No. 30 / suplemento noviembre

.Seguridad®

Cultura de prevención para TI

30 suplemento

Día Internacional de la Seguridad en Cómputo 2017

Contenido

.Seguridad
Cultura de prevención para TI

Editorial

Día Internacional de la Seguridad en Cómputo 2017

Muchos aspectos de nuestra vida cotidiana implican el uso de las tecnologías de la información y la comunicación. ¿Te has preguntado alguna vez cómo vivías antes sin redes sociales, mapas digitales, correo electrónico o servicios de mensajería? Estos avances tecnológicos facilitan la vida de muchas maneras, y nos han permitido crear, además de volvernos más productivos. Ahora existe la posibilidad de evitar las filas en el banco y realizar movimientos desde nuestro dispositivo móvil, buscar en Internet información en el momento en que lo necesitamos o pedir comida a domicilio sin salir de casa ni hablar con nadie. Estas actividades generan una enorme cantidad de información respecto a nosotros, nuestros hábitos, preferencias y aficiones, datos que son valiosos desde muchos puntos de vista, pero que a menudo no son valorados por la mayoría de las personas.

Por ello creemos que es necesario difundir entre los usuarios finales el por qué se debe valorar la información personal, en la medida en que cibercriminales y empresas de servicios en Internet codician estos datos. Para ello, publicamos este suplemento de la revista .Seguridad Cultura de prevención para TI, con la idea de difundir buenas prácticas y consejos para navegar de manera segura, de tal manera que puedan ser aplicados a la vida cotidiana.

Con este suplemento procuramos compartir el espíritu del DISC, cuya intención es concientizar a los usuarios finales sobre seguridad en cómputo y mejorar el ciberespacio en el que nos desenvolvemos todos los días, recordando que la seguridad somos todos.

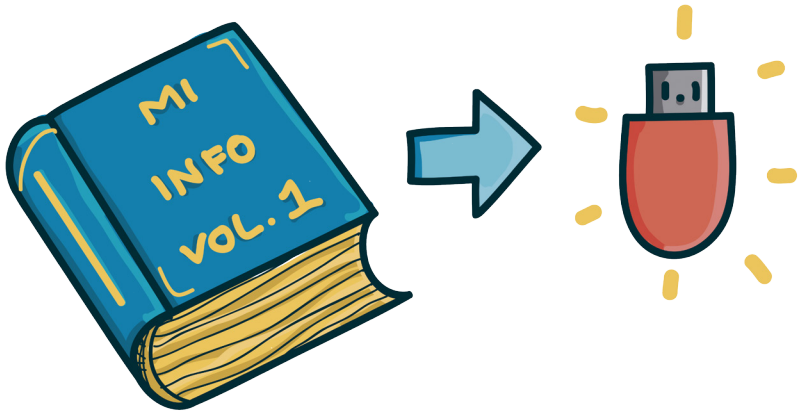
.Seguridad Cultura de prevención para TI, revista bimestral, noviembre 2017 / Certificado de Reserva (en trámite), Certificado de Licitud de Título (en trámite), Certificado de Licitud de Contenido (en trámite), Número ISSN (en trámite), Registro de Marca 1298292 | 1298293 / Universidad Nacional Autónoma de México, Circuito Exterior s/n edificio de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación, Coordinación de Seguridad de la Información, Cd. Universitaria, Coyoacán Ciudad de México, México, C.P. 04510, Teléfono: 56228169

Amenazas a los datos personales

Por Germán Lugo Martínez y Mario Alejandro Vasquez Martínez

Uno se preocupa muy poco por sus datos personales, pero adquieren interés si te preguntas:

¿Quién estaría interesado en lo que hago, en las actividades que realizo, lo que consumo, el lugar en donde vivo, qué rutas sigo al desplazarme por la ciudad, cuál es mi nacionalidad y mis preferencias?



La vida avanza de acuerdo a la premisa de que nada es gratis, todo tiene un fin monetario, publicitario, de marketing o de algún otro interés. Para nuestra información personal la situación no es nada diferente.

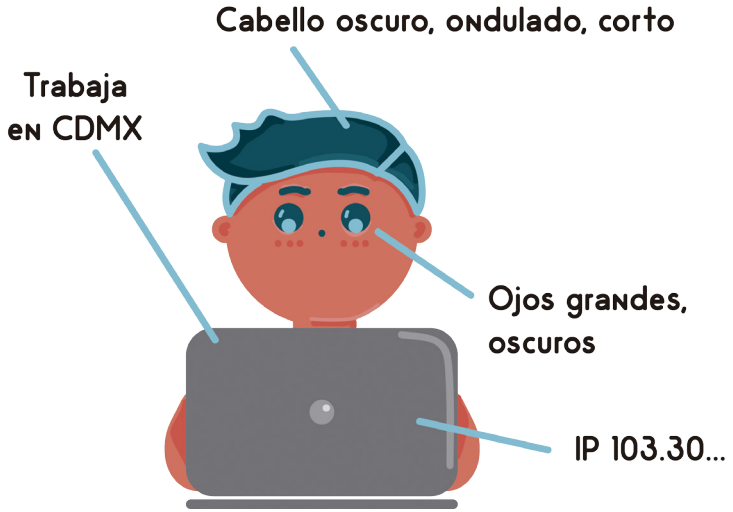
La línea de seguridad de nuestra información se ha ido desvaneciendo, ya que el campo de exposición se ha incrementado debido a la creación de nuevas tecnologías, el boom exponencial de Internet y la interacción mediante las redes sociales.

Durante años, nuestra información dependió del almacenamiento en papel, y se tenía la idea de que así estaba más "segura" en nuestras casas, bancos u otras instituciones. Pero en la actualidad nuestra información se encuentra en formatos digitales, tanto en discos duros, computadoras, celulares y memorias USB.

En este nuevo panorama hay demasiada incertidumbre, ya que con cierta facilidad muchas personas y empresas aprovechan vacíos legales, la ignorancia de algunos usuarios, usan términos y condiciones confusos para utilizar nuestros datos a su favor y explotarlos. Basta con revisar los términos y condiciones de Facebook y darnos cuenta de que, por ejemplo, aceptamos que dicha empresa recopile y utilice algunos datos personales para sus propios fines.

Ya no se trata solamente de nuestro nombre, domicilio, edad, sexo, teléfono, información financiera o laboral, como en el pasado. En la actualidad, la gran cantidad de información que circula, como direcciones IP, el número de matrícula del vehículo, los rasgos físicos (a través de fotografías, la impresión de las huellas dactilares, el escáner del dibujo del iris, la obtención de una muestra de ADN), los lugares que frecuentamos, las personas con las que conversamos, las horas y el

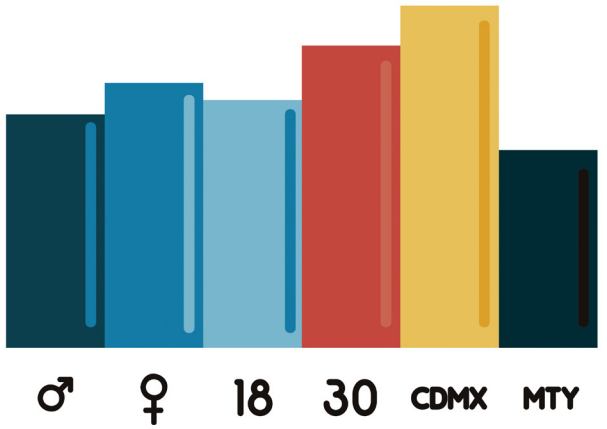
lugar donde trabajamos pueden ser aprovechados con fines mercadologícos, financieros, de extorsión o cibercriminales.



Pero, ¿quiénes y cómo pueden aprovechar esta información? A continuación, definiremos algunos de los principales interesados y las amenazas a las que se exponen nuestros datos personales.

Empresas

Este es el ejemplo más visible en el que los datos personales son procesados y usados, ya que el marketing ocupa un área clave en las grandes empresas donde algunas de ellas incluso hacen uso de herramientas como la Inteligencia Artificial o Big Data para analizar los datos que recogen a través de redes sociales, encuestas, patrones de búsquedas, historial de compras y páginas web para poder definir sus estrategias de venta. Cada vez las compañías se especializan más al respecto y realizan estudios segmentados por género, edad, área geográfica, clases sociales, gustos e intereses con la finalidad de ofrecer a cada público ofertas y productos de acuerdo a sus intereses.



El caso de la empresa Target fue muy famoso, ya que con base en la búsqueda de artículos que realizaba una adolescente, la compañía supo que esta estaba embarazada mucho antes de que el propio padre de la joven se enterara, cuando la

joven ni siquiera supo en qué momento había consentido que los datos de sus búsquedas fueran utilizados, en este caso para fines mercadológicos.

Las empresas manejan grandes cantidades de datos, tanto de su propia operación como de las personas a las que emplean: información de proveedores, datos sobre clientes, productos y/o servicios que ofrecen. Para ellas el conocimiento del mercado puede ponerlas un paso delante de la competencia. Es por ello que dependiendo de la actividad que desempeñen, a las empresas les puede interesar información muy puntual sobre los clientes y en ocasiones consiguen grandes cantidades de datos a partir de técnicas no del todo aceptables.

Las compañías deben garantizar la seguridad e integridad de los datos personales aunque muchas ocasiones no cuentan con los mecanismos de seguridad necesarios y los datos son robados, exponiendo en la red fotografías, contraseñas, datos financieros, datos médicos, datos inmobiliarios, etcétera, que los cibercriminales aprovechan para difamar o extorsionar. Vemos en la red constantemente noticias de fotografías de famosos expuestas, cuentas de redes sociales secuestradas, robos de identidad y ciberacoso desde perfiles con datos de otras personas.

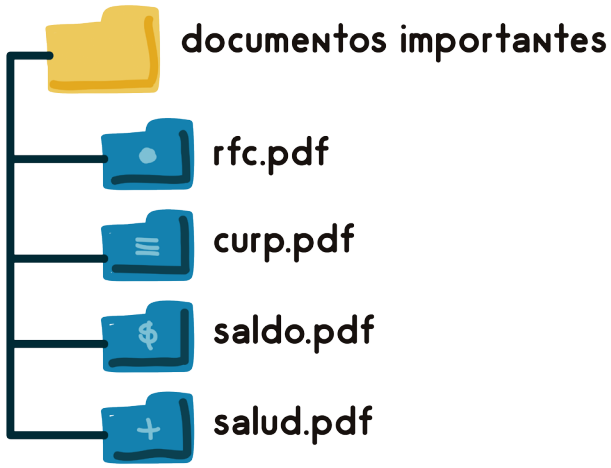
Gobiernos

La tendencia de los gobiernos, incluido México, es implementar servicios digitales para que los ciudadanos usen estas nuevas tecnologías en la realización de trámites, pagos y consultas en línea, de tal forma que la administración disminuya sus tiempos, sea más eficiente, reduzca el gasto de las finanzas públicas, y sobre todo que los procesos sean transparentes.

Pero el hecho de que ahora los ciudadanos puedan hacer uso de servicios digitales trae consigo ciertas implicaciones. Anteriormente los datos se manejaban en papel frente a la ventanilla de alguna oficina burocrática, y ahora los datos se comparten y se almacenan en Internet, lo que los hace vulnerables a las ciberamenazas y se vuelven un objetivo de ataques por el valor que representan, ya que estos datos prácticamente revelan quién eres, tu salud, tus finanzas, tus gustos, tu ideología y a tus familiares.

Como productos de estos nuevos servicios ahora los gobiernos cuentan con datos detallados en formato digital de los ciudadanos, como edad, lugar de residencia, RFC, CURP, datos financieros, datos patrimoniales, datos académicos, huellas digitales, firmas electrónicas, datos de familiares, preferencias políticas y números telefó-

nicos, los cuales deben ser tratados de tal forma que se garantice su seguridad e integridad, o de lo contrario podrían quedar expuestos en la red, ser filtrados a terceros o incluso sufrir ataques de otros gobiernos.



Ciberdelincuencia

Este sector es el que más daño ocasiona, y una vez que los ciberdelincuentes consiguen nuestros datos personales estos son utilizados para cometer delitos cibernéticos, como robo de identidad o phishing, transacciones bancarias no autorizadas, compras en línea, ciberacoso o extorsión a sus propietarios mediante ataques de ransomware.

Los correos electrónicos pueden ser usados en campañas de spam, los números telefónicos, para tratar de extorsionar usuarios y datos para tratar de comprometer cuentas en sitios web y realizar robo de identidad o buscar información más detallada como datos bancarios, familiares o empresariales.

La ciberdelincuencia aumenta día con día haciendo uso de una gran variedad de herramientas existentes permitiéndole a un atacante deducir información sobre nuestra vida privada a partir de lo que publicamos, los comentarios que realizamos, las fotos en las que somos etiquetados, los lugares que registramos como visitas, la música que nos gusta, los lugares que marcamos como trabajo, o haciendo uso de técnicas de ingeniería social.

Los daños ocasionados por estos ataques y por el robo de datos personales representan grandes pérdidas de dinero a nivel mundial, tanto para empresas como para las personas y dónde los ciberdelincuentes aprovechan el anonimato y neutralidad de la red para cometer sus ataques quedando impunes la mayoría de las veces y ganando cuantiosas cantidades de dinero.

Recomendaciones

Es inevitable que publiques datos personales en la red, ya sea por un trámite, una solicitud de empleo, operaciones bancarias o interacción con tus amigos y familiares en redes sociales, pero sí puedes tratar de minimizar lo más posible la fuga de datos. Por estas razones a continuación listamos una serie de recomendaciones a seguir:

Lee los términos y condiciones de los sitios donde te registras o de los servicios que utilizas, para evitar sorpresas.

Mantén actualizados los programas que utilizas en tus equipos.

Al realizar publicaciones en redes sociales, procura no exponer datos extra como nombres completos, lugar de trabajo, la dirección de tu escuela o tu casa.

Maneja con cuidado las características de ubicación en los dispositivos, ya que puedes ser rastreado en cualquier lugar y momento.

Revisa los permisos que solicitan las aplicaciones en cualquiera de nuestros dispositivos, si piden más de lo que deseas hacer con ellas, tal vez sea mejor no instalarla.

Si manejas información delicada (información de tarjetas, pagos, domicilios) procura transmitirla de manera cifrada.

Aplica el sentido común cuando te sea solicitado cualquier dato personal, y jamás solicites credenciales de acceso a cuentas bancarias o de redes sociales.

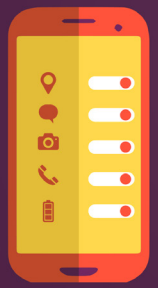
Como usuarios estamos en medio de un campo donde las empresas, instituciones, ciberdelincuentes y gobierno se disputan nuestra información y datos personales para diferentes usos: venta de información, marketing, espionaje, seguimiento de perfiles, comportamientos y actividades o algún daño que influya en la economía o imagen de un usuario o empresa.

Pero esto no es una batalla perdida, al contrario, puedes mantenerte informado sobre las últimas amenazas, cómo protegerte y compartir esta información con tus allegados. Ten en cuenta que en estos momentos cualquier persona es de interés para las empresas, gobiernos y cibercriminales, y que formamos parte de un sistema donde la información es poder y que aunque consideres tu información de lo más "insignificante" alguien estará listo para aprovecharla a su favor.

Desactivo mi ubicación

No hagas pública tu localización, o asegúrate que solo la ven los contactos que eliges. Usuarios maliciosos podrían tomar ventaja de esta función para afectarte a ti o a los tuyos.

Reviso los permisos que pide una app



Lee qué permisos otorgas a una aplicación antes de instalarla. Si los permisos no coinciden con su función, desconfía de ella y no la instales.

Protejo mi intimidad y la de mi pareja

El pack no es una muestra de amor. Cuida tu intimidad tomando precauciones para evitar que alguien haga mal uso de tu amor digital. Aunque una foto sea temporal, como en Snapchat, el destinatario aún puede hacer una captura de pantalla.

Yo no creo todo lo que publican en las redes

Cuando leas noticias en redes sociales piensa dos veces antes de compartir la información. Verifica que la nota sea real y que no sea parte de una campaña maliciosa.

DISC 2017
La seguridad somos todos

Consejos

Sopa de passwords

La primera trinchera de la ciberseguridad es tu contraseña, si es demasiado sencilla, es fácil de adivinar y tu información podría estar en riesgo. Desde hace al menos catorce años se recomienda a los usuarios usar contraseñas fuertes, es decir, palabras compuestas por letras, números y signos de puntuación, debido a que estas claves son más complicadas de encontrar para un ciberdelincuente, quien podría probar una lista de contraseñas para dar con la que permite acceder a tu información.

Para mostrar la importancia de contar con contraseñas fuertes, te invitamos a jugar sopa de letras. El juego está pensado para que pienses qué tan fuertes son tus contraseñas. Puedes jugar con usuarios jóvenes o adultos, la idea es que te des cuenta de cómo se encuentran las contraseñas de los tres niveles y ver cómo se complican conforme avanzas de nivel.

Nivel 1

W	H	U	O	A	Q	Y	P
Q	Y	S	D	G	W	M	A
A	L	O	H	S	E	H	E
P	E	D	A	T	E	W	Y
U	R	W	I	U	T	Q	D
I	L	O	V	E	Y	O	U

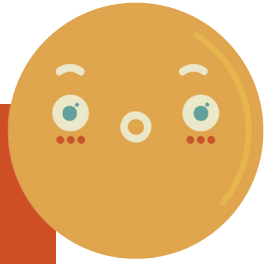
Nivel 2

abc123
14JUNIO
JUAN10

J	3	A	3	0	V	0	M	C
U	B	R	H	A	I	7	3	U
A	R	M	J	N	5	4	A	A
N	K	B	U	N	H	B	5	B
1	8	J	9	4	7	A	B	C
0	4	R	1	F	D	T	N	1
1	D	A	F	8	5	U	V	2
F	1	U	G	A	9	J	6	3

Nivel 3

m	3	#	g	P	/	-	M	g	u	z
T	#	7	3	4	m	0	r	0	5	4
9	7	x	/	r	h	K	8	@	%	u
)	U	_	m	S	f	E	%	/	F	5
&	i	n	w	@	u	#	J	0	d	7
U	@	*	a	_	w	s	3	b	A	s
m	/	Ñ	u	m	o	_	/	F	¡	Q
D	3	j	=	8	$	0	7	@	5	A
G	6	O	6	x	c	2	&	D	n	S
%	K	o	h	@	y	p	7	v	L	a



37/Sus/@na
Unam$27_
#734m0r054

Nivel 4

El cuarto nivel consta de frases que son utilizadas como contraseñas. Imagina el tamaño de la sopa de letras que se necesitaría para buscar las siguientes frases.

Tengounacontraseñafuertequenotienenúmerosnisímbolos

Nopuedomemorizarcontraseñasfuertesmejorusofrasesdecontraseñas

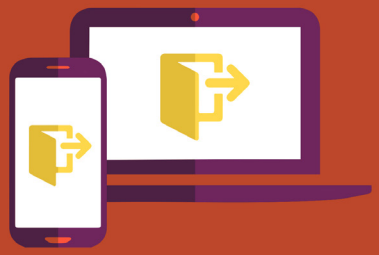
Debocambiarmiscontraseñascadaseismesesmientrasusoesta

A este tipo de frases puedes agregar números y símbolos para fortalecerla, pero la extensión y variedad de caracteres ya forman una contraseña fuerte. Aún así, te recomendamos usar un gestor de contraseñas para almacenar todas tus llaves de acceso y no tener que memorizar todas ellas.

Vacío la papelera de reciclaje y de correos no deseados

Puede ser que hayas eliminado el *spam* o archivos que consideraste maliciosos, pero si no los borras, permanecerán como amenaza latente en tu sistema. Es mejor vaciar la papelera.

Cierro mis sesiones siempre



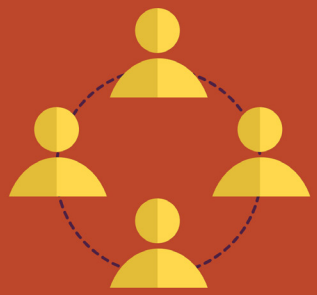
De preferencia, no dejes tus sesiones de redes sociales o de correo electrónico abiertas, mucho menos si no estás en tu máquina. Otras personas podrían hacer mal uso de tu información si tienen acceso.

DISC 2017
La seguridad somos todos

Uso un programa de borrado seguro

Si manejas información sensible y deseas deshacerte de ella, utiliza un programa de borrado seguro para reducir las probabilidades de que alguien pueda recuperarla.

No comparto información personal indiscriminadamente



Tu información es valiosa, por ello te recomendamos distinguir en quién puedes confiar y en quién no. Crea grupos en tus redes sociales para que controles quién puede ver tu información.

Consejos

PERFIL

NOMBRE
Cristal Pérez Godínez

LUGAR
México, CDMX

EMAIL
cr_pg@emial.com

HERMANOS
Pablo y Ernesto

Cumpleaños
29/febrero/1986

RELACIÓN
Soltera

compartir

Consejos para mejorar tu seguridad en las redes sociales

Por Rocío de Abril Adriana Pérez López

Las redes sociales influyen en la vida de las personas en maneras que siguen sorprendiendo. Gracias a ellas podemos hacer nuevas amistades, recuperar el contacto con seres queridos que no hemos visto en mucho tiempo, estar cerca de quien se encuentra en otra latitud o acceder a información de interés y actualidad. Pero también son motivo de preocupación por diferentes razones. Implica riesgos a la privacidad, pues es posible intervenir comunicaciones por este medio, facilitar el robo de información por medio del phishing, y otorgar información para el robo de identidad (Borbón, 2012); se ha convertido en un medio para lanzar campañas de desinformación que han afectado las votaciones en distintos países (BBC News, 2017); o pueden ser una ventana para que los menores de edad desarrollen adicción a Internet y sufrir privación del sueño o sean expuestos a depredadores sexuales, al ciberacoso, sufran problemas de privacidad y practiquen sexting (Schurgin, 2011).

A pesar de que estas amenazas por lo regular son minimizadas por los usuarios, puesto que "hay pocas probabilidades de que me sucedan a mí", es necesario tomar en cuenta algunas recomendaciones para proteger nuestra información personal en las redes sociales y reducir al máximo las probabilidades de tener problemas por su uso.

¿Qué medidas puedo tomar para cuidar mi información?

Crea contraseñas seguras utilizando una frase fácil de recordar pero difícil de adivinar

Las contraseñas deberían ser la llave de acceso a tu información, datos personales como contactos, fotografías, fecha de nacimiento, correos electrónicos de trabajo, cuentas bancarias, etcétera. Por ello es importante resguardar las contraseñas de tus redes sociales. ¿Cuántas veces utilizas la misma contraseña para Facebook y para tu correo electrónico? ¿Alguna vez has utilizado tu fecha de nacimiento para tu contraseña o alguna fecha de aniversario?

Al usar frases de contraseñas haces más difícil el trabajo de los atacantes, pues les lleva más tiempo y recursos realizar un ataque. Uno de los métodos que utilizan es la fuerza bruta o ataque de diccionario, que prueba sistemáticamente todas las contraseñas en una base de datos para ver

cuál sirve para acceder a una cuenta. Entre más sencilla es una contraseña, más probabilidades existen de que el ataque de diccionario sea exitoso. Pero si usas una frase que solo tenga sentido para ti, mejora tu seguridad.

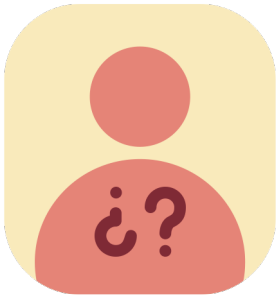
No compartas información personal con extraños

Así como en la vida cotidiana es importante cuidarse de desconocidos, en las redes sociales procura publicar solo lo necesario sin dar detalles de tus actividades, pues nunca sabes quién está mirando lo que haces; podrías tener audiencia indeseable, como tu ex novio o un acosador. Recuerda que en algunas aplicaciones puedes especificar quién puede y quién no puede ver tus publicaciones, así que recomendamos seleccionar adecuadamente tu público en las redes sociales restringiendo tus publicaciones o incluso tu cuenta. Accede a las opciones de privacidad para saber qué límites te pueden ser útiles.

No aceptes a cualquiera como tu amigo

Es mejor desconfiar de las personas desconocidas. En las redes sociales merodean miles de ciberdelincuentes que crean cuentas falsas para hacer fraudes. Estas personas son muy hábiles para falsificar información y hacerse pasar por una persona que conoce a tus amigos con tal de que lo aceptes.

Asegúrate de que tus amigos sean quienes dicen ser. No compartas información de tus amigos con terceras personas por redes sociales. Ten cuidado con los amigos que agregas a tus redes y procura que sean personas a quienes has conocido personalmente. De ser así, notifica personalmente con ellos la solicitud de "amistad" y solo comparte información con personas de confianza.



Restringe tus publicaciones para que las vean solo tus contactos

Las publicaciones en redes sociales dan mucha más información personal de lo que te imaginas,

más que tu comida favorita y los lugares que frecuentas, dónde te encuentras y con quién, tus mejores amigos y quiénes son los miembros de tu familia. Recuerda que millones de personas se encuentran en contacto vía redes sociales y ese número de personas podría tener acceso tu información. Hoy en día es muy fácil hacer viral una imagen sin el consentimiento del autor o protagonista.

Restringe tus publicaciones y fotos solo a tus amigos, no las expongas a todo el público, evita publicar fotos de documentos oficiales como credenciales, placas de auto u otra información sensible. Recuerda que ese tipo de información puede ser investigada para extraer información confidencial. Evita publicar fotografías de familiares menores de edad, ya que pueden ser utilizadas por personas con malas intenciones.

Separa lo profesional de lo personal

De manera positiva, las redes sociales permiten mantenerse en contacto con las personas para mantener relaciones laborales o escolares y fomentar la interacción entre los miembros.

En las redes sociales es importante tener en cuenta cuál es la imagen que queremos proyectar a las personas, pues a través de imágenes y estados se construyen los juicios de valor, por lo que no está por demás tener un límite para publicar los detalles de nuestra vida. Algunas empresas ya implementan la revisión de perfiles al contratar a sus miembros para indagar aún más en su personalidad.

Evita publicar información laboral confidencial en tus redes sociales, ya que podría traer consecuencias negativas, como el robo de información de la empresa. De la misma forma es mejor no publicar información personal en las redes sociales laborales.

¡No hagas públicos detalles de tu vida!

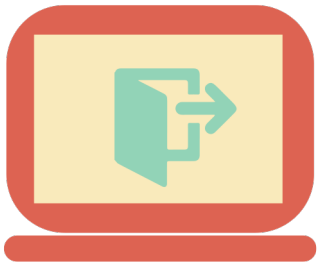
Evita compartir tu ubicación actual

Al publicar la ubicación desde las redes sociales, esta puede ser revisada por los contactos que tienes, incluso marcas de productos, páginas que sigues y grupos. Más allá de recibir un like, tus amigos podrían acompañarte al lugar donde te encuentres y también podría ayudar a identificar en tiempo real tu paradero a lo largo de un viaje.

Recuerda que el uso de las redes sociales no es gratuito, pues las compañías que proveen el servicio se encargan de vender tu información de perfil a empresas para hacer estudios de mercado específicos que les ayuda a ofrecerte publicidad de productos que puedes consumir y así dirigirte a los lugares que ellos publican. Lamentablemente existen personas en las redes sociales con perfiles falsos que se dedican a identificar a personas que comparten su ubicación para realizar robos y, en el peor de los casos, secuestros.

Cierra la sesión cuando termines de utilizar el servicio

Muy poca gente cierra su sesión de redes sociales al terminar de usarlas, muchas veces por comodidad. Si te encuentras en un dispositivo al que solo tú puedes acceder, podría comprenderse, pero es mucho más seguro cerrar las sesiones en el navegador que utilizas, pues existen circunstancias difíciles de prevenir, como el robo o pérdida de los dispositivos que utilizamos, lo cual dejaría expuesta nuestra información en manos de los delincuentes. Además las bromas se encuentran a la orden del día y alguien que pueda desbloquear tu móvil o cualquier dispositivo podría hacer una broma de mal gusto.



Otras medidas para considerar

No almacenes contraseñas de acceso en equipos compartidos

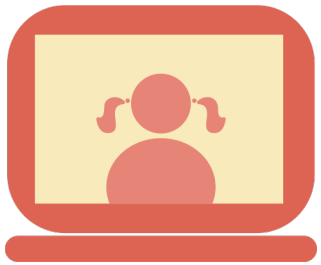
Actualmente algunas páginas te permiten guardar la contraseña para tu próxima visita como un servicio adicional. El problema es cuando se guarda en un dispositivo de uso común, como en un café Internet, el equipo de cómputo de un amigo o en alguna otra institución, donde no sea tu propio equipo.

Una persona con malas intenciones podría eliminar tu información en el mejor de los casos, pero también podría extraer datos importantes, poner en riesgo tu identidad y tu privacidad. Evita esta opción cuando no sea necesario acceder a equipos ajenos como computadora, teléfono celular, tablet, etc.

Enseña a tus hijos a usar Facebook y otras redes sociales

Las nuevas generaciones aprenden fácilmente cómo usar las herramientas digitales, teléfonos inteligentes, tablets y computadoras, por ello es importante que conozcan la manera correcta de utilizarlos, para qué sirven y cuándo utilizarlos.

Los niños son más inocentes al aceptar a personas desconocidas en sus redes sociales y al dar clic a botones que los pueden llevar a sitios infectados o no aptos para su edad. Es importante tomar en cuenta que las redes sociales tienen un mínimo de edad para activar una cuenta de usuario por alguna razón.



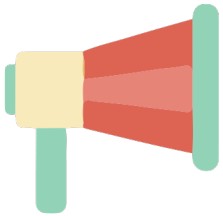
No compartas tu contraseña

Las relaciones interpersonales son fáciles de vulnerar, por lo que es posible que personas que aparentan ser confiables soliciten tu contraseña aprovechándose de tu buena voluntad con el pretexto de ofrecer algún servicio o promoción.
Desconfía de quien te pida una contraseña o que trate de convencerte de introducirla en un dispositivo ajeno. Si logran obtener tu contraseña pueden tener acceso a tu información personal y redes sociales o comprometer tus datos bancarios.

Reporta los abusos

Las redes sociales se prestan para que las personas con las que estamos conectados tengan la capacidad de comentar u opinar acerca de lo que publicamos, lo cual puede ser contraproducente. La opinión de las personas puede llegar a ser muy distinta o puede que no empate con nuestras intenciones, de manera que podrían hacer comentarios hirientes o irrespetuosos.

La mayoría de las plataformas han implementado la opción de eliminar comentarios o reportar abusos para que las personas que hacen mal uso de ellas tengan restricciones de los servicios.



Es mejor prevenir que lamentar

Estas recomendaciones te ayudarán a fortalecer tu seguridad en las redes sociales. También es buena idea compartirlas con tus amigos más cercanos o colaboradores de trabajo para popularizar buenas prácticas que hagan de las redes un ambiente más seguro. Las ciberamenazas son cada vez más sofisticadas, así que no está de más seguir información y estar enterado sobre ellas, por ejemplo suscribiéndote a sitios de noticias al respecto o visitando el portal y las redes sociales de UNAM-CERT.

- Portal seguridad: https://www.seguridad.unam.mx/
- Facebook: https://www.facebook.com/unamcert/
- Twitter: https://twitter.com/unamcert
- Youtube: https://www.youtube.com/user/SeguridadTV

Referencias

Schurgin, G., Clarke-Pearson, K., Council on Communications. (2011). The Impact of Social Media on Children, Adolescents, and Families. Pediatrics 2011. 127;800. Recuperado el 14 de noviembre de 2017, de http://pediatrics.aappublications.org/content/pediatrics/127/4/800.full.pdf

BBC News. (2017). Votes in 18 nations 'hacked' in last year [en línea]. Technology. Recuperado el 14 de noviembre de 2017, de http://www.bbc.com/news/technology-41983599?ct=t()

Borbón, S. (Enero, 2012). Redes sociales, entre la ingeniería social y los riesgos a la privacidad. Revista .Seguridad Cultura de prevención para TI. Núm. 12. Recuperado el 14 de noviembre de 2017, de https://revista.seguridad.unam.mx/numero-12/redes-sociales-entre-la-ingenier%C3%AD-social-y-los-riesgos-la-privacidad

CSI/UNAM-CERT. (Feb, 2009). Seguridad en los sitios de redes sociales. Revista .Seguridad Cultura de prevención para TI. Recuperado el 14 de noviembre de 2017, de https://revista.seguridad.unam.mx/numero-0/seguridad-en-los-sitios-de-redes-sociales

Asociación de Internet.mx. (2017) 13 Estudio sobre los Hábitos de los usuarios de Internet en Mexico 2017. Recuperado el 28 de noviembre de 2017, de https://www.asociaciondeinternet.mx/es/component/remository/Habitos-de-Internet/13-Estudio-sobre-los-Habitos-de-los-Usuarios-de-Internet-en-Mexico-2017/lang,es-es/?Itemid=

Kaspersky Lab. (2013). Los 10 peores tipos de contraseñas. Recuperado el 28 de noviembre de 2017, de https://latam.kaspersky.com/blog/los-10-peores-tipos-de-contrasenas/1723/

UNAM-CERT. (s/f). Seguridad en los sitios de redes sociales. Revista .Seguridad Cultura de prevención para TI. Recuperado el 28 de noviembre de 2017, de https://revista.seguridad.unam.mx/numero-0/seguridad-en-los-sitios-de-redes-sociales

_____ (2004). Protegiendo la privacidad. Recuperado el 28 de noviembre de 2017, de https://www.seguridad.unam.mx/protegiendo-la-privacidad

_____ (2010). Robo de identidad y consecuencias sociales. Recuperado el 28 de noviembre de 2017, de https://www.seguridad.unam.mx/robo-de-identidad-y-consecuencias-sociales

No apunto contraseñas en papelitos

Un papel no es un medio seguro, pues otras personas podrían verlo o robarlo. Tampoco lo anotes al final de tus cuadernos, es el primer lugar donde buscaría alguien interesado.

Cuido lo que imprimo en la oficina

Cuando se comparte una impresora, como sucede en las oficinas, es necesario considerar la confidencialidad de la información que estamos imprimiendo. No permitas que ojos indiscretos vean tu información sensible.

Activo el bloqueo de mis dispositivos

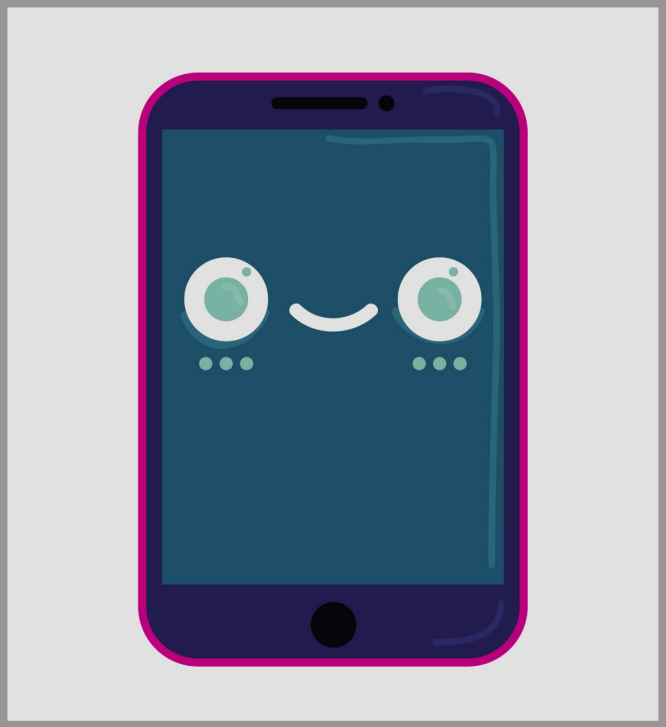
Bloquea tus dispositivos cuando no los uses, ya sea tu computadora o tu móvil. Valora tu información para evitar que personas maliciosas hagan mal uso de ella.

No comparto contraseñas con nadie

Los ciberdelincuentes pueden engañarte para que reveles tus credenciales de acceso a redes, correo electrónico o cuentas bancarias, así que no proporciones esta información nunca.

DISC 2017
La seguridad somos todos

Consejos



SE BUSCA

- Se busca teléfono celular modelo “Aycel” año 2016.
- Visto por última vez en el baño, el día 30 de noviembre del 2017.
- Llevaba una carcaza color rosa y una estampa de un gatito en la parte posterior.
- Cualquier información referente a la ubicación de este celular

Se recompensará.

¿Qué hacer ante la pérdida de tu smartphone?

Perder un teléfono móvil trae consigo dolores de cabeza. Primero se siente el flujo de adrenalina por haberlo perdido o por darnos cuenta de que hemos sido robados y después pensamos en la información importante que albergábamos en él y que ahora, por haberlo perdido, valoramos. ¿Qué información deberíamos valorar en nuestro celular, antes de perderlo? ¿Qué hubieras hecho distinto si tuvieras la oportunidad de regresar el tiempo? ¿Qué medidas de seguridad deberías tener con tu teléfono móvil?

Antes de perder tu información

Existen algunas medidas de seguridad que es bueno tomar en cuenta al usar nuestro teléfono móvil. Seguir estas recomendaciones es parte de llevar buenas prácticas de seguridad, y aliviará un poco la ansiedad de volver a perder tu información más valiosa. Para comenzar, es necesario que hagas una lista de la información que es más importante para ti y que almacenas en tu dispositivo móvil, por ejemplo, la lista de contactos, tus fotografías íntimas o información bancaria. Una vez que hayas catalogado la información valiosa en tu móvil, toma en cuenta los siguientes consejos.

1. Guarda las especificaciones del teléfono

En caso de robo o extravío, es necesario conocer las características de tu teléfono, tanto para levantar una denuncia en el ministerio público para hacer efectivo el seguro (si tienes uno) o para identificar tu teléfono en caso de que alguien lo recupere. Resguarda la siguiente información:

- Tu número de teléfono
- La marca y el modelo
- Color y detalles de apariencia
- El número IMEI (*International Mobile System Equipment Identity*)

2. Utilizar el bloqueo de pantalla

No hace falta que roben tu teléfono para acceder a tu información, si no usas un sistema de bloqueo cualquier persona podría tomar tu móvil y acceder sin problemas. Si lo extravías, el actor malicioso no tendrá ninguna dificultad de conocer tu vida a través del teléfono, por ejemplo, podrá ver tu correspondencia y conocerá tus contactos. Esta información es útil para los criminales, pues se sabe que con ella pueden realizar extorsiones telefónicas. Puedes usar diferentes métodos de bloqueo, como un patrón, una contraseña o un método biométrico como tu huella digital o tu rostro. Mientras más robusto sea el código de bloqueo más segura estará la información en tu dispositivo.

3. Guarda el código de seguridad de tu *smartphone*

Puede ser que uses un patrón de seguridad, pero si utilizas un código numérico de seguridad para acceder a tu teléfono, te recomendamos almacenarlo en un gestor de contraseñas. En poco tiempo no necesitarás revisar el gestor, puesto que memorizarás el número, aunque si crees que tienes memoria de teflón y nada se te pega, podrías considerar resguardarla. Pero, ¿qué es un gestor de contraseñas? Sigue leyendo y te contamos.

4. Utiliza un gestor de contraseñas o un agente de confianza

Haz rápidamente un listado de las credenciales de acceso que debes recordar: la clave para iniciar tu ordenador, otra para iniciar la sesión de Google para acceder a tu correo, una más para la cuenta de Netflix, del banco, de Facebook, de Twitter, de Instagram, las claves para acceder al sistema fiscal y emitir recibos, etcétera. Puede ser que uses muchas contraseñas y esto te agobie, pero por seguridad, ¡no uses la misma para todas las cuentas! Si reciclas tu contraseña, todas tus cuentas podrían ser vulneradas cuando un atacante la adivine. Por ello, te recomendamos usar un gestor de contraseñas, en el que puedes almacenar tus llaves de acceso sin tener que memorizarlas. Para utilizarlas solo tienes que abrir el gestor, copiar el nombre de usuario y la contraseña, y así acceder a tus servicios. Existen algunos gestores que sincronizan la información en distintos dispositivos cuando modificas alguna contraseña, lo cual es bastante conveniente.

Además del gestor, puedes usar un agente de confianza, que es una herramienta, como Smart Lock, mantiene desbloqueado tu teléfono en diferentes circunstancias, por ejemplo, si estás en casa, si lo tienes cerca de ti, o si te encuentras en el trabajo y no deseas desbloquearlo cada vez que lo necesitas. El agente de confianza puede identificar las condiciones que seleccionas (pre-

viamente) para mantenerse activo sin necesidad de bloquearse. Una vez que las condiciones cambian, por ejemplo, estando en la calle y fuera de casa, el bloqueo funciona como ya conoces.

5. Habilita la función "encontrar mi dispositivo"

En la actualidad, la mayoría de los dispositivos tienen una función para buscar el dispositivo móvil si se ha extraviado, pero es importante activarlo antes de que lo pierdas para poder recuperarlo. Accede a la configuración de tu teléfono y busca esta opción para habilitarla. Además, esta función permite a los usuarios bloquearlo de manera remota o borrar la información del teléfono, en caso de perderlo. Sin embargo, en caso de que el celular sea apagado o lo desconecten de una red, esta función puede no funcionar, pero el sistema de rastreo te podrá decir dónde fue detectado la última vez que tuvo conexión y cuando se encienda de nuevo o encuentre una red disponible será hallado.

6. Crear una copia de seguridad en un equipo personal y/o en la nube

Es útil tener un respaldo de tu información, y puedes hacerlo creando una copia de seguridad almacenada en algún equipo personal de manera local o en la nube. Lo importante de usar un servicio de nube es ser selectivo con la información que se respalda. Al tener una copia de seguridad, aseguras la disponibilidad de tu información en caso de que extravíes o roben tu teléfono, y podrás traspasarla a un nuevo celular. Existe un software propio de cada marca de teléfono que te ayuda a gestionar tus respaldos, y te recomendamos hacerlo de manera periódica.

7. Cifra tu teléfono

No toda la gente usa un bloqueo en su teléfono, lo cual ya expone su información en caso de robo, y mucha menos gente cifra su información en el celular. Si esta práctica fuera generalizada, los celulares ya no serían atractivos para el delincuente común porque implicaría mucho trabajo descifrar la información. Es decir, no es suficiente con bloquear el teléfono, porque una persona con suficientes habilidades podría evadirlo y tener acceso a la información, pero es otra historia intentar descifrar la información si está cifrado.

8. Utiliza una marca de seguridad

Otra forma de identificar tu teléfono es añadiendo una marca de seguridad. Puedes usar un lápiz

ultravioleta, por ejemplo, para escribir información personal en la batería, así será fácil saber si se trata de tu móvil. También puedes escribir un número alternativo para que te contacten, si tienes la suerte de que caiga en manos de una persona con buenas intenciones. Sin embargo, ten cuidado, no reveles demasiada información personal, como tu domicilio, pues podrían aprovecharla, si cae en manos de gente maliciosa.

Después de perder tu móvil

En el lamentable caso de que roben tu dispositivo, debes tomar ciertas medidas para protegerte a ti mismo de ser implicado en alguna actividad maliciosa que no cometiste o para reclamar el seguro, en caso de que hayas comprado uno. Sigue estas recomendaciones, pero sobre todo, no pierdas la calma.

1. Rastrear el móvil

Si activaste la función para buscar tu dispositivo, úsalo ahora. Cada fabricante tiene una guía para buscar tu celular con ayuda de otro dispositivo o una computadora, así que familiarízate con el proceso antes de que llegue el fatídico momento de usarlo. Algunos programas, al rastrearlo, indicarán la ubicación aproximada del teléfono.

Encontrar Mi iPhone (iOS)
https://support.apple.com/es-mx/explore/find-my-iphone-ipad-mac-watch
Encontrar mi dispositivo (Android-Google)
https://support.google.com/accounts/answer/6160491?hl=es-419

2. Reportar el teléfono extraviado o robado

Ten a la mano tú número IMEI, que es el código internacional de identidad de los dispositivos móviles. Es como la huella digital de tu dispositivo. Para saber tu IMEI, existen diferentes métodos: teclea *#06# como si hicieras una llamada e inmediatamente aparecerá el número de identificación; puedes buscar en la parte trasera de tu teléfono o en la bandeja de la tarjeta SIM; también puedes buscar en el panel de configuración, en la sección **Acerca de** y, si tienes Android, ve a **Identidad del teléfono**; el tablero de Google (dashboard) también muestra una lista de tus dispositivos y sus números de identificación; también puedes encontrarlo en la batería de tu teléfono. Copia en un lugar seguro este número de identificación.

Si lo extravías, contacta a la compañía que presta el servicio de telefonía y solicita el bloqueo de la línea, del chip y del IMEI. Existe una lista negra con los números IMEI robados que los compradores de móviles de segunda mano pueden consultar para saber si el dispositivo fue hurtado.

Debes notificar a la compañía que has extraviado tu teléfono para que deshabiliten tu número y así evitar que las personas que lo tienen lo sigan usando. Quienes roban celulares no solo tienen la intención de venderlo, sino de realizar actividades maliciosas a través de números robados.

3. Levantar una denuncia

Sabemos que no es muy grato presentarte en el ministerio público para presentar una denuncia, pero es necesario que lo hagas para iniciar una investigación. Además, las compañías de seguros solicitan una copia del documento de la denuncia ante las autoridades para hacer válida la póliza, y es probable que tu banco también la solicite en caso de que tus cuentas bancarias hayan sido afectadas. Si no tienes seguro, de cualquier manera recomendamos que lo denuncies, para tener un antecedente en caso de que tu teléfono sea usado para fines maliciosos.

4. Quitar permisos al dispositivo sobre tus aplicaciones vinculadas a tus servicios en línea

Imagina que no usas un bloqueo para tu dispositivo y la persona que lo tiene accede sin complicaciones a él. Si eres un usuario común, el delincuente tendrá acceso a tu cuenta de Facebook, Twitter, Instagram, Google, Tinder o Snapchat y podrá saber más de ti, usar esa información para extorsionarte o afectar a tus seres queridos. Por ello es necesario que accedas a tus servicios en línea y elimines los permisos al dispositivo que los utiliza a ellos. De lo contrario sería como tener a un desconocido malicioso sentado en tu sala tomando té con tus visitas.

5. Cambiar la contraseña de acceso a tus servicios en línea, Redes sociales, Uber, servicios de entretenimiento, financieros

Además de deshabilitar los permisos, aprovecha para cambiar la contraseña con la que accedes a tus servicios en línea. Piensa que tus aplicaciones están a solo un toque de mostrar tu información

personal, y esa es la facilidad con la que un intruso podría aprovecharlos, mucho más si puedes comprar con un solo clic en línea. No dejes que pase mucho tiempo para seguir este consejo, a veces la oportunidad hace al ladrón.

6. Comprobar si ha habido cualquier movimiento bancario

Si tienes información bancaria almacenada en tu teléfono inteligente y te ha llevado mucho tiempo (con un día basta) levantar las denuncias y solicitar el bloqueo, es mejor que revises los movimientos de tu cuenta bancaria para solicitar una aclaración cuanto antes. Puede ser que el delincuente haya hecho cargos a tus cuentas bancarias o haya vendido tu información a un tercero.

7. Borrado remoto

Si fuiste prevenido, seguramente activaste el borrado remoto de la información de tu teléfono inteligente. Además, debes tener habilitada el sistema de localización que reconoce la ubicación de tu teléfono. Si estas dos características están habilitadas, podrás activar el borrado remoto por medio de otro dispositivo o una computadora.

Recursos

- **Cómo quitar permisos a las aplicaciones para hacer tu móvil más seguro** https://elandroidelibre.elespanol.com/2017/02/quitar-permisos-las-aplicaciones.html
- **¿Cómo obtengo el IMEI de mi celular?** http://www.ift.org.mx/multimedia/como-obtengo-el-imei-de-mi-celular
- **Cómo eliminar los datos de un móvil robado de forma remota** http://computerhoy.com/paso-a-paso/moviles/como-eliminar-datos-movil-robado-forma-remota-36809
- **¿Qué hacer en caso de robo de celular?** http://www.ift.org.mx/usuarios-y-audiencias/que-hacer-en-caso-de-robo-de-celular

unamcert

DISC 2017

DGTIC

DIRECCIÓN GENERAL DE CÓMPUTO Y DE
TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

UNAM
CERT

Revista .Seguridad *Cultura de prevención para* TI
No.30 sumplemento / noviembre 2017