La clave está en las claves

Todos los sistemas tienen la particularidad de estar protegidos por una contraseña de acceso. Por eso, para tener una organización digital segura y protegida tenemos que contar con una clave sólida y eficiente. Así, evitaremos sufrir incidentes con nuestras cuentas online.

1. No usar la misma clave para todo
Para cada usuario que tenemos (de correo electrónico, red social, wifi, etc.) deberíamos contar con una contraseña distinta. Los ciberdelincuentes suelen robar contraseñas de sitios web que cuentan con poca seguridad, y luego intentan replicar las mismas en otros sitios. Por eso: usar distintas claves en diversos sitios de Internet.

2. Claves largas, complejas y si no tienen sentido, mejor
Las mejores contraseñas, es decir las más difíciles de adivinar y por ende de ser sustraídas, son las largas, que contienen letras, números, signos de puntuación y símbolos. Hay palabras o frases inventadas por el usuario que pueden ser fáciles de recordar para él mismo e imposibles de descifrar para quien lo intente. Ej: "Tengo1clave+segura."

3. ¡No compartirlas con nadie!
Las claves son personales y no deben ser compartidas con nadie. El usuario es el dueño de la cuenta, pero también es el dueño de la clave. La misma no debe ser conocida más que por su dueño.

4. Contraseñas fáciles, pero difíciles de olvidar y de adivinar.
Para muchos, las contraseñas complejas son un riesgo por la posibilidad de olvidarlas. Un truco es usar una palabra o frase fácil, pero cambiando las vocales por números. Por ejemplo: 'Tengoalgoparadecirte' sería "T3ng0alg0parad3c1rt3".

La clave está en las claves

5. Integrar símbolos en tus claves
También se puede tener una clave fácil de recordar y difícil de adivinar utilizando símbolos. Por ejemplo: 'vaca123' (clave fácil de adivinar) quedaría convertida en "vaca!"#".

6. Usar mayúsculas
Utilizando la opción de las mayúsculas se agrega una dificultad más a quien quiera adivinar nuestra clave. La misma puede ir al inicio o en cualquier parte de la clave. Ejemplo: "Elecciones2012" o "eleCciones2012".

7. Evitar información personal
No incluir en la contraseña Nombre, Apellido, fecha de nacimiento, número de documento, o información del estilo, ya que son más fáciles de adivinar.

8. Procurar cambiar la clave luego de un período de tiempo prudencial
Si usamos equipos compartidos o redes públicas en sitios públicos será prudente cambiar las claves de acceso que utilizamos en dichos equipos y redes luego de determinado tiempo.

9. Preguntas secretas
En el momento de la registración en un sitio web, uno de los requisitos que surgen al completar los datos es establecer una Pregunta Secreta por si alguna vez no recordamos la clave o contraseña de acceso. Por eso debemos elegir la que consideremos más complicada de adivinar, es decir evitando las de respuestas obvias. Ejemplo: Color favorito.

10. Guardar las claves en un documento de texto
Al elegir contraseñas largas, difíciles de memorizar, y tener varias (para los distintos usuarios con los que contamos) puede ser útil tenerlas almacenadas en un documento dentro de nuestra PC. Esto puede ser pesado o incomodo, pero es muy seguro.