

Caso não consiga visualizar correctamente este e-mail por favor reporte-nos esta situação para: [informacoes.clientes@millenniumbcp.pt](mailto:informacoes.clientes@millenniumbcp.pt)

In case you don't see this e-mail correctly, please report the situation to: [informacoes.clientes@millenniumbcp.pt](mailto:informacoes.clientes@millenniumbcp.pt)

**Millennium**  
bcp

Newsletter sobre Segurança

**Microsoft**

Agosto 2007 - nº 39

[English version](#)

Saiba que, no primeiro semestre deste ano, 1,681 milhões de utilizadores a residir em Portugal acederam a sites bancários, tendo o Millennium bcp um lugar no pódio com o seu espaço *online* a ser um dos mais visitados: registada a visita de 760 mil utilizadores e a navegação por 101 milhões de páginas.

- [Esquemas fraudulentos em ofertas de emprego na Internet.](#)
- [O seu computador pode estar a ser usado ...](#)

Continuamos a chegar até si, através desta Newsletter, para lhe falar de Segurança, na utilização do seu computador e na navegação na Internet: os riscos e os procedimentos a adoptar para os minimizar.

Nesta edição, "**Em Destaque**", conheça os cuidados a ter na procura de emprego através da Internet.

Em "**Princípios Básicos de Segurança**" saiba o que são *bot nets*.

Esteja alerta e utilize as nossas recomendações!  
Boa leitura.



**Em Destaque**

## Esquemas fraudulentos em ofertas de emprego na Internet

Eis duas formas comuns de oferta de emprego *online* em relação às quais deve estar atento e algumas sugestões sobre como procurar emprego *online* com mais segurança.

### Falsas oportunidades de emprego

Criando anúncios de emprego falsos, os burlões esperam conseguir receber as informações pessoais de quem procura emprego (chamado *phishing*). Os burlões colocam anúncios em *sites* de emprego legítimos.

Os anúncios de emprego falsos utilizam muitas vezes logotipos e linguagem convincentes e familiares. Por vezes, fornecem ligações para falsos *Web sites* que aparentam ser de organizações reais.

Estes *sites* podem ainda cobrar taxas por serviços que nunca virão a prestar. Normalmente, após alguns dias, os falsos recrutadores fecham o negócio e desaparecem.

### Recrutadores de empregos não solicitados

Por vezes, depois de analisarem páginas *web* pessoais e diversos Curriculum Vitae (CV) colocados em *sites* públicos, estes burlões começam por apresentar-se como funcionários de empresas de recrutamento e enviam mensagens de correio electrónico não solicitadas (ou *spam*) a eventuais candidatos, com ofertas de oportunidades ou serviços de gestão de carreira.

Um burlão que invista nesta área tenta conquistar a confiança da sua vítima com frases bem ensaiadas e falsos argumentos, para tentar extrair informações pessoais, mesmo pelo telefone.

É importante recordar que esta informação normalmente não é solicitada antes de uma entrevista pessoal.

### Melhores práticas para procura de emprego *online*

- Nunca forneça nenhuma informação pessoal *online* que não esteja relacionada com trabalho, tal como o seu número de Bilhete de Identidade, número de cartão de crédito, data de nascimento, endereço de casa e estado civil, seja através de correio electrónico, por telefone, por fax ou incluído no seu CV;
- Coloque o seu CV num *site* de procura de emprego que só permita a sua visualização por recrutadores verificados e que tenha uma política de privacidade;
- Verifique as referências dos eventuais empregadores ou das empresas de recrutamento de pessoal junto das entidades oficiais reguladoras do sector ou numa lista telefónica. Em seguida, contacte-os directamente ou, melhor ainda, visite pessoalmente a sede da empresa durante as horas normais de funcionamento;
- Se uma empresa que lhe faça uma oferta de emprego, ou se apresente como uma empresa que presta serviços de recrutamento, lhe pedir uma verificação dos dados apresentados, concorde em fazê-lo, mas apenas depois de ter contactado a empresa durante o horário normal de expediente;

- Não confie em pessoas que lhe pedem dinheiro adiantado para procurarem emprego por si. Nunca deve ser obrigado a pagar serviços "exclusivos" de procura de emprego ou pela obtenção de um emprego;
- Se contratar serviços de prospecção no mercado de trabalho, não forneça dados bancários ou associados ao cartão de crédito, nem se envolva em transacções de dinheiro, a não ser que o faça pessoalmente, depois de ter verificado as referências da entidade ou pessoa que pretende contratar;
- Avalie cuidadosamente as informações de contacto em anúncios ou mensagens de correio electrónico relacionadas com ofertas de emprego, verifique se há erros ortográficos, um endereço de correio electrónico que não corresponde ao nome da empresa e inconsistências relacionadas com a localização, ou o código postal;
- Introduza os endereços dos *Web sites* (ou URLs) no seu *browser*, em vez de seguir ligações, quando analisa ofertas de emprego. Esteja precavido contra uma nova forma de burla semelhante ao *phishing* e a que se dá o nome de *pharming*, que implica o redireccionamento dos utilizadores de *Web sites* legítimos para réplicas falsas, com a intenção de aceder a informações pessoais;
- Crie um endereço de correio electrónico exclusivo baseado na *web* e uma conta para todas as suas comunicações não pessoais;
- Apesar de não haver métodos infalíveis para identificar falsos anúncios de emprego, procure repetições de erros ortográficos e outras inconsistências, que revelam uma comunicação descuidada e interesses camuflados;
- Confie no seu instinto e tenha especial cuidado quando estiver a lidar com contactos fora do seu país. Se uma oportunidade promete demasiado, ou algo não lhe parece bem, é provável que tudo se trate de um esquema fraudulento.



## Princípios Básicos de Segurança

### O seu computador pode estar a ser usado...

Pode estar a ser usado não só por si, mas também por terceiros mal intencionados.

**Com que finalidade?** Ilustrando, imaginemos um exército. Quanto maior este for, maior será também o seu poder militar. De igual forma, terceiros mal intencionados tentam controlar o maior número possível de computadores de forma a constituir uma espécie de exército virtual, conhecido por **bot net**.

### Qual o objectivo destas *bot nets*?

Estas redes de computadores controlados por terceiros têm como objectivo principal a massificação de ataques que de outra forma não seriam possíveis. Os ataques mais comuns são os de DDoS (*Distributed Denial of Service* / Ataque Distribuído de Negação de Serviço), que como o nome indica tentam provocar um volume excessivo de pedidos e dessa forma tornar indisponível determinado alvo/*site* na Internet. Também se tornam possíveis outros tipos de ataques, como por exemplo, o envio de *SPAM* (envio massivo de correio electrónico não solicitado), ou até mesmo ataques à confidencialidade da informação com que

trabalhamos.

Outro aspecto a destacar, no caso do seu computador estar a ser usado por terceiros, é o facto de utilizarem o seu nome nos ataques efectuados. Para os devidos efeitos, é o seu computador e a sua ligação à Internet que, no caso de ser uma vítima, estão a ser utilizados para fins fraudulentos. Por estes motivos aconselhamos a ter alguns cuidados na utilização do seu computador para que este não fique contaminado.

As formas de contaminação são geralmente através da visualização de determinados anexos em mensagens de correio electrónico, ou através de programas descarregados em páginas da Internet bem como a partir das redes de *peer-to-peer* (redes utilizadas para partilha de ficheiros).

Assim, para que se previna contra este tipo de ameaça, deixamo-lhe uma vez mais os **10 Mandamentos da Segurança**, com as preocupações que deve ter sempre em mente na utilização do seu computador, em especial quando ligado à Internet.

## Proteja o seu PC

- 1 Instale um antivírus e mantenha-o permanentemente actualizado. Não actualizar o antivírus é quase o mesmo que não o ter;
- 2 Utilize uma *firewall* para que possa filtrar o tráfego da Internet que entra e sai do seu computador;
- 3 Esteja atento às actualizações de segurança que os fornecedores credíveis de software disponibilizam e aplique-as de acordo com as instruções que são fornecidas;

## Proteja a sua informação

- 4 Não aceda aos *sites* com informação pessoal ou confidencial/sensível, ou que lhe permitem realizar operações bancárias, através de *links*. Digite sempre o endereço completo do *site* a que pretende aceder na respectiva barra;
- 5 Nunca forneça dados confidenciais ou pessoais através de mensagens de correio electrónico, ou qualquer outro meio, mesmo que a solicitação seja de fonte aparentemente legítima;
- 6 Não introduza elementos identificativos ou confidenciais em *sites*, sem confirmar que está num ambiente seguro. Verifique se o endereço começa por **https://** seguido do **nome** correspondente ao *site* pretendido e se a página possui um **cadeado** na barra inferior ou superior do seu *browser*;
- 7 Não abra mensagens de correio electrónico sem garantir a identidade do remetente e confirmar o assunto. Caso duvide da origem da mensagem de correio electrónico apague-a de imediato sem executar qualquer ficheiro ou anexo que conste da mesma

## Não se deixe enganar

- 8 Não se deixe iludir por acções de terceiros associadas ao que se designa por "engenharia social" ou "arte de enganar", que utilizam "técnicas de sedução" para obtenção de informação de carácter pessoal e/ou confidencial (ex: *passwords*, números de identificação - BI, NFC), posteriormente utilizada indevidamente;

## Utilize os seus Códigos de Acesso com critério

- 9 Não escolha códigos de identificação óbvios ou facilmente identificáveis (ex.: 111111; 123456, *password*). Memorize-os e nunca os faculte a terceiros;
- 10 Defina *passwords* diferentes para aceder a *sites* seguros (ex.: *Homebanking*), e para *sites* que não requerem grandes preocupações de segurança.



[www.millenniumbcp.pt](http://www.millenniumbcp.pt)

707 50 24 24 / 91 827 24 24 / 93 522 24 24 / 96 599 24 24



"Best Corporate/Institucional Internet Bank" Empresas em Portugal - "Best Consumer Internet Bank" Particulares em Portugal - "Best Bill Payment and Presentment" na Europa - "Best Information Security Initiatives" na Europa - "Best Online Deposits Acquisition" na Europa

***Este e-mail é apenas informativo, por favor não responda para este endereço.*** Para obter esclarecimentos adicionais, sobre este ou qualquer outro assunto, ou efectuar sugestões, e para que o possamos servir melhor e mais eficazmente, sugerimos que visite [www.millenniumbcp.pt](http://www.millenniumbcp.pt) ou ligue para o número de telefone 707 50 24 24.

***Estes e-mails não permitem o acesso directo ao site [www.millenniumbcp.pt](http://www.millenniumbcp.pt), não incluem atalhos (links), nem são utilizados para lhe solicitar quaisquer 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](mailto:informacoes.clientes@millenniumbcp.pt)***

*Se não pretende receber este tipo de informação via e-mail ou se pretende alterar o seu endereço electrónico, aceda a [www.millenniumbcp.pt](http://www.millenniumbcp.pt) e escolha a opção Contas e, posteriormente, a opção Personalização.*



August 2007 - n° 39

[Versão Portuguesa](#)

1,681 million users living in Portugal have accessed bank sites in the first quarter 2007. Millennium bcp has a place on the podium, with one of the most visited online locations: 760 thousand users have visited 101 million pages on our site.

- [Phony job offers on the internet.](#)
- [Your computer may be being used...](#)

We continue to reach you through this Newsletter to let you know how to safely use your computer and surf the internet in Security: the risks and the steps to take in order to minimize risk.

In this edition, under "**Highlights**", learn about precautions you must take when searching for a job on the internet.

Learn about **bot nets** in "**Basic Security Principles**".

Be alert and follow our tips!  
Enjoy your reading.



## Highlights

### Phony job offers on the internet.

Here are two common forms of online job offers you should be wary of as well as some suggestions on how to search with increased security for jobs online.

#### Fake job offers

By coming up with fake job ads, swindlers try to collect personal information on job seekers (what is known as phishing). Swindlers place ads in legitimate job sites.

Fake job ads often use convincing and familiar logos and language. Sometimes they even have links to fake websites, which look like they belong to real organizations.

These sites may even charge fees for services they will never actually render. Usually, the fake recruiters close their business after a few days and vanish.

#### Unsolicited job recruiters

Sometimes, after having analyzed personal webpages and a number of CVs on public sites, these swindlers introduce themselves as workers from recruiting companies and send spam to potential candidates offering job posts or career management services.

A swindler who operates in this area tries to gain the trust of its victim through the use of rehearsed speeches and false arguments, with the aim of obtaining personal details, even on the phone. It is important to note that this sort of information is not commonly requested prior to a personal interview.

### **A set of best practices for seeking jobs online**

- Never give any personal information over the internet that is not job-related, such as your ID or credit card numbers, date of birth, home address and marital status, be it via email, phone or fax, or included in your CV;
- Place your CV on a job site that can only be viewed by verified recruiters and that follows a privacy policy;
- Verify the authenticity of the references of potential employers or staff recruiting companies next to official regulating bodies or looking them up in a phone book. Next, contact them directly, or better still, visit the company headquarters during working hours;
- If a company that offers you a job or presents itself as a recruiting company asks you to check that your details are correct, only agree to do so after having visited the company during normal working hours;
- Do not trust people who ask for money in advance for job seeking services. You should never have to pay for 'exclusive' job seeking services or for getting a job;
- If you hire employment surveying services do not supply any bank or credit card details nor transact money, unless you do so in person, and after having checked the references of the company or the person you intend to hire;
- Carefully study contacts information on job offer ads or emails. Check for spelling mistakes, an email address that does not match the company's name and inconsistencies regarding location or zip code;
- When looking through job offers enter the websites addresses (URLs) directly into your browser instead of clicking on links. Be on the lookout for a new type of fraud, similar to phishing, called pharming. Users of legitimate websites are redirected to phony replicas as a means of collecting personal information;
- Create an email address exclusive for non-personal communication;
- Even though there are no infallible methods for detecting false job ads, you should search for spelling mistakes and other inconsistencies that reveal sloppy communication and masked interests;
- Trust your instincts and be particularly careful when dealing with overseas contacts. If an opportunity looks too promising or something seems out of place it is probably a phony offer.



## Basic Security Principles

### Your computer may be being used...

May be being used not only by you, but also by malicious users.

**With what purpose?** Imagine an army. The bigger it is, the larger its military power. In similar manner, malicious users try to seize control of as many computers as they can to form a kind of virtual army, known as a bot net.

### What is the purpose of bot nets?

These remotely controlled computer networks are used to create otherwise impossible massive attacks. DDoS (Distributed Denial of Service) is the most common type of attack. As the name indicates, these attacks try to generate an excessive volume of requests, rendering a particular internet target/site unavailable. Other types of attacks, as for example spamming (mass sending of junk mail) or attacks on data confidentiality, are also made possible through this method.

Keep in mind that if your computer is being controlled by others, then they are using your name in the attacks. For all purposes, it is your computer and net connection that are being used for fraudulent ends. We thus advise you to take some precautions so that your computer does not become infected.

Infection usually occurs when viewing certain email attachments or running programs downloaded from the internet or from peer-to-peer networks.

So that you can take some steps against this sort of threat, we once again leave you the **10 Security Commandments**, with points you should keep in mind, especially when connected to the internet.

## Protect your PC

- 1 Install an antivirus and always update it. Not updating your antivirus is almost the same as not having one;
- 2 Use a firewall so that you can filter incoming and outgoing internet traffic;
- 3 Keep your eye open for security updates from trustworthy software suppliers and install them according to their instructions;

## Protect your information

- 4 Do not access sites by entering personal or confidential/sensitive information, or ones that ask you to make bank transactions by clicking on links. Always enter the site's complete address into your browser's address bar;
- 5 Never supply confidential or personal information in emails or any other means of communication, even if the request comes from a supposedly legitimate source;

- 6 Do not enter information that is confidential or that can identify you in sites without first being sure that you are operating in a secure environment. Check that the address begins with **https://** followed by the **name** of the desired site. Also check that the page has a **padlock** on the bottom or top bar on your browser;
- 7 Do not open emails without checking the sender's identity and its subject. If you have doubts about the origin of the email, delete it at once without running any file or included attachment;

## Do not let yourself be tricked

- 8 Do not let yourself be deceived by what is known as 'social engineering' or 'the art of deception', which use 'techniques of seduction' to obtain personal and/or confidential information (e.g.: passwords, identification numbers - ID, Taxpayer) which can later be unduly used;

## Choose your Access Codes wisely

- 9 Do not choose identification codes that are obvious or can be easily discovered (e.g.: 111111; 123456, password). Memorize them and never give them to others;
- 10 Set different passwords for sites that are safe (e.g.: Homebanking) and those that do not require great security concerns;



[www.millenniumbcp.pt](http://www.millenniumbcp.pt)

707 50 24 24 / 91 827 24 24 / 93 522 24 24 / 96 599 24 24



"Best Corporate/Institucional Internet Bank" Empresas em Portugal - "Best Consumer Internet Bank" Particulares em Portugal - "Best Bill Payment and Presentment" na Europa - "Best Information Security Initiatives" na Europa - "Best Online Deposits Acquisition" na Europa

***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 [www.millenniumbcp.pt](http://www.millenniumbcp.pt) or dial 707 50 24 24.

***These emails do not grant direct access to [www.millenniumbcp.pt](http://www.millenniumbcp.pt), nor do they include links, nor are they sent to ask for any personal details (namely access codes). If you do receive any such email, 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](mailto:informacoes.clientes@millenniumbcp.pt)***

*If you do not wish to receive such information via email or if you wish to change your email address, please go to [www.millenniumbcp.pt](http://www.millenniumbcp.pt) and click on Accounts, then Customize.*