O comércio local precisa acordar para a segurança virtual e mostramos por onde começar sem gastar nada

Category: GERAL
escrito por Adecio Piran | 30 de abril de 2026

Foto:Reprodução/Internet- Cada vez mais lojas de bairro aceitam pagamentos pelo Bizum, gerenciam pedidos pelo WhatsApp e publicam suas novidades no Instagram. A digitalização chegou ao quiosque de ferragens da esquina, à oficina mecânica e ao salão de cabeleireiro. E, com ela, também surgiram os riscos. Pois quanto mais digital é um negócio, mais portas ele deixa abertas para quem quiser entrar sem permissão. A boa notícia é que, para se proteger, basta estar atento.

Por que as pequenas empresas são as mais visadas pelos golpistas

Os cibercriminosos preferem as pequenas empresas às grandes corporações porque são mais fáceis de atacar. Não porque seus dados valham menos, mas porque raramente possuem barreiras de proteção. E isso as torna o alvo preferido de fraudes que, em muitos casos, são lançadas de forma automática e em massa.

O email corporativo é um dos pontos de entrada mais comuns. Por meio de mensagens que se fazem passar por fornecedores, bancos ou até mesmo órgãos públicos, os golpistas conseguem que alguém da equipe forneça senhas ou dados bancários sem perceber. Esse tipo de ataque, conhecido como phishing, cresceu mais de 200% nos últimos anos. E a maioria das vítimas simplesmente não sabia que precisava estar alerta.

A isso se soma o fato de que, à medida que mais empresas locais ampliam sua presença no ambiente digital, a exposição a esse tipo de ameaça também cresce. Uma pesquisa da Opinion Box revelou que 22% das micro e pequenas empresas brasileiras não aplicam nenhuma medida de segurança interna. Nenhuma. O que significa que, para um invasor, entrar é quase tão simples quanto abrir uma porta sem fechadura.

O Sebrae resume bem isso em seu guia de segurança cibernética para pequenas empresas, no qual explica que muitos empresários nem sabem o que fazer quando são vítimas de um ataque. E esse desconhecimento é, por si só, uma vulnerabilidade.

Como começar a se proteger sem gastar nada

Sabendo agora por que as pequenas empresas estão na mira, a pergunta que se segue é: por onde começar?

Comece pelas senhas. Não por instalar nenhum software, nem por contratar nenhum serviço: pelas senhas. Usar a mesma senha para o e-mail, o sistema de caixa e o perfil do Instagram é como usar a mesma chave para a casa, o carro e o cofre. Se alguém a conseguir, tem tudo. Trocar as combinações por outras mais longas e diferentes para cada plataforma é gratuito e leva menos de dez minutos.

O próximo passo é ativar a verificação em duas etapas em todas as contas que permitam isso. Essa função, oferecida

gratuitamente pelo WhatsApp Business, Google, Instagram e pela maioria das plataformas pagas, adiciona uma camada de proteção em que, mesmo que alguém descubra a senha, não poderá acessar sem o código enviado para o celular do titular.

E depois há o fator humano, que costuma ser o mais esquecido. Um funcionário que abre um link suspeito pode comprometer em segundos tudo o que a empresa possui no ambiente digital. Por isso, vale a pena dedicar uma conversa para explicar à equipe como reconhecer uma mensagem falsa, por que não se deve usar redes Wi-Fi públicas para acessar os sistemas da empresa e o que fazer se algo parecer incomum. Não é preciso ser especialista em tecnologia para ter bom senso digital. E esse bom senso é a melhor defesa que uma pequena empresa pode ter hoje.

Em suma, proteger um negócio local no ambiente digital requer senhas diferentes, verificação em duas etapas e uma equipe que saiba reconhecer uma armadilha quando a vê. Os ataques estão se tornando cada vez mais frequentes, mas também mais previsíveis. Quem se prepara com antecedência já está com grande vantagem.

> *Por que os criadores de conteúdo precisam humanizar o texto gerado por IA para manter o tráfego orgânico?*