Preguntas frecuentes

CLAVES PARA PROTEGER TUS CONTRASEÑAS

¿CÓMO NO CREAR UNA CONTRASEÑA?

#1

Lo que nunca tienes que hacer es utilizar contraseñas cortas que puedan obtenerse mediante ingeniería social, como el nombre de tu mascota, fechas importantes para ti o códigos postales. Tampoco hagas sustituciones clásicas como cambiar una e por un 3 o una o por un 0, ya que son trucos que los cibercriminales se conocen.

¿CÓMO GESTIONAR TUS CONTRASEÑAS?

#2

Hoy en día de poco sirve haber tomado las molestias oportunas para crear una buena contraseña, si luego no las gestionamos correctamente. Por eso,una de las recomendaciones principales es no reutilizar las contraseñas en más de una web. Intenta tener una contraseña diferente en cada web, para que si alguien consigue descifrar una de tus contraseñas o la obtiene gracias a una filtración no pueda utilizarla para acceder a tus cuentas en más de una web o servicio online.

¿QUÉ ES LA VERIFICACIÓN EN DOS PASOS?

#3

Una opción de seguridad que ofrecen la mayoría de grandes servicios como WhatsApp, y que hace que para terminar de identificarte en un servicio necesites un segundo paso después de introducir la contraseña. El segundo paso que se requiere depende del servicio; puede ser un código por SMS que tienes que introducir después de la contraseña, mientras que otros te piden crear un pin o interactuar con la misma aplicación utilizando otro dispositivo como el móvil.

LAS CONTRASEÑAS, ¿CÓMO NOS PROTEGEN?

#4

Son el principal mecanismo de protección que tenemos contra los ataques de suplantación de identidad y todo tipo de estafasy fraudes que estén relacionados con el acceso a la información que se almacena en una cuenta de cualquier servicio, ya que evitan que terceros puedanacceder a toda esta información. De ahí su importancia en tener una contraseña robusta, es decir difícil de averiguar pero que demos recordado.

¿QUÉ TIPO DE CONTRASEÑAS DEBO EVITAR?

#5

Para que sea realmente segura, los ciberdelincuentes tienen diferentes medios para adivinar o tener acceso a nuestras contraseñas “habituales”. Aquí que debemos evitar:

- Fechas de Cumpleaños (el nuestro o de cualquiera de nuestros parientes)
- Números de teléfono
- Información de la empresa (por ejemplo su NIF)
- Nombres, incluyendo películas y equipos deportivos

www.canalsenior.es

GOBIERNO DE ESPAÑA
MINISTERIO DE DERECHOS SOCIALES Y AGENDA 2030
POR SOLIDARIDAD
OTROS FINES DE INTERÉS SOCIAL