# ALERTA CIBERCRIME

## 11 de setembro de 2025

## Obtenção ilícita de dados de cartões de crédito

**(uso abusivo do nome e imagem dos supermercados *Continente*)**

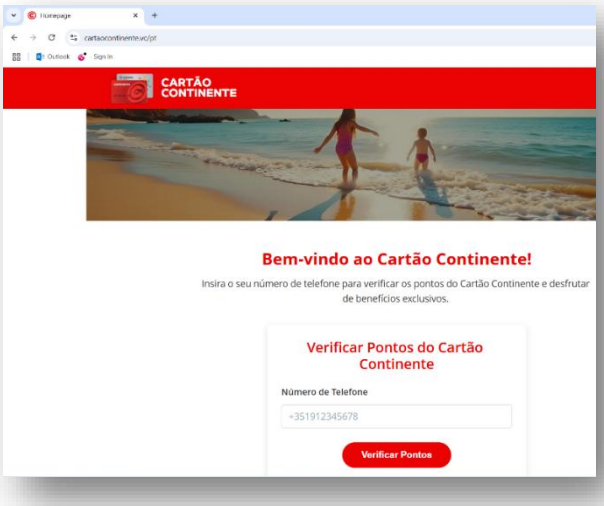
**1.** Está em curso mais uma campanha de *phishing* que têm em vista obter, de forma ilícita, os dados dos cartões de crédito de vítimas indiscriminadas. Esta campanha segue o mesmo modelo de várias outras que ocorreram no passado: abusando de um nome comercial ou empresarial, procura ilicitamente que as vítimas facultem aos agentes criminosos dados de cartões bancários de pagamento. No caso presente, os agentes criminosos utilizam ilicitamente o nome e a imagem dos supermercados *Continente* e do respetivo cartão de fidelização.

**2.** Como em todos os casos de *phishing*, o processo criminoso começa com a expedição, para muitíssimos destinatários, de mensagens fraudulentas – na presente campanha tem sido primordialmente utilizado o serviço telefónico de mensagens curtas (SMS).


**3.** Em tais mensagens, os agentes criminosos incluem informação que leva o destinatário a acreditar que as mesmas foram expedidas pelos supermercados *Continente*. Além disso, das mensagens resulta que o destinatário pode beneficiar de vantagens, concedidas a titulares de cartão de fidelização dos supermercados *Continente*, mas que as mesmas estão prestes a expirar. Incitam pois o destinatário a, de imediato, aceder a um *link* que é facultado. Todas as mensagens referenciadas contém um *link*, a que o destinatário deve aceder. Ao longo dos últimos dias/semanas verificou-se que os *links* foram variando. Porém, todos eles contêm sempre, de alguma forma, a expressão "*cartaocontinente*".

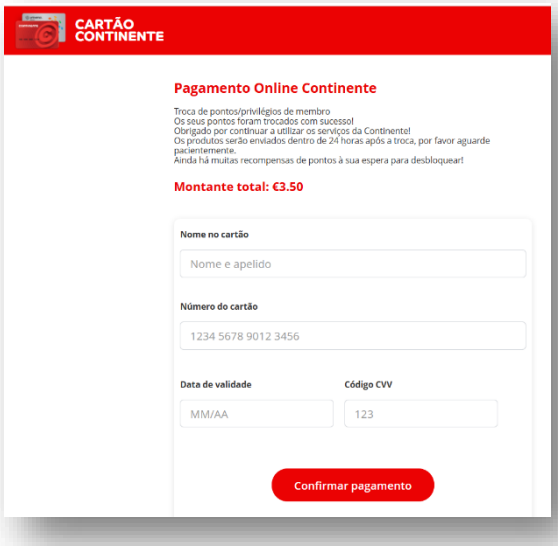
**4.** Estas mensagens são fraudulentas. Não são provenientes dos supermercados *Continente* nem de qualquer entidade ou servidor por eles autorizado a emiti-las. A sua origem é invariavelmente um número de telefone *mascarado*, cuja titularidade legítima pertence a um terceiro, desconhecedor deste procedimento criminoso.

**5.** Por outro lado, os *links* contidos nas mensagens fraudulentas não conduzem à autêntica página, na Internet, dos supermercados *Continente* nem do seu cartão de fidelização. Com efeito, se a vítima aceder a tais *links*, abre uma página que visualmente parece ser a do cartão de fidelização dos supermercados *Continente*. Mas não é: trata-se de uma página *web* fraudulenta, disponibilizada pelos agentes criminosos. Embora o *URL* que conduz a esta página tenha variando ao longo da campanha, sendo utilizados vários endereços *web* diferentes, os mesmos apontam para servidores da chamada *cloud* (que são facilmente geridos pelos agentes criminosos a partir de qualquer parte do mundo).




**6.** Aberta a página fraudulenta, a vítima é informada de que, por ter acumulado pontos no seu cartão de fidelização, pode escolher uma recompensa, tendo para o efeito, apenas, que pagar uma pequena quantia.

**7.** É depois solicitado à vítima que, sucessivamente vá introduzindo diversos dados pessoais. Primeiro, o seu número de telefone e depois o seu nome, morada completa e endereço de correio eletrónico. Este pedido de informações pessoais culmina com a solicitação dos dados do cartão bancário da vítima – 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.




**8.** 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. 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.