ALERTA CIBERCRIME

24 de outubro de 2024

'*Phishing*' dirigido a utilizadores da Chave Móvel Digital

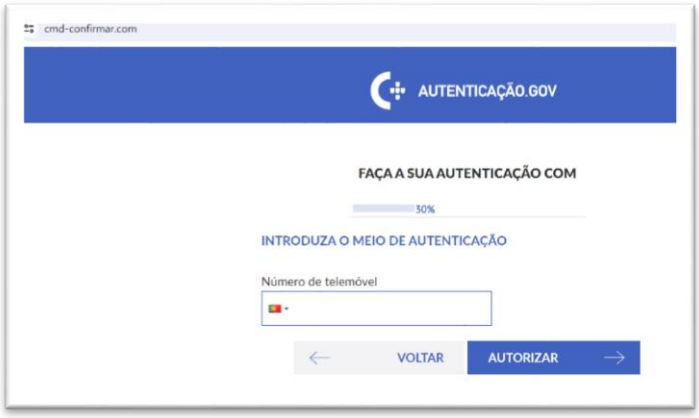
1. Está em curso uma campanha criminosa pela qual, por meio de técnicas combinadas de ***phishing*** e de **engenharia social**, os agentes criminosos procuram aceder de forma ilícita a contas bancárias de clientes de diversos bancos, para delas retirarem montantes monetários.
Não se trata, como tem ocorrido frequentemente noutros casos, de uma mera campanha criminosa para obtenção dos dados de cartões bancários, mas antes de uma iniciativa muito mais sofisticada e agressiva. Este procedimento, que já vem sendo identificado desde o verão, intensificou-se nas últimas semanas.

2. Como na generalidade dos casos de *phishing*, este método criminoso passa pela expedição, para muitíssimos destinatários, de forma indiscriminada, de mensagens eletrónicas fraudulentas – foram sobretudo identificadas mensagens de *WhatsApp*.

3. Como costuma ocorrer com outras campanhas de *phishing*, o teor das mensagens fraudulentas tem evoluído e variado ao longo das semanas, consoante o grupo criminoso que leva a cabo a campanha. Porém, todas elas aludem à Chave Móvel Digital. Em geral, as mensagens informam que, por via da Aplicação Móvel (*Autenticacao.gov*), a Chave Móvel Digital do destinatário da mensagem (vítima) foi ativada num outro aparelho telefónico. Além disso, advertem que "*se não fez esta ativação, vá de imediato a…*" – indicando de seguida um *link* a que o destinatário deve aceder. Estas mensagens pretendem alarmar, apelando à urgência no acesso ao *link* que indicam.

4. Trata-se de mensagens fraudulentas. São muito parecidas com aquelas que os cidadãos habitualmente recebem quando fazem a normal e legítima ativação da Chave Digital Móvel. Pretendem convencer os destinatários de que são mensagens legítimas e autênticas da Agência para a Modernização Administrativa (AMA). Porém, isso não corresponde à verdade: estas mensagens não são remetidas pela AMA nem a partir de servidores desta entidade pública.

5. Quanto aos *links* incluídos naquelas mensagens fraudulentas, supostamente encaminham para a página oficial da AMA e de autenticação da Chave Móvel Digital. Porém, ao aceder aos mesmos, na verdade, a vítima acede a páginas fraudulentas, que imitam a página oficial da AMA.



Nestas páginas, é-lhe solicitado que insira o seu número de telefone. De seguida, é-lhe dada a possibilidade de escolher o seu banco e pede-se-lhe que introduza as credenciais de acesso à sua conta bancária *online*.

Os dados que a vítima insere são capturados pelos agentes criminosos.

6. Os *sites* correspondentes aos *links* indicados vão variando (consoante os fornecedores de serviço Internet onde estão alojados vão detetando o respetivo teor fraudulento e, consecutivamente os vão desativando). Em geral, estão alojados em prestadores de serviço de alojamento gratuito, na *cloud*. Todos eles pretendem imitar a aparência, aos olhos do utilizador comum, da autêntica página da AMA.

7. Após a vítima ter introduzido os seus dados bancários no *site* fraudulento, é informada de que deverá aguardar um contacto telefónico da "*nossa equipa de cibersegurança*" brevemente, "*nas próximas 24 horas*".

8. Efetivamente, foram identificados casos em que, mais tarde, na posse dos dados das vítimas, os agentes criminosos telefonaram para a vítima. Como tiveram acesso às credenciais de acesso à respetiva conta bancária, puderam verificar o respetivo saldo, entre outros dados. Relatando à vítima estes dados, deram credibilidade à sua chamada telefónica.

Depois, informaram a vítima de que foi efetuado um movimento bancário suspeito na sua conta. Perguntaram-lhe se se trata de um movimento por ela efetuado – normalmente, referem um

movimento na ordem de alguns milhares de euros – e, portanto, se o mesmo é para confirmar. Normalmente, esta abordagem causa perplexidade na vítima, que não fez movimento nenhum e fica assustada por poder vir a perder aquela quantia. Por isso, naturalmente refuta tal movimento e, normalmente, pergunta ao seu interlocutor como pode cancelar-se o mesmo. Em resposta, o agente criminoso diz que não pode fazê-lo por mera conversa telefónica, por razões de segurança, mas pode desencadear um processo nesse sentido. Indica-lhe então que irá receber uma mensagem de SMS com um código, o qual deverá indicar-lhe, para autenticar o cancelamento da dita transação fraudulenta.
No entretanto, o agente criminoso procede a uma verdadeira transferência bancária, a partir da conta da vítima, para uma conta por si controlada. Para autenticar a mesma, o sistema bancário *online* emite uma mensagem SMS para o telefone da vítima, a qual, induzida em erro por esta encenação, o fornece ao agente criminoso, que assim autentica a transação.

9. O propósito dos agentes criminosos é transferir quantias das contas bancárias das vítimas para outras, por eles controlada. Por essa razão, inicialmente usam as credencias bancárias da vítima para aceder à conta desta. Porém, como sabem que a transferência de quantias monetárias a partir da generalidade das instituições bancárias exige um segundo fator de autenticação (designadamente um código emitido por SMS para o telefone do respetivo titular), abordam telefonicamente a vítima, como se referiu, procurando induzi-la em erro, com o objetivo de obter esse código.

10. Mensagens de SMS ou *WhatsApp* como as que descreveram devem ser ignoradas e apagadas, sem resposta.
Telefonemas como os que se referiram, que supostamente têm origem em bancos, devem ser cuidadosamente avaliados. A respetiva autenticidade deve ser confirmada com o gestor de cliente, ou outro funcionário ou representante bancário.
Caso a vítima, sem se aperceber, acabe por facultar aos agentes criminosos os dados de acesso à sua conta bancária, importará, como primeira diligência a empreender, alterar as respetivas credenciais de acesso e contactar o banco em causa.