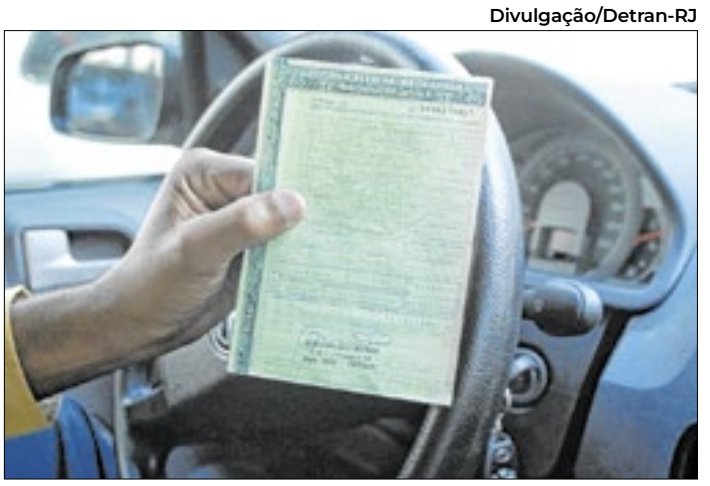
CORREIO ECONÔMICO

POR MARTHA IMENES

Divulgação/Detran-RJ



Quadrilhas usam sites falsos para emitir boletos do IPVA

Alerta: IPVA 2026 entra na lista dos golpes digitais

Estelionatários dão jeito para ganhar dinheiro fácil em cada mudança ou data importante. Foi assim no natal, no Dia da Mães, e agora com a virada do ano, chegou a vez do Imposto sobre a Propriedade de Veículos Automotores (IPVA) 2026, que começa o calendário de pagamentos em diversos estados brasileiros. A preocupação das autoridades e especialistas em segurança digital com a evolução das fraudes cibernéticas que visam proprietários de veículos em todo o país faz aumentar a preocupação de especialistas e até de entes federativos. Os golpes mais recentes exploram técnicas sofisticadas de engenharia social, mensagens com links maliciosos, domínios falsificados e promessas de descontos que não existem para atrair contribuintes e desviar recursos.

Tática criminosa adaptada

O diretor da Datalege Consultoria Empresarial Mario Toews, especialista em Direito Digital e Segurança da Informação, explica que os cibercriminosos estão adaptando suas táticas para o contexto do IPVA 2026, combinando engenharia social com métodos técnicos que auxiliam na captura de dados pessoais e na indução ao pagamento fraudulento. "Esses golpes estão evoluindo muito rapidamente e exigem atenção das pessoas para não se tornarem vítimas", afirma.

Divulgação/ Banco Central

Pix tem ferramenta para devolução do dinheiro

Atenção às mensagens falsas

Entre as técnicas que se destacam, Toews fala que é possível identificar métodos para aplicar fraudes relacionadas ao IPVA. Entre elas estão o envio de mensagens de texto (SMS) que contêm links para sites fraudulentos que imitam portais oficiais ou prometem ofertas de descontos, atraindo a vítima a clicar e inserir dados pessoais e financeiros em páginas maliciosas e criação de sites dublês com aparência quase idêntica às páginas oficiais de secretarias da fazenda, dos departamentos de trânsito (Detrans) ou portais de pagamento, com URLs e design que dificultam a identificação de fraude.

Cuidado com oferta de descontos

O proprietário deve ter atenção também ao envio de e-mails persuasivos que prometem descontos significativos no valor do IPVA, muitas vezes com valores retirados de fontes legítimas para dar maior sensação de autenticidade. Ao clicar em links desses e-mails, a vítima é levada a sites falsos que coletam dados sensíveis ou capturam pagamentos via Pix com QR code gerado para contas de criminosos.

Boleto falso

Os golpistas utilizam ainda o envio de boletos falsos por e-mail ou por meios que sugerem origens oficiais, mas que direcionam o pagamento para destinatários ilícitos. O especialista alerta que um dos elementos mais explorados nessas fraudes é a promessa de descontos elevados ou condições que não existem.

Dados pessoais

Segundo Toews, essas técnicas representam um risco tanto financeiro quanto de exposição de dados pessoais, já que muitos golpes solicitam informações como CPF, placa do veículo e Renavam antes de induzir à geração de boletos ou QR codes para pagamento via Pix. Uma vez realizada a transferência o prejuízo já está feito.

Em alta

Relatórios recentes sobre fraudes digitais no Brasil apontam que o país enfrenta um elevado índice de crimes virtuais, inclusive de phishing e golpes financeiros, que tendem a aumentar em datas de alta movimentação financeira como o período de pagamento de tributos.

Orientações I

* Acesse exclusivamente os canais oficiais das secretarias da Fazenda dos estados ou dos Detrans para emitir guias de pagamento e gerar QR codes para pagamento.
* Não clique em links recebidos por SMS, e-mail ou redes sociais que prometam descontos ou ofertas aparentes relacionadas ao IPVA, sem antes verificar a origem.

Orientações II

* Verifique atentamente a URL do site antes de inserir qualquer informação pessoal, observando a presença de certificados de segurança (cadeado e "https://") e a terminação institucional dos domínios.
* Desconfie de descontos que fogem dos parâmetros oficiais estabelecidos por cada estado, como promoções.

Orientações III

* Mantenha sistemas de segurança (antivírus e anti-malware) atualizados em dispositivos pessoais para ajudar a identificar links maliciosos e possíveis tentativas de phishing.
* Oriente familiares e colegas sobre as táticas de engenharia social mais comuns, fortalecendo a conscientização sobre fraudes digitais.

Marcello Casal Jr/Agência Brasil

Propostas sobre proteção de dados são debatidas no Congresso

Proteção e privacidade de dados ainda geram dúvida

Lei que visa proteger informações está em vigor há cinco anos

Da redação

Após cinco anos de vigência da Lei nº 13.709/2018, que define regras para coleta, tratamento, armazenamento e compartilhamento de informações pessoais por pessoas físicas ou jurídicas, temas relacionados à privacidade e à proteção de dados ainda são cercados por interpretações imprecisas. O debate inclui percepções que se consolidaram ao longo do tempo e que nem sempre refletem o que a legislação determina.

Fabiano Carvalho, especialista em Transformação Digital e CEO da Ikhon, aponta que o maior mito é a ideia de que a adequação à LGPD é um processo com início, meio e fim, no qual o ajuste de contratos e a inclusão de um banner de cookies finaliza todo o processo. "Na verdade, a proteção da privacidade dos usuários é um projeto que envolve monitoramento e melhoria contínua. Isso porque os dados fluem, os processos mudam e novas tecnologias (como a IA) surgem todos os dias", diz Carvalho.

Para o especialista, muitos equívocos surgem porque a regulação foi introduzida em um ambiente no qual questões de privacidade tinham pouca visibilidade. Ele explica que a interpretação mais comum está relacionada ao consentimento. Parte das organizações supõe que o usuário deve autorizar todas as operações de tratamento. A LGPD, porém, estabelece dez bases legais, das quais o consentimento é apenas uma. Cumprimento de contrato, obrigação legal e interesse legítimo são alternativas previstas e, em diversos contextos, mais adequadas do que solicitar autorização contínua.

Dados públicos podem ser usados livremente?

A LGPD é muito clara nesse ponto: o uso do dado deve respeitar a finalidade para a qual ele foi tornado público. Um exemplo: se um dado está no Diário Oficial para dar transparência a um ato público, você não pode raspar essa base para criar um perfil de crédito e vender para terceiros.

Proteção de dados pode travar a inovação?

Segundo ele, a governança de dados impõe uma etapa a mais no design de produtos, o que pode parecer uma lentidão inicial. Porém, no médio prazo, soluções que já nascem seguras sofrem menos interrupções legais, têm maior aceitação do público e evitam retrabalhos. O exemplo mais conhecido no setor de inovação nacional é o open finance. Todo o ecossistema de compartilhamento de dados bancários só existe porque há regras rígidas de padronização e segurança.

Outro exemplo prático ocorre dentro das empresas: quando se inicia o processo de adequação à LGPD, é preciso mapear os dados. Nesse processo, pode se descobrir o chamado "dark data" — informações valiosas que estavam perdidas em servidores esquecidos.