MINISTÉRIO PÚBLICO
PORTUGAL
PROCURADORIA-GERAL DA REPÚBLICA
GABINETE CIBERCRIME

ALERTA CIBERCRIME

2 de outubro de 2023

'Phishing' - cartões de crédito do Banco Wizink

1. Está em curso mais uma campanha de *phishing*, desta vez dirigida a titulares de cartões de crédito do Banco Wizink. Os seus autores pretendem convencer as vítimas a facultarem-lhes os dados dos seus cartões de crédito.

2. Como habitual em casos de *phishing*, o processo criminoso começa com a expedição, para muitos destinatários, de mensagens fraudulentas – no caso desta campanha, foram identificadas mensagens de WhatsApp e também mensagens de correio eletrónico.

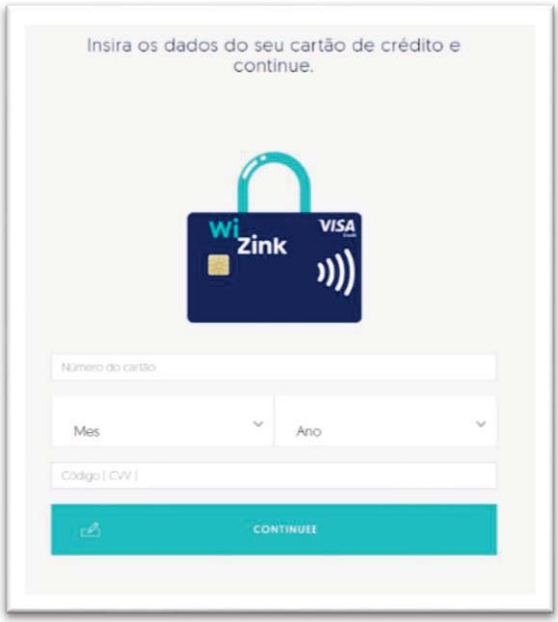
3. No caso das mensagens de correio eletrónico identificadas, sob o título "*Detetada Tentativa de Pagamento Suspeito*", diz-se que "*devido a uma tentativa de pagamento suspeito, suspenderemos o seu cartão de crédito por motivos de segurança. Para reativar o seu cartão, aceda à sua área de cliente e preencha o formulário de reativação*". De seguida indica-se um *link*, ao qual o destinatário deverá aceder.

4. Quanto à modalidade de mensagens curtas identificadas, a comunicação é de idêntico teor: adverte-se o destinatário de que as suas credenciais de utilização irão expirar muito em breve, incitando-se o mesmo a aceder a um *link*, que é indicado, a fim de evitar o "*bloqueio do seu cartão*".

5. Trata-se, evidentemente, de mensagens fraudulentas, não provenientes do Banco Wizink. Não foram remetidas pelo Banco Wizink nem a partir de sistemas informáticos ou números telefónicos pertencentes a esta instituição bancária. Têm como propósito exclusivo o de provocar o acesso aos *links* que indicam. Invariavelmente incitam a uma reação muito urgente no sentido de evitar um suposto bloqueio de um cartão. Com esta abordagem, os agentes criminosos

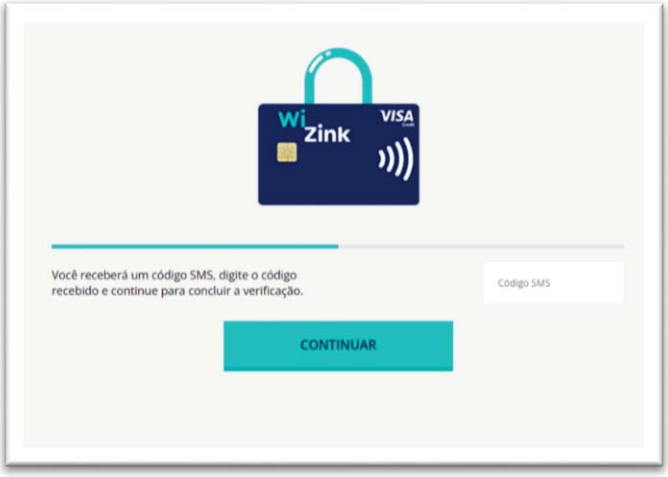
pretendem que os titulares deste tipo de cartões, de forma instintiva e não refletida, sigam de imediato a solicitação que lhes é feita e acedam aos *links* indicados nas mensagens.

6. Tais *links*, contidos nas mensagens fraudulentas, conduzem a s*ites na* Internet que, embora grosseiramente, pretendem aparentar ser o do Banco Wizink, exibindo o logotipo corporativo utilizado por aquele. Estes *sites* incluem espaços em que se solicita a introdução de dados respeitantes à conta: designadamente o nome de utilizador e o código de acesso (*palavra-passe*). Além disso, o utilizador é ainda solicitado a introduzir os dados respeitantes ao seu cartão de crédito: o número do cartão, a respetiva data de validade e ainda o código de segurança (CVV).



7. Como se disse, estas páginas pretendem imitar a aparência, aos olhos do utilizador comum, da autêntica página do Banco Wizink na Internet. Se a vítima nelas introduzir a informação que se lhe solicita, fornecerá aos autores destes factos, além do mais, todos os dados do seu cartão de crédito, permitindo assim àqueles que utilizem livremente este cartão, em compras ou pagamento de serviços.

8. Foram identificados casos em que, imediatamente após o utilizador inserir os dados do seu cartão de crédito naquela página, os agentes criminosos usaram os mesmos, efetuando logo compras *online*.



9. Como o procedimento de compras *online* requere 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, logo depois da introdução dos dados do cartão de crédito na página falsa, abre-se uma nova página, supostamente do servidor do Banco Wizink.
Nesta nova página o utilizador é informado de que *"Você receberá um código SMS, digite o código recebido e continue para concluir a verificação"*, sendo deixado espaço para se inserir tal código.

10. Efetivamente, logo que o criminoso efetua a compra, a vítima recebe um código, por SMS, no seu telefone. Se o introduzir na página falsa permite ao criminoso autenticar e efetivar aquela compra. Porém, recorrentemente, na página surge uma mensagem de erro: "*Código incorreto, você receberá um novo em segundos".* 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.

11. Estes *sites* não são geridos pelo Banco Wizink nem são por ele autorizados. Trata-se de páginas falsas, que pretendem imitar a autêntica página daquela instituição bancária. A generalidade destas páginas está alojada em fornecedores de serviço na chamada *cloud*, sendo possível a sua aquisição e disponibilização a partir de qualquer parte do mundo.

12. Como se disse, este método criminoso tem como objetivo e único propósito capturar os dados dos cartões de crédito das vítimas, para serem usados indevida e abusivamente. Mensagens como as acima descritas devem ser apagadas. Caso o utilizador introduza os dados numa das páginas a que se acede pelos *links* facultados pelos agentes do crime, importará, como primeira diligência a empreender, proceder ao cancelamento do cartão.