



ALERTA CIBERCRIME

25 de março de 2021

**“Roubo” de dados de cartões de crédito
(uso abusivo das imagens da Autoridade Tributária,
dos CTT e da EDP)**

1. Estão em curso campanhas 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 em meses passados.

Por este tipo de processo criminoso, os seus autores pretendem induzir as vítimas a facultar-lhes dados dos seus cartões de crédito, com o argumento enganoso de que vão ser-lhes reembolsadas quantias. Para este efeito, utilizam abusivamente imagens corporativas de diversas entidades. Nos casos das campanhas presentemente em execução, têm sido manipuladas as imagens de entidades públicas portuguesas, ou prestadoras de serviços públicos, designadamente a *AT – Autoridade Tributária*, os *CTT – Correios* e a *EDP – Energias de Portugal*. Em menor número, têm também sido abusivamente utilizadas as designações e marcas de outras entidades.

2. Como em todos os casos de *phishing*, o processo criminoso começa com a expedição, para muitíssimos destinatários, de mensagens fraudulentas de correio eletrónico ou de SMS. Na presente campanha, têm sido observadas as duas modalidades. O mesmo tinha já ocorrido noutras campanhas anteriores, durante o ano de 2021 e já também em 2020.

3. Nestas mensagens, o teor do conteúdo é variado. Um dos elementos que costuma estar presente é o de arrogarem-se serem expedidas por uma entidade credível: a *AT – Autoridade Tributária*, os *CTT – Correios* ou a *EDP – Energias de Portugal*, entre outras. Normalmente, as mensagens de correio eletrónico incluem também os logotipos ou marcas institucionais daquelas entidades. Além disso, todas elas incitam o destinatário da mensagem a aceder, por via de um *link*, que a mensagem inclui, a uma página na Internet.

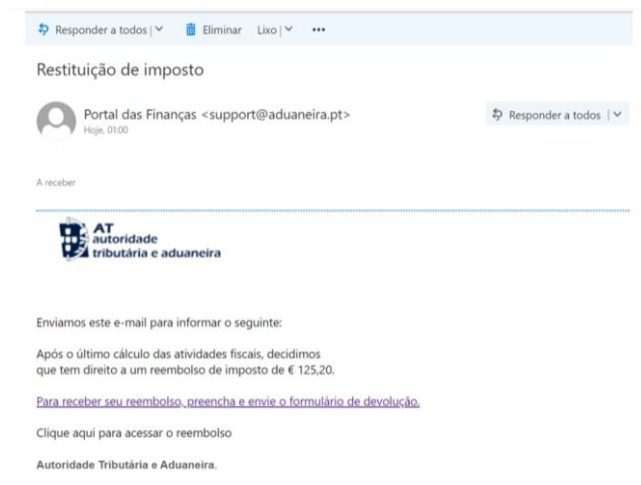
4. Por exemplo, no caso de mensagens supostamente remetidas pela *Autoridade Tributária*, com frequência têm sido identificados casos em que se refere que o destinatário *“tem direito a um reembolso de imposto”* excessivamente cobrado pelo Estado. Depois, solicita-se que *“para receber o seu reembolso, preencha e envie o formulário de devolução”*, o qual está disponível numa página cujo *link* é indicado.

Disso, é bom exemplo, a imagem que segue, retirada de uma mensagem expedida a 24 de março de 2021.



MINISTÉRIO PÚBLICO
PORTUGAL

PROCURADORIA-GERAL DA REPÚBLICA
GABINETE CIBERCRIME



5. Noutros casos, as mensagens fraudulentas supostamente expedidas pela *Autoridade Tributária* têm chegado por mensagem de texto (sobretudo por SMS, mas também por outras aplicações, como o WhatsApp), como sucedeu na situação a que respeita a imagem que segue.



6. Já em casos de mensagens supostamente remetidos pela *EDP – Energias de Portugal*, refere-se por exemplo, que uma fatura teria sido indevidamente debitada duas vezes, razão pela qual se solicita ao cliente que solicite o reembolso da mesma. Para tal reembolso, normalmente pede-se nestas mensagens que seja acedido um *link*. É exemplo deste tipo de mensagem, aquela que se reproduz na imagem que segue, identificada durante o mês de março de 2021.

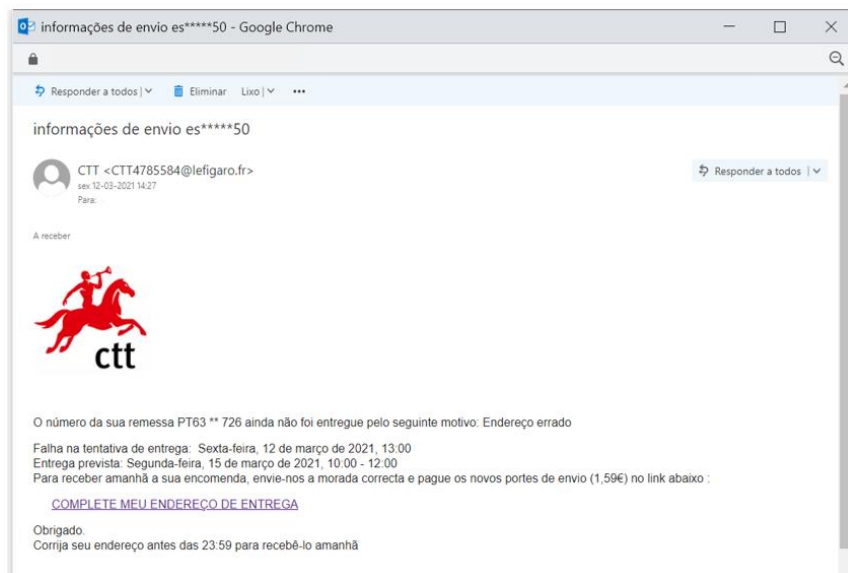




7. As mensagens, supostamente com origem na *EDP – Energias de Portugal*, têm também surgido por via telefónica. É exemplo disso a mensagem copiada na imagem que segue, na qual, ao contrário da anterior, se apele que a que seja paga uma fatura em dívida. Neste caso, o propósito do agente do crime é o de convencer a vítima, sob tensão, a que pague uma quantia monetária. Trata-se, pois, de um fenómeno criminal de natureza diferente.



8. Têm também ocorrido muitas mensagens supostamente expedidas pelos *CTT – Correios*, em que se comunica ao destinatário que tem uma encomenda pendente de entrega. Tais mensagens adiantam que tal encomenda será entregue nos próximos dias. Informam ainda que, para a respetiva entrega, se torna necessário que seja paga uma pequena taxa alfandegária (o valor indicado é sempre muito baixo e ronda, normalmente, os 2 ou 3 euros). Exemplo deste tipo de mensagens é aquela que se reproduz na imagem que segue.



9. Também neste caso, ocorrem ser identificadas mensagens recebidas por via telefónica, por SMS. Embora por canais e formato diferentes, tais mensagens são da mesma natureza e têm o mesmo propósito das mensagens remetidas por correio eletrónico, o qual é o de encaminhar para uma página *web* fraudulenta.



Seu pacote PT09 ** esta pronto,
Envio da encomenda (2,99 euro)
para entrega a 02/01.
Mais informacoes podem ser
encontradas aqui: <http://bit.ly/alpt1ct>

10. Todas estas mensagens são fraudulentas. Não são provenientes de nenhuma das entidades a que supostamente são associadas. Não foram emitidas pelas mesmas nem a partir de sistemas informáticos pertencentes às mesmas. A origem real destas mensagens é muito variada. Costumam ser remetidas a partir de caixas de correio de servidores de *webmail*, nos quais qualquer pessoa pode criar uma conta, sem que para isso lhes seja exigido facultar qualquer tipo de dados de identificação verdadeiros. Em regra, estas contas de correio eletrónico são criadas propositadamente para este efeito e incluem palavras ou expressões parecidas às das entidades em causa, com pequeníssimas alterações, para potenciar o engano da vítima.

11. Assim, como exemplo, foram identificadas mensagens provenientes do domínio @aduaneira.pt, como provindo da *Autoridade Tributária*. Porém, tais mensagens provinham de outro domínio (o domínio *InMotion Hosting* (<https://www.inmotionhosting.com/>), um fornecedor de serviços baseado na Califórnia, nos Estados Unidos, creditado no registrar *Tucows Domains Inc.*, com sede no Canadá). Noutros casos, foram identificadas mensagens com origem no domínio *tmweb.ru* (<https://vh222.timeweb.ru/>), baseado na Rússia. Em ambos os casos, se trata de servidores da chamada *cloud*, que permitem a utilização dos seus serviços a qualquer utilizador da Internet.

12. Por outro lado, os *links* contidos nas mensagens fraudulentas que acima se descreveram, não conduzem aos autênticos *sites* Internet daquelas entidades. Pelo contrário, apontam para sites fraudulentos, ilicitamente construídos com intuítos criminosos. No caso das diversas supostas mensagens da *Autoridade Tributária* identificadas, o *link* conduz a um *site* que visualmente parece ser o da *Autoridade Tributária e Aduaneira*. Nele, solicita-se que sejam preenchidos todos os dados pessoais do destinatário da mensagem, como resulta da imagem que segue.

Área do Cliente

epgv01.fr/pablo/httpsaduaneiroportal.dasfinancas.gov.pt/js/main.jsp/8bf1/

quarta, 24 de março de 2021

Registrar-se Iniciar Sessão

AT autoridade tributária e aduaneira

Cidadãos Negócios Outras Entidades Informação

SISTEMA DE REEMBOLSO AUTOMÁTICO NO CARTÃO DO BANCO

Formulário de Reembolso

Nome

O seu nome

Primeiro nome

O seu primeiro nome

Data de nascimento

O seu número de telefone

O seu número de telefone

Endereço

O seu endereço

Cidade

Código Postal

Código Postal

Continuar

09:21 24/03/2021

13. Depois, preenchidos esses, com a promessa da devolução de uma quantia, solicita-se que sejam facultados todos os dados do cartão de crédito do destinatário da mensagem, como pode ver-se na imagem que de seguida se reproduz.

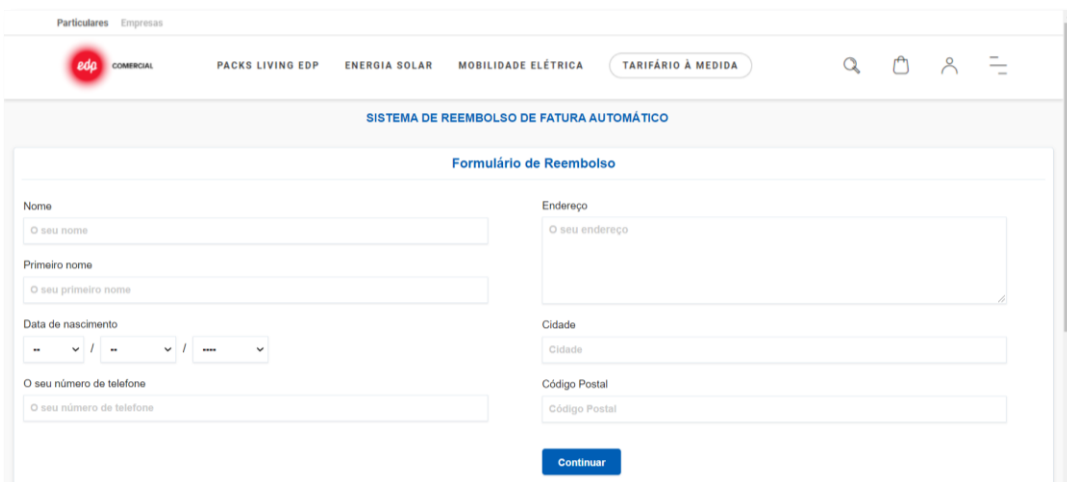


INFORMAÇÃO GLOBAL DE REEMBOLSO	
Beneficiário do reembolso	
Modo de recepção	Cartão de crédito
Número de ficheiro	13828AXD197
Montante do reembolso	125,20 €
Data	24/03/2021
Condições de pagamento	24 Horas

14. O objetivo deste procedimento criminoso é o de captar os dados do cartão de crédito da vítima: o número, a data de validade e o respetivo código CVV. Com estes dados, o agente do crime pode livremente utilizar este cartão e proceder a todas as transações que pretender, designadamente *online*. Para convencer a vítima, como se disse, o agente do crime ilude-a com um reembolso de dinheiro, supostamente respeitante a imposto indevidamente pago.

15. No caso dos *sites* a que se acede com mensagens supostamente remetidas pela *EDP – Energias de Portugal*, sucede algo parecido. O *link* conduz a uma página *web* com um logotipo correspondente ao normalmente utilizado por aquela companhia.

O método é parecido ao que anteriormente se descreveu: o agente do crime seduz a vítima com um reembolso de uma quantia que teria sido indevidamente paga. Para tal devolução, num primeiro momento é solicitado que aquela faculte dados pessoais, como pode verificar-se na imagem seguinte.



16. Preenchidos estes – independentemente da correção dos mesmos, que não são verificados – é de imediato solicitado à vítima que introduza os dados do seu cartão de crédito (além do nome, que já introduziu): o número do seu cartão de crédito, a respetiva data de validade e ainda o código de segurança (CVV).



The screenshot shows a web browser window with the URL <https://snpgroup.fr/wp-includes/httpswww.edp.pt/particulares/93c29/>. The page is titled "SISTEMA DE REEMBOLSO DE FATURA AUTOMÁTICO" and "Reembolso - Dados bancários do beneficiário". It contains a form for entering credit card details and a table of reimbursement information.

INFORMAÇÃO GLOBAL DE REEMBOLSO	
Beneficiário do reembolso	Cartão de crédito
Modo de recepção	Z1WNEDJ991
Numero di file	98,10 €
Montante do reembolso	03/03/2021
Data	48 Horas
Condições de pagamento	

17. No caso dos *sites* a que se acede com mensagens supostamente remetidos pelos *CTT - Correios*, o procedimento é muito similar: pretende-se convencer a vítima a facultar os dados do seu cartão de crédito. Assim, num primeiro momento, o *link* facultado pela mensagem fraudulenta conduz a vítima para uma página *web* onde é informada de que em breve receberá uma encomenda; porém, tal encomenda requiere o pagamento de uma pequena taxa.



The screenshot shows a web browser window with the URL https://pt3576correios-ctt-pt.com/fe2f9babf082e93b729cfc2bec1e2c64/Seleccione_medio_de_pago.php. The page features the CTT logo and the following information:

DATA : 09/03/2021

PASSO 1 : : PAGAR OS NOVOS CUSTOS DE ENTREGA

VALOR A PAGAR : 1,59 €

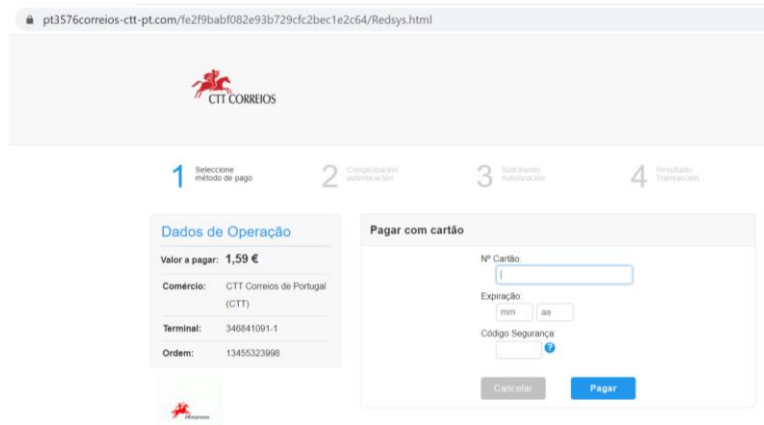
MÉTODO DE PAGAMENTO :

CARTÃO

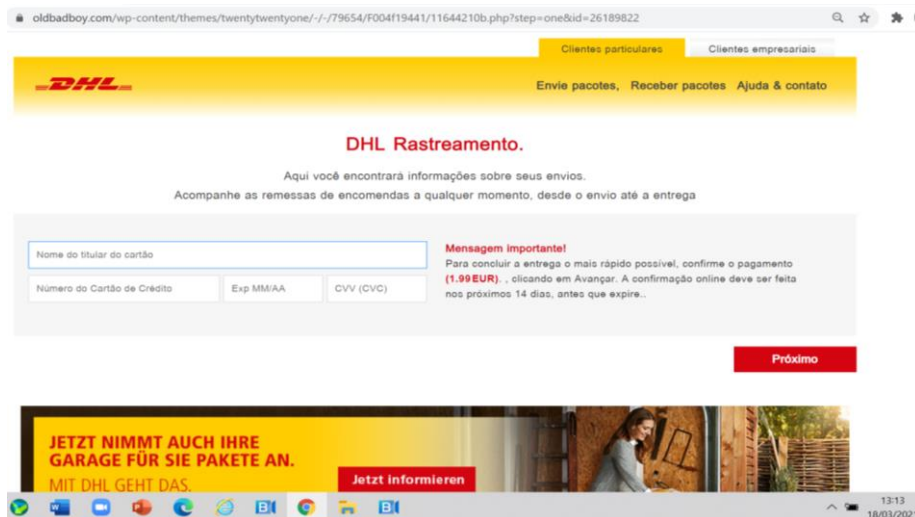
PAGAR E CONTINUAR

CANCELAR

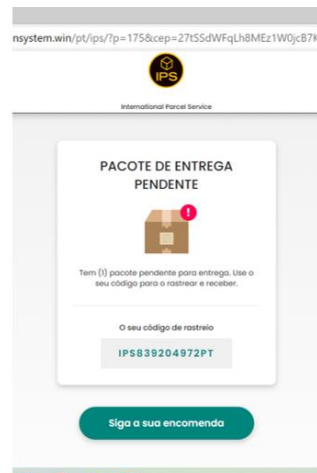
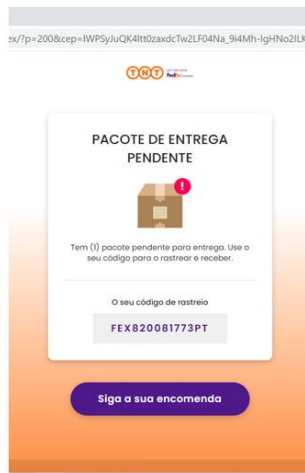
18. Logo depois, a vítima é solicitada a facultar os dados do seu cartão de crédito.



19. O procedimento criminoso tem mostrado variantes criativas, incluindo designadamente outras entidades que prestam serviços de entrega postal. Foi o que sucedeu no caso, de meados de março de 2021, que se documenta na imagem que segue.



20. O A mesma variante tem explorado a circunstância, motivada pelo período de pandemia e confinamento, de ter havido um grande incremento 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. As imagens que seguem são exemplo disso.





MINISTÉRIO PÚBLICO
PORTUGAL

PROCURADORIA-GERAL DA REPÚBLICA
GABINETE CIBERCRIME

21. Em todos estes procedimentos criminosos há traços comuns: o agente do crime intenta, de forma ardilosa, obter dados de cartões de crédito das vítimas.

Nenhum destes sites é gerido pelas entidades referidas nas mensagens fraudulentas, nem por elas são autorizados. Todas elas correspondem a páginas *web* falsas. Pretendem imitar, aos olhos do utilizador comum, as autênticas páginas *web* daquelas entidades, com o propósito de capturar os dados de cartão de crédito das vítimas – os quais serão depois livremente utilizados pelo agente do crime, em seu proveito.

22. Como se disse, as vítimas destes crimes cedem a criminosos os dados dos seus cartões de créditos. Portanto, em posse daqueles dados, aqueles agentes criminosos poderão proceder a todas as operações permitidos pelos cartões. Importará, pois, como primeira diligência a empreender, proceder ao cancelamento daqueles cartões.