CARTILHA

ANTIGOLPE

Sindilojas RS

Porto Alegre

Sindicato do Sistema Comércio

CARTILHA ANTIGOLPE

Os meios de pagamentos digitais trouxeram uma enormidade de facilidades para os lojistas e para os consumidores que têm mais opções na hora de realizar uma compra – tanto no meio físico quanto no virtual. Porém, isso também é uma oportunidade para que golpistas se aproveitem de fragilidades e do desconhecimento para explorar essas fragilidades.

É por isso que o Sindilojas Porto Alegre, sempre atento e preocupado com a situação dos lojistas, preparou essa cartilha, que objetiva conscientizar e ensinar aos lojistas sobre os principais golpes que visam as transações financeiras digitais e a como evitá-las.

E lembre-se sempre, caso você acredite que foi vítima de um golpe, ligue imediatamente para o 190 e abra um Boletim de Ocorrência.

GOLPE DO CARTÃO POR APROXIMAÇÃO:

O golpe por cartão de aproximação é uma das armadilhas mais recentes. Nele, o consumidor precisa inserir o cartão na maquininha após um erro na aproximação, e, ao realizar o pagamento, as informações do cartão são roubadas e utilizadas em outros golpes.

COMO OCORRE O GOLPE:

1° PASSO: O lojista recebe uma ligação – ou ainda uma visita presencial - de um golpista se passando por funcionário de uma instituição financeira ou gerenciadora da maquininha. Nesse momento, o lojista é informado que precisa realizar uma manutenção nos equipamentos

2° PASSO: O lojista é orientado pelo golpista a baixar no computador um programa ou arquivo que lhe foi enviado. Esse programa ou arquivo quando baixado vai, automaticamente, instalar um vírus no computador. A partir desse momento, qualquer maquininha conectada ao computador por cabo será infectada pelo vírus.

3° PASSO: Quando um cliente tentar realizar o pagamento, uma mensagem informando erro na aproximação e solicitando a inserção do cartão será exibida na tela da maquininha. Ao digitar a senha, o vírus, que está no computador, irá ler todas as informações contidas no cartão. Assim, todos os dados são repassados para os golpistas

4° PASSO: Após o envio das informações aos golpistas, a maquinha volta a gerar uma mensagem de erro e solicita a realização de uma nova tentativa de pagamento. Essa última tentativa será legitima e o valor será descontado da conta do cartão e repassado ao lojista.

Em posse das informações do cartão, os golpistas podem realizar transações em outros estabelecimentos físicos ou on-line. Normalmente, com o objetivo de enganar as instituições financeiras, o valor da transação realizada pelo golpista será o mesmo valor da compra no momento em que foram roubados os dados do cartão.

COMO SE PROTEGER?

A principal dica para os lojistas é a prevenção. Por isso, seguem algumas dicas essenciais:

1. Nunca passe qualquer informação pessoal quando estiver atendendo uma ligação. Empresas nunca entrarão em contato telefônico ou por e-mail para confirmar ou solicitar dados.

2. Nunca instale programas ou arquivos enviados por e-mail que tenham por origem um destinatário que você não conhece.

3. Caso fique em dúvida quanto a legitimidade de uma ligação ou e-mail, desligue a chamada ou ignore o e-mail e ligue para o SAC da empresa que lhe presta serviço a fim de confirmar a veracidade das operações.

CHARGEBACK

O Chargeback é a contestação por um cliente de uma venda online que foi realizada em cartão de crédito ou débito. Nela, o cliente que já está com o produto em mãos, solicita a devolução do valor pago à operadora do cartão alegando que o produto não foi entregue.

COMO OCORRE O GOLPE:

1° PASSO: Uma compra online é realizada utilizando o cartão de débito ou de crédito.

2° PASSO: Com o produto em mãos ou um pouco antes de receber o produto, o comprador solicita o estorno da sua compra, alegando que ela não foi recebida ou que seu cartão foi roubado.

3° PASSO: O lojista tem os valores da compra retidos pela operadora do cartão.

Com uma contestação em vigor, todos os valores devidos se tornam um custo para o lojista, inclusive com o risco de não reaver o produto enviado. Há também o risco de isso interferir na imagem da empresa diante das operadoras que prestam serviços de pagamento.

COMO SE PROTEGER?

A principal dica para os lojistas é a prevenção. Por isso, seguem algumas dicas essenciais:

1. Construa um cadastro completo para suas vendas on-line e utilize plataformas que permitam a verificação de IP, localização e dispositivo pelo qual se realizou a compra.

2. Privilegie outras formas de pagamento como boleto e Pix.

3. Terceirize suas vendas com cartão. Outras plataformas, como Mercado Pago e Paypal, garantem a segurança tanto do consumidor quanto dos lojistas.

4. Sistemas antifraude são um bom investimento, principalmente para lojas que transacionam valores mais altos. Essas ferramentas permitem realizar uma análise dos perfis e avaliar os riscos das transações.

EMISSÃO DE CARTÕES NO VAREJO:

Os golpistas solicitam, com dados falsos, a emissão de cartões de crédito em lojas que oferecem essa facilidade.

COMO OCORRE O GOLPE:

1° PASSO: O golpista solicita um cartão de crédito se utilizando de dados de terceiros sem o conhecimento desses.

2° PASSO: Ao realizar compras com esse cartão, o prejuízo recaí sobre a pessoa que teve seus dados roubados e sobre o estabelecimento comercial que emitiu o cartão.

Se aproveitando das facilidades e vantagens oferecidas pelo varejo com um cartão de crédito próprio, os golpistas realizam compras de nome de terceiros, deixando o prejuízo para quem teve seus dados clonados e para o varejista que emitiu o cartão.

COMO SE PROTEGER?

A principal dica para os lojistas é a prevenção. Por isso, seguem algumas dicas essenciais:

1. Verifique a situação cadastral do solicitante na Receita Federal e empresas responsáveis por averiguar o crédito.

2. Solicite informações cadastrais completas e comprovantes, como o de residência e o de renda.

3. Mantenha um setor específico para cuidar das emissões de cartão e verificar as informações prestadas.

TROCA DA MAQUININHA

O lojista tem sua maquininha trocada durante uma tentativa de compra ou em uma abordagem falsa.

COMO OCORRE O GOLPE:

1° PASSO: O golpista recebe, das mãos do vendedor ou de um funcionário, a maquininha para realizar o pagamento de uma compra. Uma outra possibilidade, é um golpista se passar por um técnico e solicitar a troca da maquininha para a manutenção

2° PASSO: Utilizando um comparsa ou um momento de distração, ocorre a troca da maquininha por uma outra idêntica, mas que tem a conta vinculada a um outro golpista.

3° PASSO: Enquanto o lojista não perceber que a maquininha foi trocada, todas os valores pagos através da maquininha fraudada serão repassados aos golpistas.

Utilizando técnicas de engenharia social, os golpistas se aproveitam de um momento de fragilidade e de distração do lojista para realizar a troca da maquininha. A fraude pode ser difícil de ser detectada, já que a maquininha é idêntica a original

COMO SE PROTEGER?

A principal dica para os lojistas é a prevenção. Por isso, seguem algumas dicas essenciais:

1. Caso sua maquininha seja móvel, considere colocá-la em um ponto fixo de pagamento, ou, sempre manter ela na sua mão ou em local visível durante qualquer transação.

2. Lembre-se sempre de manter contato com a empresa da sua maquininha, verificando a veracidade de qualquer ocorrência, como trocas e manutenções.

INSERÇÃO DE DADOS FALSOS NO LINK DE PAGAMENTO

O golpista realiza o pagamento de uma compra através do link de pagamento usando um cartão de crédito clonado e dados roubados.

COMO OCORRE O GOLPE:

1° PASSO: O golpista inicia o processo de compra via redes sociais, normalmente WhatsApp, e solicita como forma de pagamento o link de pagamento. O golpista pode usar imagens e nomes que evitem levantar suspeitas, como pessoas mais velhas e nomes religiosos.

2° PASSO: Após receber o link, o golpista insere dados roubados e clonados do cartão de crédito.

3° PASSO: O golpista, normalmente, enviará um motorista de aplicativo para retirar o produto. Com a compra em mãos, o golpista pode tentar novas aquisições até que o limite do cartão clonado seja estourado.

4° PASSO: A vítima ou o banco, ao perceber as transações, congela os pagamentos, deixando o lojista no prejuízo dos produtos enviados.

Aproveitando-se da facilidade do link e da disponibilidade das lojas de realizarem uma entrega personalizada, o golpista se utiliza de dados roubados e clonados para adquirir os produtos e, basicamente, impossibilitando o retorno dos bens entregues.

COMO SE PROTEGER?

A principal dica para os lojistas é a prevenção. Por isso, seguem algumas dicas essenciais:

1. Evite enviar o link de pagamento para pessoas que não são consumidores recorrentes.

2. Se possível, garanta que o comprador, o portador de cartão e quem vai retirar ou receber a mercadoria seja a mesma pessoa. O golpista pode usar uma identidade falsa ou roubada.

ALTERAÇÃO DO CADASTRO NA JUNTA COMERCIAL:

O golpe ocorre através de uma fragilidade de login da plataforma GOV.BR para alterar os dados cadastrais na Junta Comercial e realizar uma alteração no quadro societário e realizar empréstimos e outras dívidas de forma indevida.

COMO OCORRE O GOLPE:

1° PASSO:

Aproveitando-se de um vazamento de dados, o golpista utiliza o login através da plataforma GOV.BR para acessar o site de cadastro da Junta Comercial. Nesse momento, também são alterados os dados de acesso na Plataforma GOV, de forma a dificultar a recuperação da conta.

2° PASSO:

Com esse acesso, o golpista realiza uma alteração cadastral no quadro societário, retirando os proprietários originais e os substituindo por laranjas.

3° PASSO:

Com esse controle, ele pode retirar empréstimos, emitir notas e contrair outras dívidas através do acesso às contas bancárias.

COMO SE PROTEGER?

A principal dica para os lojistas é a prevenção. Por isso, seguem algumas dicas essenciais:

1. Ative a verificação de duas etapas de sua conta GOV.BR. Verifique como proceder:

    • É necessário instalar o aplicativo GOV.BR em seu celular e realizar o login nele com a sua conta GOV.BR. É nele que você vai gerar o código de acesso. Lembre-se que apenas poderá haver um único dispositivo vinculado por vez.

    • Para ativar a verificação em duas etapas, acesse o seu aplicativo gov.br e em Segurança da conta, habilite a Verificação em duas etapas. Pronto! Sua conta já está mais segura.

2. Não informe seus dados como senha para terceiros.

3. Troque sua senha regularmente, preferindo senhas mais extensas e com caracteres diversos.

Sindilojas RS

Porto Alegre

Sindicato do Sistema Comércio