Consejos y recomendaciones para prevenir riesgos y evitar amenazas

Consejo Profesional de Ciencias Económicas de la CABA

Fuente: Revista Consejo – Nº 19 – Septiembre 2011 – ISSN 1851-6610

“La seguridad depende principalmente del factor humano y no del factor tecnológico”.

Las amenazas informáticas han ido evolucionando a la par de las Tecnologías de la Información y la Comunicación. Por ello es necesario que los usuarios incorporen buenas prácticas para proteger la información y no convertirse en potenciales víctimas de malas prácticas o delitos informáticos.

A continuación ofrecemos un amplio panorama sobre algunas medidas de seguridad y mecanismos de prevención que el usuario debe adoptar a fin de minimizar los riesgos.

Buenas prácticas en la utilización de contraseñas

La clave de acceso es un conjunto de caracteres escritos por el usuario siguiendo una norma preestablecida que lo identificará ante el sistema de información a utilizar.

La clave de acceso debe ser:

1. Personal.
2. Secreta.
3. Intransferible.
4. Difícil de averiguar.
5. Modificable solo por su titular.

Tips de seguridad en la utilización de contraseñas

1. No preste ni divulgue a nadie sus contraseñas.
2. Cambie periódicamente sus claves personales, al menos una vez cada 30 días.
3. Asegúrese de que nadie esté viendo su clave cuando la ingresa.
4. Quite la selección de recordar usuario y clave cuando accede a sus cuentas de correos personales.
5. No use recordatorios de contraseñas pegados en el monitor, teclado o escritorio.
6. Intente no generar contraseñas que sean combinaciones de la primera.
7. Modifique su contraseña si considera que pudo ser expuesta e infórmelo inmediatamente.

¿Cómo crear una clave de acceso robusta?

1. Emplee palabras de difícil deducción y de al menos 8 caracteres de longitud (por ej.: nombre de mascota: Blanquita).
2. Use un acrónimo de algo fácil de recordar y agréguele un número (por ej.: Lucía y Jorge: LucyJor02).
3. Utilice una frase no conocida (por ej.: Verano del 42: Verdel42).
4. Reemplace letras por números (por ej.: DosMil10).

5. Emplee letras mayúsculas, minúsculas, números y caracteres especiales (por ej.: Los4@migo$).

Buenas prácticas en la utilización de su computadora

1. Instale herramientas adecuadas de seguridad en los equipos informáticos en función del tipo de negocio que tenga y de la información a proteger.
2. Permita que el detector de virus se actualice y verifique el conte- nido de su computadora como asi también de los dispositivos que se conectan a ella.
3. Deshabilite la opción de compartir recursos de su computadora si no la necesita.
4. Haga uso responsable de los dispositivos portátiles, tales como iPods, memorias USB, mp3, en tre otros.
5. Mantenga actualizado los sistemas operativos de todos los equipos y las herramientas de protección utilizadas, con la últimos/anterior versión disponible.
6. Cuente con un plan de resguardo de la información que le permita administrar y verificar su correcto funcionamiento.
7. Capacítese y/o capacite a los usuarios, empleados o familiares en materia de seguridad y protección.

Buenas prácticas en Internet

1. No conecte su equipo a Internet sin antes haberlo protegido adecuadamente mediante la configuración de sistemas de protección, como firewall, antivirus, etc.
2. Escriba la dirección de la página de Internet tal cual la conoce en una ventana nueva del navegador.
3. Verifique la seguridad en los sitios de Internet adonde accede.
4. No acceda a enlaces menciona dos en correos electrónicos.
5. No ingrese ni envíe sus datos personales y/o números de tarjetas de crédito si no conoce el origen de donde le es solicitado.
6. Evite acceder a sitios desconocidos o no confiables.
7. No acepte la instalación automática de software.
8. No conecte sistemas a Internet con cuentas de usuarios y contraseñas que vienen instaladas por defecto o que son fáciles de adi vinar.
9. No descargue archivos ejecutables.
10. No deje información sensible en páginas o foros.
11. Si debe enviar información sensible:
    - Solo hacerlo en sitios seguros (https).
    - Verifique el certificado del sitio.
12. Verifique la configuración segura del navegador.

Buenas prácticas accediendo a sus cuentas bancarias desde Internet

1. Evite acceder a su homebanking desde locutorios.
2. Escriba la dirección de la página de su homebanking para acceder en una ventana nueva del explorador.

3. Antes de cargar sus datos personales o financieros verifique que el navegador muestre un candado cerrado y que la dirección empiece con https.
4. Quite la selección de recordar usuario y clave cuando accede a sus cuentas bancarias desde sitios públicos.
5. No utilice recordatorios de usuarios y contraseñas guardados en su billetera o cartera.
6. Cambie periódicamente sus claves personales, en especial luego de haber accedido a sus cuentas desde lugares poco seguros.
7. Nunca ingrese todos los datos de su tarjeta de coordenadas, ni tampoco los envíe por correo electrónico, mensaje de texto o por teléfono.
8. Tampoco envíe sus datos de ingreso, número de documento, identificador de usuario y/o clave por correo electrónico o por algún otro medio.

Buenas prácticas enviando y recibiendo correos electrónicos

1. No abra archivos adjuntos de origen desconocido o que no espera recibir aunque le parezca que su origen es conocido.
2. No abra archivos que tengan extensiones ejecutables.
3. No abra archivos adjuntos que tengan más de una extensión.
4. Verifique con el remitente la razón por la cual le envió un archivo adjunto.
5. Descargue archivos de sitios en los cuales confíe.

Si tuviera motivos para reenviar un correo electrónico, le sugerimos hacerlo de la siguiente forma.

1. Elimine las direcciones de correo electrónico de los remitentes o copie el contenido del correo original y arme uno nuevo.
2. Si lo reenvía a más de una persona, utilice la opción de enviar con copia oculta.
3. No sea un reenviador compulsivo de correos electrónicos.

A continuación le sugerimos algunas recomendaciones para evitar los correos masivos de tipo "spam".

4. No deje su dirección de correo electrónico en cualquier formulario o foro de Internet.
5. No responda los correos no solicitados, bórrelos.
6. Evite enviar respuestas a la dirección que figura en los correos para evitar reenvíos posteriores.
7. Configure filtros o reglas en el programa de correo para filtrar mesajes de determinadas direcciones.
8. No configure la opción de respuesta automática para los pedidos de acuse de recibo.
9. No responda a los pedidos de acuse de recibo de orígenes dudosos.

En el caso de recibir pedidos de envío de información confidencial, a los efectos de evitar su robo o mal uso, se recomienda proceder de la siguiente forma.

1. Comunicarse telefónicamente con la empresa que envió el correo para confirmar el pedido.
2. Nunca envíe por correo electrónico información confidencial sin cifrar.
3. Verifique el origen del correo y el destino de los enlaces.
4. Compre siempre en sitios conocidos o de los que se pueda obtener referencias reales.

Buenas prácticas en el uso de redes sociales

Si se utilizan redes sociales, existen ciertas consideraciones a tener en cuenta a la hora de compartir información.

1. Quite la selección de recordar usuario y clave cuando acceda a sus cuentas desde sitios públicos.
2. Restrinja el acceso a su perfil solo a sus amistades.
3. Evite en lo posible poner fotos y/o cualquier tipo de información personal o datos de su familia en comunidades y/o foros de Internet.
4. No acepte solicitudes de amistad a gente que es desconocida o de dudosa procedencia.
5. Advierta el peligro de dialogar o peor aún de citarse con desconocidos.
6. Comparta con un conocido cual quier duda o situación que parezca extraña en Internet.

Buenas prácticas en el uso de Internet en el hogar

1. Herramientas de seguridad: proteja la información de su PC usando herramientas disponibles, como actualizaciones del sistema operativo, antivirus, firewall, etc.
2. Reglas claras: establezca reglas acerca de lo que pueden hacer los niños en y con Internet tanto dentro como fuera de sus hogares.
3. Control visual: periódicamente supervise el contenido de pantal mientras sus hijos utilizan la computadora.
4. Ubicación de la PC: intente ubicar el equipo en lugares de tránsito del hogar; evite ponerlo en el cuarto de los niños.
5. Comparta Internet: esté junto a su hijo mientras navega por Internet de manera de conocer sus hábitos de navegación y aconsejarlo respecto de estos.
6. Enseñe a consultar: instruya a sus hijos a indagar antes de facilitar datos personales por Internet.
7. Converse: sobre sus amigos y actividades en línea del mismo modo que sobre cualquier otra actividad.
8. Ante lo inesperado: acuerde que, ante cualquier duda, inquietud, problema, angustia o situación molesta habrá que conversar.
9. Filtros de contenido: incorpore filtros que permitan controlar el acceso solo a los sitios que son considerados seguros, configurándose y controlándose periódicamente para ajustar su adecuado funcionamiento.