NEWSLETTER SEGURANÇA

Millennium bcp

MAIO 2015 Nº71

English version

O termo *Phishing* é utilizado para descrever ataques efetuados por *e-mail* que, por norma, são enviados em nome de uma pessoa/entidade supostamente confiável, como um amigo, um banco, um provedor de serviços, etc...

Estes *e-mails* podem conter o logotipo/marca de uma entidade fidedigna levando o utilizador a aceder a um *link*, a abrir um anexo ou a responder a uma mensagem. Este tipo de ação não tem um alvo específico, pelo que, quantos mais *e-mail*s forem enviados pelos atacantes cibernéticos, mais pessoas/entidades são defraudadas.

As ações de *Phishing* podem ter finalidades distintas. Contudo, destacamos aqui algumas que são dirigidas a *sites* bancários:

Obtenção de dados pessoais

Após persuadir o destinatário a aceder a um *link*, redireciona-o para uma página de *Internet* onde podem ser solicitados Códigos de Acesso, passwords, ou, dados pessoais como,

Trata-se de dois casos de *Phishing* com recurso à instalação de *malware* que adultera os navegadores (*browsers*) no acesso a *sites* bancários.

Os *links* das mensagens dão acesso a uma **página fictícia** da EDP ou dos CTT, a partir da qual é efetuado o download de um ficheiro que contém software malicioso. Ao executar o mesmo, irá proceder à instalação do malware no computador.

No acesso ao *site* do Millennium bcp verificámos que era solicitado o **Código de Utilizador** e, após continuar na página, três dígitos aleatórios do **Código Multicanal,** seguido de um erro de **"dados inválidos", solicitando os outros quatro dígitos do Código Multicanal,** bem como o **número de telemóvel do utilizador**.

Após a identificação do número de telemóvel o utilizador recebe um SMS, que contêm um *link*, a solicitar a instalação de uma Aplicação de Segurança no telemóvel. **Esta suposta aplicação, reencaminha os SMS's com os Códigos de Autorização para outro número de telemóvel ou via**

por exemplo, o número do cartão de crédito. Estas páginas parecem legítimas, tendo inclusive a mesma aparência e funcionalidades do *site* que costuma visitar.

Disponibilizamos alguns exemplos de mensagens fraudulentas, **supostamente** emitidas pelo Millennium bcp:


To:
Subject: Pagamento 270,50 Euro
From: Pagamento-bcp@local-bcp.pt
Date: Wed, 0 Apr 2015 00:00:00 +0200

Prezado Cliente,

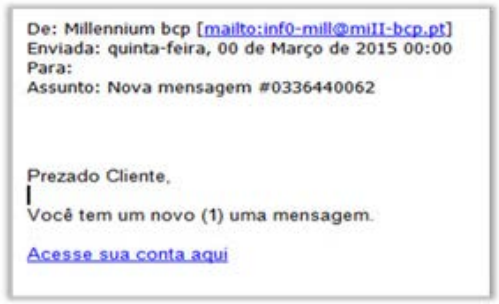
Você recebeu um reembolso de imposto.
Clique aqui para receber.


Date: Fri, 00 Mar 2015 00:00:00 +0900
To:
Subject: Mensagem - #00582245
From: bnc-mill@info-mill-comerical.pt

Notificação

Prezado Cliente,

Você recebeu uma nova notificação.
Clique aqui para resolver o problema.


De: Millennium bcp [mailto:inf0-mill@miII-bcp.pt]
Enviada: quinta-feira, 00 de Março de 2015 00:00
Para:
Assunto: Nova mensagem #0336440062

Prezado Cliente,

Você tem um novo (1) uma mensagem.

Acesse sua conta aqui

Ao aceder aos *links* destas mensagens, é apresentada uma página de *login*, **semelhante à apresentada pelo Millennium bcp**, mas localizada noutro *site* (URL), sendo solicitado o **Código de Utilizador** e, após continuar na página, **o Código Multicanal completo** bem como **um Código de Autorização, obtido via SMS ou Token para, supostamente, "restituição do imposto" ou "Desbloqueio da conta"**.

Contudo, o texto do SMS contém um Código de Autorização para confirmar uma transferência.

internet para um destino controlado pelo atacante cibernético, sem que o proprietário do equipamento se aperceba.

Fraudes (*Scam*)

É uma prática fraudulenta que consiste em extorquir fundos ou objetos. Exemplos clássicos incluem notícias de que ganhou a lotaria, pedidos de caridade logo após catástrofes recentes ou alguém que precisa de transferir uma avultada quantia de dinheiro em troca de uma comissão para quem o ajudar. Na grande maioria destas mensagens é indicada a necessidade fazer um pagamento inicial, justificando com honorários de advogados, despesas alfandegárias, despesas do banco, etc., mas não só…

Disponibilizamos dois exemplos de **mensagens fraudulentas** utilizando a marca Millennium bcp:

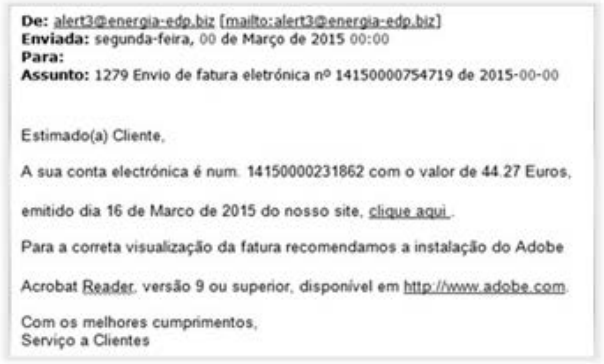
Este esquema é aplicado aos utilizadores de *sites* de vendas/compras, dos mais diversos artigos (carros, telemóveis, jogos, etc), e a finalidade é obter o objeto sem efetuar o respetivo pagamento utilizando o nome do Millennium bcp por forma a credibilizar a fraude.

Porque a segurança é uma das prioridades do Millennium

Infetar computador com *software* malicioso

Após aceder ao *link* da mensagem, o utilizador é direcionado a uma página de *Internet*, e sem que este se aperceba, o navegador de *Internet* é infetado, ficando o atacante cibernético com a capacidade de obter a informação de tudo o que foi digitado durante o acesso à internet ou apresentar páginas a solicitar os códigos de acesso aos sites de *homebanking*.

Disponibilizamos alguns exemplos de mensagens fraudulentas, **supostamente** emitidas por entidades fidedignas:



De: alert3@energia-edp.biz [mailto:alert3@energia-edp.biz]
Enviada: segunda-feira, 00 de Março de 2015 00:00
Para:
Assunto: 1279 Envio de fatura eletrónica nº 14150000754719 de 2015-00-00

Estimado(a) Cliente,

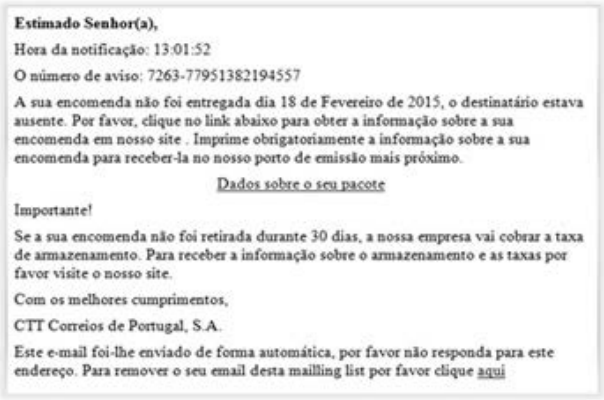
A sua conta electrónica é num. 14150000231862 com o valor de 44.27 Euros,

emitido dia 16 de Marco de 2015 do nosso site, clique aqui .

Para a correta visualização da fatura recomendamos a instalação do Adobe

Acrobat Reader, versão 9 ou superior, disponível em http://www.adobe.com.

Com os melhores cumprimentos,
Serviço a Clientes



Estimado Senhor(a),

Hora da notificação: 13:01:52

O número de aviso: 7263-77951382194557

A sua encomenda não foi entregada dia 18 de Fevereiro de 2015, o destinatário estava ausente. Por favor, clique no link abaixo para obter a informação sobre a sua encomenda em nosso site . Imprime obrigatoriamente a informação sobre a sua encomenda para receber-la no nosso porto de emissão mais próximo.

Dados sobre o seu pacote

Importante!

Se a sua encomenda não foi retirada durante 30 dias, a nossa empresa vai cobrar a taxa de armazenamento. Para receber a informação sobre o armazenamento e as taxas por favor visite o nosso site.

Com os melhores cumprimentos,

CTT Correios de Portugal, S.A.

Este e-mail foi-lhe enviado de forma automática, por favor não responda para este endereço. Para remover o seu email desta mailling list por favor clique aqui

bcp, cumpre-nos alertar ativa e preventivamente os nossos Clientes para situações idênticas às acima descritas as quais podem ser consultadas em millenniumbcp.pt, menu M - Tudo sobre: Segurança e, na página seguinte, aceda a "Avisos de Segurança".

Desta forma, relembramos 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 www.millenniumbcp.pt;**
- O acesso à área de **Particulares**, do site do Millennium bcp, apenas solicita ao utilizador a identificação do **Código de Utilizador e três (3) dígitos aleatórios do Código Multicanal**, **caso erre** as posições solicitadas o site **insiste nas mesmas três posições**, pelo que, sempre que lhe forem solicitados dados adicionais, NUNCA introduza os seus códigos;
- O acesso à área de **Empresas**, do site do Millennium bcp, solicita ao utilizador a identificação do **Código de Utilizador, Password e dois (2) dígitos aleatórios do Número de Identificação Fiscal pessoal**, caso erre as posições solicitadas o site insiste nas mesmas duas posições, pelo que, sempre que lhe forem solicitados dados adicionais, NUNCA introduza os seus códigos;
- **Leia atentamente o conteúdo dos SMS's recebidos com Códigos de Autorização**, uma vez que os dados da operação executada no *site* são identificados no texto do SMS;
- O site do Millennium bcp **NUNCA solicita a identificação do número de telemóvel** ao utilizador;
- O aspeto da página (*homepage*) pode ser **diferente ou com erros ortográficos e/ou gramaticais**;
- Verifique/confirme sempre **a data do último acesso ao *site*** (informação disponibilizada logo após o *login*);
- 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.

Fonte: Millennium bcp

LEMBRE-SE QUE...

Se verificar alguma situação anómala em www.millenniumbcp.pt ou necessitar de esclarecimentos, por favor contacte-nos através do telefone 707 50 24 24 (Atendimento personalizado 24 horas).

Lembre-se que a proteção dos seus dados e computador 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

FRAUDULENT E-MAILS

Currently, the term Phishing is used to describe attacks made by e-mailthat, generally, are sent on behalf of an allegedly trustworthy person/entity, like a friend, a bank, an utilities supplier, etc...

These e-mails may show the logo/brand of a trustworthy company and lead the user to open a link or attachment or to reply to a message. This type of action does not have a specific target and, therefore, the more e-mails are sent by the hackers, more individuals/entities become victims of fraud.

Phishing actions may have several purposes. We highlight here some actions targeting bank websites:

Getting Personal Data

After persuading the recipient to open a link, it re-directs him /her to an internet page where Access Codes, passwords or personal data can be requested such as a credit card number. These pages look legitimate and actually look very much like the website you usually open, with the same tools.

Here are some examples of fraudulent messages allegedly sent by Millennium bcp:

These are two cases of Phishing by resorting to the installation of malware that adulterates the browsers when you go to bank websites.

The message links open a fictitious webpage of EDP or of CTT, from which a malicious file is downloaded. When the file is executed, it installs the malicious software on your computer.

We verified that when accessing the Millennium bcp's website it requests the **User Code.** After you continue in the page, it requests three random positions of the **Multichannel Code followed by an error message saying "dados inválidos", then requesting the other four digits of the Multichannel Code,** as well as the User's **mobile phone number**.

After identifying the mobile phone number, the user receives an SMS, with a link requesting the installation of a Security App on the mobile phone. **This alleged application, redirects the SMS with the Authorization Codes to another mobile phone number or via internet to a destination controlled by the hacker** without the owner of the mobile phone even noticing it.

Scams

This is a fraudulent practice that consists of the extortion of money. Classical examples are news telling you that you won the lottery, offering you a job, requesting donations immediately after the occurrence of catastrophes or someone that needs to transfer a large sum of money paying a fee to those who help him/her doing that. Most of these messages require an initial payment, justified by lawyers fees, customs


To:
Subject: Pagamento 270,50 Euro
From: Pagamento-bcp@local-bcp.pt
Date: Wed, 0 Apr 2015 00:00:00 +0200

Prezado Cliente,

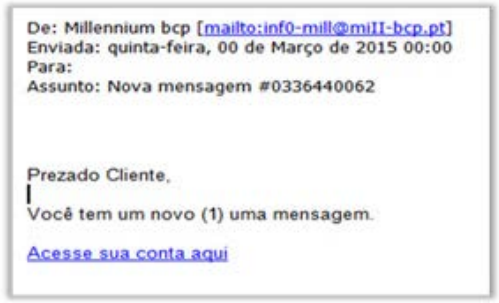
Você recebeu um reembolso de imposto.
Clique aqui para receber.


Date: Fri, 00 Mar 2015 00:00:00 +0900
To:
Subject: Mensagem - #00582245
From: bnc-mill@info-mill-comerical.pt

Notificação

Prezado Cliente,

Você recebeu uma nova notificação.
Clique aqui para resolver o problema.


De: Millennium bcp [mailto:inf0-mill@miII-bcp.pt]
Enviada: quinta-feira, 00 de Março de 2015 00:00
Para:
Assunto: Nova mensagem #0336440062

Prezado Cliente,

Você tem um novo (1) uma mensagem.

Acesse sua conta aqui

When you open the links on those messages you see a login message **similar to the one shown by Millennium bcp**, but located in another website (URL); it requests the **User Code** and, afterwards, the **Complete Multichannel Code** as well as an **Authorization Code, obtained via SMS or Token for the alleged "restituição do imposto" or "Desbloqueio da conta"**.

However, the text of the SMS contains an Authorization Code to confirm a transfer.

Infect computers with malware

After opening the message link, the user is re-directed to an internet page and, without the user noticing, the Internet browser is infected and the hacker is able to get information on everything entered while online or present pages requesting the access codes for bank websites.

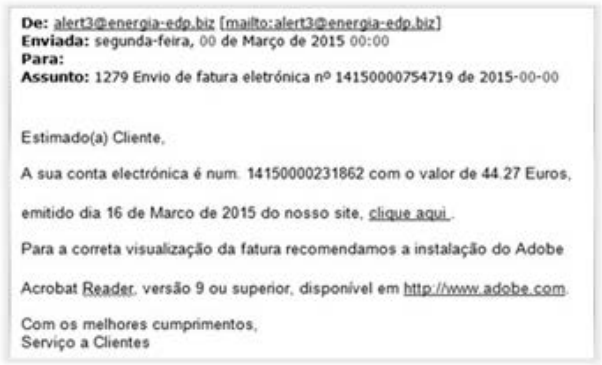
expenses, bank expenses, and so on...

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

This scheme targets users of online shopping/selling websites of various items (cars, mobile phones, games, etc), and it aims to get the object without making the payment using the Millennium bcp brand to make the fraud appear legitimate.

Because safety is one of the priorities of Millennium bcp, it is our duty to, in an active and preventive manner, warn our Customers about situations similar to those described above. You can find all you need to know at millenniumbcp.pt, at the end of the homepage - Read more: Security and, on the next page, read the "Security

Here are some examples of fraudulent messages allegedly issued by trustworthy entities:



De: alert3@energia-edp.biz [mailto:alert3@energia-edp.biz]
Enviada: segunda-feira, 00 de Março de 2015 00:00
Para:
Assunto: 1279 Envio de fatura eletrónica nº 14150000754719 de 2015-00-00

Estimado(a) Cliente,

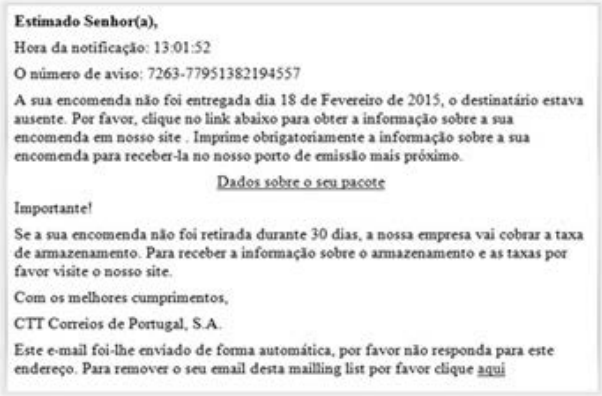
A sua conta electrónica é num. 14150000231862 com o valor de 44.27 Euros,

emitido dia 16 de Marco de 2015 do nosso site, clique aqui .

Para a correta visualização da fatura recomendamos a instalação do Adobe

Acrobat Reader, versão 9 ou superior, disponível em http://www.adobe.com

Com os melhores cumprimentos,
Serviço a Clientes



Estimado Senhor(a),

Hora da notificação: 13:01:52

O número de aviso: 7263-77951382194557

A sua encomenda não foi entregada dia 18 de Fevereiro de 2015, o destinatário estava ausente. Por favor, clique no link abaixo para obter a informação sobre a sua encomenda em nosso site . Imprime obrigatoriamente a informação sobre a sua encomenda para receber-la no nosso porto de emissão mais próximo.

Dados sobre o seu pacote

Importante!

Se a sua encomenda não foi retirada durante 30 dias, a nossa empresa vai cobrar a taxa de armazenamento. Para receber a informação sobre o armazenamento e as taxas por favor visite o nosso site.

Com os melhores cumprimentos,

CTT Correios de Portugal, S.A.

Este e-mail foi-lhe enviado de forma automática, por favor não responda para este endereço. Para remover o seu email desta mailling list por favor clique aqui

Notices".

Hence, we do remind you that:

- Millennium bcp **does not send** e-mail messages with links;
- Never open Millennium bcp's website through links on messages, search engines or even through your "Favourites". **Always type in the complete address ww?w.millenniumbcp.?pt;**
- To access to the **Individuals** area of Millennium bcp's website the user is only requested to enter the **User Code and three (3) random positions of the Multichannel Code.** In case there is an error when you enter the three positions, the website will always ask you to **enter the same three positions**. Therefore, if additional information is requested, NEVER enter your codes;
- To access the **Companies** area of Millennium bcp's website the user is requested to enter the **User Code, the Password and two (2) random digits of the Personal Tax Identification Number.** In case there is an error when you enter the three positions, the website will always ask you to enter the same two positions. Therefore, if additional information is requested, NEVER enter your codes**;**
- **Please read carefully the SMSs received containing Authorisation Codes** since the transaction data are identified in the SMS;
- Millennium bcp 's website **NEVER asks the user to identify mobile phone number**;
- Beware if the homepage looks **different, shows spelling errors and/or bad grammar**;
- Always verify/confirm the **date of the last access to the website** (information provided when you *login*);
- 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.

Source: Millennium bcp

REMEMBER...

If you ever find something out of place at www.millenniumbcp.pt/en or if you need further information please call us on 707 50 24 24 (Personal Assistance 24/7).

Remember: the protection of your data and computer depends on you!

Source: Millennium bcp

Millennium bcp is responsible for this information

This is an automated notification. Please do not reply to this message. We're happy to help you with any questions or concerns you may have and listen to your suggestions. So that we can provide you best service, please go to the Millennium bcp website or dial 707 50 24 24.

If you call 707 50 24 24 using the landline you will pay a maximum of 0.10 € per minute; if you choose to call us using a mobile phone, the maximum cost per minute will be of 0.25 €. These charges are subject to VAT.

These e-mails do not grant direct access to the Millennium bcp website, nor do they include links*, nor are they sent to ask for any personal details (namely access codes). If you do receive any such e-mail, apparently sent by Millennium bcp but not in accordance with the above information, do not reply: delete and report it immediately to: informacoes.clientes[@]millenniumbcp.pt

If you do not wish to receive such information via e-mail or if you wish to change your e-mail address, please go to the Millennium bcp Homebanking, then chose “Customize/Email” in the menu option “M Area”.

* Some mail services will, automatically, assume certain words as links, without any liability from Millennium bcp.