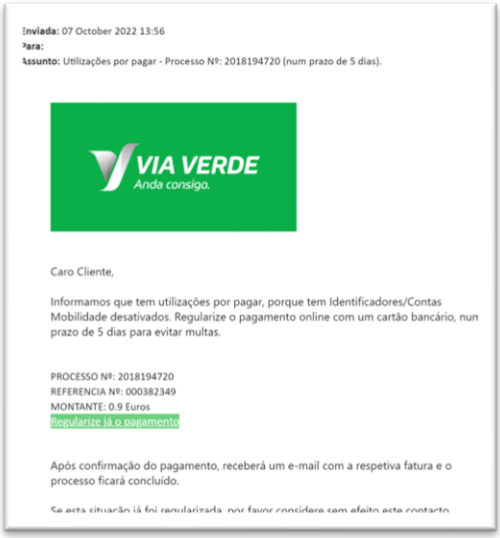
ALERTA CIBERCRIME

10 de outubro de 2022

'Phishing' de cartões bancários usando a imagem da Via Verde

1. Está em curso uma campanha criminosa de *phishing*, usando abusivamente a imagem da Via Verde, dirigida a vítimas que sejam titulares de cartões bancários de débito ou de crédito. Nesta campanha, os seus autores pretendem convencer as vítimas de que têm em dívida um pequeno pagamento à Via Verde, por utilização dos respetivos serviços, nas autoestradas para, desta forma, as levarem a facultar-lhes todos os dados dos seus cartões bancários.

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. Têm-se registado recentemente, com frequência, campanhas desta natureza, usando abusivamente a imagem corporativa de outras entidades públicas e privadas. Foram sinalizadas pelo Gabinete Cibercrime concretas mensagens desta campanha, usando abusivamente a imagem da Via Verde, com mais intensidade, a partir da tarde de 7 de outubro de 2022.


Enviada: 07 October 2022 13:56
Para:
Assunto: Utilizações por pagar - Processo Nº: 2018194720 (num prazo de 5 dias).

VIA VERDE
Anda consigo.

Caro Cliente,

Informamos que tem utilizações por pagar, porque tem Identificadores/Contas Mobilidade desativados. Regularize o pagamento online com um cartão bancário, num prazo de 5 dias para evitar multas.

PROCESSO Nº: 2018194720
REFERENCIA Nº: 000382349
MONTANTE: 0.9 Euros
Regularize já o pagamento

Após confirmação do pagamento, receberá um e-mail com a respetiva fatura e o processo ficará concluído.

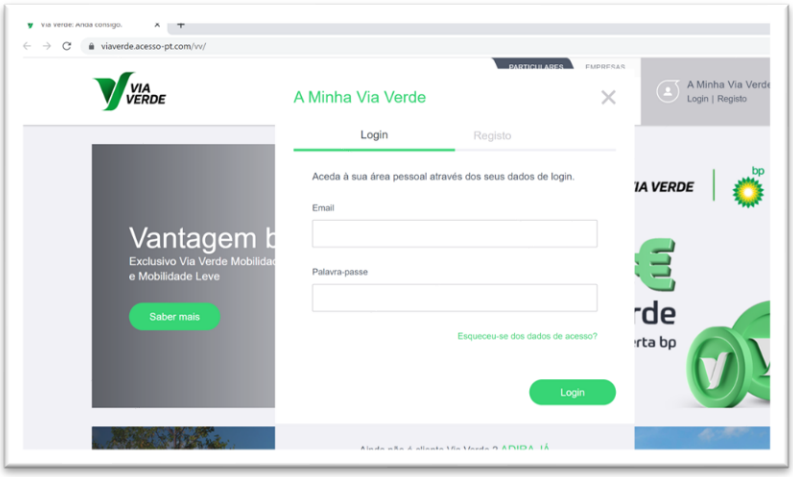
Se esta situação já foi regularizada, por favor considere sem efeito este contacto

3. Nestas mensagens, com o título, no assunto, "*Utilizações por pagar - Processo Nº: 2018194720 (num prazo de 5 dias)*", dirigindo-se as mesmas a "*Caro Cliente*", anuncia-se que "*Informamos que tem utilizações por pagar, porque tem Identificadores/Contas Mobilidade desativados. Regularize o pagamento online com um cartão bancário, num prazo de 5 dias para evitar multas*". Depois, fornecem-se supostas referências de um suposto processo interno, com a referência de uma dívida do *cliente* no valor de 0,9 euros. De seguida, indica-se, de forma destacada um botão com a legenda "*Regularize já o pagamento*" e anexa-se um suposto "*Detalhe de Movimentos*", com indicação de uma data e hora de

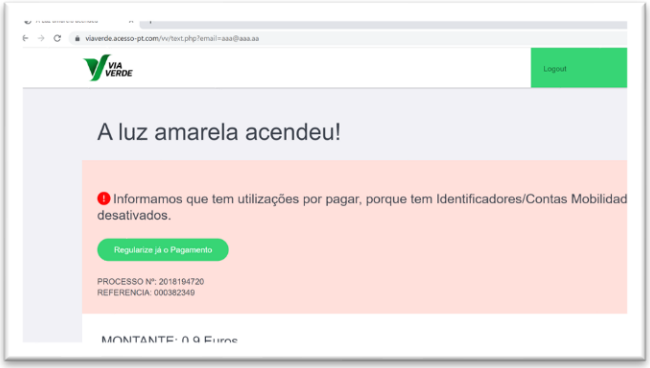
suposta utilização da Via Verde sem pagamento. As mensagens vêm assinadas com a expressão "*©2022 Via Verde*" e, no seu corpo, é incluído o logotipo normalmente utilizado por aquele serviço.

4. Trata-se de mensagens fraudulentas, não provenientes da Via Verde: não foram remetidas pela Via Verde nem a partir de sistemas informáticos com ela relacionados. Aparentemente, tais mensagens foram remetidas de uma caixa de correio "*Via Verde*", mas na verdade não é assim. Provieram de endereços de diversos servidores, ou de contas de correio eletrónico ilegitimamente acedidas pelos criminosos e abusivamente usadas para este específico efeito.

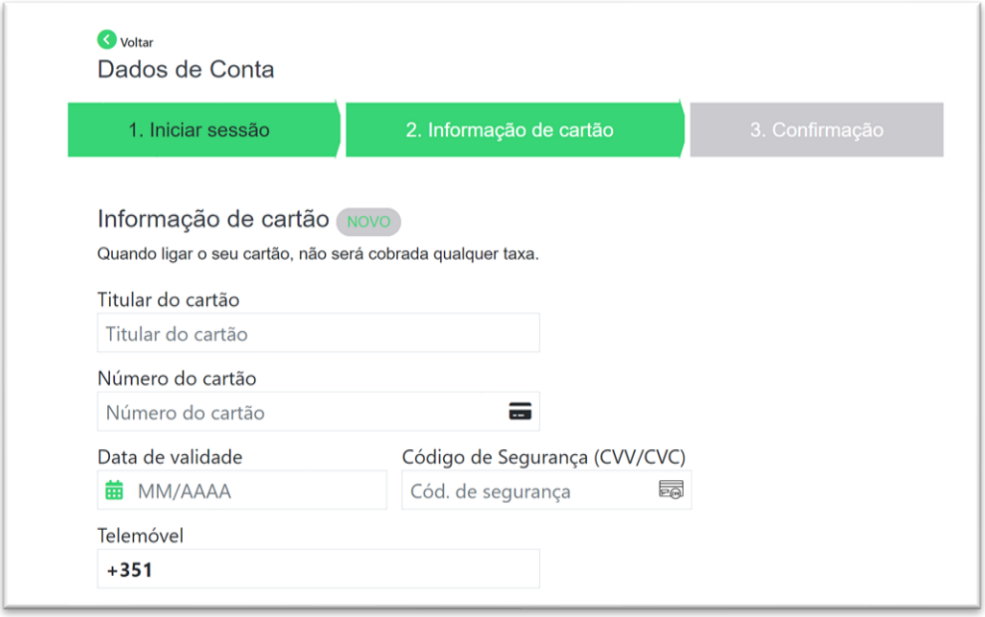
5. Por sua vez, o botão que se referiu, assinalado com a expressão "*Regularize já o pagamento*", contido nas mensagens fraudulentas, incluiu um *link* que conduz a um *site* na Internet que aparenta ser o da Via Verde, exibindo uma imagem gráfica e logotipos normalmente utilizados por aquela. Nessa página, solicita-se ao utilizador que inicie a sua sessão de cliente, como se se tratasse da verdadeira página *web* da Via Verde.



6. Porém, ao contrário do que aconteceria com uma página autêntica, não é necessário introduzir credenciais de acesso verdadeiras ou fidedignas. Se se introduzirem dados falsos ou inventados também é possível aceder à suposta área de cliente, sendo suficiente que se prima o botão "*Login*". Depois de premir este botão, acede-se a nova página, pela qual o utilizador é advertido que de tem uma quantia em dívida, sendo exibido um novo e destacado botão com a menção "*Regularize já o pagamento*".



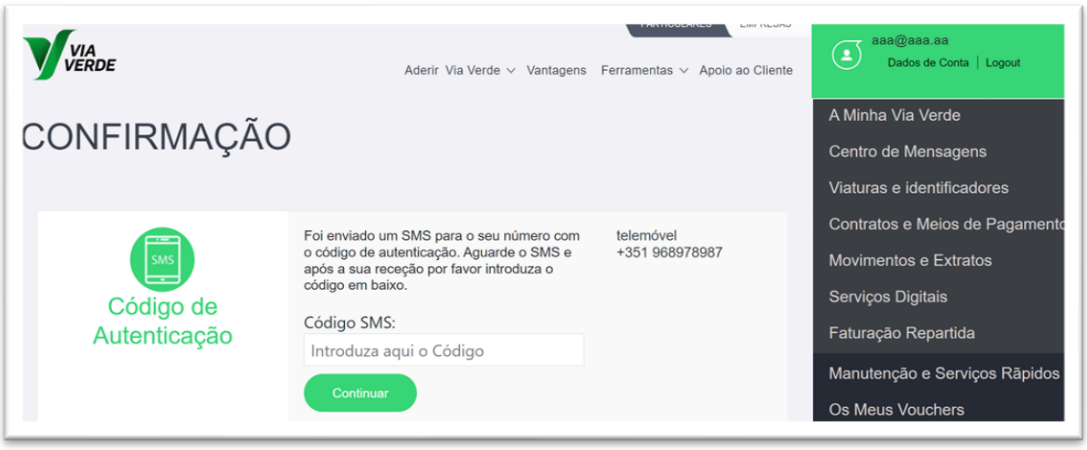
7. Pressionado este último, acede-se a uma nova página na qual, tendo em vista efetuar o referido pagamento, é solicitado ao utilizador / vítima, que introduza os dados do seu cartão de crédito: o nome que nele é mencionado, o número do cartão de crédito, a respetiva data de validade e ainda o respetivo código de segurança (CVV).



8. Este *site* não é gerido pela Via Verde nem é por ela autorizado. Trata-se de uma página falsa, que pretende imitar a respetiva página autêntica. Tem como único propósito captar os dados do cartão bancário da vítima – os quais serão depois abusivamente utilizados pelo agente do crime.
No decurso desta campanha, 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*, sem que possa apurar-se a identidade do seu dono.

9. Como se disse, esta página pretende imitar a aparência, aos olhos do utilizador comum, da autêntica página da Via Verde. 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 bancário, permitindo assim àqueles que utilizem livremente este cartão, em compras ou pagamento de serviços.

10. Aliás, em geral, após o utilizador inserir os dados do seu cartão de crédito naquela página, os agentes criminosos usam imediatamente os mesmos, efetuando, de imediato, compras *online*. Como o procedimento de compras *online* requere, nalguns casos, 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, em que é solicitado que se autentique o pagamento com o código recebido por telefone.



11. Efetivamente, tal como acontece com compras normais e legítimas, por via de cartão de crédito, logo que o criminoso efetua a compra *online* com os dados do cartão da vítima, esta recebe um código, por SMS, para autenticar a mesma. Se o introduzir na página falsa, permite-se ao criminoso autenticar e efetivar aquela compra.

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