ALERTA CIBERCRIME

12 de agosto de 2021

'*Phishing*' dirigido a clientes da EDP e titulares de cartões de crédito

1. Está em curso mais uma nova campanha de *phishing*, dirigida a vítimas que sejam simultaneamente clientes da *EDP* e titulares de cartões de crédito. Nesta campanha, os seus autores pretendem convencer as vítimas a facultar-lhes dados dos seus cartões de crédito, com o argumento de que pretendem reembolsar-lhes quantias.

2. Como habitual em casos de *phishing*, o processo começa com a expedição, para muitos destinatários, de forma indiscriminada e aleatória, de mensagens fraudulentas de correio eletrónico. Registaram-se campanhas anteriores idênticas[1] durante o ano de 2020[2]. Agora, foram sinalizadas pelo Gabinete Cibercrime concretas mensagens desta campanha a 9 e 10 de agosto de 2021.

3. Nestas mensagens, com o título no assunto, "*Réf. :[## 303 ##] ultimo lembrete*", anuncia-se que o destinatário, cliente da *EDP*, pagou a fatura de *agusto* (sic), no valor de 74,47 euros, por duas vezes, motivo pelo qual "*convidamos você a solicitar um reembolso clicando no link abaixo*". Para o efeito, indica-se um *link*, assinalado com a expressão "*Solicitação de reembolso*". As mensagens vêm assinadas com a expressão "*EDP Comercial – www.edp.pt – Portugal*".
Além disso, é ainda destacada a "*Observação: se esse problema não for resolvido nas próximas 12 horas, nenhum reembolso estará disponível*."


Informamos que o último pagamento da sua fatura de agusto de 2021 foi pago duas vezes.

Entidade: **20174**
Referência: **565 169 410**
Montante: **74,47**

Convidamos você a solicitar um reembolso clicando no link abaixo:

Solicitação de reembolso

Observação: se esse problema não for resolvido nas próximas 12 horas, nenhum reembolso estará disponível.

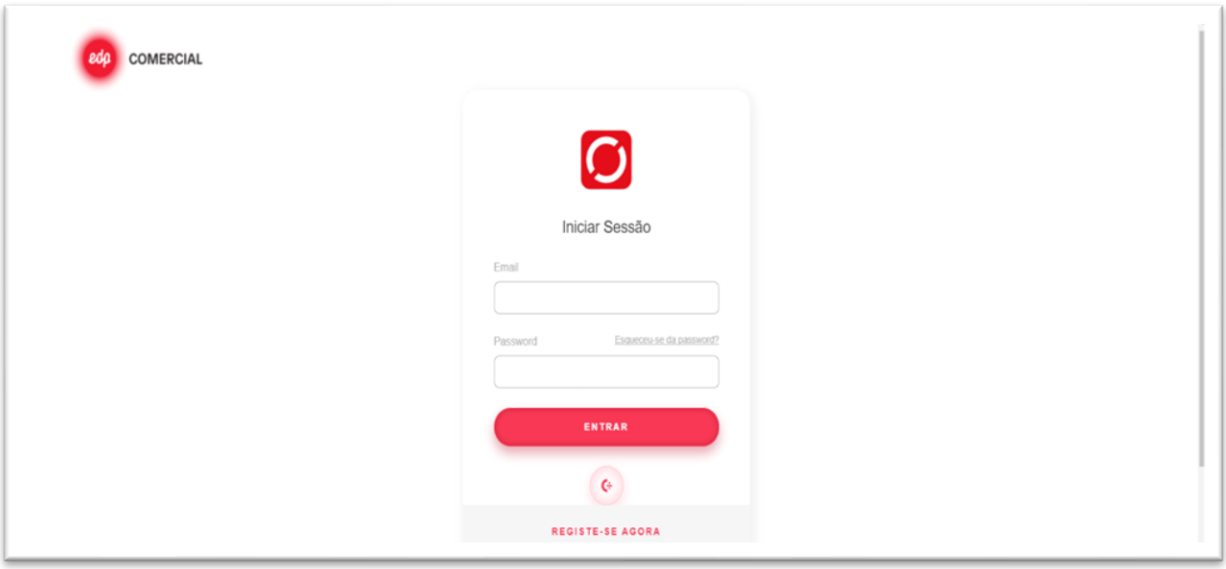
obrigado pela sua cooperação.

[1] Em março de 2020 uma campanha deste tipo foi relatada no alerta cibercrime de 16 de março de 2020, disponível aqui: http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/alerta_edp_visa_2020_03_14.pdf.
[2] Em maio de 2020 uma campanha deste tipo foi relatada no alerta cibercrime de 15 de maio de 2020, disponível aqui: https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/7969_2020_05_15_alerta_phishing_edp_visa.pdf.

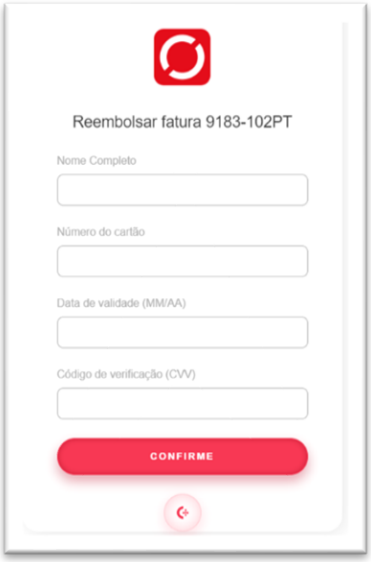
4. Trata-se de mensagens fraudulentas, não provenientes da *EDP*: não foram remetidas pela *EDP* nem a partir de sistemas informáticos pertencentes a esta companhia.

5. Aparentemente, tais mensagens foram remetidas da caixa de correio "*EDP*", mas na verdade não é assim. Provieram de endereços de servidores de *webmail* (por exemplo, do domínio @plesk.page), ou de contas de correio eletrónico ilegitimamente acedidas pelos criminosos e abusivamente usadas para este específico efeito.
Neste último caso, foi por exemplo identificada uma mensagem expedida a 10 de agosto de 2021, às 13h39, a partir da conta de correio eletrónico kasse@avelinotapas.de: trata-se de uma conta pertencente ao servidor de correio eletrónico de um restaurante *Avelino Tapas y Vino*, de Hamburgo, Alemanha (https://avelinotapas.de/).

6. Por sua vez, o *link* que se referiu, assinalado com a expressão "*Solicitação de reembolso*", contido nas mensagens fraudulentas, conduz a um s*ite* na Internet que aparenta ser o da *EDP*, exibindo aparência gráfica e um logotipo normalmente utilizados por aquela companhia. Nessa página, solicita-se ao utilizador que inicie a sua sessão de cliente, como se se tratasse da verdadeira página *web* da *EDP*.



7. Porém, ao contrário do que aconteceria com uma página autêntica, não é necessário introduzir dados verdadeiros, ou fidedignos: podem introduzir-se dados falsos ou inventados, bastando que se introduza em cada espaço um qualquer caracter e se prima o botão "*Entrar*".
Depois de premir este botão, acede-se a nova página em que é solicitada a introdução dos dados da vítima: o seu nome completo, o número do seu cartão de crédito, a respetiva data de validade e ainda o respetivo código de segurança (CVV).



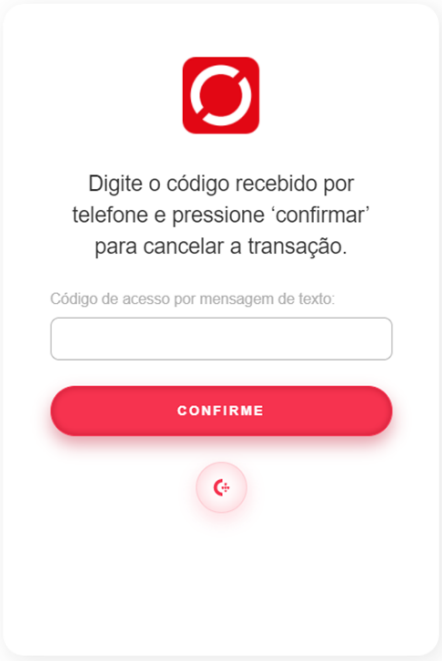
8. Este *site* não é gerido pela *EDP* nem é por ela autorizado. Trata-se de uma página falsa, que pretende imitar a autêntica página da *EDP*. Tem como único propósito captar os dados de cartão de crédito das vítimas – os quais serão depois abusivamente utilizados pelo agente do crime.
Esta página fraudulenta utiliza o serviço WebOps, disponibilizado pela plataforma Plesk (www.plesk.com), um serviço baseado na *cloud* que permite, entre outros, gerir páginas na Internet. Embora de origem suíça, este serviço pode ser integralmente contratado *online*, sem que possa apurar-se a identidade do seu utilizador.

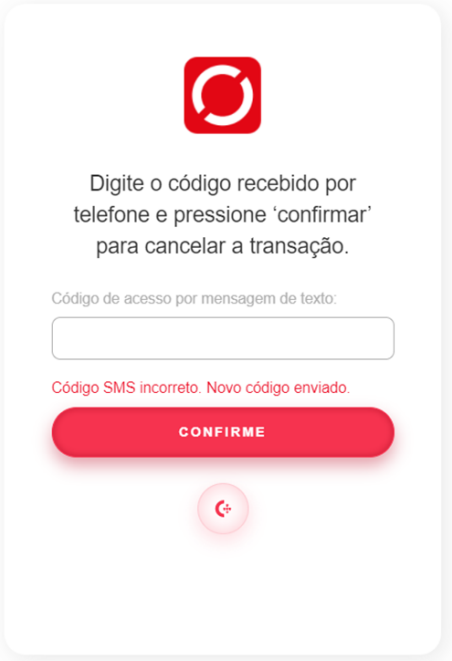
9. Como se disse, esta página pretende imitar a aparência, aos olhos do utilizador comum, da autêntica página da *EDP*. Se a vítima aceder a ela e nela introduzir a informação que se lhe solicita, fornecerá aos autores destes factos todos os dados do seu cartão de crédito, permitindo assim àqueles que utilizem livremente este cartão, em compras ou pagamento de serviços.

10. Aliás, com efeito, em geral, imediatamente após o utilizador inserir os dados do seu cartão de crédito naquela página, os agentes criminosos usam os mesmos, efetuando, de imediato, compras *online*. Como o procedimento de compras *online* requere, com frequência, confirmação das mesmas mediante a introdução de um código (*token*) expedido por mensagem escrita (SMS) para o telefone do titular do cartão, este método criminoso prevê essa possibilidade.
Assim, depois da introdução dos dados do cartão de crédito na página falsa, abre-se uma nova página, supostamente do servidor da *EDP*, em que é solicitado que "*Digite o código recebido por telefone e pressione confirmar*".

11. Efetivamente, logo que o criminoso efetuar a primeira compra, a vítima recebe um código, por SMS. Se o introduzir na página falsa permite ao criminoso autenticar e efetivar aquela compra.
Porém, recorrentemente, na página surge uma mensagem de erro: "*Código SMS incorreto. Novo código enviado*." O propósito deste procedimento é permitir ao criminoso efetuar uma segunda compra, e

uma outra, e ainda outras, até que a vítima, por estranhar ou outra razão, deixe de inserir os códigos na página.





12. Como se disse, este método criminoso tem como objetivo obter dados de cartões de crédito das vítimas, para os usar indevidamente. Mensagens como as acima descritas devem ser apagadas, sem as abrir e sem aceder ao *link* facultado. Caso tal aconteça, importará, como primeira diligência a empreender, proceder ao cancelamento daqueles cartões.