LITORALPRESS

Fecha: 20-07-2023
Medio: El Mercurio
Supl. : El Mercurio - Cuerpo C
Tipo: Noticia general
Título: Siete claves para crear contraseñas seguras

Pág. : 9
Cm2: 266,2
VPE: $ 3.496.257

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

Protege tu información personal:

Siete claves para crear contraseñas seguras

Es un aspecto que, a juicio de los expertos, los usuarios nunca deben descuidar pues las *password* son el punto de acceso a todos nuestros datos.

En el mundo digital en que vivimos, cada vez estamos más interconectados con la tecnología para realizar un sinnúmero de actividades cotidianas. Por eso, es muy relevante ser precavidos y tomar los resguardos necesarios para protegerse de cualquier intromisión cibernética que ponga en riesgo información personal y financiera.

Erick Cisternas, jefe de Servicios Tecnológicos de UDLA, sede Viña del Mar, comenta que establecer contraseñas seguras es uno de los aspectos que nunca deben descuidar los usuarios, pues estas claves son el punto de acceso a todos los datos que se manejan en línea para actividades como trabajar, estudiar, consultas médica, compras y transacciones, entre otras.

"Una contraseña es una forma de autentificación que usa información secreta para controlar el acceso a algún recurso digital, entre ellos, distintos dispositivos, cuentas de correo, recursos y documentos de nuestra empresa y aplicaciones bancarias. Que sea segura y robusta es la primera línea de defensa para mantener la información personal, sistemas y dispositivos digitales a salvo", explica.

El profesional advierte que al usar contraseñas inseguras nos volvemos vulnerables y los cibercriminales pueden usar diversos programas para intentar descubrirlas. "Cuanto más sencilla sea una clave, más rápidamente podrá ser descifrada por personas malintencionadas, teniendo la posibilidad de acceder a nuestros datos confidenciales", dijo.

Cómo crear una contraseña segura:

1. **Debe ser impersonal:** no hacer referencia a una persona ni nada familiar. Evite utilizar fechas de cumpleaños, direcciones, nombres o palabras comunes.

2. **Larga:** mientras más caracteres tenga más difícil es que sea descifrada en un corto tiempo.

3. **Compleja:** incluir símbolos, mayúsculas, minúsculas y números. (Ejemplo; G1r4$0l.90#Yell0w&),

4. **Secreta:** no ser compartida con nadie, a excepción de una situación extrema. Evitar anotarlas en libretas o en notas en un teléfono móvil.

5. **Modificarla:** debe cambiarla en forma periódica.

6. **No la repita:** evite usar la misma contraseña para varios accesos. Ideal es crear una para cada aplicación o sistema.

7. **Ilógica:** entre más larga e ilógica sea la contraseña, más segura será.

Tácticas

Cisternas agrega que para asegurar una mayor solidez de las herramientas de seguridad lo mejor es utilizar múltiples tácticas. Dos de ellas son:

* **Activar la autentificación de dos pasos (2FA):** es el método que ofrece mayor protección, dado que posibilita comprobar la identidad con más de una forma. Además de la contraseña, permite verificar la identidad agregando un segundo factor de autenticación, aparte del *password*, como el número de PIN, un patrón, identificación biométrica, huella de voz o digital.

* **Autenticación multifactorial (MFA):** confirmar la identidad del usuario utilizando *tokens* físicos o aplicaciones móviles. Garantiza que, incluso si una contraseña se ve comprometida, los ciberdelincuentes no puedan acceder a la información personal.