



## ALERTA CIBERCRIME

11 de maio de 2023

### *Burlas – Compras por via de Agente Transportador*

1. Está em curso mais uma sofisticada campanha de **burlas por via das redes de comunicações**, que passa pela simulação de recolha de compras no domicílio do vendedor.

2. Este método criminoso está a vitimizar quem disponibiliza bens para venda numa das diversas legítimas plataformas de venda *online*. Com efeito, anunciantes de bens que pretendem vender, têm sido abordados por desconhecidos que têm manifestado vontade de comprar aqueles bens. Afirmam querer comprar sem verem o bem, sem saberem qual é o respetivo estado de conservação e sem discutir o seu preço. Estes desconhecidos, agentes criminosos, estabelecem todos os contactos sempre e apenas por via de mensagens de WhatsApp, frequentemente escritas com evidentes erros, que indiciam ter sido usado um tradutor automático (sendo, portanto, porventura estrangeiros).

3. Tais agentes criminosos, logo na primeira abordagem, informam que pretendem enviar a casa do vendedor um estafeta ou uma empresa transportadora, para recolher o artigo.

Caso o vendedor aceda ao negócio, o agente criminoso desenvolve então um processo fraudulento, que visa levar o vendedor a efetuar-lhe um pagamento – em vez de lhe pagar o bem. O método fraudulento varia entre os diversos grupos criminosos que se dedicam a esta prática.

4. Num dos métodos identificados, o burlão informa o vendedor de que o estafeta levará com ele, em numerário, o dinheiro para pagamento do respetivo preço. Além disso, o agente criminoso acorda logo com o vendedor um dia e uma hora para a transação. Informa ainda o vendedor de que a



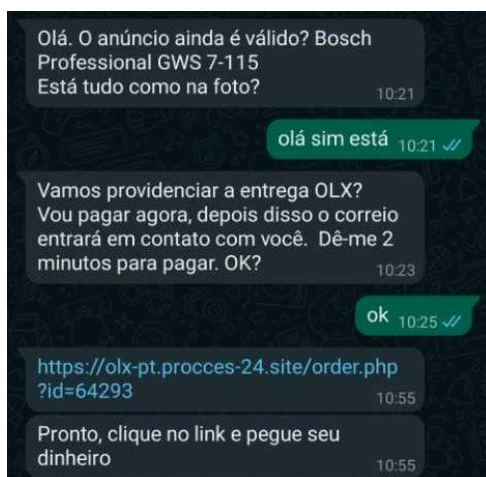
empresa transportadora exige que seja feito um seguro para o transporte. Tal seguro deve ser antecipadamente pago pelo vendedor do bem – mas o agente criminoso garante que o mesmo será por si prontamente reembolsado, sendo até já incluído no valor que há-se ser entregue em mão ao vendedor.

5. Tendo em vista o pagamento de tal suposto seguro, o criminoso remete ao vendedor/vítima o *link* de uma página *web* onde o mesmo pode fazer tal pagamento. Normalmente, o *link* abre uma das várias plataformas legítimas que se dedicam à venda de cartões virtuais de pagamento, pré-pagos. Isto é, o criminoso encaminha a vítima para uma página na qual incita esta a comprar, *online*, um cartão virtual. Pede-lhe ainda que tire e lhe mande uma *fotografia* desse cartão virtual e dos respetivos códigos de utilização. Quer com isto que a vítima adquira um *valor* e lhe faculte os códigos de utilização desse mesmo valor.

Uma vez na posse do número de série do cartão virtual e do respetivo código, o criminoso usa o valor respetivo em seu proveito.



6. Noutro dos métodos identificados, o burlão informa que irá solicitar a recolha do bem a uma entidade transportadora, sendo o próprio pagamento por si efetuado, *online*, por via de uma plataforma eletrónica daquela transportadora. Esta, também *online*, transferirá o valor para o vendedor. De seguida, o agente criminoso informa o vendedor de que efetuou já o pagamento *online*, no site do operador / transportador, enviando à vítima um *link* que



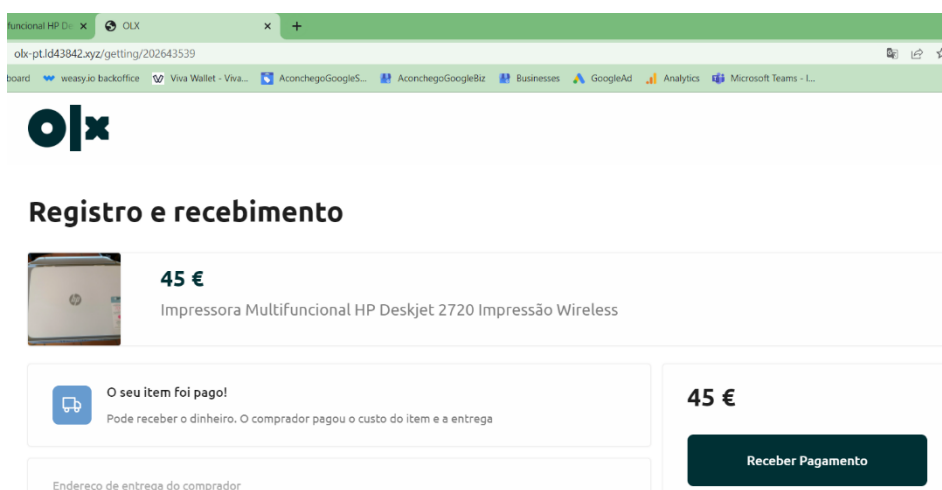
esta deverá utilizar para receber o seu dinheiro.

Tal *link*, se acedido, abre uma página na Internet que, graficamente, parece ser a legítima página da transportadora, mas que, na verdade, não é. Trata-se de uma página falsa, criada e disponibilizada pelos agentes criminosos, usando de forma abusiva e não autorizada a



imagem e outros elementos identificadores do operador (logotipos, etc.).

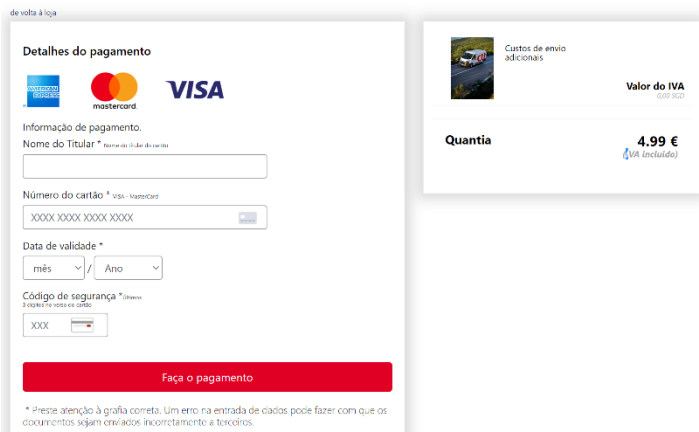
7. Normalmente, na página falsa é exibido o bem que a vítima pôs à venda, com a menção de que o mesmo foi já pago pelo comprador. Além disso, na página é exibido um botão, com a referência *“Receber Pagamento”*, ou outra de natureza semelhante.



Pretende-se com este conteúdo, enganosamente, levar a vítima a acreditar que está perante uma autêntica página de um legítimo operador e que o processo de aquisição e pagamento do bem que disponibilizou para venda é lícito e verdadeiro.

8. Porém, se a vítima premir o botão *“Receber Pagamento”* não irá receber o seu dinheiro.

**ctt**



Foram a este respeito identificados dois métodos criminosos distintos: algumas das páginas fraudulentas, com o subterfúgio de ser necessário liquidar um pequeno custo do envio, solicitam às vítimas que paguem uma pequena taxa, utilizando o seu cartão de crédito. Noutros casos, as páginas informam que o pagamento do bem à venda será efetuado por transferência para o saldo do seu cartão de crédito, solicitando assim à vítima que insira na página todos os dados do seu cartão: o nome que nele é mencionado, o

número do cartão de crédito, a respetiva data de validade e ainda o respetivo código de segurança (CVV). Se a vítima introduzir esta informação que se lhe solicita, fornecerá aos autores destes factos todos os dados do seu cartão bancário, permitindo assim àqueles que utilizem livremente este cartão, em compras ou pagamento de serviços.

9. As páginas na Internet para as quais as vítimas são encaminhadas são falsas, isto é, não são geridas pelos operadores cujos elementos identificadores neles figuram (nem por elas foram autorizadas). Foram identificadas páginas *“falsas”* OLX, CTT, UPS, DHL, DPD, GLS, Nacex, entre outras. Trata-se de páginas fraudulentas, que pretendem imitar, aos olhos do utilizador comum, a aparência das autênticas páginas dos operadores, plataformas ou



transportadoras. Têm como único propósito captar os dados do cartão bancário da vítima – os quais serão depois abusivamente utilizados pelo agente do crime. Como tem acontecido recorrentemente com outras campanhas de *phishing*, os criminosos têm feito alojar a página falsa em sucessivos servidores de alojamento na *cloud*, os quais permitem a contratação *online*, criando séria dificuldade à determinação da identidade do seu dono.

**10.** Nas diversas situações descritas (quer naquelas em que foi exigido o pagamento de um seguro, quer naquelas em que o suposto pagamento seria feito *online*), quando a vítima segue as indicações do burlão e, portanto, paga ou faculta os dados do seu cartão de crédito, o suposto comprador não mais entra em contacto, passando a ser impossível contactá-lo. Fica com a quantia paga antecipadamente pelo vendedor (os cartões virtuais) ou os dados do cartão de crédito e desaparece. Não paga nunca o bem em causa. Da mesma forma, não comparece ao encontro para compra do bem, nem envia ao local qualquer estafeta para esse efeito.

Estes agentes criminosos não têm qualquer intuito de comprar qualquer bem. Na verdade, todo o processo de manifestação de vontade de compra do bem e da sua recolha na casa do vendedor é uma encenação que tem apenas em vista criar a expectativa de venda e levar o vendedor/vítima a proceder ao pagamento antecipado de uma quantia supostamente devida a título de seguro, ou a facultar os dados do seu cartão de crédito.

**11.** Foram identificados casos em que, tendo a vítima suspeitado do intuito fraudulento do suposto comprador, não procedendo ao pagamento e manifestando já não estar interessada no negócio, o agente criminoso a abordou de forma agressiva e intimidatória, ameaçando mover-lhe processos judiciais e até referindo ameaças físicas, caso recusasse pagar o que pedia.

**12.** Este fenómeno criminoso tem origem em grupos profissionais e organizados, que procuram enganar vítimas mais crédulas e menos atentas, utilizando métodos insistentes de convencimento e persuasão. O propósito dos autores destes factos criminosos é exclusivamente burlar, convencendo as vítimas a efetuarem pagamentos indevidos ou a facultarem indevidamente dados de cartões de crédito.

É recomendável que se avaliem cautelosamente as mensagens escritas que se recebem, propondo compras de bens. Caso se afigurem duvidosas não deve responder-se às mesmas, devendo antes tais mensagens ser comunicadas ao Ministério Público ou aos órgãos de polícia criminal. Para lá disso, mensagens deste tipo devem ser ignoradas, sem se lhe dar qualquer sequência.

Minha senhora, faça o que entender, mas quem determina as formas de venda dos meus produtos sou eu!

Martine

Saiba que se se recusar a finalizar a transacção com o serviço Happy-post, procederá a um PROCESSO JUDICIAL contra si por quebra de confiança Happy-post ou receberá uma visita desconhecida não é um assédio, mas dou-lhe a minha boa fé para encerrar esta transacção para evitar estes problemas

Acabou o diálogo, faça o que entender necessário! Se precisar envio o contacto do meu advogado

Martine

Declino toda a responsabilidade