

Motoristas têm sido alvo de um novo golpe que explora o sistema de pedágio eletrônico sem cancela, conhecido como “free flow”. Criminosos criaram dezenas de sites falsos que simulam a consulta e o pagamento de débitos de pedágio e desviam o dinheiro das vítimas por meio de transferências via Pix.

O esquema foi identificado pela empresa de segurança digital Kaspersky, que mapeou mais de 50 domínios fraudulentos registrados desde meados de dezembro de 2025. As páginas falsas imitam plataformas legítimas de pagamento e usam dados reais dos veículos para dar aparência de autenticidade à fraude.

Segundo a empresa, o golpe começa quando o motorista busca na internet por serviços de consulta ou quitação de pedágios. Os criminosos usam anúncios patrocinados em buscadores e redes sociais para posicionar os sites falsos entre os primeiros resultados, levando a vítima a clicar em links aparentemente confiáveis.

Ao acessar a página fraudulenta, o usuário informa a placa do veículo e visualiza um suposto débito em aberto. O valor costuma ser baixo, semelhante ao custo real de um pedágio, e o site exibe informações corretas do automóvel, como modelo e ano, o que reforça a sensação de legitimidade.

Convencido de que se trata de um serviço oficial, o motorista realiza o pagamento, geralmente por Pix. O dinheiro, no entanto, é enviado para contas de “laranjas”, abertas em fintechs pouco conhecidas, com o nome do recebedor mudando com frequência para dificultar o rastreamento e o bloqueio dos valores.

Segundo ele, o uso de contas de laranjas indica um esquema organizado e voltado a dificultar a ação policial. “É crucial que os motoristas fiquem atentos, pois com a popularização do free flow, mais golpes podem aparecer, como aplicativos móveis falsos para pagamentos”, diz.

Especialistas alertam que esse tipo de fraude tende a se intensificar sempre que novos serviços passam a ser adotados em larga escala. “Criminosos aproveitam o momento para aplicar diversos tipos de golpes. Como boa parte da população não possui informações concretas sobre tal serviço, os criminosos criam mídias falsas para enganar as vítimas em potencial”, afirma Daniel Barbosa, especialista em cibersegurança da Eset Brasil.

Como se proteger

Mesmo sem conhecer todos os detalhes sobre novos servi-



Motoristas são alvo de golpistas na hora de pagar o pedágio automático implantado em rodovias do país

Golpe do pedágio ‘free flow’ usa sites falsos

Criminosos simulam consulta e o pagamento e desviam o dinheiro

Divulgação/ANTT



Golpe do pedágio ‘free flow’ usa sites falsos para roubar motoristas

ços, Barbosa diz que é possível adotar cuidados básicos para reduzir o risco de cair em golpes.

“Preste atenção ao endereço dos sites, que sempre será diferente da página oficial. Para evitar ser vítima, pesquise em sites de busca pela página oficial do serviço ou empresa que você está tentando acessar”, recomenda o especialista.

Também é importante desconfiar de anúncios patrocinados. “Sabemos que boa parte das comunicações que partem dos criminosos acontecem por email ou por mensagens em aplicativos, mas está cada vez mais frequente a contratação de propagandas em sites legítimos e redes sociais, aumentando bastante a credibilidade da abordagem”, afirma Barbosa.

Além disso, pagamentos de pedágio devem ser feitos apenas para concessionárias oficiais. Se o Pix estiver em nome de pessoas físicas ou empresas desconhecidas, é sinal de alerta. “Quanto mais chamar sua atenção, maior a chance do conteúdo não ser legítimo.”

Fazer o download de arquivo ou acessar sites falsos são ainda riscos para infectar dispositivos com vírus. “Para evitar que isso aconteça, tenha um software de proteção ou antivírus instalado. Ele ajudará a impedir que atividades maliciosas ocorram sem que você se dê conta”, diz o especialista.

A orientação geral é acessar sempre os sites oficiais das concessionárias responsáveis pelo trecho do pedágio, digitando o endereço diretamente no navegador, e evitar pagamentos feitos a partir de links recebidos por anúncios ou mensagens.

Por Gabriella Cecchin -
Folhapress