



“La prevención es responsabilidad de todos”

Instructivo de Seguridad Informática

Mensajería Instantánea y Redes Sociales

.DAC

El Departamento de Asistencia Comunitaria (DAC), es la oficina Central de Seguridad de la Comunidad Judía de Buenos Aires, encargada de centralizar las tareas de prevención y seguridad comunitaria.

El DAC brinda servicio a la Comunidad Judía, tanto a sus instituciones como a particulares de la misma, funcionando las 24hs, los 365 días del año.

.Funciones del DAC

- Vinculación con las Fuerzas de Seguridad
- Toma de denuncias
- Recomendaciones de postulantes de seguridad
- Sistemas de Comunicación e Informes de Prevención
- Capacitaciones
- Elaboración de “Informes de Recomendaciones de Seguridad”
- Protección de Eventos Comunitarios
- Protección de Shabat
- Asesoramiento en Medios Físicos
- Plan de Emergencia Comunitario (PEC)

.Introducción

El objetivo de este instructivo es echar luz sobre un fenómeno relativamente nuevo que puede comprometer a la seguridad personal, familiar y comunitaria; el uso de los sistemas de mensajería instantánea y redes sociales que nos puede brindar Internet.

Estas dos aplicaciones informáticas ya se han convertido en parte integrante de las rutinas diarias de los miembros de la comunidad, ya sean niños, adolescentes o adultos.

Lo que no resulta suficientemente conocido aún, son las consecuencias negativas que el uso -o mal uso- de estas nuevas tecnologías informáticas puede generar.

Intentaremos brindarle información para prevenir algunas de ellas y herramientas para protegerse y proteger a su familia.

.Coyuntura

Global

La globalización de las comunicaciones y el advenimiento de Internet ha revolucionado la interacción remota de personas y más recientemente, el nacimiento de los sistemas de mensajería instantánea y el asombroso fenómeno de las redes sociales han abierto un nuevo campo de relaciones virtuales.

Nacional

En nuestro país la utilización de este tipo de aplicaciones está ampliamente extendida. Entre los más jóvenes resulta un elemento indispensable para su interacción.

Existen incluso, tribus urbanas que vinculan a ciertos grupos de adolescentes por su “vida virtual”.

.Redes Sociales y Sistemas de Mensajería Instantánea

Los sistemas de mensajería instantánea son aquellos que permiten a los usuarios comunicarse mediante cuadros de mensaje. Recientemente estos mismos también permiten conversaciones de voz y video. Los más populares: Messenger, Skype, Yahoo Messenger.

Las redes sociales son grandes redes que nuclea usuarios, cada uno construye una página de presentación y la red les permite interrelacionarse.

En estas redes se promueve la interacción entre desconocidos, se suelen postear o colgar datos personales, actividades, fotos y videos.

Algunas de las más populares son: Blog, Facebook, Flickr, Flixter, Hi5, Linked-in, Fotolog, MSN, Myspace, Orkut, Plaxo, Sonico.

.Hipótesis

En todo el mundo, la popularidad de estos sistemas abrió la puerta a su uso malicioso.

Existen numerosos casos de personas que han manipulado estas herramientas para cometer delitos de distinto tipo:

Robos, secuestros, extorsiones, antisemitismo, terrorismo y fraudes, entre otros.

Algunas hipótesis de posibles usos maliciosos son:

- Infección maliciosa con virus.
- Ingeniería Social por internet para delitos informáticos y no informáticos.
- Intento de infiltración en empresas o instituciones.
- Difusión de material antisemita.
- Corrupción de menores.
- Robo de información para extorsión.
- Robo de cuentas de correo para extorsión.
- Robo de cuentas de correo para derivación de fondos.
- Robo de información para planificación de robos presenciales.
- Robo de información para secuestros virtuales.
- Robo de información para secuestros reales.
- Robo de identidad para cualquiera de los delitos anteriores.
- Falsificación de identidad para realizar en forma personal: robos, secuestros, ataques violentos.
- Infección maliciosa de Virus para robo de información.
- Ingeniería social para todos los anteriores.
- Intento de infiltración en comunidades, franqueo de ingreso a actividades comunitarias para realizar ataques o recopilar información para futuros ataques.

• Hechos reales en Argentina y el mundo

- Suplantación de identidad para generar encuentros personales y consumir secuestros extorsivos.
- Secuestro virtual en base a actividades publicadas en Facebook.
- Citaciones por MSN para ataque físico Skinhead.
- Infiltración vía MSN y Facebook en un grupo juvenil comunitario luego materializado en infiltración con objetivos de relevar información institucional y de miembros de la comunidad.
- Intento de infiltración en institución comunitaria vía Facebook y hi5.
- Ingeniería social por MSN para robo de claves.

.Modalidades delictivas tradicionales y fraudes basados en Internet

Grooming, Cyberbullying u Hostigamiento Digital o Electrónico, SMishing, Hoax, Drive-by Pharming, Spam Financiero, Vishing, Phishing-Car, RansomWare, Ofertas de trabajo, Robo de contraseñas, Phishing, Robo del DNI, Carta Nigeriana, Cajeros automáticos, Pharming, Servicio de teléfono celular, Fraude de cheques, Compras por Internet, Tarjetas de crédito.

Para mayor información sobre estas modalidades de fraude ingrese a:
www.identidadrobada.com > tipos de Fraude

.Información Sensible

Denominamos información sensible a **aquella cuya difusión puede comprometer nuestra seguridad** y convertirse en un punto de exposición innecesario.

Consideramos información sensible a **nuestros datos personales, dirección, números de identificación, teléfonos, rutinas personales y familiares, horarios y lugares de actividades, datos de vehículos o caminos elegidos para traslados rutinarios.**

.Ingeniería Social

En el campo de la seguridad informática, ingeniería social es la práctica **de obtener información confidencial a través de la manipulación de usuarios legítimos.** Es una técnica que pueden usar ciertas personas para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga, a la persona u organismo comprometido, a riesgo o abusos. **Son ACCIONES O CONDUCTAS útiles para conseguir información de parte de las personas cercanas a un sistema.**

El principio que sustenta la ingeniería social es el que en cualquier sistema "los usuarios son el eslabón débil".

En la práctica, **un ingeniero social usará comúnmente el teléfono o Internet para engañar a la gente.** Vía Internet se usa, adicionalmente, el envío de solicitudes de renovación de permisos de acceso a páginas web o memos falsos que solicitan respuestas e incluso las famosas "cadenas", la generación de falsas amistades, llevando así a **revelar información sensible, o a violar las políticas de seguridad típicas.**

Uso de la Ingeniería Social

En el mundo de la seguridad de la información, este arte es utilizado, entre otros, para dos fines específicos:

- **El usuario es tentado a realizar una acción necesaria para dañar el sistema:** este es el caso en donde el usuario recibe un mensaje que lo lleva a abrir un archivo adjunto o abrir la página web recomendada que terminará dañando el sistema.

- **El usuario es llevado a confiar información necesaria para que el atacante realice una acción fraudulenta con los datos obtenidos.** Este es el caso del phishing, en donde el usuario entrega información al delincuente creyendo que lo hace a una entidad de confianza.

Aquí notamos otra característica importante: la excelente relación costo-beneficio obtenida de su aplicación, ya que a un costo ínfimo (una llamada telefónica o un correo electrónico) corresponde un beneficio incalculable (acceso a información o a un sistema).

Si bien podríamos entrar en particularidades de cada caso, es fundamental comprender que no hay tecnología capaz de protegernos contra la Ingeniería Social, como tampoco hay usuarios ni expertos que estén a salvo de esta modalidad de ataque. La Ingeniería Social no pasa de moda, se perfecciona y sólo tiene la imaginación como límite.

Evitar ser utilizado por Ingenieros Sociales

Evite brindar información que pueda comprometer la seguridad de su sistema o su persona. Datos como usuario, contraseña, fecha de nacimiento, familiares, empresas, tarjetas, situación social, salud, costumbres, datos económicos, u otros. pueden ser utilizados por una persona inescrupulosa para efectuar acciones dañinas.

.Contraseña Segura

Como crear una contraseña segura y fácil de recordar

Una contraseña (palabra clave o password) segura es una contraseña que otras personas no pueden determinar fácilmente adivinándola o utilizando programas automáticos.

Para crear una contraseña segura que pueda recordar fácilmente pero que sea difícil de determinar por terceras personas, intente una de las siguientes técnicas:

- **Utilice dos o más palabras de forma conjunta o combine números con letras.** Ejemplos: Pasear[Mi]Perro, Pa#34tata, Campeones=1995.
- **Abrevie una frase que recuerde fácilmente. Puede estar formada por números, signos o palabras que puede cambiar por números o signos.** Por ejemplo: Cada sábado voy en bici 20 kilómetros podría convertirse en la contraseña cdseb20kms.
- **Utilice signos de puntuación y números para combinar las iniciales de personas u objetos de un grupo conocido como, por ejemplo, sus deportistas, amigos, películas o libros favoritos o personajes históricos.** Ejemplos: Gandhi, Abraham Lincoln y Juana de Arco podrían convertirse en la contraseña 1G,2AL,JA.
- **Seleccione las vocales de una frase que le guste y agregue números o signos.** Ejemplo: Tengo tres perros podría convertirse en la contraseña Tng3Prs.

Reglas para crear una contraseña segura:

1. Tener al menos siete caracteres y no más de 16
2. Combinar tres de los cuatro tipos de caracteres siguientes:
 - Letras mayúsculas (ejemplo: A, B, C)
 - Letras minúsculas (ejemplo: a, b, c)
 - Números (ejemplo: 1, 2, 3)
 - Símbolos (ejemplo: ` ~ ! @ # \$ % ^ & * () _ + - = { } | [] \ : " ; ' < > ? , . /)
3. No usar una palabra común o nombre, ni una variación parecida
4. Incluya sustituciones de aspecto similar, como el número cero en lugar de la letra 'O' o el símbolo '\$' en lugar de la letra 'S'
5. Crear un acrónimo exclusivo
6. Incluya sustituciones fonéticas, como 'es3ado' por 'estresado'
7. No utilice una contraseña que se ofrezca como ejemplo de buena contraseña
8. No utilice información personal en la contraseña (como su nombre, fecha de nacimiento, nombre del novio, por ejemplo.)
9. No utilice patrones de teclado (asdf) ni números en secuencia (1234)
10. No repita caracteres (aa11)
11. No comunique la contraseña a nadie
 - No escriba nunca su contraseña
 - No envíe nunca su contraseña en un mensaje de correo electrónico

Algunos proveedores de servicios exigen que una contraseña segura:

- No sea la misma que cualquiera de sus cuatro contraseñas anteriores.
- No sea una variación mínima con respecto a su antigua contraseña. Por ejemplo, si su antigua contraseña era Campeones=1995, no se aceptaría como nueva contraseña Campeones=1996.

Otros Consejos

- No revele nunca su contraseña en una conversación de mensajes instantáneos ni la comparta con nadie.
- Si dispone de más de una cuenta de correo electrónico como, por ejemplo, una para el trabajo y otra para uso personal, debería utilizar una contraseña diferente para cada una de ellas.

.Precauciones Generales

El mejor modo de protegerse es usar el sentido común y el criterio.

Usted SABE qué tipo de información es sensible y puede ser utilizada para dañarlo.

Debe siempre ser consciente de que la información que llamemos sensible, puede ser manipulada maliciosamente para suplantar su identidad, deducir sus hábitos o movimientos.

Esté siempre atento ante posibles casos de Ingeniería Social

Recuerde que una vez que sus imágenes y comentarios se suben a la red, son públicos y están fuera de su control.

Quien desee averiguar cosas de usted se nutrirá en primera medida de la información que usted publique y en segunda instancia de la que pueda obtener directamente de usted o sus allegados.

No difunda sus claves. Configúrelas de forma segura.

- No agregue a su lista de contactos a personas desconocidas.
- Esté atento a personas llamativamente interesadas en usted, sus rutinas o las de sus allegados.
- Procure nunca reunirse con personas que no conoce.
- No acepte archivos, enviados por contactos conocidos, que no esté esperando, ya que existen diferentes virus que envían archivos automáticamente sin el consentimiento del usuario.
- Difunda la menor cantidad de información posible.
- Configure las opciones de seguridad para que únicamente sus contactos puedan tener acceso a su información.
- En caso de crear grupos, restrinja el acceso a los mismos.
- Mantenga su antivirus actualizado.
- No acepte conversaciones por webcam de desconocidos o de conocidos cuya dirección de mail no sea la que usted conoce.
- Procure realizar sus transacciones de dinero en internet solo en sitios seguros (busque indicadores que le demuestren la seguridad del sitio, como por ejemplo el ícono del candado en la barra de estado del navegador o un domicilio Web o URL que comience con “https:” la letra “s” corresponde a “seguro”).
- Es recomendable que la computadora se encuentre en un lugar transitado de la casa y no en la habitación de los chicos.
- Instruya a sus hijos para que se comporten de forma segura en la comunidad virtual.

Para mayor información en materia preventiva para niños y adolescentes, ingrese a: <http://www.chicos.net/internetsegura>

. Configuración de seguridad de Facebook

Seleccione

Configuración > Configuración de Privacidad > Perfil

Verá la siguiente pantalla.

🔒 Privacidad ▶ Perfil

Información básica Información de contacto

Controla quién puede ver tu perfil e información relacionada. Visita la [página Aplicaciones](#) para cambiar la configuración de las aplicaciones.

Ver cómo tus amigos ven tu perfil:

Perfil	🔒	Sólo mis amigos	▼	[?]
Información básica	🔒	Sólo mis amigos	▼	[?]
Información personal	🔒	Sólo mis amigos	▼	[?]
Estado y enlaces	🔒	Sólo mis amigos	▼	[?]
Fotos en las que se te ha etiquetado	🔒	Sólo mis amigos	▼	[?]
Videos en los que se te ha etiquetado	🔒	Sólo mis amigos	▼	[?]
Amigos	🔒	Sólo mis amigos	▼	[?]
Publicaciones en el muro	<input checked="" type="checkbox"/>	Mis amigos pueden publicar en mi muro		[?]
	🔒	Sólo mis amigos	▼	
Información académica	🔒	Sólo mis amigos	▼	[?]
Información laboral	🔒	Sólo mis amigos	▼	[?]

Seleccione “Solo mis Amigos” en todos los campos y haga click en “Guardar Cambios”.

Guardar cambios

Cancelar

Luego haga Click en “Información de Contacto” y vera la siguiente pantalla:

 Privacidad ▶ Perfil

Información básica Información de contacto

Controla quién puede ver tu información de contacto. Visita la [página Aplicaciones](#) para cambiar la configuración de la aplicaciones.

Ver cómo tus amigos ven tu perfil:

Nombre de mensajería instantánea para mostrar	 Sólo mis amigos	
Teléfono móvil	 Sólo mis amigos	
Otro número de teléfono	 Sólo mis amigos	
Dirección actual	 Sólo mis amigos	
Sitio web	 Sólo mis amigos	
@gmail.com	 Sólo mis amigos	

Seleccione “Solo mis Amigos” en todos los campos y haga click en “Guardar Cambios”.

Guardar cambios

Cancelar

TODAS LAS REDES SOCIALES TIENEN SIMILARES ENTORNOS PARA CONFIGURAR LA PRIVACIDAD Y SEGURIDAD DE SU PERFIL, UTILÍCELOS.

.Conclusiones

- Comunique a su familia los riesgos y las medidas preventivas.
- Implemente las medidas recomendadas anteriormente.
- Mantenga y transmita calma en todo momento.
- Envíenos su inquietud o denuncia a: dac@daia.org.ar
- Dé aviso al DAC. Ante cualquier problema, duda o consulta comuníquese las 24 hs. a los siguientes teléfonos: **4378-3212/16.**