NEWSLETTER
M_SEGURANÇA
Millennium bcp

MAIO 2014 Nº 66

English version

PRINCÍPIOS BÁSICOS DE SEGURANÇA
MENSAGENS DE CORREIO ELETRÓNICO *(E-MAILS)* FRAUDULENTAS

Atualmente o correio eletrónico (*e-mail*), é um dos canais mais utilizados na comunicação eletrónica tanto ao nível pessoal como ao nível profissional.

Este meio de comunicação tem inúmeras funcionalidades sendo utilizado para envio de publicidade, avisos, alertas, questionários, partilha de informação, de entre outras, pelo que se tornou num dos métodos mais utilizados pelos atacantes cibernéticos.

Originalmente, o termo *Phishing* era utilizado para descrever um ataque desenvolvido para "roubar" os códigos de acesso pessoais utilizados em *sites* bancários. Neste momento, este termo 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 fornecedor de serviços (ex. eletricidade, gás, telefone, correio), etc..

Por norma, estes *e-mail*s contêm uma mensagem aparentemente genuína suportada pela 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 poderão vir a ser defraudadas.

As ações de *Phishing* podem recorrer a meios distintos, dos quais destacamos:

- **Cópia do site:** 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, por exemplo, o número do cartão de crédito. Estas páginas parecem legítimas, tendo inclusive a mesma aparência e funcionalidades do site que costuma visitar;
- **Infetar o computador com *software* malicioso:** Após aceder ao *link* da mensagem, o utilizador é direcionado para uma página de *Internet*, e "silenciosamente", sem que se aperceba, o navegador de Internet é infetado dando acesso total do computador, via Internet, ao atacante cibernético;
- **Anexos maliciosos:** São *e-mail*s de *Phishing* com anexos maliciosos, que podem ser ficheiros PDF ou documentos W*ord* infetados. Ao aceder aos anexos, é instalado um programa malicioso e, se bem-sucedido, permite ao atacante controlo total do computador;
- **Esquemas Fraudulentos (*Scam*):** É uma prática
- Posicione o cursor do rato sobre o *link* da mensagem, que mostrará o verdadeiro endereço para onde será direcionado se o selecionar. Se o destino do *link* for diferente do escrito na mensagem ou contenha um nome ou código de país diferente da entidade emissora, pode ser uma indicação de fraude;
- Não clique nos *link*s. Ao invés disso, copie a URL (endereço do *link*) do *e-mail* que recebeu e cole no seu navegador de Internet ou, de preferência, digite o endereço no seu navegador;
- Suspeite de anexos. Abra-os apenas quanto estiver à espera de os receber;
- O facto de ter recebido um *e-mail* de um amigo não significa que tenha sido mesmo ele a enviar. O computador do seu amigo pode ter sido comprometido por um *malware* (software malicioso), cujo comportamento é enviar *e-mail*s para todos os seus contatos. Se receber um *e-mail* suspeito de um amigo ou colega, confirme, ligando para o número de telefone que tem e nunca para o número que seja identificado na mensagem.

Utilizar o *e-mail* de forma segura é uma questão de bom senso!

Se suspeitar do conteúdo de uma mensagem, é bem provável que seja um ataque de *Phishing*.

Porque a segurança é uma das prioridades do Millennium 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".

Resta-nos deixar alguns alertas sobre situações suspeitas que podem ocorrer em ind.millenniumbcp.pt utilizando um computador infetado com um software malicioso, as quais nos devem ser comunicadas de imediato:

- Dificuldades no acesso;
- A página não é apresentada corretamente ou não permite introduzir o Código Multicanal;
- O site do Millennium bcp apenas solicita ao utilizador a identificação do Código de Utilizador e de três (3) dígitos aleatórios do Código Multicanal. Caso erre as posições solicitadas o site insiste nas mesmas posições, pelo que, sempre que lhe sejam solicitados dados adicionais, NUNCA introduza os seus códigos;

fraudulenta que consiste em extorquir fundos. Exemplos clássicos incluem notícias de que ganhou a lotaria, ofertas de emprego, 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. Em todas estas mensagens é indicada a necessidade de fazer um pagamento inicial, justificando com honorários de advogados, despesas alfandegárias, despesas do banco, etc..

Na maioria das vezes, abrir simplesmente o *e-mail* é seguro, contudo:

- Suspeite de qualquer *e-mail* que peça uma "ação imediata" ou crie um senso de urgência;
- Suspeite de *e-mails* endereçados a "Querido Cliente" ou qualquer outra saudação atípica;
- Suspeite dos erros gramaticais ou de escrita;
- Se o aspeto da página inicial (homepage) for diferente ou se tem uma linguagem inadequada (por exemplo, em Português do Brasil);
- Se ao aceder ao histórico de movimentos visualizar alguma transação que não reconhece ou que não foi efetuada por si;
- Sempre que a data do último acesso (informação disponibilizada após o login em "A minha página") seja diferente daquela em que realizou o último acesso à conta;
- Se suspeitar ou detetar que os códigos foram indevidamente obtidos por terceiros (por exemplo, em situações de furto ou roubo);
- Sempre que seja contactado por terceiros, via *e-mail* ou telefone, a solicitar dados pessoais ou dados da sua conta- o Banco NUNCA efetua pedido de dados ou códigos por estas vias;
- Sempre que tenha uma sugestão de melhoria dos nossos serviços.

Se verificar alguma situação anómala em ind.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!

Esta informação é da responsabilidade do Millennium bcp

NEWSLETTER M_SEGURANÇA

Millennium bcp

MAY 2014 Nº 66

Versão portuguesa

SECURITY BASIC PRINCIPLES
FRAUDULENT E-MAILS

Nowadays, both in personal and professional relationships, the e-mail is one of the most used electronic communication channels.

This mean of communication has numerous tools and is used, among other purposes, for advertising, remittance of notices, alerts, surveys, exchange of information and, therefore, became one of the privileged methods used by hackers.

Originally, the expression *Phishing* was used to describe an attack made to "steal" the personal access codes used in banking websites. Currently, this term is used to describe attacks made by e-*mail* that, generally, are sent on behalf of an allegedly trustworthy person/entity, like a friend, a bank, an utilities supplier (ex. energy, phone, mail), etc..

As a rule these e-mails contain an apparently genuine message supported by a trustworthy brand and lead the user to access a *link*, open an attachment or 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 may become victims of fraud.

Phishingactions may assume several forms, of which we highlight the following:

- **Copy of the website:** After persuading the recipient to access a link, it re-directs him /her to an internet page where access codes, passwords or, personal data, can be requested as, for example, your credit card number. These pages look legitimate and, inclusive, look very much like the site you usually access and have same tools of the website you usually go to;
- **Infect computers with malware:** After accessing the message link, the user is re-directed to an internet page and "silently", the user does not even notice it , the Internet browser is infected and the hacker gets total access to the computer, via internet;
- **Malicious Attachments:** These are Phishing e-mail messagescontainingmalicious attachments that may consist in infected PDF files or Word documents. When you open the annexes a malware is installed and, if well-succeeded, it will enable the hacker to achieve full control of the computer;
- ***Scam*:** It is a fraudulent practice that consists in the extortion of money. Classical examples are information telling you that you won the lottery, offering you a job, requesting you donations immediately after the occurrence of catastrophes or someone that needs to transfer a large sum of money in exchange of a fee for those who help him/her doing that. All these messages indicate as a requirement the making of an initial payment due to lawyers fees, toll expenses, bank expenses, and so on.....

Most of the times, it is safe if you just open the e-mail. However:

- Be suspicious of any e-mail that requires an "immediate action" or creates a sense of urgency;
- Be suspicious of any e-mails addressed to “Dear Customer” or showing any other unusual salute;
- Don't click on the links. Instead, copy the URL (*link address*) of the *e*-mail you receivedand paste it in your Internet navigator or, preferably, digit the address in your browser;
- Be suspicious of attachments. Only open them if you are expecting them;
- The fact that you received an e-mail from a friend does not necessarily mean that he/she really sent it. Your friend's computer may have been infected with a malware whose behaviour is to send e-mail messages to all your contacts. If you receive a suspicious e-mail from a friend or colleague, confirm it by calling him/her using the phone number you have and never the phone number that appears in the message.

Using e-mail in a safe manner is just a matter of common sense!

If you become suspicious of a message, it is very likely that you are under a Phishing attack.

Because safety is one of the priorities of Millennium bcp, it is our duty to, in an active and preventive manner, alert our Customers for situations similar to those described above. You may find all you need to know at millenniumbcp.pt, “About Millenniumbcp.pt: Security” and, in the next page, go to “Security Notices”.

Let us provide you with some alerts on suspicious situations that may happen at ind.millenniumbcp.pt if you are using a computer infected with a malware, which must be immediately reported to us:

- Access troubles;
- The page is not presented correctly or does not allow entering the Multichannel Code;
- Remember, the Bank will only ask you to enter the User Code and **three random positions** of your Multichannel Code. In case there is an error when you enter the three positions, the website will always ask you to enter the same positions. Therefore, if any additional information is requested, NEVER enter your codes;
- If the look of the homepage is different or its presents an inappropriate language (for example, Brazilian Portuguese);
- If, when you access the history of entries, you see any transaction that you do not recognise or that you did not make;
- Whenever the date of the last access (information made available after the login in ”My Page”) is different from the date when you really accessed your account for the last time;
- If you become suspicious or detect that the codes were unduly obtained by third parties (for example in situations of theft or robbery);
- Whenever you are contacted by third parties via e-mail or by phone to request your personal data or the data of your bank account, please be aware that the Bank NEVER requests this type of data by e-mail or phone;
- Whenever you have a suggestion able of improving our

- Be suspicious of grammar or spelling mistakes;
- Put the mouse pointer on the message link that will show the real address you will go if you click on it. If the destination of the link is different from the one written in the message or it shows a country name or code different from the one belonging to the issuing entity, be careful it may be a fraud;

services.

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

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

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.

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 website and click on Accounts, then Customize.

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