



GUIA RÁPIDO • EDIÇÃO 2026

Uma senha esquecida. Uma conta perdida. Meses de trabalho apagados.

Sete hábitos simples para proteger Instagram, Facebook, WhatsApp Business, e-mail e os acessos digitais da sua empresa.

Material educativo para pequenos e médios negócios brasileiros no Japão.

Prático, direto e sem exigir conhecimento técnico.

Seu negócio depende de algo que raramente aparece no orçamento: o acesso.

Quando uma conta é invadida, suspensa ou fica presa ao celular de alguém, os clientes deixam de encontrar a empresa, os pedidos param e anos de histórico podem desaparecer. Muitos incidentes começam em falhas simples de corrigir.

1

Separe o pessoal do profissional

Contas empresariais vinculadas ao e-mail ou celular pessoal criam dependência.

- Crie um e-mail exclusivo para o negócio e use-o como proprietário.
 - Troque dados de recuperação que ainda pertençam a ex-funcionários ou prestadores.
-

2

Separe recuperação e atendimento

O número público do WhatsApp Business não deve recuperar todas as contas.

- Use um número separado e não divulgado para recuperação.
 - Registre e guarde e-mail e telefone de recuperação fora do celular de uso diário.
-

3

Ative a verificação em duas etapas

É uma das barreiras mais simples e eficazes contra invasões.

- Ative 2FA nas redes sociais, WhatsApp Business e e-mail.
- Prefira aplicativo autenticador a SMS e guarde os códigos de recuperação.

Quem precisa trabalhar não precisa, necessariamente, controlar tudo.

4

Não compartilhe senhas por mensagem ou papel

Quando uma senha circula, ela deixa de ser secreta e fica difícil saber quem ainda possui acesso.

- Use um gerenciador como Bitwarden ou 1Password.
- Revogue o acesso no mesmo dia em que alguém sair da empresa.

5

Dê o papel certo para cada pessoa

Nem todo mundo que publica conteúdo precisa trocar proprietários ou excluir páginas.

- Reserve o papel de administrador ao dono ou responsável principal.
- Use funções limitadas para equipe e fornecedores.
- Revise os acessos ao menos a cada três meses.

6

Desconfie de “verificação”, “selo azul” e urgência

Golpes usam medo e pressa para fazer o empresário entregar credenciais.

- Nunca informe senha ou código recebido por SMS.
- Não use links enviados por mensagem para “evitar suspensão”; abra o aplicativo oficial.

7

Tenha um plano B antes de precisar

No momento de uma invasão, um registro simples reduz o tempo de recuperação.

- Anote proprietários, recuperação e data aproximada de criação das contas.
- Mantenha cópia de documentos e saiba onde ficam os canais oficiais.

Pequenas mudanças reduzem muito o risco.

Situação frágil	Prática mais segura
Senha simples e repetida	Senha longa e única em gerenciador
2FA por SMS no número público	Aplicativo autenticador + códigos de backup
Senha enviada no grupo	Acesso compartilhado sem revelar a senha
Todos são administradores	Dono administrador; equipe com acesso limitado
Recuperação só no celular da empresa	Registro offline com e-mail, número e códigos

Você recuperaria sua empresa amanhã?

☐ Tenho acesso ao e-mail principal da empresa.

☐ Tenho os códigos de recuperação.

☐ Sei quem são todos os administradores.

☐ Domínio e hospedagem estão em nome da empresa.

☐ Tenho backup de dados críticos.

☐ Consigo revogar rapidamente o acesso de alguém.

Marcou “não” ou ficou em dúvida em três ou mais itens? Há pontos importantes que podem ser corrigidos antes de virar emergência.

Some os pontos e identifique por onde começar.

01 As contas possuem 2FA por aplicativo?

Sim (0) · Parcialmente (1) · Não (2)

02 As senhas são únicas e ficam em gerenciador?

Sim (0) · Algumas (1) · Não (2)

03 Existe uma lista atualizada de administradores?

Sim (0) · Não tenho certeza (1) · Não (2)

04 A recuperação é separada do atendimento público?

Sim (0) · Parcialmente (1) · Não (2)

05 Há backup dos documentos e dados importantes?

Sim e testado (0) · Existe, mas não testei (1) · Não (2)

06 A empresa sabe como agir se perder uma conta?

Sim (0) · Mais ou menos (1) · Não (2)

0–3

Boa base. Revise acessos e teste a recuperação.

4–7

Atenção. Corrija as vulnerabilidades nas próximas semanas.

8–12

Risco alto. Priorize 2FA, acessos, recuperação e backup.

Quer ajuda prática?

A Nihon IT pode apoiar 2FA, senhas, acessos, backups e proteção básica do site e e-mail — em português, inglês ou japonês.

contact@nihon-it.tech

+81 50-6867-0130

nihon-it.tech

Este material é educativo e não substitui auditoria técnica. Nunca compartilhe senhas ou códigos de verificação.