CONTAB
JC CONTABILIDADE

Porto Alegre, quarta-feira, 29 de abril de 2026 | Ano 24 - nº 85 | Jornal do Comércio

BRUNO PERES/AGÊNCIA BRASIL/JC

Acesso a informações fiscais deve ser feito exclusivamente pelos canais oficiais, como o site da Receita Federal, o portal e-CAC ou o aplicativo Meu Imposto de Renda

REPORTAGEM

Golpes no IR usam medo da malha fina para atrair vítimas

GABRIEL MARGONAR
gabrielm@jcrs.com.br

Em meio ao calendário do Imposto de Renda, cresce também um outro movimento, silencioso e cada vez mais sofisticado: o de golpes digitais que usam o nome da Receita Federal para enganar contribuintes. Mensagens por e-mail, SMS e aplicativos de conversa simulam comunicações oficiais, com alertas de pendências, dívidas ou risco de bloqueio do CPF. O objetivo é sempre o mesmo: induzir a vítima a clicar em links falsos, fornecer dados sensíveis ou até realizar pagamentos indevidos.

O fenômeno não é novo, mas se intensifica justamente neste período. A própria Receita Federal informou, no início deste mês, ter recebido relatos de mensagens fraudulentas com tom alarmante, indicando supostas irregularidades na declaração e ameaçando consequências como restrições bancárias, bloqueio de Pix ou inclusão em cadastros de inadimplência. O órgão reforça que não envia links para regularização nem solicita dados pessoais por mensagens.

Para a diretora de Ensino e Educação do Sescon-RS, Caroline Oliveira, o principal equívoco dos contribuintes é acreditar que esse tipo de comunicação pode ser verdadeiro. "A Receita Federal nunca manda e-mail, nunca manda SMS. Mesmo assim, as pessoas recebem mensagens dizendo que a declaração caiu em malha fina e acabam clicando", afirma.

Segundo ela, os golpes mais comuns exploram exatamente esse momento de insegurança. "Vêm mensagens dizendo 'sua declaração está em malha, clique aqui', ou 'você ainda não entregou o Imposto de Renda'. O contribuinte, com pressa para resolver, acaba confiando no link", explica.

A orientação, reforça, é nunca informar dados fora dos canais oficiais. "A senha do Gov.br é de uso pessoal. Jamais deve ser informada a partir de um link recebido".

O comportamento das vítimas, muitas vezes, é influenciado pela urgência. "A pressa faz com que a pessoa nem entre no site da Receita para conferir. Ela acredita no e-mail e acaba caindo no golpe", diz Caroline. Segundo ela, no dia a dia dos escritórios contábeis, é comum que clientes encaminhem essas mensagens para validação. "A gente sempre orienta: não clique, não abra, porque pode ser vírus."

No ambiente empresarial, os golpes assumem outras formas. A vice-presidente técnica do Conselho Regional de Contabilidade do Rio Grande do Sul (CRCRS), Eliane Soares, relata aumento de fraudes envolvendo boletos falsos, especialmente de guias do Simples Nacional e Documento de Arrecadação de Receitas Federais (Darfs). "Os clientes recebem por e-mail documentos que parecem oficiais, muitas vezes até com o nome do escritório de Contabilidade. Só depois percebem que o pagamento iria para outra empresa", afirma.

Conforme ela, há casos em que os documentos apresentam o nome da Receita Federal, mas trazem CNPJs de terceiros. "Quando vamos verificar, às vezes está em nome de empresas completamente diferentes. Isso dificulta para o empresário identificar o golpe", diz. Outro tipo recorrente envolve mensagens por SMS ou WhatsApp alertando sobre dívidas inexistentes. "Principalmente para MEIs, dizendo que vão ser excluídos ou desenquadrados", alerta Eliane.

Apesar do avanço da reforma tributária no debate público, ainda não há registro significativo de golpes diretamente associados ao tema. Tanto Caroline quanto Eliane afirmam não ter identificado fraudes recorrentes usando a reforma como isca. Ainda assim, especialistas alertam que temas complexos e em evidência podem ser facilmente incorporados por criminosos.

O professor Jeferson Campos Nobre, do Instituto de Informática da Universidade Federal do Rio Grande do Sul (Ufrgs), explica que esse tipo de golpe se baseia em engenharia social - estratégia que explora aspectos psicológicos das vítimas. "Períodos como o do Imposto de Renda concentram golpes porque as pessoas estão mais suscetíveis. Elas já estão preocupadas com prazos, documentos e possíveis pendências", afirma.

Segundo ele, os criminosos utilizam tanto a promessa de ganho quanto o medo de punição. "Pode ser uma mensagem oferecendo antecipação de restituição ou alertando sobre malha fina. Em ambos os casos, há um estímulo emocional que leva a uma decisão mais impulsiva", explica.

A linguagem também é parte da estratégia. "Eles usam termos técnicos, falam de legislação, de faixa de isenção, até de mudanças como a reforma tributária, para dar mais credibilidade. Isso sobrecarrega cognitivamente o usuário e aumenta a chance de ele acreditar", acrescenta.

Outro elemento comum é o senso de urgência. Mensagens que exigem ação imediata - "regularize agora", "evite bloqueio", "responda em até 24 horas" - reduzem o tempo de reflexão e favorecem o erro. "A pessoa já está sobrecarregada de informações e acaba reagindo de forma automática", diz Nobre.

Diante desse cenário, a principal recomendação é simples: desconfiar. Qualquer mensagem que peça dados pessoais, ofereça facilidades ou ameace penalidades deve ser tratada com cautela. O acesso a informações fiscais deve ser feito exclusivamente pelos canais oficiais, como o site da Receita Federal, o portal e-CAC ou o aplicativo Meu Imposto de Renda.

Caroline reforça que, mesmo com a existência de um campo de e-mail na declaração, a Receita não utiliza esse meio para notificação de malha fina. "Se houver problema, o contribuinte deve consultar diretamente o sistema ou receber uma correspondência em casa. Nunca por link enviado", orienta.

LEIA MAIS NA PÁGINA 3