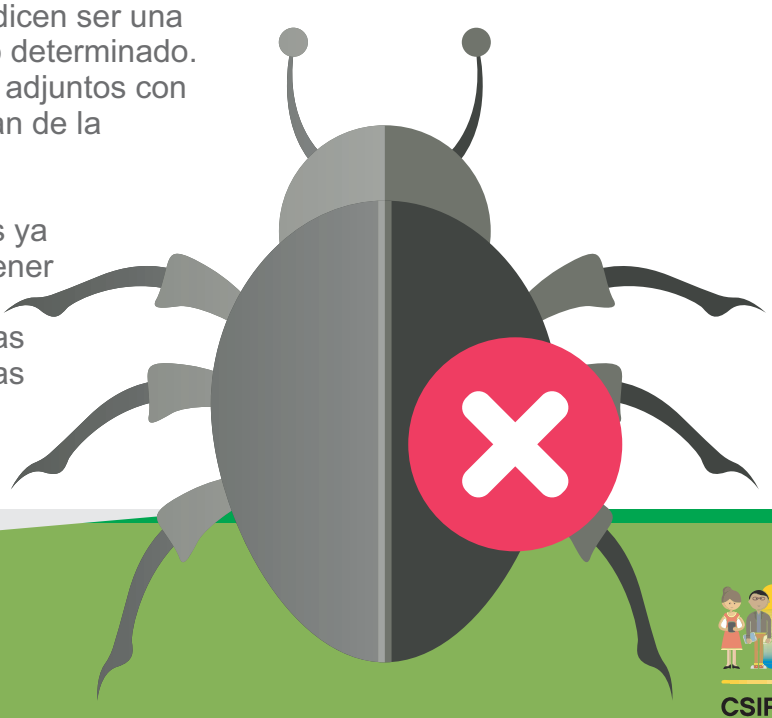
Contar con un Antivirus con capacidades proactivas que permita detectar un programa dañino descargado desde un correo electrónico. Esto también aplica para cualquier otro tipo de descarga.

Al recibir archivos o enlaces para descarga, preguntar si la otra persona ha enviado ese enlace.

No es recomendable descargar archivos de redes P2P, dado que se corre riesgo de infectar el equipo. De no poder evitar el uso de redes P2P, hacerlo en una PC sólo destinada a este fin, y que los datos sensibles no sean almacenados en la misma.

Al utilizar el sistema operativo evitar hacerlo con perfil “Administrador”, dado que no es necesario en la mayoría de los casos e incrementa el nivel de daños en caso de infección.

Prestar atención cuando se navega a fin de evitar ingresar a sitios peligrosos y evitar ejecutar programas dañinos que simulan ser soluciones de seguridad o antivirus.



Uso de Dispositivos Móviles

Riesgos en Redes Sociales e Internet

El teléfono móvil forma parte de uno de los elementos indispensables para nuestra comunicación y comodidad.

Este dispositivo requiere de un uso adecuado y es conveniente seguir unas reglas de buena educación que resultan imprescindibles a la hora de relacionarnos en sociedad.

Nuestra información personal y sensible está expuesta al robo físico del dispositivo y que puede resultar valiosa para los ciberdelincuentes que buscan obtener ganancias ilícitas utilizando malware u otras amenazas.

La seguridad debería ser considerada como una inversión, que nos puede ayudar a prevenir una situación comprometida en el caso que seamos víctima de un robo o un extravío.

Recomendaciones

Activar el acceso al dispositivo mediante contraseña.

Realizar copias de seguridad frecuentes de los datos del dispositivo.

No introducir nunca contraseñas en espacios públicos.

No activar conexión a redes (Bluetooth, Infrarrojos y WiFi), salvo de ser necesario. Conectarse solo a equipos (routers WiFi, modems 3G/4G, etc.) de confianza.

Comprobar ausencia de malware antes de insertar dispositivos externos (pendrives o tarjetas de memoria, etc.).

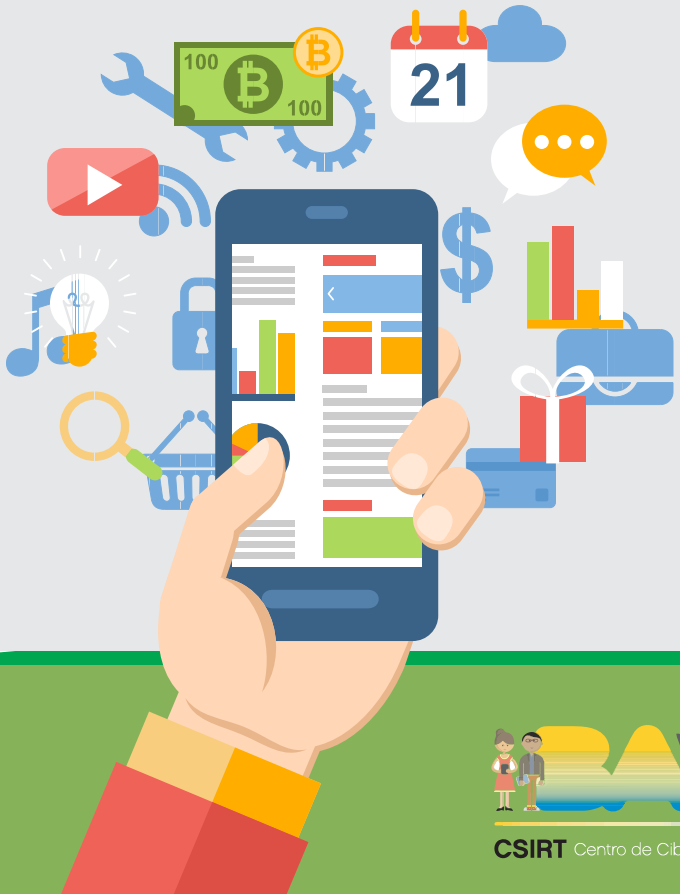
Descargar software sólo desde sitios de confianza o de las tiendas oficiales.

No acceder a enlaces facilitados a través de mensajes no solicitados (SMS, MMS, etc.) y que impliquen la descarga de contenidos en el equipo.

Cerrar la sesión en los servicios web que usan contraseña, antes de cerrar el navegador.

Agendar el número IMEI de su teléfono (identificador único de dispositivo) para desactivar el teléfono en caso de robo.

Instalar un software reconocido de detección de código malicioso en el dispositivo.



Juegos Online

Los juegos en línea permiten al usuario estar conectado por internet y así poder interactuar con otros jugadores.
Esto implica una nueva forma de ataque para los ciberdelincuentes.

Qué buscan los ciberdelincuentes?

Robar datos personales: nombre, apellido, edad, sexo, correo electrónico, contraseñas, número de tarjeta de crédito, información personal o sensible almacenada por el usuario en el dispositivo que utilice para jugar online.

Hackear dispositivos y ganar su control: convertir la computadora, teléfono u otro dispositivo en un botnet o zombie para cometer actos maliciosos, enviar spam, virus, gusanos, etc.

Robar cuentas de usuarios: controlar cuentas de usuarios que estén en un nivel avanzado de determinado juego. El tiempo y la dificultad que requieren ciertos juegos, hacen que haya otros usuarios que paguen por cuentas con niveles avanzados.

Robar dinero virtual: hay juegos en los el usuario obtiene dinero que no es real (ejemplo: Póker). Los delincuentes roban la cuenta, para luego venderla por dinero real.

Violar la intimidad: En ocasiones, los juegos en línea animan a los niños a hacer amistades, compartir datos personales o, incluso, reunirse con otros jugadores desconocidos fuera del juego.

Recomendaciones

Es necesario proteger cada dispositivo vinculado con juegos online.

Desconfiar de las notificaciones que nos pidan otorgar nuestro usuario y contraseña y fundamentalmente, no descargar juegos de sitios no oficiales. Son un peligro para la seguridad del jugador.

Instalar antivirus en las computadoras, smartphones u otros dispositivos.
Jamás introducir datos de tarjetas de crédito en chats.

Utilizar una cuenta de correo alternativa en caso de tener que registrarse como usuario.

No olvidar que aunque siempre juguemos con los mismos amigos, continúan siendo desconocidos.

Advertir a los más chicos que no den datos personales a otros jugadores, ni que acepten reunirse a menos que cuenten con la aprobación de sus padres.