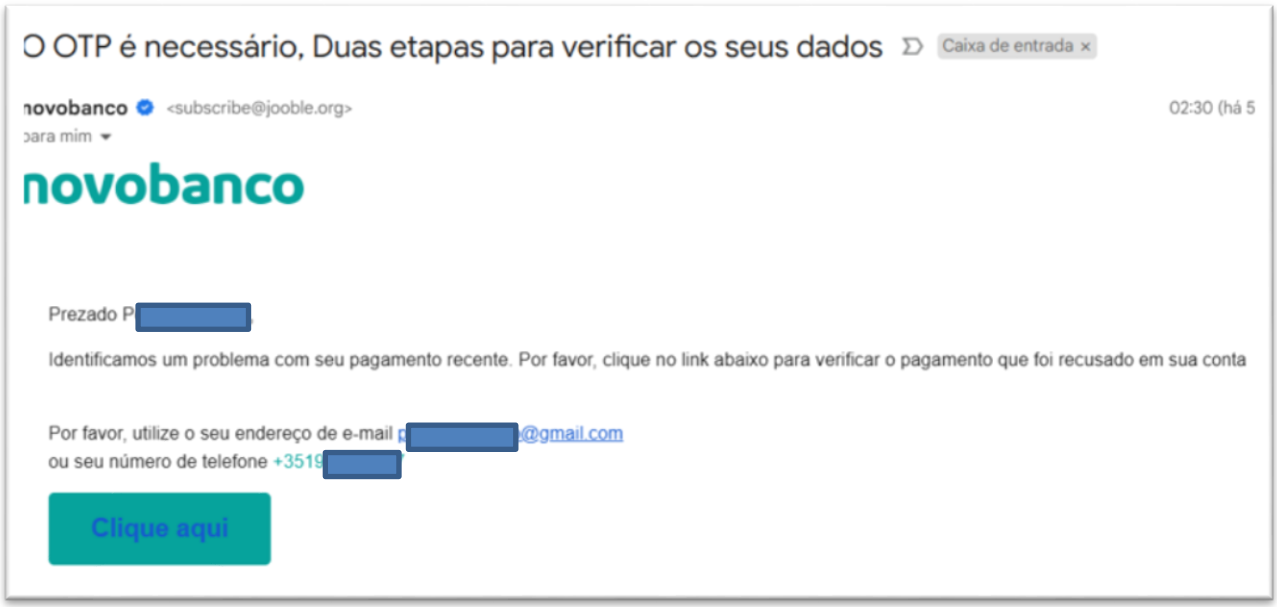
MINISTÉRIO PÚBLICO
PORTUGAL
PROCURADORIA-GERAL DA REPÚBLICA
GABINETE CIBERCRIME

ALERTA CIBERCRIME
17 de julho de 2024
'*Phishing*' dirigido a clientes do Novobanco

1. Está em curso mais uma campanha de *phishing* que tem em vista obter, de forma ilícita, os dados dos cartões bancários de vítimas indiscriminadas. Esta campanha dá continuidade a várias outras, que ocorreram no passado. No caso presente, os agentes criminosos procuram, com a campanha, atingir clientes do *Novobanco* que sejam titulares de cartões bancários de pagamento.

2. Como em todos os casos de *phishing*, o processo criminoso começou com a expedição, para muitíssimos destinatários, de mensagens fraudulentas – em casos anteriores foi utilizado o serviço de mensagens *WhatsApp* ou mensagens de SMS. Na presente campanha foi identificado o uso de mensagens de correio eletrónico. A primeira das mensagens desta campanha sinalizada pelo



Gabinete Cibercrime foi referenciada a 17 de julho de 2024, às 2 horas e 30 minutos.

3. Destas mensagens consta o seguinte texto: "*Identificámos um problema com seu pagamento recente. Por favor clique no* link *abaixo para verificar o pagamento que foi recusado em sua conta.*"
Além disso, a mensagem vem personalizada com o nome do destinatário e, para lhe dar credibilidade, refere ainda "*Por favor, utilize o seu endereço de email xxx@xx.xxx ou o seu número de telefone +351.xxx.xxx.xxx*". Estes dados correspondem efetivamente a cada um dos destinatários da mensagem de correio eletrónico e são autênticos. Trata-se pois de uma campanha criminosa mais agressiva e insidiosa que as anteriores, porque recorre ao uso cirúrgico de dados autênticos das vítimas, obtidos de forma ilícita e desconhecida.

4. Estas mensagens, supostamente remetidas em nome do *Novobanco*, não tiveram origem em qualquer serviço de correio eletrónico daquele banco: a sua origem técnica é o servidor de correio eletrónico *mail11.jooble.com*, propriedade da sociedade de direito americano "*Domains By Proxy, LLC*", com sede em Tempe, Arizona, Estados Unidos da América.

Porém, na verdade, tais mensagens provieram do endereço de IP 185.25.116.20, pertencente à *Hosting Ukraine Infrastructure Network*, propriedade do fornecedor de serviços "*Hosting Ukraine Ltd*.", com sede em Kiev, na Ucrânia.

São pois mensagens fraudulentas, não provenientes do *Novobanco*.

5. Além do texto que se referiu, as mensagens incluem ainda um *link*, destinado a facilitar o acesso à conta bancária do destinatário. Incita-se o destinatário a aceder a tal *link*, para "*verificar o pagamento recusado*". Este *link* conduz a uma página *web* que exibe imagens e logotipos que pretender imitar a imagem normalmente utilizada pelo *Novobanco*.

6. Em tal página, é imediatamente solicitado ao "cliente" que introduza o seu número de telefone, para "continuar". Logo de seguida, abre-se uma nova página em que lhe é solicitado que introduza os dados do seu cartão bancário – o nome que dele consta, o número do mesmo, 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 permitam utilizar o cartão em causa. Uma vez introduzidos estes dados, a vítima é informada de que "*você receberá um OTP para confirmar seus detalhes*".

O acrónimo OTP não é utilizado no comércio jurídico e bancário em Portugal. Corresponde a *One Time Password*, expressão que no circuito bancário português é substituída por *código SMS*, ou *SMS token*, com isto se referindo a um código de utilização única, recebido por via de mensagem telefónica, para validação de transações bancárias.

7. Este *site*, para onde a vítima é conduzida e onde lhe são solicitadas informações, não é gerido pelo *Novobanco* nem por ele foi autorizado. Trata-se de uma página falsa, que pretende simular ser a autêntica página *web* daquela entidade bancária.

Esta página fraudulenta está registada no registrar *Enomdomains* (www.enomdomains.com) pertencente à sociedade de direito canadiano "*Enom Inc*" (https://enom.com), que se dedica à revenda de nomes de domínio e ao serviço de alojamento de domínios DNS na *cloud.* Pertence ao grupo empresarial "*Tucows*", (https://www.tucows.com/), fornecedor de serviços de Internet e telecomunicações baseada em

Toronto, Canadá, mas constituída e registada segundo o direito da Pensilvânia, Estados Unidos da América.

8. Como se disse, aquela página *web* pretende imitar a aparência, aos olhos do utilizador comum, da autêntica página do *Novobanco*. Por este processo criminoso, os seus autores pretendem induzir a vítima a facultar-lhes dados dos seus cartões. Se a vítima introduzir a informação que se lhe solicita (os dados do cartão bancário), estará a facultar aos agentes criminosos informação que lhes permite utilizarem abusivamente os dados daquele cartão, em seu prejuízo.

9. Mensagens como as que acima se descreveram devem ser ignoradas e apagadas, sem resposta. Caso a vítima se aperceba de que acabou por facultar aos agentes criminosos os dados do seu cartão bancário, importará, como primeira diligência a empreender, contactar o banco emissor e proceder ao cancelamento daquele cartão.

10. Foram identificadas situações em que, após a vítima ter introduzido os dados do seu cartão, a mesma foi abordada telefonicamente por alguém que se intitulava como representante do seu banco. Este tipo de contactos são em geral fraudulentos: têm em vista obter da vítima códigos de autenticação por esta recebidos por SMS (*SMS token*), na sequência da utilização ilícita dos dados do cartão, pelos agentes criminosos.
Recomenda-se a avaliação criteriosa de chamadas telefónicas desta natureza: os funcionários das entidades bancárias não solicitam nunca que se lhes faculte códigos recebidos por SMS. Chamadas em que os mesmos sejam solicitados devem ser interrompidas, devendo a vítima contactar o banco em causa pessoalmente ou, se por telefone, por uma outra via.