

Seu bolso Black Friday



COMO IDENTIFICAR SITES E ANÚNCIOS FALSOS DURANTE A LIQUIDAÇÃO

Especialista em tecnologia ensina como reconhecer páginas e promoções suspeitas para evitar golpes

Com a proximidade da Black Friday, cresce também a ação de golpistas que aproveitam a data para aplicar fraudes no comércio eletrônico. De acordo um levantamento da Visa, durante o fim de semana da liquidação de 2024 houve aumento em 270% no número de transações suspeitas de fraude bloqueadas no país.

Outro dado interessante é que, no primeiro semestre do ano passado, o ticket médio das fraudes foi 60% superior ao das vendas legítimas. Em 55% dos casos, as fraudes observadas partiram de dispositivos móveis. Os números acendem um alerta sobre os riscos de golpes online e reforçam a necessidade de adotar práticas de segurança digital.

Para Gilberto Reis, COO de uma empresa de Soluções Digitais especializada em consultoria de TI, os criminosos estão cada vez mais sofisticados no uso de tecnologias e inteligência artificial para enganar consumidores. “Hoje, o phishing

automatizado, os chatbots falsos e os anúncios fraudulentos em redes sociais estão entre as principais estratégias. O usuário precisa redobrar a atenção, especialmente diante de ofertas muito abaixo do preço de mercado”, alerta o especialista.

Além da Black Friday, Reis destaca também a época do Natal e do Ano-Novo, quando o volume de compras online costuma se manter elevado.

“É importante redobrar atenção em períodos em que a ação dos golpistas se intensifica, mas também é essencial adotar boas práticas de segurança ao longo do ano. Cuidados como usar senhas fortes e únicas, ativar autenticação em dois fatores e manter o sistema operacional e o antivírus sempre atualizados reduzem significativamente as chances de golpes”, orienta o especialista da Runtalent.

CONFIRA ALGUNS SINAIS DE ALERTA E COMO SE PROTEGER



URLS FALSAS OU PARECIDAS COM AS ORIGINAIS

Golpistas costumam criar endereços que lembram os de grandes varejistas, trocando ou adicionando letras. Antes de clicar, verifique cuidadosamente o domínio. Desconfie de sites com terminações incomuns (.net, .org) e de links compartilhados por mensagens ou redes sociais.



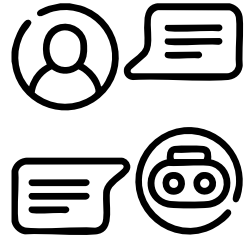
FALTA DO CADEADO DE SEGURANÇA E DO “HTTPS”

Sites legítimos usam criptografia para proteger as informações do usuário. Sempre confira se há o ícone do cadeado na barra de endereços e se o endereço começa com https:// – o “S” indica uma conexão segura.



PEDIDOS DE DADOS PESSOAIS OU BANCÁRIOS FORA DA PLATAFORMA

Empresas sérias não pedem informações sensíveis via formulário, mensagem ou chat externo. Evite preencher dados em links desconhecidos e confirme sempre se o ambiente de pagamento é seguro.



CHATBOTS FALSOS

Os consumidores podem ser enganados por chatbots falsos alimentados por inteligência artificial. Essas armadilhas costumam aparecer em sites clonados, pop-ups ou mensagens no WhatsApp, oferecendo descontos exclusivos que não existem. Por meio desses bots, os golpistas solicitam dados pessoais, número do cartão e código de segurança, simulando uma comunicação legítima.



AVALIAÇÕES E HISTÓRICO DE VENDEDORES

Antes de efetuar uma compra, o ideal é verificar o histórico e as avaliações do vendedor ou da loja. Perfis recentes, sem comentários ou com avaliações duplicadas podem indicar fraude. Plataformas consolidadas oferecem sistemas de reputação e canais seguros de comunicação, por isso é mais seguro realizar a transação dentro desses ambientes.

SKY-Consultoria em leilões

COMPRE SEU IMÓVEL
COM PREÇOS ATÉ 50%
ABAIXO DO VALOR
DE MERCADO

ASSESSORAMENTO E ANÁLISE
DE DÍVIDAS PARA GARANTIR
SUA SEGURANÇA

16 98177-8254

RUA EDUARDO PRADO, 720.
VILA TIBÉRIO - RIBEIRÃO PRETO