NEWSLETTER
SEGURANÇA

Millennium bcp

NOVEMBRO 2016 Nº 77

English version

É necessário ler atentamente o conteúdo dos SMS's com Códigos de Autorização, antes de confirmar uma operação no homebanking!

Ao longo dos anos, os processos de autenticação segura foram objeto de análise, estudos, testes e, claro, alterações e adaptações.

Certamente, que alguns destes processos vieram complicar a utilização da internet, mas… o intuito é unânime - disponibilizar uma solução de autenticação segura na utilização da internet!

No entanto, mesmo com a aplicação de políticas de segurança decorrentes de regulamentação nacional e europeia, a consciencialização e, alertas sobre os cuidados a adotar na utilização da internet, o ser humano continua a ser o elo mais fraco!

Exemplos de situações recentes experimentadas por clientes do Millennium bcp.

PC infetado com malware:

Durante o acesso ao site do Millennium bcp, surgia uma janela de pop-up a mencionar que era necessário proceder à instalação de um módulo de segurança:

Porque o tema é Segurança, o cliente executava o solicitado! Contudo, para concluir a “Instalação do Módulo de Segurança” era também solicitado um código de autorização:

O atacante solicitava a emissão do código SAFe (Serviço de Autenticação Forte eletrónico), que o Millennium bcp remetia para o número de telemóvel do cliente, com o seguinte conteúdo:

*“Pedido de registo na App Millennium - Cod. Autorização: *******. Contacte o Banco caso não tenha solicitado este código.”.*

O Código de Autorização, recebido via SMS, menciona o registo na App Millennium.

Por desconhecimento (do que é a App Millennium), pela urgência (em “despachar” a instalação fraudulenta do módulo se segurança) ou por boa-fé (porque tem o nome do Millennium bcp), o cliente transcreve o Código de Autorização para a janela fraudulenta.

A instalação do suposto Módulo de Segurança é uma fraude, que tem como objetivo obter um Código de Autorização para o registo na App Millennium, e executar operações na conta bancária do cliente.

Acesso ao site a partir de um link numa mensagem de Correio Eletrónico:

O cliente recebeu uma mensagem de correio eletrónico com links. O cliente acedeu ao link fraudulento para validar o conteúdo da mensagem (neste exemplo, um bloqueio da conta). **Na réplica do site criado pelo atacante** para promover a captura do Código Multicanal, o atacante solicitou três dígitos aleatórios do Código Multicanal e, ao continuar na página, apresentou uma mensagem de erro: "dados inválidos". Solicitou **novas posições do Código Multicanal.** O erro na introdução de dados manteve-se, indicando que a conta estaria bloqueada.

Por fim, o atacante solicitou a emissão do código SAFe (Serviço de Autenticação Forte eletrónico), que o Millennium bcp remeteu

para o número de telemóvel do cliente, com o seguinte conteúdo:

*“MillenniumBCP - Transferência Nacional - IBAN Destino: PT50…. Montante: ****.00 EUR - Código Autorização: *******”.*

Porque a página apresentada é muito idêntica à do site do Millennium bcp esta fraude pode ocorrer por distração do cliente, o qual identifica o Código Multicanal na totalidade, bem como, transcreve o Código de Autorização para executar uma transferência.

Aproveitamos a oportunidade para relembrar que:

- Nunca faculte a terceiros os Códigos de Autorização recebidos por SMS ou obtidos via Token, bem como, leia atentamente todo o conteúdo dos SMS's recebidos com Códigos de Autorização, os quais identificam os dados da operação que registou;
- O Millennium bcp **não envia** mensagens de correio eletrónico (e-mails) com *links*;
- **Nunca aceda** ao *site* do Millennium bcp **através de *links*** de mensagens, motores de pesquisa ou, mesmo, através da opção "Favoritos". Digite sempre o endereço completo www.millenniumbcp.pt ;
- **Não deve fornecer quaisquer dados pessoais ou bancários por telefone** a supostas entidades que o contactem, sugerindo que desligue a chamada e contacte a entidade em causa, por forma a confirmar a veracidade desse contacto;
- Os Códigos de Acesso ao Millennium bcp são pessoais e intransmissíveis pelo que sempre que suspeite que estes possam estar comprometidos, não hesite em alterá-los ou pedir o bloqueio através do serviço de atendimento telefónico ou de uma Sucursal Millennium bcp.

LEMBRE-SE QUE...

Com a época festiva que se aproxima, avizinha-se o aparecimento de falsos questionários, com “ofertas milionárias”, bem como, supostas, transferências pendentes/bloqueadas no banco que aguardam comprovativos do envio do artigo por correio, das compras efetuadas através da internet.

A oferta de presentes/promoções online é bastante usual. Uma mensagem de felicitação por ser o milionésimo visitante, a oferta

de um tablet/smartphone, a atribuição de um prémio em troca do preenchimento de um inquérito ou a promoção de formas rápidas e fáceis de ganhar dinheiro, provavelmente, não serão ofertas fidedignas. Assim, se for “contemplado” com este tipo de oferta(s) e caso lhe peçam para preencher um formulário/inquérito com informações pessoais, não se sinta tentado a fazê-lo, pois, caso tenha começado a introduzir os seus dados e mesmo que não selecione "Enviar", pode já estar a disponibilizar a sua informação a cibercriminosos.

Com a preocupação de encontrar o presente ideal a um preço acessível, cada vez mais se recorre a sites de leilões ou de vendas/compras online. Rápido, cómodo, fácil e de acesso simples, este método permite a consulta de inúmeros anúncios fidedignos de artigos diferenciados, contudo, também disponibilizam **anúncios fraudulentos.** Por muito que as empresas responsáveis por estes sites tentem combater este crime, os cibercriminosos beneficiam quase sempre da fragilidade e do desconhecimento do comum utilizador.

Sobre estes temas e para acautelar surpresas desagradáveis, sugerimos a consulta da Newsletter de Segurança, emitida em novembro de 2015, disponível para consulta em Soluções » Tudo sobre: Newsletters » Segurança.

Lembre-se que a proteção dos seus dados, património, computador e equipamentos móveis depende de si!

Feliz Natal e Próspero Ano Novo!

Fonte: Millennium bcp

elementos identificativos, nomeadamente códigos de acesso. Se receber um e-mail, aparentemente com origem no Millennium bcp, que não esteja de acordo com esta informação, não responda, apague-o e comunique, de imediato, este facto para: informacoes.clientes @ millenniumbcp.pt.

Se não pretende receber este tipo de informação via e-mail ou se pretende alterar o seu endereço eletrónico, aceda ao Homebanking no site do Millennium bcp e, no menu "Área M", selecione a opção "Criar / Alterar e-mail".

Versão portuguesa

You should carefully read the contents of the SMSs with Authorisation Codes, before confirming a transaction on the website!

Throughout the years, the secure authentication procedures have been analysed, studied, tested and, of course, altered and adapted.

Some of these procedures have obviously made online banking more complicated, but... it is all for a common purpose - to provide you with a secure authentication solution for online banking!

Yet, even with the adoption and use of security policies resulting from the Portuguese and European regulation, increased awareness and warnings about precautions to take when using online banking, the human being is still the weakest link!

Here are some examples of situations involving Millennium bcp customers recently

PC infected with malware:

While a Client was using Millennium bcp's website a pop up told him to install a security module:

Because the message is about security, the Client does what the message tells him to do! Yet, to finish "Installing the Security Module" he is required to enter an authorisation code:

The hacker requests a SAFe Code (Strong Authentication System), which Millennium bcp sends to the Client's phone number, with the following text:

*“Pedido de registo na App Millennium - Cod. Autorização: *******. Contacte o Banco caso não tenha solicitado este código.”*
*(Request to register the Millennium App - Authorisation Code: *******. Contact the Bank if you did not request this code)*

The Authorisation Code, received via SMS, mentions the registration of the App Millennium.

Due to ignorance (of what the Millennium App is), to the urgency (to get on with the fake installation of the security module) or to good faith (because it is all done using the name Millennium bcp), the Client enters the Authorisation Code in the fake pop up window.

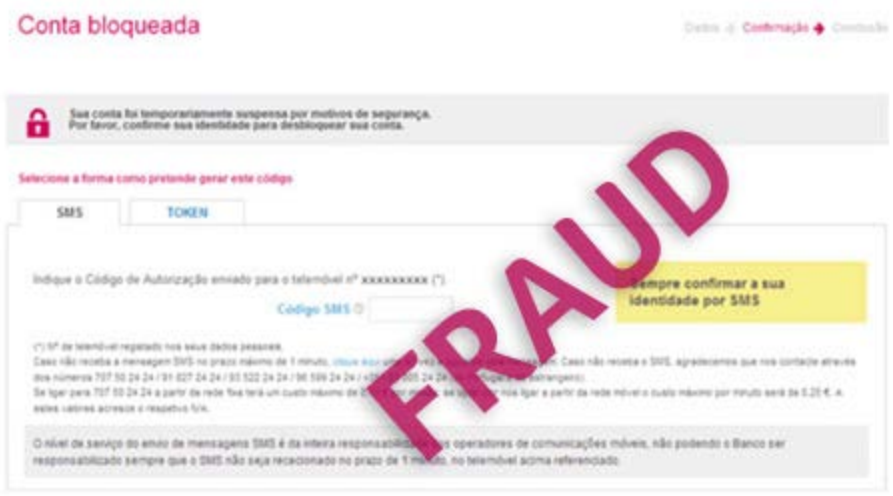
The installation of the so called Security Module is a fraud, aiming to get an Authorisation Code for the registration of the Millennium App and to carry out transactions using the Client's bank account.

Access to the website from a link on an e-mail:

Our Client receives an e-mail with links. The Client opens the fake link to validate the contents of the message (in this example, a blocked account). **In the replica of the website created by the hacker** to capture the Multichannel Code, the hacker requests three random digits of the Multichannel code and when the Client hits next, an error message comes up: "dados inválidos" (invalid data). The hacker asks for **different positions of the Multichannel Code.** The error while entering the data remains and it shows that the account is blocked.

Finally the hacker requests a SAFe Code (Strong Authentication System), which Millennium bcp sends to the Client's phone number, with the following text:

*“MillenniumBCP - Transferência Nacional - IBAN Destino: PT50…. Montante: ****.00 EUR - Código Autorização: *******”*
*(MillenniumBCP - Domestic Transfer - Destination IBAN: PT50…. Amount: ****.00 EUR - Authorisation Code: *******).*



This fraud may result out of good faith (because the fake website is identical to that of Millennium bcp) and due to the Client's distraction, which makes him enter the Multichannel Code in full as well as enter an Authorisation Code for a transfer.

We also take advantage of this opportunity to remind you that:

- You should never provide the Authorisation Codes received via SMS or Token to third parties, and you should carefully read the contents of the SMSs with the authorisation codes identifying the data of the operation you requested;
- Millennium bcp **does not send** e-mail messages with links;
- You should **never open** Millennium bcp's website **through links** on messages, search engines or even through your "Favourites". Always type the complete address www.millenniumbcp.pt;
- **You should never provide personal or bank data by phone** to alleged entities that contact you and we suggest that you disconnect the call and contact the entity in question to verify the authenticity of the contact made.
- Access codes for Millennium bcp are personal and not transferable, therefore should you suspect that they have been compromised, please change them as soon as possible or request that they be blocked using the phone channel or at a Millennium bcp branch.

Source: Millennium bcp

REMEMBER...

With the holidays fast approaching, we can anticipate the fake questionnaires, offering "great amounts", as well as transfers that are allegedly pending/blocked by the bank or waiting for proof of the item being sent by e-mail, after some online shopping.

Offering gifts / promotions online is also quite usual. Messages congratulating you for being visitor nr. 1 million, offering a Tablet or

Smartphone, a prize being given in exchange for answering a survey or promoting quick and easy ways to make money, are probably not trustworthy offers. Therefore, should you be "gifted" some of these offers or asked to answer a survey/inquiry with personal information, do not feel tempted to do so, because just by entering your data, even if you have not yet hit "send", you may already be providing your personal information to cyber-criminals.

Determined to find the ideal gift at an accessible price, people increasingly go to auction websites or to online shopping websites. Fast, comfortable and easy, this method enables the consultation of countless trustworthy offers of different articles but also leads to **fraudulent offers.** No matter how hard the companies responsible for this type of websites try to fight this crime, cyber-criminals are able to almost always take advantage of the fragility and lack of knowledge of the common user.

Regarding these issues and to take precautions against unpleasant surprises, we suggest that you read the Security Newsletter published in November 2015, available at M Tab » Security » All about » Security Newsletters.

Remember: the protection of your data, assets, computer and mobile devices depends on you!

Merry Christmas and Happy New Year!

Source: Millennium bcp