

10 pasos para proteger tu negocio

25 min

SIN SABER DE TECNOLOGÍA

La mayoría de ataques a negocios pequeños no son de película: son contraseñas robadas, cuentas sin protección y estafas por WhatsApp o correo. Estas 10 acciones cierran las puertas más usadas y en total toman unos 25 minutos. Imprime la hoja y ve marcando.

- ☐

01 Activa la verificación en dos pasos en tu correo
2 min

Así, aunque alguien robe tu contraseña, no puede entrar sin tu celular.
Cómo: Gmail » Gestionar tu cuenta de Google » Seguridad » Verificación en dos pasos. En Outlook: cuenta de Microsoft » Seguridad.
- ☐

02 Ponle PIN a tu WhatsApp Business
1 min

Evita que te roben el WhatsApp con el truco de "te llegó un código por error, pásamelo".
Cómo: WhatsApp » Ajustes » Cuenta » Verificación en dos pasos » Activar. Nunca le compartas a nadie el código de 6 dígitos.
- ☐

03 Usa una contraseña distinta para el correo y el banco
3 min

Si una página donde te registraste se filtra, la misma clave abre todo lo demás.
Cómo: cambia primero la del correo y la del banco. Para recordarlas, usa un gestor gratuito como Bitwarden en vez de una libreta o un archivo.
- ☐

04 Revisa si tu correo aparece en filtraciones
1 min

Te dice si tu contraseña ya anda circulando por internet.
Cómo: entra a haveibeenpwned.com y escribe tu correo. Si aparece, cambia esa contraseña en todos los sitios donde la usabas.
- ☐

05 Acuerda una regla para cambios de cuenta bancaria
1 min

La estafa más común: un "proveedor" escribe que cambió de cuenta y pide pagar a otra.
Cómo: regla fija en tu negocio: todo cambio de cuenta se confirma **llamando** a un número que ya tenías, nunca al que viene en el mensaje.
- ☐

06 Saca a quien ya no trabaja contigo
3 min

Exempleados con acceso al correo, las redes o la página web son una puerta abierta.
Cómo: revisa los administradores de tus redes sociales, tu página web y las cuentas compartidas. Cambia las claves que conocían.
- ☐

07 Confirma los datos de recuperación de tus cuentas
2 min

Si pierdes el acceso, el correo y el teléfono de recuperación son tu única salida.
Cómo: en el correo y en cada red del negocio, verifica que el teléfono y el correo de recuperación sean tuyos y estén vigentes.
- ☐

08 Activa las actualizaciones automáticas
2 min

La mayoría de las actualizaciones corrigen fallas que los atacantes ya conocen.
Cómo: en el celular y el computador del negocio, activa las actualizaciones automáticas del sistema y de las aplicaciones.
- ☐

09 Ten una copia de lo que no puedes perder
5 min

Facturas, base de clientes, contabilidad: si se dañan o los secuestran, la copia te salva.
Cómo: súbelos a Google Drive u OneDrive, y una vez al mes guarda otra copia en un disco que desconectes después.
- ☐

10 Separa el Wi-Fi de tus clientes
5 min

Quien se conecta a tu red puede ver los equipos del negocio.
Cómo: cambia la clave que trae el router de fábrica y crea una red de invitados para los clientes (suele estar en la configuración del router).

¿Pueden hacerse pasar por tu empresa por correo?

Esa no la puedes revisar tú solo. Te hacemos un diagnóstico gratis de tu web y tu correo, con datos y en lenguaje claro.

almenaciber.com
contacto@almenaciber.com