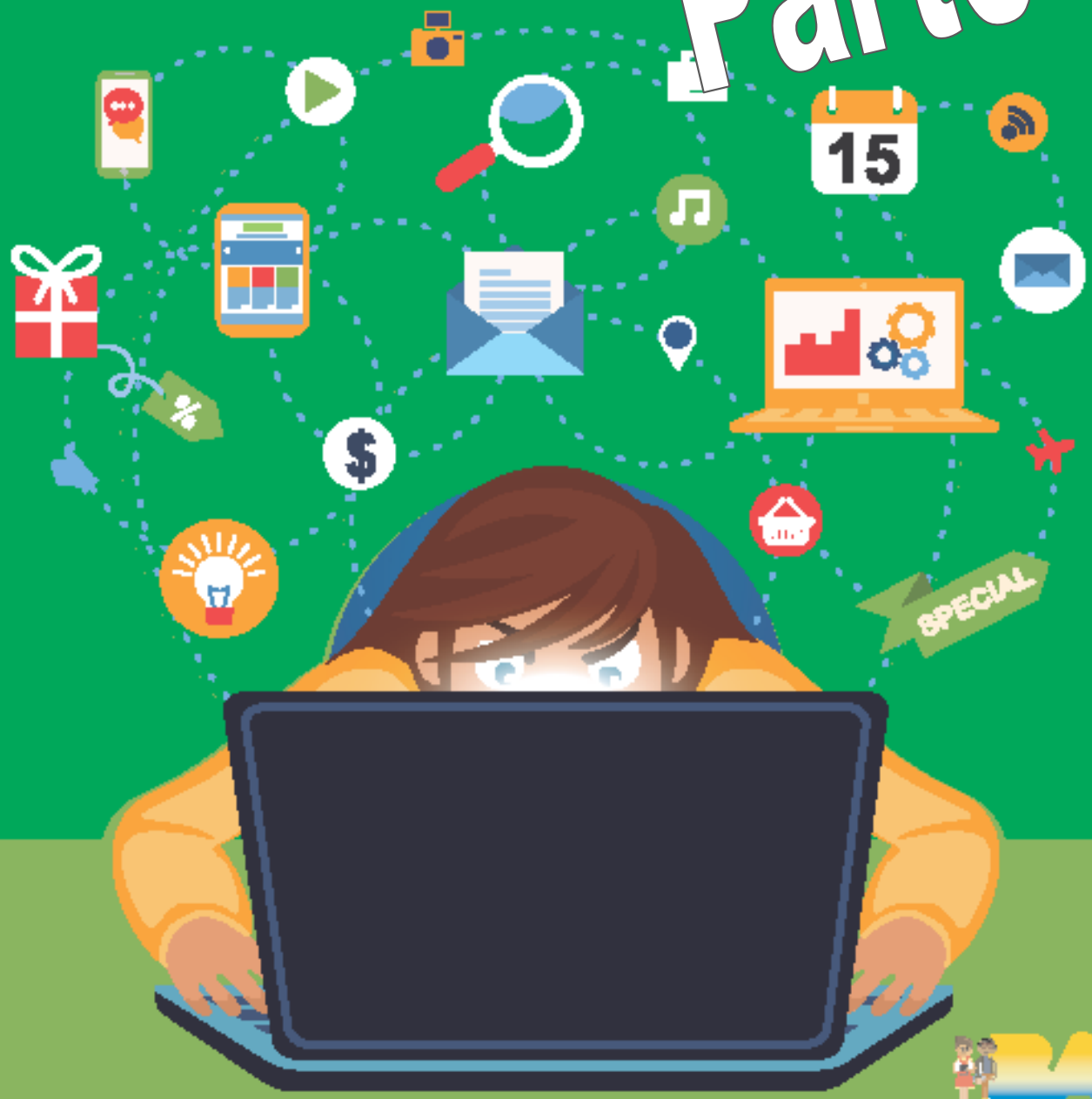
GUIA PRACTICA PARA PADRES, NIÑOS Y DOCENTES

PELIGROS *en Internet*

Parte II



Ministerio de Educación Buenos Aires

CSIRT

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.

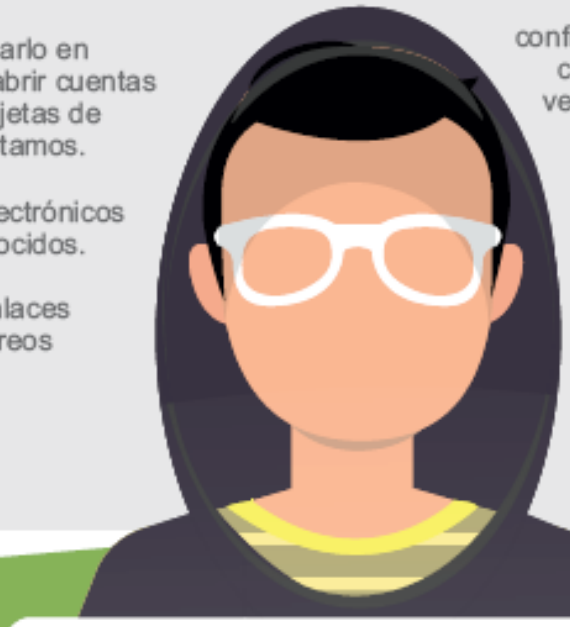
Usar contraseñas fuertes compuestas por mayúsculas, minúsculas y números. Las contraseñas fuertes son más difíciles de descifrar por los atacantes.

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

Riesgos en Redes Sociales e Internet

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.

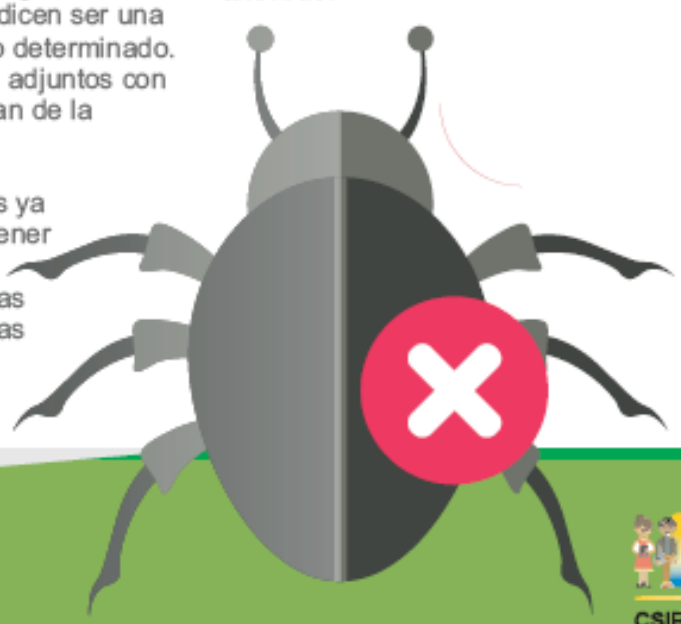
Contar con un Antivirus con capacidades proactivas que permita detectar un programa dañino descargado desde un correo electrónico. Esto también aplica para cualquier otro tipo de descarga.

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.



Vamos Buenos Aires
CSIRT Centro de Ciberseguridad

Uso de Dispositivos Móviles

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.

Riesgos en Redes Sociales e Internet

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

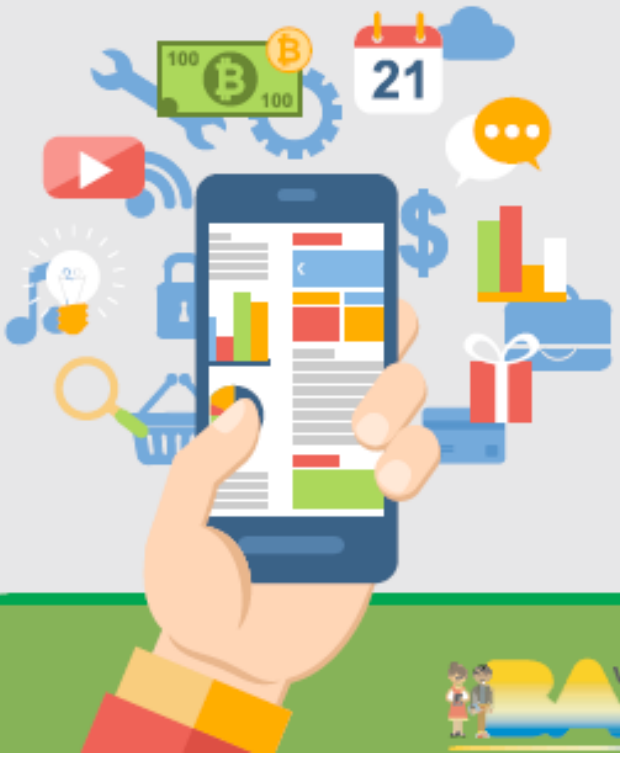
Descargar software sólo desde sitios de confianza o de las tiendas oficiales.

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.



Vamos Buenos Aires

Juegos Online

Riesgos en Redes Sociales e Internet

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.

Vamos Buenos Aires