A ESCADA DE PROTEÇÃO: DA SENHA ÀS PASSKEYS

Cada nível que você sobe reduz drasticamente a chance de roubarem uma conta sua. Identifique em qual degrau você está hoje.

>> SUBA DE NÍVEL

NÍVEL 0 — ZONA DE RISCO

Senha fraca ou reutilizada

Formada por dados pessoais, fácil de adivinhar, ou a mesma em vários serviços: se uma for comprometida, caem todas.

NÍVEL 1

Senha forte

Maiúsculas, minúsculas, números e caracteres especiais. Use uma regra mnemônica: por exemplo, as primeiras letras de uma frase.

NÍVEL 2

Única por serviço + gerenciador de senhas

Uma senha diferente em cada sistema. Com muitas contas, um gerenciador de senhas lembra delas por você.

NÍVEL 3

Autenticação multifator (MFA)

Um segundo fator além da senha: mesmo que a roubem, não basta para entrar.

NÍVEL 4 — OBJETIVO

Passkeys

Acesso sem senha, vinculado ao seu dispositivo: não há nada para roubar nem para adivinhar por phishing.

>> REGRAS QUE VALEM EM TODOS OS NÍVEIS

→ Não compartilhe suas senhas

Se por urgência você precisou compartilhar uma, troque-a imediatamente depois.

→ Perguntas de segurança difíceis

Se qualquer um pode respondê-las com dados públicos sobre você, elas são uma porta de entrada.

→ Não anote senhas em papéis nem arquivos

Nem cadernos, nem notas do celular. Se não houver outro jeito, guarde o papel em um lugar muito seguro.

→ Troca urgente diante de atividade estranha

Se notar movimentações estranhas em uma conta, troque a senha imediatamente. E renove suas senhas de tempos em tempos, sem esperar o sistema obrigar.

ATENÇÃO

Cuide para que ninguém observe você digitando sua senha: os olhares também roubam senhas.