albada
Servicios Informáticos

albadaNet
Servicios de Internet

Principales fundamentos de seguridad

No nos preocupamos de la seguridad de nuestras contraseñas al pensar que no somos un objetivo interesante para los estafadores en línea. Asumimos que los criminales están interesados en peces más gordos, como servidores de bancos o cuentas de personas importantes, pero no siempre es el caso.

Cuando necesitamos pensar en una contraseña compleja que nos ofrezca seguridad y que podamos recordar fácilmente, no siempre sabemos cómo hacerlo.

Desde Albada, queremos ofrecerle unos consejos de seguridad para su aplicación en el entorno laboral y personal que nos ayuden a evitar en la medida de lo posible, los riesgos a los que actualmente estamos expuestos.

Contraseñas y cuentas de usuario:

Mantenga sus contraseñas en secreto, incluso de los más cercanos.

No comparta **NUNCA** sus contraseñas, ni siquiera a los especialistas de seguridad, los responsables de la seguridad en su empresa no necesitan su contraseña y nunca se la pedirán.

Si recibe correos (por ejemplo, de Google) indicándole que les proporcione la información de su cuenta y que si no lo hace la borrarán en un plazo determinado de tiempo, elimine ese email, es fraudulento. Si introduce sus datos, le robarán su contraseña.

Qué puede pasar si saben mi contraseña:

Tendrán control sobre su sistema, podrán acceder a su correo, enviar spam o solicitudes de ayuda económica en su nombre, obtener acceso a datos confidenciales y usarlos en su provecho, acceder a su cuenta bancaria y/o hacer compras en su nombre…

Si alguien le pide la contraseña piense: ¿Quién se la pide?, ¿Por qué necesita su contraseña?, ¿Podría pasar sin ella?... verá que no es necesario compartirla.

Almacenar las contraseñas:

Lo mejor es recordarlas, pero si esto no fuera posible, guardarla en su cartera es una buena opción o en la memoria de su smartphone. Otros lugares, como el escritorio o en una libreta o un cajón, son totalmente accesibles para cualquiera.

La mejor opción para crear una contraseña segura es insertar un par de símbolos aleatorios en medio de la contraseña, sustituir un par de símbolos, escribir una parte de la contraseña y recordar el resto (truco nemotécnico).

NO le diga a nadie donde guarda su contraseña.

Si tiene la sospecha de que alguien sabe su contraseña, **CÁMBIELA** inmediatamente y notifíquelo al personal de seguridad informática de su empresa.

Y si ha usado sus cuentas personales en equipos de la empresa, es recomendable cambiar también sus contraseñas personales.

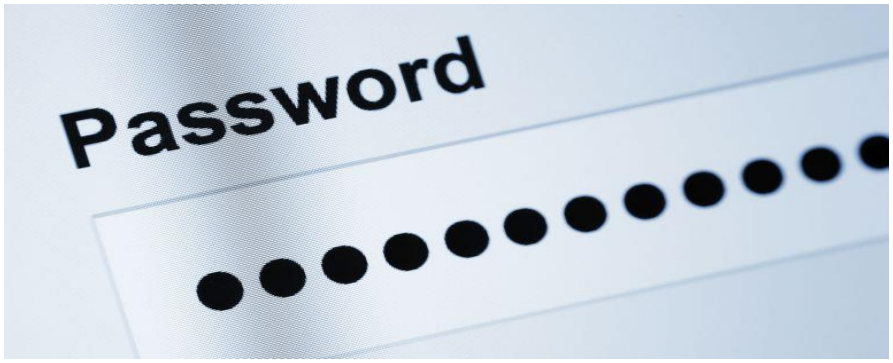
- ***USE SIEMPRE CONTRASEÑAS SEGURAS***

Las contraseñas muy largas no son las más seguras, porque son más difíciles de recordar y la longitud no lo es todo.

La longitud mínima aceptable son 8 caracteres, conteniendo letras mayúsculas y minúsculas, números y caracteres especiales -, @, #, $, %, etc.…

Para crear contraseñas seguras, lo más recomendable es usar un programa Generador de Contraseñas.

- ***NO UTILICE NUNCA LA MISMA CONTRASEÑA PARA SU USO PERSONAL Y CORPORATIVO***



¿Cómo puedo saber si un estafador ha accedido a mi cuenta?

Si un servicio en la red le envía un mensaje de "***un intento de acceso no autorizado a su cuenta",*** es posible que no se haya accedido a la misma o que sí lo hayan logrado, en cualquier caso, por seguridad, cambie su contraseña.

Si detecta respuestas en redes sociales o correo a mensajes que usted no ha enviado o los mensajes estaban marcados como "No leídos" y aparecen de repente como "Leídos" … cualquier cambio significativo que aprecie, es motivo para cambiar su contraseña.

Si todo esto ocurre en el entorno de trabajo, debe ponerse inmediatamente con el equipo de seguridad de la empresa.

Peligros en el correo electrónico:

El correo electrónico es uno, por no decir el principal, canal de comunicación que existe. Enviamos y recibimos correos, archivos y gran variedad de información cada día.

¿Qué es el PHISHING?

Es un tipo de fraude en internet en el cual su objetivo es obtener dinero o información confidencial. Los correos de phishing son los que llegan a su bandeja de entrada disfrazados de mensajes genuinos del banco, sistemas de pago, facturas, correos y otras organizaciones.

Qué pueden conseguir con estos mails:

- Lograr que les envíe sus datos de cuenta y contraseña.
- Engañarle para que instale un programa de malware.
- Robar documentos confidenciales.

- ***NUNCA HAGA CLICK EN UN ENLACE DENTRO DE UN CORREO SOSPECHOSO. SI SOSPECHA QUE ALGUIEN INTENTA PIRATEAR SU CUENTA, CAMBIE LA CONTRASEÑA DEL CORREO INMEDIATAMENTE***

Recibir un mail de notificación de cambio de contraseña en su correo de verificación o un mensaje de texto en el móvil con un código para iniciar la sesión en el correo, no poder iniciar la sesión de correo porque su contraseña dice que es incorrecta, si al acceder al correo hay una notificación de un acceso desde un dispositivo desconocido o una IP de otro país, cambios de diseño en el correo, han desaparecido correos o hay contactos que no conoce en su libreta de direcciones… son indicios claros de que **su cuenta ha sido pirateada**.

Cómo actuar si creemos que han accedido a nuestra cuenta de correo

Si todavía tiene acceso a su cuenta, cambie la contraseña inmediatamente. Si esa contraseña es la misma en otros servicios o recursos, cámbiela en todas las ubicaciones que la haya usado.

Si no puede acceder al correo, restaure su contraseña con el correo de verificación o reserva (he perdido mi contraseña o no recuerdo mi contraseña son los accesos para recuperarla).

Si es una cuenta de correo corporativo, póngase en contacto con el administrador de sistemas de su empresa.

Consejos para hacer el correo más seguro ante pirateos:

- Use el acceso en dos pasos, la contraseña y un mensaje temporal con un código que recibirá en el móvil.
- Cree contraseñas seguras.
- Cambie con frecuencia las contraseñas del correo y las cuentas vinculadas a él.
- Utilice contraseñas diferentes para cada cuenta y servicio.

- NUNCA INTRODUZCA SU CONTRASEÑA DE CORREO EN NINGUNA PÁGINA WEB, CORREO ELECTRÓNICO QUE SE LO SOLICITE O VENTANAS EMERGENTES DE UNA PÁGINA QUE NO SEA EL CORREO WEB OFICIAL

- NUNCA ENVÍE POR CORREO ELECTRÓNICO SU CONTRASEÑA O INFORMACIÓN CRÍTICA DE LA TARJETA DE CRÉDITO

Antes de enviar documentación sensible verifique si la petición es legítima, el banco le pide copias del DNI o documentación fiscal, etc.

- NUNCA ENVÍE UNA FOTO O ESCANEO DE UNA TARJETA BANCARIA, CON ESOS DATOS PUEDEN SACAR DINERO O REALIZAR COMPRAS NO AUTORIZADAS-

Si se realizan compras por internet es muy recomendable usar tarjetas especiales o prepago para tal fin, ciber-tarjetas, tarjetas CASH o tarjetas exclusivas para compra online.

Si recibe un correo para que introduzca sus datos de tarjeta bancaria, elimínelo. Ningún servicio o banco se lo pedirá, la compra online usa la propia página y pasarela de pago del servicio (comprar un viaje, Amazon, etc.)

Estafas más comunes en el correo electrónico:

- Engañar al usuario para seguir un enlace de un banco o sitio web para que introduzca sus datos personales y/o se descargue malware (correo de Endesa, Correos, cheques regalo de Amazon, etc.)
- Completar un formulario para confirmar su cuenta o introducir sus datos bancarios. (ganador de lotería, cesta compra Mercadona, etc.)
- Descargar un archivo adjunto en el correo electrónico (factura recibida de algo que no se espera)
- Timo del príncipe nigeriano (heredero de gran fortuna, astronauta, mecenas multimillonario de Nueva York), correo indicando que se necesita su cuenta bancaria para transferirle una herencia multimillonaria por un porcentaje.

Estos son algunos de los muchos ataques y vulnerabilidades que actualmente existen en internet. Desde **Albada Informática** y **albadaNet**, estamos a su disposición para brindarle las soluciones tecnológicas de seguridad más avanzadas y ofrecerle las opciones más adecuadas a su empresa, con el fin de salvaguardar toda su información.