

%%Exm%% %%customerName%%



## Em destaque

Como ajudar os seus filhos a utilizar os sítios Web de redes sociais de uma forma mais segura.

Mais +



## Princípios básicos de segurança

*Back to Basics...* Como aumentar a segurança do computador e proteger a sua informação pessoal.

Mais +

[English version](#)

Se os beneficiários das operações que frequentemente realiza são da sua confiança, porquê continuar a utilizar o Código de Autorização?

## Universo Financeiro Pessoal



Visite a área de Contas em [www.millenniumbcp.pt](http://www.millenniumbcp.pt)



## Em destaque

### Como ajudar os seus filhos a utilizar os sítios Web de redes sociais de uma forma mais segura

Que ninguém tenha dúvida! Os sítios Web de redes sociais são extremamente populares entre a camada mais jovem da população. Vieram para ficar.

Por isso, é importante perceber o que são estes sítios, porque são tão populares e, acima de tudo, como é que os nossos jovens os podem utilizar de uma forma mais segura.

Os tempos mudaram, os dias de hoje estão mais perigosos e deixou de ser comum vermos as crianças a brincar na rua com os amigos. Nos seus tempos livres, especialmente agora que chegaram as férias grandes, os jovens utilizam as novas tecnologias para alargar o seu círculo de amizades. É normal que o seu filho tenha amigos, literalmente, nos quatro cantos do mundo! Para além das comunicações em tempo real (como, por exemplo, o *Windows Live Messenger*), são cada vez mais os jovens que mantêm um registo público *online* das suas actividades e, como os mais pequenos não querem ficar atrás, já é comum ver esse tipo de actividade mesmo em crianças.

Há uns anos atrás, criar uma página Web era uma tarefa árdua, somente ao alcance de profissionais. Hoje em dia tornou-se tão fácil que uma criança não vê grande dificuldade em criar e manter a sua própria página.

Estas páginas estão, tipicamente, hospedadas em sítios Web de redes sociais tais como o **Windows Live Spaces** (<http://spaces.live.com>), *MySpace*, *Facebook*, *Hi5*, entre outros. Segundo a *Wikipedia* ([http://pt.wikipedia.org/wiki/Lista\\_de\\_redes\\_sociais](http://pt.wikipedia.org/wiki/Lista_de_redes_sociais)), existem pelo menos 132 sítios Web de redes sociais!

Por si só, um sítio de rede social não tem nada de mal. Um jovem pode ter a sua página pessoal onde pode expressar as suas emoções, gostos e preferências relacionadas com o seu universo, tais como livros, jogos, disciplinas favoritas, entre outras. Partilhando o endereço da sua página, este jovem pode facilmente ser encontrado por outros com gostos similares e, por isso mesmo, amizades podem ser estabelecidas através desta forma de comunicação. O problema está numa utilização menos apropriada. Estes sítios são, por norma, agregadores de muita informação do utilizador, informação essa com carácter de alguma ou grande confidencialidade, tais como vídeos, fotografias, nome completo, morada, escola onde estuda, número de telemóvel, endereço de correio electrónico, enfim, uma devassa da privacidade caso não sejam tidas em conta as mais elementares medidas de segurança. Infelizmente, existem os chamados predadores que se aproveitam da inocência de crianças e jovens utilizadores destas redes.

Há muito pouco tempo (em Junho 2008) foi detectado um ataque de "**phishing**"(1) contra o *Hi5* e o *FaceBook*, afectando, provavelmente, muitos milhares de utilizadores. Este ataque, iniciado através do envio de mensagens de SPAM desde uma rede de computadores "escravos" (*botnet*), foi baseado na criação de páginas internet que imitavam (e muito bem) as páginas originais. Um dos objectivos deste ataque era o roubo da identidade dos utilizadores destas redes; julgando que se encontravam na página original, o utilizador colocava as suas credenciais (nome de utilizador e palavra passe). Os atacantes, tendo esta informação em seu poder, poderiam fazer-se passar por quem não eram e, por isso mesmo, tirar benefícios fraudulentos deste ataque.

O atrás exposto não invalida a utilidade dos sítios das redes sociais, o importante é uma utilização mais segura. Para tal, aconselhamos que tenha em consideração os seguintes pontos:

1. **Crie as regras de utilização da Internet lá em casa.** Quando as crianças começam a utilizar a Internet, é importante existirem regras claramente definidas. Não devem existir dúvidas do que devem e não devem fazer. Estas regras deverão incluir quando e como as crianças deverão utilizar os sítios das redes sociais.
2. **Garanta que as crianças cumprem com os limites de idade estipulados nos sítios.** Geralmente a idade mínima recomendada para utilizar um sítio de rede social são os 13 anos. Se tem crianças com idade inferior, simplesmente não as autorize a utilizarem esses sítios. Infelizmente não existem medidas eficazes de confirmação da idade na altura da subscrição / utilização do sítio.
3. **Obtenha o máximo de conhecimento acerca do sítio.** Seja um utilizador do sítio, antes do seu filho o começar a utilizar. Leia a política de privacidade e a prática de conduta e confirme se o mesmo tem processos que analisem o conteúdo lá colocado. Depois do seu filho ter criado a sua página, reveja-a periodicamente.
4. **Deixe muito claro que o seu filho NUNCA deverá encontrar-se com alguém que comunique com ele apenas de forma digital.** As crianças poderão colocar-se em situações de perigo ao encontrarem-se com pessoas que apenas conheceram no mundo digital. Esta é a forma típica dos predadores funcionarem. Travam conhecimento *online*, ganham a sua confiança e depois atacam. Encoraje-o apenas a comunicar com os seus amigos e não com pessoas que desconhece pessoalmente. Tenha uma conversa directa e clara sobre este assunto porque, para muitas crianças, dizer para não se encontrarem com um estranho pode não ser claramente percebido uma vez que se conhecem essa pessoa *online*, então já não é um estranho para elas.
5. **Garanta que o seu filho não utiliza o nome completo.** Explique porque não deve utilizar nem o nome completo nem o nome completo dos seus amigos, encoraje-o a utilizar um *nickname* que não deixe impressões erradas.
6. **Seja cauteloso na informação que o perfil do seu filho contém.** Confirme que o perfil não contém qualquer tipo de informação que possa, directa ou indirectamente, identificá-lo.
7. **Considere utilizar um sítio que tenha permissões de modo a que nem todos possam ver tudo.** Alguns sítios permitem a utilização de credenciais por forma a que o sítio do seu filho seja visível apenas por quem ele conhece. Por exemplo, com o *MSN Spaces* pode colocar permissões na utilização desde qualquer pessoa na internet até às pessoas que escolher.
8. **Seja especialmente perspicaz nos detalhes das fotografias.** Explique que as fotografias podem revelar muita informação pessoal, pelo que não devem conter elementos que possam

servir de identificação, tais como nomes de ruas, matrículas de carros, nome da escola, etc.

9. **Mantenha uma comunicação aberta.** Encoraje-o a partilhar consigo se ele encontrar algo que o deixe desconfortável ou ameaçado. Se isso acontecer, não perca a calma, é fundamental que ele perceba que não arranja problemas por falar consigo.
10. **Se necessário, tome a medida drástica: remover a página do seu filho.** Caso ele se recuse a cumprir com as regras atrás referidas.

(1) Para saber o que é o **phishing** veja a *newsletter* de segurança número 4, Setembro 2004; número 5, Outubro 2004; número 6, Novembro 2004; Número 7, Dezembro 2004; número 12, Maio 2005; número 13, Junho 2005; número 21, Fevereiro 2006; número 24, Maio 2006; número 25, Junho 2006 e número 28, Setembro 2006.

Fonte: Microsoft

Topo 



## Princípios básicos de segurança

### Back to Basics... Como aumentar a segurança do computador e proteger a sua informação pessoal

#### Cavalo de Tróia (*Trojan*)

O Cavalo de Tróia é um programa de código malicioso, que aparenta ser software útil mas compromete a segurança dos computadores ao executar acções inesperadas e não autorizadas. Apesar de comprometer a segurança dos sistemas, não se propaga, como acontece com um vírus.

#### Vírus

Um vírus é um programa que possui a capacidade de se replicar. Como tal, pode propagar-se muito rapidamente e é, muitas vezes, de difícil erradicação.

Os vírus podem propagar-se através de ficheiros enviados de utilizador para utilizador como, por exemplo, anexados a mensagens de correio electrónico, infectando um elevado número de computadores em escassos minutos, com consequências desastrosas.

Os vírus com rotinas de actuação apenas se activam quando determinadas condições estão reunidas. Podem, por exemplo, activar-se em datas específicas ou a partir de determinadas acções do utilizador infectado.

#### Como podemos proteger e aumentar a segurança do nosso computador?

Existem várias formas de protegermos o nosso computador contra códigos maliciosos sendo a principal através da utilização de um antivírus de confiança, tendo o cuidado de o manter permanentemente actualizado.

#### Cuidados a ter com o correio não solicitado

Nos últimos anos, com a utilização regular dos emails, tornou-se necessário ter o cuidado de verificar se o anexo ou o *link* contido numa mensagem de correio electrónico provêm de um emissor de confiança. Em caso de dúvida, deve eliminar a mensagem uma vez que a maioria dos vírus se propagam por esta via.

Cada vez mais, as nossas caixas de correio electrónico são inundadas de correio não solicitado. Por vezes, essas mensagens remetem para *links* onde são solicitadas informações de carácter pessoal ou confidencial, cujo objectivo é recolher informação visando a sua eventual utilização maliciosa. São as chamadas acções de *phishing*.

Os links de *phishing* abrem páginas que são cópias do site do Millennium bcp, solicitando o preenchimento de dados para, posteriormente, aceder às contas dos Clientes.

O Millennium bcp reforça as seguintes regras básicas para realizar uma utilização segura dos serviços de *internet banking*:

- O acesso ao site do millenniumbcp.pt deverá ser sempre **efectuado através de digitação directa** do endereço respectivo. Se receber uma mensagem de correio electrónico, que solicite o acesso ao site do Millennium bcp através de um *link*, desconfie! As **mensagens de correio**

**electrónico enviadas pelo Millennium bcp** nunca contêm *links* nem qualquer **software** para instalação imediata;

- **Os Clientes nunca deverão introduzir as suas credenciais** em sites que tenham origem em *links*, provenientes de mensagens de correio electrónico ou de outros sites da Internet;
- **Nunca são solicitados** elementos de carácter privado ou confidencial aos seus Clientes, por via de mensagens de correio electrónico.

Sempre que tenha dúvidas ou necessite de esclarecimentos, consulte a área de Segurança do millenniumbcp.pt ou contacte-nos através do telefone 707 50 24 24.

[Topo](#) 

***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.*

*Banco Comercial Português, S.A., Sociedade Aberta com Sede na Praça D. João I, 28, Porto, o Capital Social de 4.694.600.000 Euros, matriculada na Conservatória do Registo Comercial do Porto sob o número único de matrícula e de pessoa colectiva 501 525 882*

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

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

## Security Newsletter

**Millennium**  
bcp

nº 45

July 2008

%%Exm%% %%customerName%%



### Highlights

How to help your kids use social networking websites more safely.

[More](#) 



### Basic security principles

Back to Basics... How to improve your computer's security and protect your personal information.

[More](#) 

[Versão portuguesa](#)



## Highlights

# How to help your kids use social networking websites more safely

Don't fool yourself! Social networking websites are extremely popular among youngsters. And they're here to stay. That's why it is so important to realise what these sites are all about, why they're so popular and, above all, how our kids can use them more safely.

Times have changed. These are more dangerous days, and it's no longer common to see kids playing out in the streets with their friends. In their free time, especially now that summer holidays are here, kids use new technologies to meet new friends. It's not out of the ordinary for your child to have friends literally stretched across the four corners of the world! On top of real-time communications (e.g. Windows Live Messenger), more and more teens keep an online public record of their activities and, since the youngest don't want to be left behind, this kind of activity is typical, even among young children.

Some years back, creating a webpage was an arduous task, left to professionals. Nowadays it's become so easy that children have no trouble creating and maintaining their own page. These pages are typically stored online on social networking sites such as Windows Live Spaces (<http://spaces.live.com>), MySpace, Facebook, Hi5, among others. According to Wikipedia ([http://en.wikipedia.org/wiki/List\\_of\\_social\\_networking\\_websites](http://en.wikipedia.org/wiki/List_of_social_networking_websites)), there are at least 132 social networking websites!

On its own, a social networking website is nothing to worry about. Youngsters can keep personal pages where they can express their own emotions, tastes and preferences, such as their favourite books, games, subjects, etc. By sharing web addresses, they can easily meet others who have things in common with them, establishing online friendships. The problem lies in improper uses. These sites, as a general rule, gather lots of (more or less confidential) information on its users, such as videos, photos, full name, address, school, mobile phone number, email address... well, all in all constituting a breakdown in privacy if certain basic security measures are disregarded. Unfortunately, there are what are known as 'predators' out there, who take advantage of the innocence the young users of these networks.

Just recently (June 2008) a phishing(1) attack was detected against Hi5 and FaceBook, probably affecting many thousands of users. This attack began when spam was sent using a network of 'slave' PCs (*botnet*), featuring webpages which were in fact very good fakes. One of the goals of this attack was to obtain the identity of the users of these networks; believing they were viewing the right webpage, users entered their log-in information (user name and password). The attackers, once they had this information, could pass off as a user and get benefits illicitly.

All this does not mean that social networking sites should not be used - only that a more secure use is in order. For that purpose, we recommend you take the following steps into account:

1. **Establish Internet usage rules at home.** When your kids start using the Internet, it's important that certain rules are clearly in place. There must be no doubts as to what they can/can't do. These rules must include when and how they should use social networking websites.
2. **Make sure your kids respect age limits on websites.** Generally the minimum recommended age for using a social networking website is 13. If your kids are younger, then do not let them use these websites. Unfortunately there are no effective measures of checking someone's age online.
3. **Learn the most you can about the website.** Use the website before your children do. Read the privacy policy and terms of use and find out if the website verifies the content of what is on it. After your children have created their webpage, check it from time to time.
4. **Make it very clear to your children that they must NEVER meet up with anyone with whom they have only communicated online.** Children may place themselves in danger if they meet up with people they have only met online. This is how predators typically operate. They meet people online, gain their trust and then attack. Encourage your children to communicate only with their friends and not with people they do not know personally. Have a direct and clear talk with them on this issue since, for many children, telling them not to meet up with a stranger may not be understood correctly because, for them, if they've met someone online, they may feel that they're no longer strangers.

5. **Make sure your children do not use their full names.** Explain why they shouldn't use their (or their friends') full name, and prompt them to use a nickname that doesn't give off the wrong idea.
6. **Be careful about the information on your children's profile.** Confirm that their profile doesn't contain the type of information which may, directly or indirectly, identify them.
7. **Think about using a website which uses permissions, so as to determine who can view the webpage.** Some websites allow you to use credentials so that your kids' websites are only visible to their acquaintances. For example, in MSN Spaces you can set usage permissions if you like.
8. **Pay special attention to details on photos.** Explain that photos may reveal a lot of personal information and shouldn't contain identifying elements, such as street names, licence plates, school name, etc.
9. **Maintain an open communication.** Encourage your kids to confide in you if something happens which leaves them uncomfortable or if they feel threatened. If this happens, keep your calm, for it's imperative that they understand that they won't be in trouble if they open up to you.
10. **If necessary, take a drastic step: remove the webpage.** That is, if your child doesn't follow these rules.

(1) To learn more about **phishing** read Security Newsletter no. 4, September 2004; no. 5, October 2004; no. 6 November 2004; no. 7, December 2004; no. 12, May 2005; no. 13, June 2005; no. 21, February 2006; no. 24, May 2006; no. 25, June 2006 and no. 28, September 2006.

Fonte: Microsoft

[Top](#) 



## Basic security principles

### Back to Basics... How to improve your computer's security and protect your personal information

#### What is a Trojan?

A Trojan is malicious code that looks like useful software but which compromises computer security by executing unexpected and unauthorised actions. Even though it does compromise the system's security, it does not propagate, like a virus does.

#### What is a Virus?

A virus is a self-replicating programme. As such, it can propagate very quickly and is, more often than not, very difficult to eliminate.

Viruses can propagate through files sent between users (e.g. email attachments), thus infecting many computers in a few minutes, with disastrous effects.

Some viruses have payloads, which are only activated under certain conditions. They might, for example, be activated on a certain date or be triggered by certain actions of the infected user.

#### How can we protect and increase the security of our computer?

There are a number of ways of protecting your computer against malicious code - most importantly the use of reliable and updated antivirus software.

#### Security precautions regarding junk mail

During the past few years, with the widespread use of emails, it has become necessary to check whether attachments or links in emails have been sent by a sender you trust. In case of doubt, it's best to simply delete the message, since most viruses spread through this method.

More and more, our inboxes are flooded with junk mail. Sometimes these messages contain links to pages requesting personal and confidential information. Their goal is to collect information for possible malicious use. This is called phishing.

Phishing links lead to replicas of the Millennium bcp website, where you are requested to provide details so that they can later access your accounts.

Millennium bcp would like to stress the following basic rules for secure online banking:

- When accessing the millenniumbcp.pt website you should always **directly type our address into the browser**. If you receive email asking you to click on a link to access Millennium bcp, be suspicious! **Emails sent by Millennium bcp** never contain links nor any software requiring immediate installation;
- **Clients must never enter log-in information** in websites originating from links found in emails or other internet websites;
- **We never ask our Clients for** private or confidential information by email.

If you have any doubts or require further information, please go to the millenniumbcp.pt Security area or call us on 707 50 24 24.

---

Top 

***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.*

*Banco Comercial Português, S.A., Sociedade Aberta com Sede na Praça D. João I, 28, Porto, o Capital Social de 4.694.600.000 Euros, matriculada na Conservatória do Registo Comercial do Porto sob o número único de matrícula e de pessoa colectiva 501 525 882*

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

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