PHISHX

CÓMO MANTENER SEGUROS TUS ACCESOS

Las buenas contraseñas son el comienzo

Gran parte de nuestra seguridad comienza cuando creamos y mantenemos contraseñas seguras:

• Una contraseña segura debe estar más cerca de una frase que de una palabra, y su longitud debe ser lo más larga posible.

• Una contraseña segura debe ser una combinación de caracteres, letras mayúsculas, letras minúsculas y números.

• Primero, escriba una contraseña aleatoria y luego, letra por letra, siga cambiando el tipo de cada carácter.

• Las contraseñas son individuales, temporales y únicas, no las repitas ni las compartas con nadie.

• Para mantener su identidad en línea segura y protegida, debe continuar cambiando sus contraseñas a intervalos regulares.

Evita en tu contraseña

Para tener una contraseña segura, evite las contraseñas con:

• Palabras comunes: cualquier palabra o combinación que se puede encontrar en un diccionario.

• Pequeñas variaciones: tenga cuidado al usar variaciones muy leves de palabras o nombres comunes.

• Contexto: no use contraseñas que reflejen algo sobre usted, como los nombres de personas o lugares que conoce.

• Secuencia del teclado: olvídate de usar una secuencia basada en letras adyacentes al teclado.

• Contraseña similar o la misma: no guarde la misma contraseña para todas sus cuentas.

Actualice su perfil

Siempre verifique que su información de contacto esté actualizada, para que todos los proveedores de servicios puedan contactarlo, a través de notificaciones o procesos de reactivación, con usted de manera rápida, segura y eficiente.

Es esencial que verifique su información de contacto periódicamente y la mantenga actualizada si realiza cambios en su dirección, teléfono o correo electrónico. Cuando reciba una notificación de nuevo acceso que no haya hecho, vaya al portal de su proveedor para comprender qué sucedió y, si es necesario, actualice su contraseña y otras configuraciones.

CÓMO MANTENER SEGUROS TUS ACCESOS

Administra tus contraseñas

Así como dependemos de nuestro calendario para recordar cumpleaños y contactos, use un administrador de contraseñas en sus dispositivos para mantener sus contraseñas complejas aún más seguras.

Además de almacenar sus contraseñas, estas aplicaciones pueden ayudarlo a crear contraseñas aleatorias seguras de acuerdo con los consejos y estándares de seguridad, así como también recordarle que las actualice con frecuencia.

Otro punto adicional es tener firmas para identificar si se ha descubierto una cuenta personal o contraseña, o si hubo problemas con algún servicio que utilice, indicando que debe cambiar sus contraseñas y accesos.

No te quedes conectado

Tan importante como acceder de forma segura, también está finalizando su acceso cuando ya no lo está utilizando, saliendo de la aplicación o el sistema.

Cuando use un dispositivo compartido, recuerde cerrar sesión en sus cuentas y evite marcar la casilla "Mantenerme conectado" cuando inicie sesión.

Si está lejos de su dispositivo, pero regresa, bloquee la pantalla para que nadie pueda acceder a los datos sin realizar una autenticación segura.

Factores múltiples

La autenticación debe ser multifactorial, por ejemplo, cuando usamos dos factores (2FA) o más (MFA, para aumentar la seguridad de nuestros accesos).

Debe habilitar la autenticación multifactorial para todas las aplicaciones, servicios y sistemas que utiliza en su vida laboral y personal.

Los factores pueden incluir lo siguiente:

- Información que solo usted conoce: su contraseña única y segura.
- Algo que posee: una aplicación de generador de código en su teléfono.
- Algo que eres: tu cara o huella digital.
- Dónde se encuentra: su ubicación a través de un GPS o su punto de acceso a la red.

phishx.io