LA ESCALERA DE PROTECCIÓN: DE LA CONTRASEÑA A LAS PASSKEYS

Cada nivel que subís reduce drásticamente la probabilidad de que te roben una cuenta. Identificá en qué escalón estás hoy.

>> SUBÍ DE NIVEL

NIVEL 0 — ZONA DE RIESGO

Contraseña débil o reutilizada

Formada por datos personales, fácil de adivinar, o la misma en varios servicios: si comprometen una, caen todas.

NIVEL 1

Contraseña fuerte

Mayúsculas, minúsculas, números y caracteres especiales. Usá una regla mnemotécnica: por ejemplo, las primeras letras de una frase.

NIVEL 2

Única por servicio + gestor de contraseñas

Una contraseña distinta en cada sistema. Con muchas cuentas, un gestor de contraseñas las recuerda por vos.

NIVEL 3

Autenticación multifactor (MFA)

Un segundo factor además de la contraseña: aunque la roben, no alcanza para entrar.

NIVEL 4 — OBJETIVO

Passkeys

Acceso sin contraseña, ligado a tu dispositivo: no hay nada que robar ni que adivinar mediante phishing.

>> REGLAS QUE APLICAN EN TODOS LOS NIVELES

→ No compartas tus contraseñas

Si por urgencia tuviste que darla, cambiala inmediatamente después.

→ Preguntas de seguridad difíciles

Si cualquiera puede responderlas con datos públicos tuyos, son una puerta de entrada.

→ No las anotes en papeles ni archivos

Ni libretas, ni notas del celular. Si no queda otra, guardá el papel en un lugar muy seguro.

→ Cambio urgente ante actividad extraña

Si detectás movimientos raros en una cuenta, cambiá la contraseña de inmediato. Y renovalas de tanto en tanto sin esperar a que el sistema te obligue.

ATENCIÓN

Cuidá que nadie te observe al escribir tu contraseña: las miradas también roban claves.