ALERTA CIBERCRIME

5 de julho de 2023

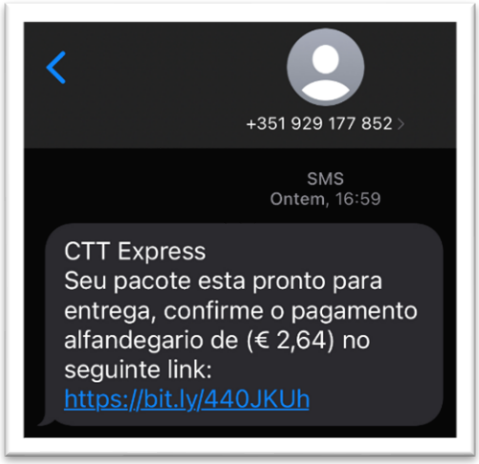
Obtenção ilícita de dados de cartões de crédito

(uso abusivo do nome e imagem dos CTT)

1. Está em curso mais uma campanha de *phishing* que têm em vista obter, de forma ilícita, os dados dos cartões de crédito de vítimas indiscriminadas. Estas campanhas dão continuidade a várias outras, que ocorreram no passado. No caso presente, os agentes criminosos utilizam o nome e a imagem dos *CTT - Correios de Portugal*.

2. Como em todos os casos de *phishing*, o processo criminoso começa com a expedição, para muitíssimos destinatários, de mensagens fraudulentas – no passado era utilizado o correio eletrónico ou mensagens de SMS, mas na presente campanha tem sido primordialmente utilizado o serviço de mensagens *WhatsApp*.

3. Em tais mensagens, os agentes criminosos incluem informação que leva o destinatário a acreditar que as mesmas foram expedidas pelos *CTT – Correios de Portugal*. Além disso, das mensagens resulta que o destinatário tem uma encomenda pendente de entrega por aquele serviço postal, existindo, porém, a necessidade de pagar, antes da entrega, uma pequena taxa (o valor indicado é sempre muito baixo e ronda, normalmente, os 2 ou 3 euros).

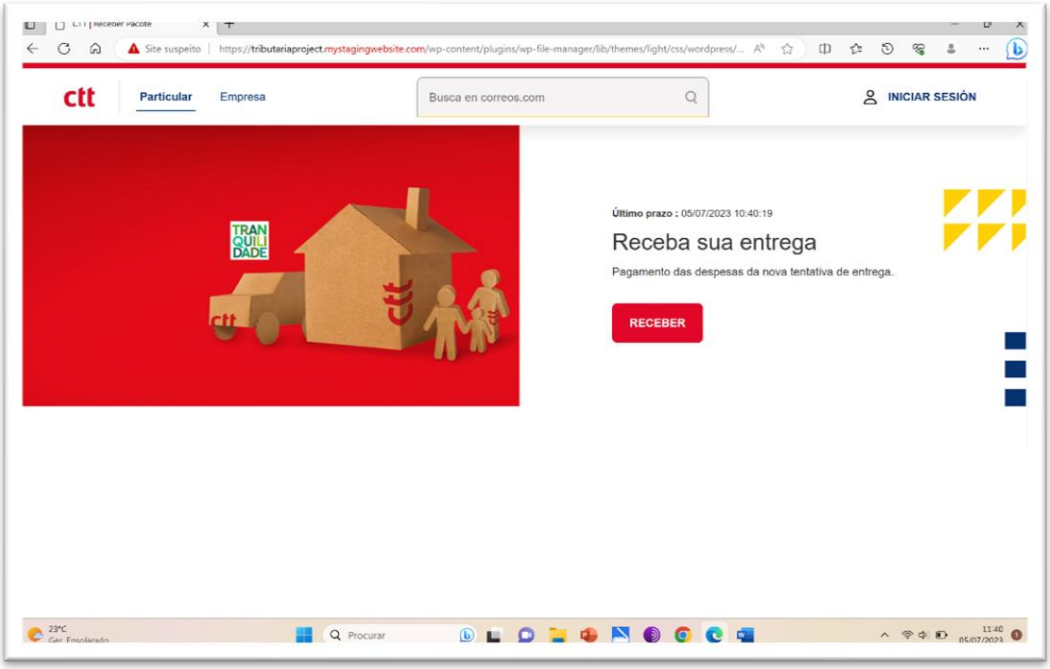


4. Nalguns casos, resulta das mensagens que a suposta entrega foi já tentada, embora sem sucesso, podendo, porém, vir a ser de novo agendada, por iniciativa do destinatário. Caso o mesmo não tome qualquer iniciativa, adverte-se que a encomenda será devolvida.

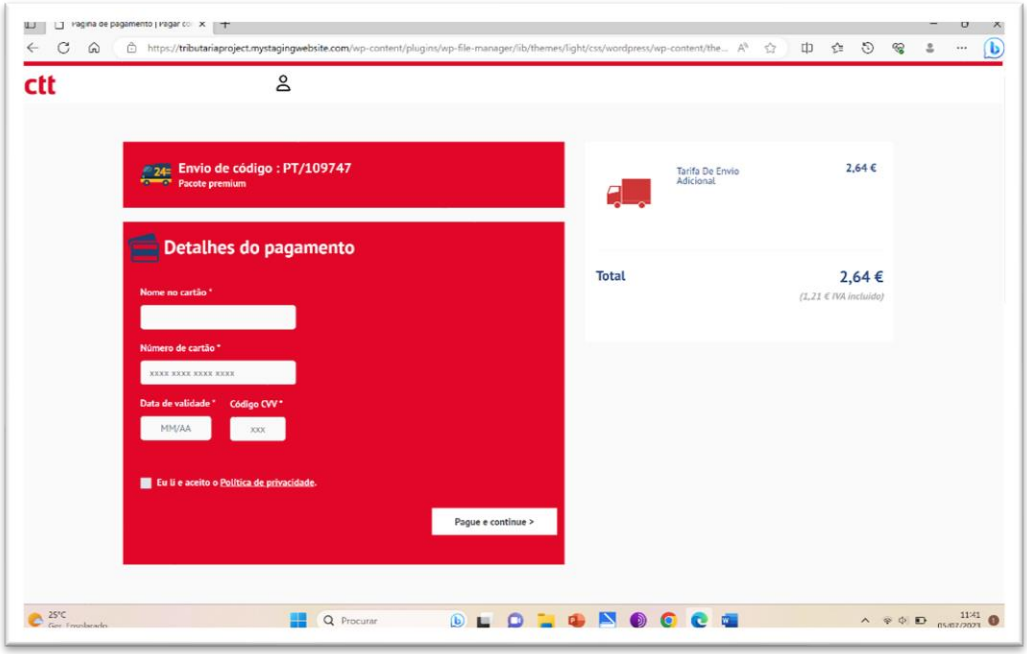
5. Em qualquer dos casos, incita-se o destinatário a ação imediata – designadamente, a aceder ao *link* facultado, para "regularizar" a entrega e o pagamento. Todas as mensagens indicam um *link*, a que o destinatário deve aceder.

6. Estas mensagens são fraudulentas. Não são provenientes dos *CTT – Correios de Portugal*. A sua origem é variada, consoante o grupo de crime organizado (de entre os vários que se dedicam a esta atividade) que as emitiu. Não existe entrega alguma nem encomenda alguma a ser entregue. Se alguma das vítimas está, porventura, à espera de alguma encomenda, não será aquele a que se referem estas mensagens.

7. Por outro lado, os *links* contidos nas mensagens fraudulentas não conduzem ao autêntico s*ite*, na Internet, dos *CTT – Correios de Portugal*. Com efeito, se a vítima aceder a tais *links*, abre uma página que visualmente parece ser o dos *CTT – Correios de Portugal*. Mas não é: trata-se de uma página *web* fraudulenta, disponibilizada pelos agentes criminosos. Em geral, são páginas alojadas em servidores da chamada *cloud*, que podem ser geridos pelos agentes criminosos a partir de qualquer parte do mundo.



8. Nestas páginas, é solicitado à vítima que introduza dados pessoais e, invariavelmente, os dados do seu cartão bancário – o nome que nele figura, o número, a data de validade e o código CVV (*Card Verification Value*). Isto é, na prática, é pedido à vítima que faculte todos os dados que permitem utilizar o cartão em causa.



9. Após a vítima facultar os dados, segue-se um pequeno compasso de espera, abrindo-se uma outra página, que informa a vítima do seguinte: "*aguardando confirmação para validar seu cartão – por favor não feche esta guia*".

Logo de seguida, surge uma outra página em que é solicitado à vítima que introduza um código, recebido por SMS.

10. Este procedimento, de espera de uns segundos, até ser solicitado o código SMS, é deliberado: após a vítima introduzir os dados do cartão de crédito, os agentes criminosos, de imediato os utilizam *online*, designadamente para efetuar compras de elevado valor; para a validação dessa utilização é necessária a introdução do chamado segundo fator de autenticação, o qual é o código, remetido por SMS para a vítima. Se a vítima introduzir na página fraudulenta esse código (dando-o a conhecer ao agente criminoso), está a permitir que o criminoso o utilize, para confirmar o movimento que realizou, com o seu cartão de crédito.

11. Por este processo criminoso, os seus autores pretendem induzir as vítimas a facultar-lhes dados dos seus cartões, para os utilizarem abusivamente, em prejuízo daquelas. Este método explora o grande incremento do comércio eletrónico e das compras *online* com a consequente entrega dos bens em casa, por serviços de entrega. Estes serviços de entrega têm constituído um terreno fértil para exploração deste método criminoso.
Mensagens como as que acima se descreveram devem ser ignoradas e apagadas, sem resposta. Caso a vítima se aperceba de que acabou por facultar indevidamente os dados do seu cartão, importará, como primeira diligência a empreender, contactar o banco emissor e proceder ao cancelamento daquele cartão.