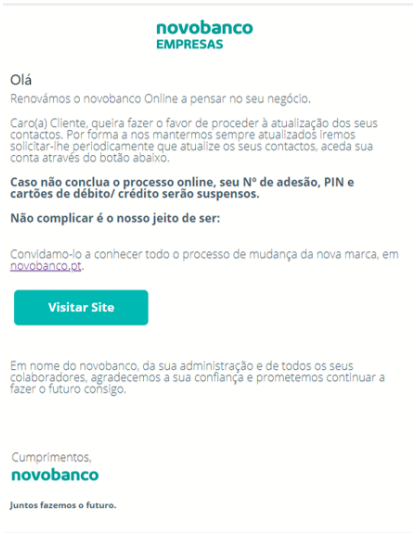
ALERTA CIBERCRIME

13 de janeiro de 2022

'*Phishing*' dirigido a clientes de bancos

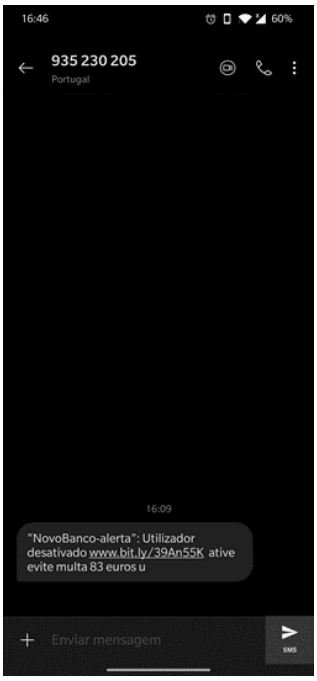
1. Estão em curso diversas campanhas de *phishing*, dirigidas a clientes de bancos estabelecidos em Portugal. Em desenvolvimento de todas elas, a atuação criminosa começou, como habitual, com a remessa, para muitos destinatários, de mensagens fraudulentas de correio eletrónico. Após campanhas dirigidas a clientes do Banco Santander e do Banco Millennium, ainda em 2021, foram sinalizadas pelo Gabinete Cibercrime mensagens de uma campanha dirigida a clientes do Novobanco a partir de 7 de janeiro e, com mais intensidade, a 12 de janeiro de 2022. Do mesmo modo, foi identificada uma outra campanha dirigida a clientes do Bankinter, a 13 de janeiro de 2022.

2. Em todas estas mensagens, os seus emitentes alegam ser representantes dos bancos em causa e solicitam urgência na resposta. Incitam ao acesso à página, ou à aplicação informática, dos bancos e áquilo que chamam de "autenticação", ou "verificação", ou interação de natureza análoga.
Por exemplo, numa mensagem de correio eletrónica supostamente emitida pelo Novobanco, cujo título, no assunto é "*Último Aviso! Seu aplicativo NB-Empresa mudou. Será necessário activar novamente seu registo*", inclui-se o seguinte texto: "*Renovámos o novobanco Online a pensar no seu negócio. Caro(a) Cliente, queira fazer o favor de proceder à atualização dos seus contactos. Por forma a nos mantermos sempre atualizados iremos solicitar-lhe periodicamente que atualize os seus contactos, aceda sua conta através do botão abaixo. Caso não conclua o processo online, seu Nº de adesão, PIN e cartões de débito/ crédito serão suspensos. Não complicar é o nosso jeito de ser*."
Noutra mensagem, supostamente remetida pelo Bankinter, com o título "*A nova atualização do Bankinter - N:8761887386*", dizia-se que "*Você tem uma nova atualização aguardando confirmação. Nosso sistema deteta que você ainda não ativou nosso novo aplicativo de segurança, permitindo que você controle facilmente sua conta online*".



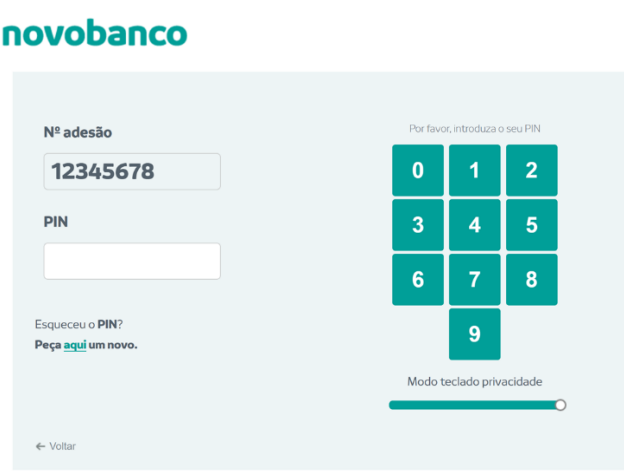
3. Em todas estas mensagens, de uma forma ou de outra, inclui-se sempre um botão com um *link* que, supostamente, deve facilitar o acesso à conta bancária do destinatário.
Tal tipo de mensagens é, evidentemente, de natureza fraudulenta. Não são provenientes de nenhum daqueles bancos nem foram remetidas pelos mesmos, nem a partir de sistemas informáticos a eles pertencentes.

4. Nalguns casos, este tipo de mensagens foi expedido por via telefónica, ou por via de aplicações de mensagens (sobretudo, por WhatsApp). Em todo o caso, embora adaptados ao formato em causa, o propósito das mensagens é exatamente o mesmo: incitar ao acesso a um *link*.



5. Os *links* contidos em todas estas mensagens fraudulentas não conduzem aos sites dos bancos referenciados: na verdade, se abertos, conduzem a s*ites* na Internet com *URLs* diferentes daqueles que aparentam ter, embora sempre encaminhem para páginas *web* que exibem imagens normalmente utilizadas pelos bancos em causa.

6. As páginas *falsas* pretendem parecer as autênticas páginas dos bancos. Nestas campanhas mais recentes, as páginas falsas têm pretendido ter um aspeto correspondente à versão das páginas dos bancos no formato adequado a serem acedidas por telefone ou as respetivas aplicações, igualmente para utilização em *smartphones*.



7. Em todas as situações identificadas, quando se utiliza o *link* incluído nas mensagens fraudulentas, a página *falsa* acedida solicita ao utilizador que introduza as suas credenciais de acesso ao legítimo *site* do banco em causa.
Porém, nenhum destes *sites*, onde tais informações são introduzidas, é gerido por nenhum daqueles bancos nem por eles autorizado.
Se a vítima aceder a eles e neles introduzir a informação que se lhe solicita (os códigos de acesso à conta bancária *online*), fornecerá aos autores destes factos dados de acesso, no legítimo *site* dos bancos, à sua conta bancária. E assim, permitirá que terceiros procedam a movimentos bancários por esta via.

8. A generalidade destas páginas está alojada em fornecedores de serviço na chamada *cloud*, disponibilizada para qualquer utilizador, de qualquer parte do mundo.
Quanto às mensagens de correio eletrónico, da mesma forma, ocorre terem sido emitidos a partir de servidores de *webmail*. Mas foram igualmente identificadas situações em que foram utilizados serviços de email php, baseados, portanto, em páginas *web*.