# Newsletter de Segurança

Millennium bcp

nº 58 Maio de 2012

## Em destaque

Conheça os conceitos mais importantes para a sua proteção.

Mais

## Princípios básicos de segurança

Proteger a sua privacidade na Internet.

Mais

English version


Visite a área de Shopping no *site* do Millennium bcp

## Em destaque

### Conheça os conceitos mais importantes para a sua proteção

Com a utilização das novas tecnologias e o acesso massivo à internet, surgem, cada vez mais, novos esquemas de roubo de informação pessoal e confidencial, associados ao mundo virtual.

Recordamos então alguns conceitos importantes para que possa facilmente identificar ameaças e assim promover a proteção dos seus dados pessoais e confidenciais e do seu computador:

- *Phishing*
- *Pharming*
- *Smishing e Vishing*
- Engenharia social
- *Malware*
- *Spam*
- *Spyware*
- Vírus
- *Worms*
- Cavalo de Troia (*Trojan*)

- *Phishing*
  Ação que visa roubar dados pessoais. Tem normalmente como origem o envio de mensagens de correio eletrónico que conduzem o utilizador a *sites* falsos, cópias fiéis daqueles a que o utilizador acede habitualmente, solicitando a introdução de dados confidenciais.

- *Pharming*
  Atividade realizada por *hackers* informáticos que, com intenções criminosas, redirecionam o tráfego da internet de um *website* para outro idêntico, por forma a enganar e convencer os utilizadores a introduzir os seus dados pessoais no *site* falso. Semelhante aos esquemas de *Phishing*, o *Pharming* é mais insidioso uma vez que redireciona o utilizador para um *site* falso, sem qualquer participação ou conhecimento da parte do utilizador.

- *Smishing e Vishing*
  Ações que visam roubar dados pessoais. Em vez do tradicional *email*, utilizado no *Phishing*, o *Smishing* e o *Vishing* utilizam, respetivamente, o SMS e o Telefone (voz) para tentar obter informações pessoais e confidenciais.

- Engenharia social
  Designam-se por engenharia social as técnicas utilizadas para obter informações importantes ou sigilosas através de ações que enganam ou exploram a confiança das pessoas. Para isso, são enviadas mensagens em nome de empresas ou organizações com as quais o recetor terá algum

tipo de relação, contendo, na sua maioria, avisos de consequências negativas caso não haja resposta às mesmas.

- *Malware*
  Termo proveniente de *software* malicioso (malicious *software*). Trata-se de um *software* que tem como objetivo infiltrar-se no sistema de um computador, de forma ilícita, podendo causar danos ou apoderar-se de informação.

- *Spam*
  Envio massivo de correio eletrónico não solicitado, que pode ter como objetivo a propagação de vírus para recolha da lista de contactos do utilizador ou de ficheiros.

- *Spyware*
  Termo geral usado para *software* que executa certas ações como divulgação de publicidade, recolha de informação pessoal ou alteração da configuração do computador, geralmente sem obter o consentimento do destinatário. Utiliza manobras de disfarce da origem da mensagem e permite aos seus autores reunir dados sobre os gostos do utilizador, tipicamente utilizada para fins publicitários ilegais.

- Virus
  Um vírus é um programa informático que tem como objetivo infetar um computador e que possui a capacidade de se replicar. Como tal, pode propagar-se muito rapidamente e é, muitas vezes, de difícil erradicação. Pode propagar-se através de ficheiros enviados de utilizador para utilizador (por exemplo anexado a mensagens de correio eletrónico) ou pode ter rotinas de atuação, ativando-se apenas quando determinadas condições estão reunidas (datas específicas ou a partir de determinadas ações do utilizador).

- *Worms*
  Programa malicioso capaz de se propagar automaticamente através de redes de computadores, enviando uma cópia de si mesmo a cada computador da rede. A diferença para um vírus, é que este programa não necessita ser executado para ficar ativo. A sua rápida propagação ocorre devido a vulnerabilidades nas configurações dos programas instalados no computador. Regra geral, permitem acessos não autorizados e a paralisação das redes e sistemas informáticos.

- *Cavalo de Troia (Trojan)*
  Um Cavalo de Troia (ou Trojan) é um programa malicioso, que, no entanto, aparenta ser útil. Compromete a segurança dos computadores por executar ações inesperadas e não autorizadas. Apesar de comprometer a segurança dos sistemas, não se propaga, como acontece com um vírus.

**Proteja a sua informação. Depende muito de si!**
**Consulte as nossas Newsletters e outros temas de Segurança no *site* do Millennium bcp.**

Fonte: millenniumbcp.pt

Topo

## Princípios básicos de segurança

### Proteger a sua privacidade na Internet

A privacidade na Internet depende da sua capacidade de controlar a quantidade de informação pessoal que fornece e os indivíduos que podem aceder a essa informação. Siga as recomendações práticas apresentadas abaixo e aumente a sua privacidade *online*.

**Comece por ler a política de privacidade do *website***

As políticas de privacidade devem explicar claramente quais os dados que o *website* recolhe sobre si, o modo como são utilizados, partilhados e protegidos, assim como o modo como pode editá-los ou eliminá-los.

**Não partilhe mais informações do que o estritamente necessário:**

- Não publique informações *online* que não gostaria de tornar públicas;
- Minimize a quantidade de dados que o identificam ou que revelem a sua localização;
- Mantenha confidenciais os seus números de conta, nomes de utilizador e palavras-passe;
- Partilhe apenas o seu endereço de correio eletrónico principal ou nome de Mensagem Instantânea (MI) com as pessoas que conhece ou com organizações reputadas. Evite indicar a sua morada ou nome em diretórios da Internet e *sites* de anúncios de emprego;
- Introduza apenas as informações necessárias - frequentemente nos campos assinalados com um asterisco (*) - em formulários de registo ou outros formulários.

**Selecione o grau de privacidade para o seu perfil ou blogue**

Altere as definições do *browser* ou do *website* ou as opções que permitem gerir que pessoas podem ver o seu perfil ou fotografias *online*, o modo como as pessoas o podem pesquisar, as pessoas que podem fazer comentários sobre as suas publicações e o modo de bloquear um acesso não desejado por parte de terceiros.

**Monitorize aquilo que é publicado por outras pessoas**

- Pesquise o seu nome na Internet utilizando pelo menos dois motores de busca. Pesquise por texto e imagens. Se encontrar informações confidenciais sobre si num *website*, procure informações de contacto no *website* e envie um pedido para remoção das suas informações;
- Reveja regularmente o que outros escrevem sobre si em blogues e *website*s de redes sociais. Peça aos seus amigos para não publicarem fotografias suas ou da sua família sem a sua autorização. Se não se sentir confortável com material, tal como informações e fotografias que são publicadas em *website*s de outras pessoas, solicite a sua remoção.

## Proteja as suas informações

**Proteger o computador**

Pode reduzir significativamente o risco de roubo de identidade *online* dando estes quatro passos para proteger o seu computador:

1. Utilize uma *firewall* de Internet
   **Nota:** O Windows 7, Windows Vista e Windows XP com SP2 e SP3 possuem uma *firewall* incorporada e automaticamente ativada;
2. Visite Microsoft Update para verificar as suas definições e procurar atualizações.
   **Nota:** O Microsoft Update também atualizará os seus programas do Microsoft Office.
3. Subscreva *software* antivírus e mantenha-o atualizado. Microsoft Security Essentials pode ser transferido gratuitamente para o Windows 7, Windows Vista e Windows XP.

**Crie palavras-passe forte**

As palavras-passe fortes devem ter no mínimo 14 caracteres e incluírem uma combinação de letras (em minúsculas e maiúsculas), números e símbolos. Devem ser fáceis de memorizar mas difíceis de outros adivinharem.

1. Não partilhe as suas palavras-passe.
2. Evite utilizar a mesma palavra-passe em todo o lado. Se alguém a roubar, todas as informações protegidas por essa palavra-passe ficam comprometidas.

**Limite todas as atividades mais confidenciais ao seu computador doméstico.**

Evite pagar contas, efetuar operações bancárias e compras num computador público ou em qualquer dispositivo através de uma rede sem fios pública.

Alguns *browsers* podem ajudar a apagar o seu rasto num computador público, não deixando vestígios de qualquer atividade específica.

## Proteja-se de fraudes

**Saiba reconhecer indícios de esquemas**

Esteja atento a oportunidades de negócio demasiado aliciantes para serem verdadeiras, anúncios de emprego falsos ou avisos de que ganhou a Lotaria, assim como pedidos para ajudar um desconhecido distante a transferir fundos. Outras pistas incluem mensagens urgentes ("A sua conta será fechada!"), erros ortográficos e gramaticais.

**Pense bem antes de:**

1. Visitar um *website* ou efetuar uma chamada para um número incluído numa mensagem de correio eletrónico ou numa mensagem telefónica – ambos podem ser falsos. Em vez disso, utilize os seus favoritos ou marcadores.
2. Clicar em *links* para vídeos, jogos ou para abrir fotografias, músicas ou outros ficheiros - mesmo que conheça o remetente. Confirme primeiro junto do remetente.

**Procure os sinais que indicam que a página Web é segura**

Antes de introduzir dados confidenciais, procure evidência de que:

1. O *site* utiliza encriptação, uma medida de segurança que codifica os dados à medida que estes atravessam a Internet. Um bom indicador de que o *site* está encriptado é o facto do endereço Web apresentar https ("s" significa seguro) e um cadeado fechado. (O cadeado poderá também estar no canto inferior direito da janela.)


2. Está no *site* correcto, por exemplo, no *website* do seu banco e não num fictício. Se estiver a utilizar o Internet Explorer, um sinal de confiança é uma barra de endereços verde como a que é mostrada acima.

**Utilize um filtro de *phishing***

Obtenha um filtro que o advirta sobre *website*s maliciosos e que bloqueie visitas a *sites* de *phishing* denunciados. Por exemplo, experimente o Filtro SmartScreen incluído no Internet Explorer 8 e 9.

**Seguindo estas indicações, estará a promover a sua privacidade *online*!**

**Fonte: Microsoft**

Topo



# Security Newsletter

Millennium bcp

nº 58 May 2012

## Highlights

Know the top security concepts

More

## Basic security principles

Protect your online privacy

More

Versão portuguesa

Highlights

## Know the top security concepts

Given the way new technologies and internet are massively used, new ways of stealing personal and confidential information are also on the rise in the virtual world.

This is why we'd like to remind you of some important concepts so that you can more easily spot threats and protect the personal and confidential data on your computer:

- Phishing
- Pharming
- Smishing e Vishing
- Social engineering
- Malware
- Spam
- Spyware
- Vírus
- Worms
- Trojan

- Phishing
  An attempt to steal personal data. This normally consists of email messages leading you to fake websites (very good copies of websites you often visit), where you are asked to enter confidential information.

- Pharming
  When hackers redirect, with criminal intent, internet traffic from a website to an apparently identical website in an attempt to trick and convince users to enter their personal details on the fake website. Similar to phishing, pharming is even more insidious since it redirects users to fake websites without them even realising it.

- Smishing e Vishing
  Attempts to steal personal details. Instead of the traditional email (as in Phishing), Smishing and Vishing respectively use SMS (text messages) and telephone (voice) channels to try to obtain your information. People are usually asked to confirm details or send confidential information.

- Social engineering
  Techniques used to gather important or confidential information by tricking people and exploiting their trust. Messages are sent out, supposedly on behalf of companies or organisations the addressees may have some relation to. Most of these messages contain warnings that try to scare receivers into replying.

- Malware
  Combination of the words 'malicious' and 'software . Software that tries to illicitly enter a computer system with the intent of damaging or stealing data from it.

- *Spam*
  Mass sending of unsolicited email, which may have the goal of spreading a virus to obtain contact lists or files.

- Spyware
  General term for software that carries out certain actions, such as advertising, retrieving personal details or changing your PC setup, most often without your consent. It masks the origin of the message and allows its authors to gather data on your preferences, usually for illegal advertising purposes.

- Virus
  A virus is a computer programme created with the intention of infecting a computer and that can replicate itself. As such, it can propagate very quickly and is, more often than not, very difficult to eliminate. A virus can propagate through files sent between users (e.g. an email attachment) and may contain instructions to become active under certain conditions (a specific date or certain user actions).

- Worms
  Malicious software that can automatically propagate itself across a computer network by sending a copy of itself to each computer in that network. Unlike a virus, a worm doesn't need to be executed to become active. Its fast propagation is due to vulnerabilities in the software installed on computers. Generally, worms grant unauthorised access and paralyse networks and computer systems.

- Trojan
  A trojan is malicious software that pretends to be of some use to you. It can compromise your PC's security by carrying out unexpected and unauthorised actions. Even though it does compromise the system's security, it doesn't propagate, like a virus does.

  Understanding these and other security concepts is one of the best ways of knowing how to best protect yourself when surfing the web.

**Protect your information. It depends on you!**
**Read our Newsletters and learn more about other security issues at the Millennium bcp**

**website.**

Source: millenniumbcp.pt

Top

## Basic security principles

## Protect your online privacy

Your internet privacy depends on your capacity to control the amount of personal information you make available and who can access that information. Follow the tips below and increase your online privacy.

**Begin by reading the website's privacy policy.**

Privacy policies must explain very clearly which of your details the website collects, and how it uses, shares and protects this information, as well as how it may come to edit or delete it.

**Don't share more information than you need to:**

- Don't publish information online you wouldn't like to make public;
- Keep the amount of details that identify you or reveal your location to a minimum;
- Keep your account numbers, user names and passwords confidential;
- Only share your main email address or Instant Messaging (IM) nickname with people you know or renowned organisations. Avoid entering your name or address in online directories and job advertisement websites;
- Just enter the mandatory information - usually marked with an asterisk (*) - when registering or filling in other forms.

**Select the privacy level on your blog or profileperfil ou blogue**

Change the definitions on your browser or website, or the options that allow you to manage who can see your profile or photos online, how people can search for you, who can comment on your posts and how you can block others from viewing your information.

**Monitor what other people publish about you**

- Search your own name on the web using at least two different search engines. Search for text and images. If you find confidential information about yourself on a website, look up their contact and ask them to remove all your information from it.
- Review on a regular basis what others write about you in blogs and social network websites. Ask your friends not to publish photos of you or your family without your consent. If you're uncomfortable with material that has been published on other people's websites, ask them to remove it.

## Protect your information

**Protect your computer**

You can significantly reduce the risk of online identity theft by following these four steps:

1. Use a firewall.
   **Note:** Windows 7, Windows Vista and Windows XP SP2 and SP3 already have an inbuilt firewall.
2. 2. Visit Microsoft Update to check your definitions and look for updates.
   **Note:** Microsoft Update also updates your Microsoft Office software.
3. 3. Get antivirus software and keep it updated. Microsoft Security Essentials can be downloaded for free on Windows 7, Windows Vista and Windows XP.

**Create strong passwords**

Strong passwords should have at least 14 characters and include a combination of letters (both lower and upper cases), numbers and symbols. They should be easy to remember but hard for others to guess.

1. Don't tell others what your password is.
2. Avoid always using the same password. If someone steals it, all the information protected by that password will be compromised.

**Limit your most confidential activities to your home computer.**

Avoid paying bills, carrying out banking operations or purchases on shared computers or any device on a wireless shared network.

Some browsers can help you delete your trail on a shared computer, leaving no trace of any specific activity.

## Protect yourself from fraud

### Learn how to spot signs of a scam

Be wary of business opportunities that are too good to be true, fake job ads or notifications that you've won the Lottery, as well as requests to aid a distant stranger transfer funds. Other clues include urgent messages ('We are going to close your account!'), and spelling and grammar mistakes.

### Think twice before you:

1. Visit websites or call phone numbers included in emails or phone messages - they might be false. Instead, use your favourites or bookmarks.
2. Click on links to videos, games, or even open photos, songs or other files - even if you know the sender. First check with the sender.

### Look for signs indicating the webpage is secure

Before entering confidential details, look for evidence that:

1. 1. The website is encrypted - a security measure that encodes data as it crosses the internet. A good sign that a website is encrypted is that its address begins with https ('s' stands for secure) and displays a closed padlock. (The padlock may also be on the bottom-right hand corner of your window.)


2. 2. You're on the right website, that is, for example, that you're on your bank's website and not a fake one. If you're using Internet Explorer, a sign that the website can be trusted is the green address bar, as shown above

### Use a phishing filter

Get a filter that warns you of malicious websites and blocks you from visiting phishing or reported websites. For example, try the SmartScreen Filter included in Internet Explorer 8 and 9.

**By following these tips you'll be protecting your online privacy!**

Source: Microsoft

Top