NEWSLETTER
SEGURANÇA

Millennium bcp

NOVEMBRO 2015 Nº 73

English version

Em época festiva a troca de lembranças e presentes determina um aumento da atividade económica, com o inerente agravamento de situações de risco para os utilizadores da Internet, que nos deve levar a redobrar a atenção e os cuidados a ter na utilização deste canal.

SEGURANÇA EM TRANSAÇÕES *ONLINE*

Com a preocupação constante 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.

Como era previsível, os cibercriminosos também encontraram uma oportunidade neste tipo de sistema, começando a desenvolver fraudes mais ou menos elaboradas.

Algumas das fraudes mais frequentes utilizadas em *sites* de leilões ou de compra e venda de artigos são:

Conta falsa: Conta/página do vendedor aberta com dados e documentos falsos, oferecendo mercadorias muito atrativas (qualidade e preço), com o único intuito de receber o pagamento adiantado (numa conta também aberta com documentos falsos), a qual é encerrada depois de receber o valor. Os cibercriminosos têm a vantagem de poder aplicar este golpe várias vezes antes de encerrar a conta/página, uma vez que a receção das mercadorias demora algum tempo antes que a vítima (comprador) se aperceba da fraude. Para evitar este tipo de situações, verifique antecipadamente se existem mensagens de alerta ou comentários de outros utilizadores sobre o vendedor em questão, confirme se existe algum sistema de avaliação do vendedor sobre os produtos já adquiridos e desconfie de preços questionavelmente baixos.

Páginas adulteradas: Ofertas publicadas utilizando falhas deste tipo de *sites*, que fazem com que as ofertas pareçam verdadeiras. Na realidade redirecionam a vítima para outro endereço (URL) onde é aplicado o golpe e solicitando, como sempre, o pagamento adiantado de uma mercadoria que não existe. Esteja alerta para qualquer alteração na apresentação da página do *site* ou para o endereço apresentado na linha do *browser* (URL).

Triangulação de pagamentos: Trata-se de um esquema bastante elaborado. Neste método, o cibercriminoso:

1. Procede à negociação da compra da mercadoria com a vítima (vendedor), solicitando-lhe o número da conta de depósitos à ordem para fazer o pagamento adiantado;

2. Publica num *site* a venda de uma mercadoria inexistente e, obtendo o interesse de outras vítimas, pede para fazerem o pagamento na conta de depósitos à ordem que a primeira vítima forneceu;

3. Assim que o pagamento é feito, solicita o envio da mercadoria à primeira vítima (normalmente a entrega é numa morada no estrangeiro).

Quando as vítimas das vendas inexistentes denunciam a fraude, a primeira vítima para além de perder a sua mercadoria, pode ter que devolver o montante recebido.

Pagamento com fundos desviados: Utilizando *software* malicioso instalado nos computadores das vitimas ou mesmo encaminhando-as para *sites* fraudulentos (por meio de *spam*) os cibercriminosos conseguem obter os Códigos de Acesso/*Passwords* (por meio de *phishing*) e aceder aos *sites* bancários. Com o acesso às contas bancárias das vítimas efetuam

pagamentos de mercadorias a particulares ou pequenas empresas, por meio de transferências bancárias. Ocorrendo transações com este tipo de esquemas, o vendedor poderá ter problemas com os bancos e autoridades, podendo passar:

1. Por ser processado por participação em atividades ilícitas;

2. Pelo bloqueio da conta bancária durante a investigação. As autoridades podem ordenar o bloqueio da conta e dos valores existentes;

3. Pela incapacidade de movimentar a conta bancária o que pode originar um encargo financeiro significativo.

A finalidade de todos os esquemas acima descritos é obter o artigo (carros, telemóveis, jogos, computadores, etc) sem efetuar o respetivo pagamento.

Na maioria das vezes e por forma a credibilizar estes esquemas, remetem à vítima mensagens de correio eletrónico fraudulentas usando a marca de instituições bancárias ou outras entidades idóneas.

Estes são alguns exemplos de **mensagens fraudulentas, emitidas com o nome do Millennium bcp,** a indicarem à vítima que o montante só será creditado após a disponibilização do comprovativo de envio do artigo:

Exemplo 1

Caro
NIB - Número de Identificação Bancária

Este e-mail confirma que você tem um pagamento pendente, a partir de Transac ID: **W47Q2GZA2Q8A4**. O status atual da transação é de * **PENDENTE** * O fundo foi debitado da conta do comprad aguardan ora a t ferê para a frente a sua conta do MILLENNIM BCP após a confirmação de remessa para fins de segurança.

Você agora são obrigados a enviar a mercadoria para o endereço confirmado mprador e ie-nos uma prova de transferência, tais como o número de referência de código / recibo de confirmação de envio, isso é sário para a ficação d pedição no outro para transferir os fundos em questão a sua conta imediatamente.

Você tem MILLENNIM BCP autoridade garantia de 100%, ap cont de envio, a sua conta será creditado imediatamente a seguir.

MILLENNIM BCP Security Center está u io para ar que assim que receber os detalhes, vamos continuar com o credenciamento da sua conta MILLENNIM BCP.

Você tem garantia de 100% de MILLE BC idade.

AVISO IMPORTANTE: Uma este requis mprido n imas 12 horas, os recursos serão liberados em sua conta instantaneamente. Não enviar e-mail / envia o agente do comprador o número de mento de envio a tenhamos completamente creditado a sua conta para fins de segurança. Por favor, entenda que estamos tomando essa medida para proteger ambas as Devida para lo melhor.

Para mais informações, p clique e rever o nosso departamento deconta: serviço@millenniumbcp.pt

O millenniumbcp.pt é um serviço do Banco Comercial Português S.A.
Estamos em processo de adoção do Novo Acordo Ortográfico

Exemplo 2

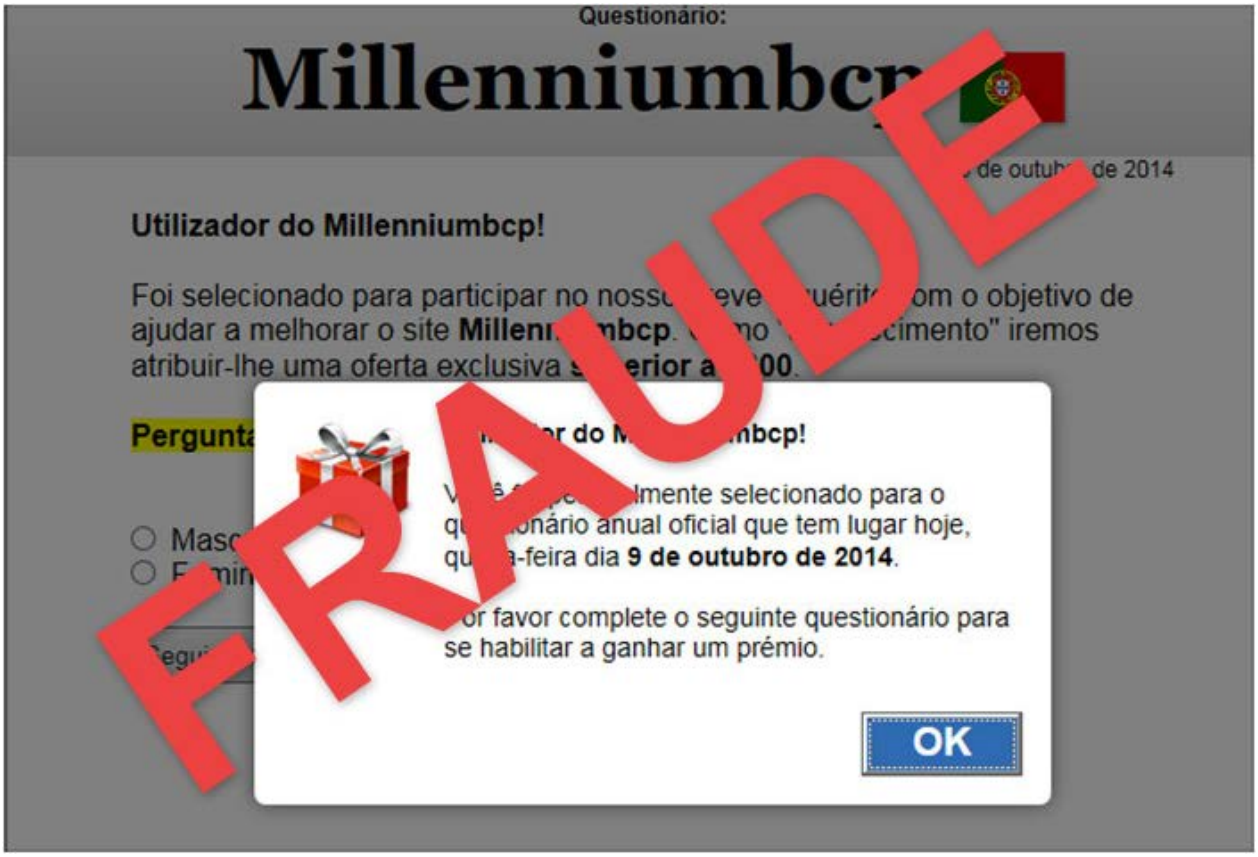
Esclarecemos que o objetivo das instituições bancárias é proceder em conformidade com a instrução de transferência, cujo crédito não é passível de ficar pendente a aguardar instruções de terceiros (particulares), pelo que qualquer instrução nesse sentido constitui uma tentativa de fraude.

INQUÉRITOS FRAUDULENTOS

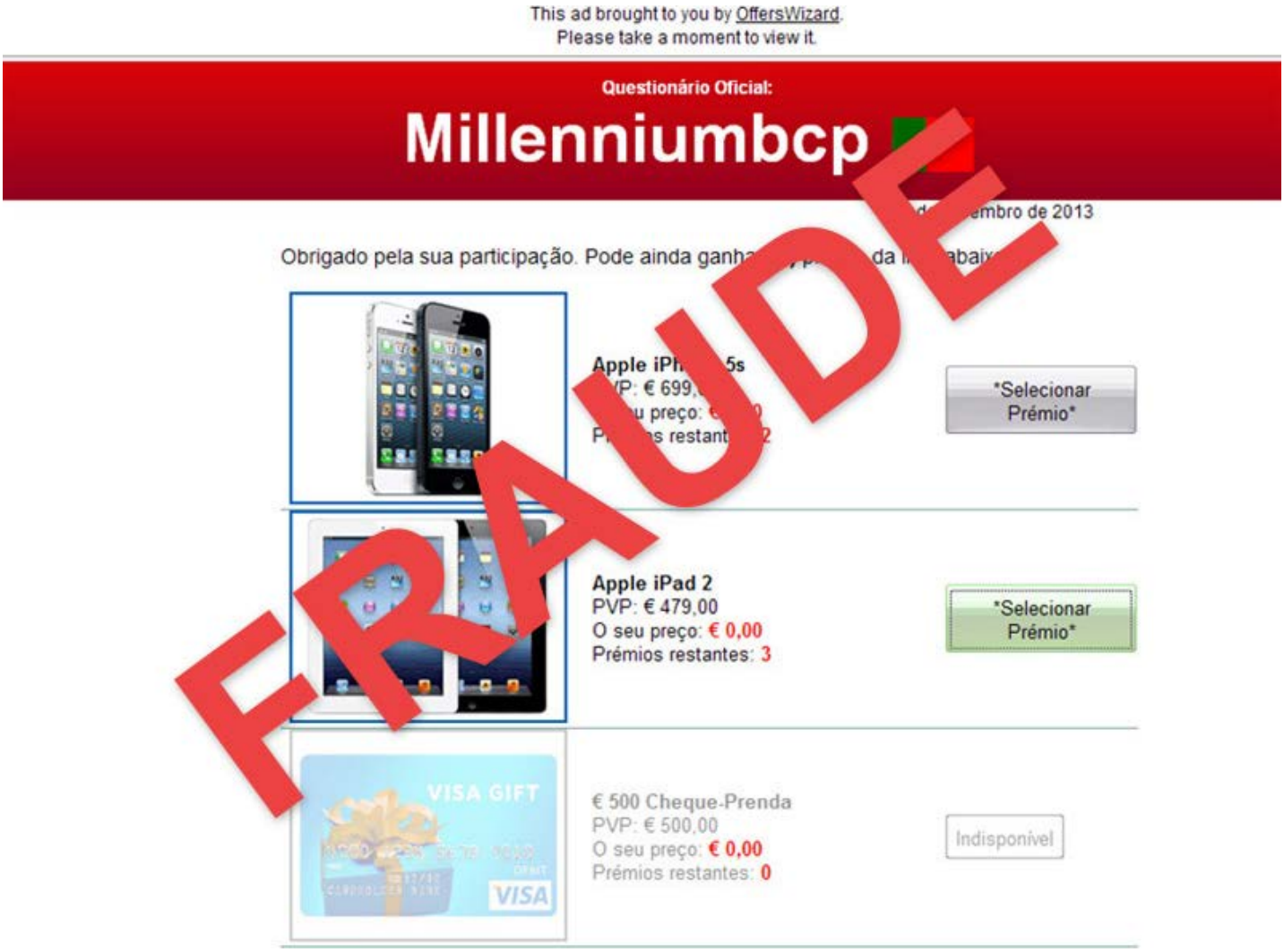
Neste período a oferta de presentes *online* também é bastante usual. Uma mensagem de felicitação por ser o milionésimo visitante, a oferta de um *tablet*/*smartphone*, a atribuição de um prémio em troca do preenchimento de um inquérito ou a promoção de formas rápidas e fáceis de ganhar dinheiro, provavelmente, não serão ofertas fidedignas. Pelo que 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.

Alguns exemplos de inquéritos fraudulentos, utilizando o nome do Millennium bcp:

Exemplo 1


Questionário:
Millenniumbcp
Utilizador do Millenniumbcp!
Foi selecionado para participar no nosso
ajudar a melhorar o site
atribuir-lhe uma oferta exclusiva
Pergunta
OK
FRAUDE

Exemplo 2


This ad brought to you by OffersWizard.
Please take a moment to view it.
Questionário Oficial:
Millenniumbcp
Obrigado pela sua participação.
Apple iPad 2
PVP: € 479,00
O seu preço: € 0,00
Prémios restantes: 3
Selecionar Prémio
€ 500 Cheque-Prenda
PVP: € 500,00
O seu preço: € 0,00
Prémios restantes: 0
Indisponível
FRAUDE

Aproveitamos a oportunidade para relembrar que:

- O Millennium bcp **não envia** mensagens de correio eletrónico 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 ww w.millenniumbcp. pt;
- **Leia atentamente** o conteúdo dos SMS's recebidos com Códigos de Autorização, uma vez que os dados da operação são identificados no texto do SMS;
- **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;
- Atingindo as três falhas consecutivas de PIN, a App Millennium só pode ser desbloqueada através da introdução de um **código PUK** o qual está disponível para consulta em millenniumbcp.pt, após login, menu Área M, Consultar PUK APP;
- **Caso precise de reinstalar a App Millennium**, por exemplo, por atualização do sistema operativo do *smartphome/tablet* é necessário que proceda ao "Desbloqueio da App Millennium", operação disponível em ww w.millenniumbcp. pt e, após login, menu Área M. Na recente versão da App em IOS já não é necessário este procedimento.

Desejamos um Feliz Natal e Próspero Ano Novo!

Fonte: Millennium bcp

LEMBRE-SE QUE...

Se verificar alguma situação anómala em ww w.millenniumbcp.pt ou nas App's do Millennium bcp, por favor contacte-nos através do telefone 707 50 24 24 (Atendimento personalizado 24 horas).

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

Fonte: Millennium bcp

SERVIÇO DE ALERTAS
QUER ESTAR SEMPRE INFORMADO?

siga-nos no facebook

MOBILE

Esta informação é da responsabilidade do Millennium bcp.

Versão portuguesa

During the holidays, the exchange of gifts determines an increase in the economic activity with the consequent aggravation of risk situations for internet users. This must lead us to double our attention and care when using this channel.

SAFE ONLINE TRANSACTIONS

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.

As predicable, cyber-criminals also saw a window of opportunity in this type of system and began to develop frauds which are increasingly tricky.

Some of the most frequent frauds using auction and shopping websites are:

False Account: Seller's account/page opened with false data and documents offering very attractive products (quality and price)

with the single purpose of receiving a payment in advance (to an account also opened using false documents) which is closed after the amount in question is credited. The cyber-criminals have the advantage of being able to use this scam several times before closing down the account/page, because the reception of the products takes some time, and before the victims (buyers) become aware of the fraud. To avoid this type of situations, verify in advance if there are any alert messages or comments made by other users regarding the seller in question and confirm if there is some type of system to rate the seller or review the products already sold and beware of questionably low prices.

Fake Pages: Offers published using breaches in this type of website that make the fake offers look real. In fact they redirect the victim to another website (URL) where the scam is made, which, as always, requests the advance payment of a product that does not exist. Remain alert for any changes to the layout of the website or to the website address in the browser (URL).

Payment Triangulation: This is quite a complex scheme. Through this method, the cyber-criminal:

1. Negotiates the purchase of the products with the victim (seller) and requests the seller's current account number in order to make the advance payment;

2. Publishes in a website the sale of a merchandise that does not exist and, when this captures the attention of other victims, the cybercriminal requests that they pay for the product using the current account supplied by the first victim;

3. As soon as the payment is completed the criminal asks the first victim to send the product to him/her (usually to a foreign address).

When the victims of the inexistent sales report the fraud, the first victim may have to return the amounts received, besides having lost the merchandise.

Phishing and Transfer scams: Using malware installed in the victims' computers or even by forwarding them to fake websites (using spam) cyber-criminals can get access codes/passwords (via phishing) to gain access to bank websites. With this access they use the victims bank accounts to pay for merchandise bought to individuals or small companies, by bank transfer. In the event of this type of scheme, the seller may get into trouble with the banks or authorities, and may risk:

1. Being charged with participating in illegal activities;

2. The bank account being blocked during the investigation. The Authorities ordering that the account and values deposited in it be blocked;

3. Being prevented from using the bank account, which may result in significant financial cost.

The purpose of the above mentioned schemes is to get the item (cars, mobile phones, games, computers, etc) without paying for them.

In most cases, wishing to make the schemes look more credible, they send the victims fake e-mails using the brands of well reputed banking institutions or other institutions.

Examples of **fake messages, sent using Millennium bcp's name,** informing the victims that the amounts would only be credited after they provide a proof of having sent the item:

Example 1

Caro
NIB - Número de Identificação Bancária
0033 0000 [redacted] 05

Este e-mail confirma que você tem um pagamento pendente, a partir de [redacted] Transac[redacted] ID: **W47Q2GZA2Q8A4**. O status atual da transação é de * **PENDENTE** * O fundo foi debitado da conta do comprador aguardan[redacted]ora a t[redacted]ferê[redacted] para a frente a sua conta do MILLENNIM BCP após a confirmação de remessa para fins de segurança.

Você agora são obrigados a enviar a mercadoria para o endereco confirmado [redacted]mprador e[redacted]ie-nos uma prova de transferência, tais como o número de referência de código / recibo de confirmação de envio, isso é [redacted]esário para a [redacted]ficação d[redacted]pedição no outro para transferir os fundos em questão a sua conta imediatamente.

Você tem MILLENNIM BCP autoridade garantia de 100%, ap[redacted] cont[redacted]de envio, a sua conta será creditado imediatamente a seguir.

MILLENNIM BCP Security Center está u[redacted]eio para [redacted]ar que assim que receber os detalhes, vamos continuar com o credenciamento da sua conta MILLENNIM BCP.

Você tem garantia de 100% de MILLE[redacted] BC[redacted]idade.

AVISO IMPORTANTE: Uma [redacted] este requis[redacted]mprido na[redacted]imas 12 horas, os recursos serão liberados em sua conta instantaneamente. Não enviar e-mail / envia o agente do comprador o número de [redacted]mento de envio a[redacted]tenhamos completamente creditado a sua conta para fins de segurança. Por favor, entenda que estamos tomando essa medida para proteger ambas as [redacted] Devida[redacted]e para [redacted]lo melhor.

Para mais informações, p[redacted] clique e rever o nosso departamento deconta: serviço@millenniumbcp.pt

O millenniumbcp.pt é um serviço do Banco Comercial Português S.A.
Estamos em processo de adocão do Novo Acordo Ortográfico

Example 2

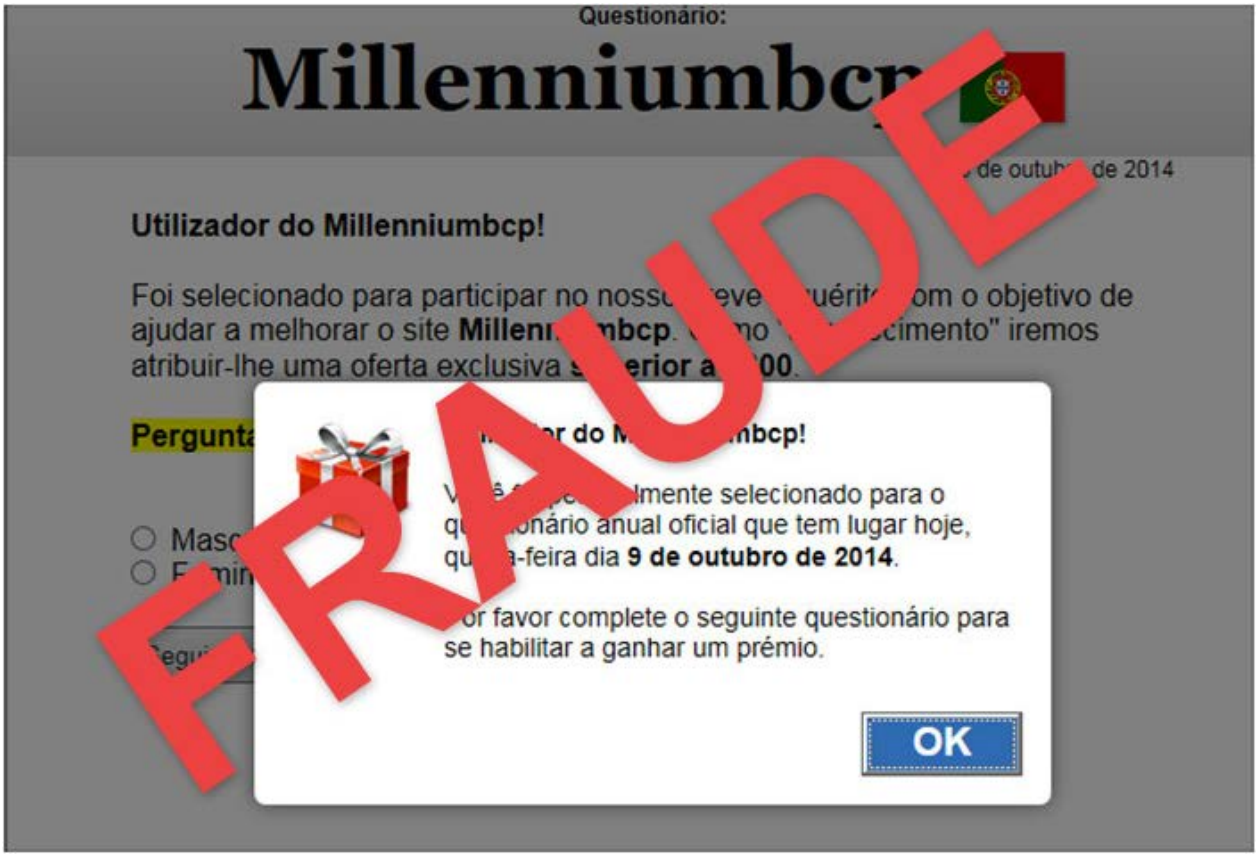
We would like to clarify that the purpose of the banking institutions is to act in accordance with the transfer order, and the credit of the amount cannot depend on instructions given by third parties (individuals), therefore any such instruction represents an attempt to commit fraud.

FALSE SURVEYS

During the holidays, the offer of online gifts 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 "chosen" for 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.

Below are some examples of fraudulent survey messages using the Millennium bcp brand:

Example 1



Example 2

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

- 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 ww w.millenniumbcp. pt;
- Please **read carefully** the SMS received containing the Authorisation Codes since the transaction data are identified in the SMS;
- **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;
- When the PIN code is wrong three times in a row, the Millennium App can only be unlocked using a **PUK code** that can be viewed at millenniumbcp.pt, after the login, menu M, View PUK APP;

- **If you need to reinstall the Millennium App**, for instance, due to an update of the smartphone/tablet's operating system, you must "Unlock the Millennium App", which is available at ww w.millenniumbcp. pt, after the login, on menu M. The most recent version of the App for IOS no longer requires this procedure.

We wish you a Merry Christmas and a Happy New Year!

Source: Millennium bcp

REMEMBER...

If you ever find something out of place at ww w.millenniumbcp. pt/en or on Millennium bcp's Apps, please call us on 707 50 24 24 (Personal Assistance 24/7).

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

Source: Millennium bcp

Millennium bcp is resposible for this information