



## Em destaque

Neste Natal, aproveite as compras online em Segurança!

Mais +



## Princípios básicos de segurança

Crie palavras-passe fortes

Mais +

[English version](#)



# Token Reader

Códigos de Autorização, para confirmação das suas operações na internet, em Portugal ou no estrangeiro.



Visite a área de Shopping do site do Millennium bcp



## Em destaque

### Neste Natal, aproveite as compras online em Segurança!

Efectuar compras pela *Internet* é um hábito cada vez mais comum entre os cibernautas e, se outro motivo não existisse, a simples comodidade justifica a crescente adesão a este tipo de serviço.

Efectuar compras no conforto do lar permite-nos realizar uma análise mais detalhada e, por isso, uma compra mais adequada às nossas necessidades. Tal como fazemos na compra numa loja ou num hipermercado, existem alguns cuidados a ter para garantir que não temos nenhuma surpresa desagradável!

Tenha em atenção as seguintes dicas para quando efectuar compras na *Internet*:

1. **Procure informações sobre a entidade na *Internet*** - Para confirmar a veracidade da empresa pesquise-a pelo nome através de motores de busca. Obtenha referências de amigos e familiares que possam já ter efectuado compras a essa entidade ou pesquise, por exemplo, em foruns de discussão, confirmando que não existem reclamações recorrentes sobre a mesma.
2. **Verifique o endereço físico** do fornecedor, ou seja, se existem contactos de telefone, *e-mail*, fax, etc. Tenha atenção a *sites* que só apresentem contactos de telemóveis. Antes de efectuar uma compra verifique que o contacto corresponde à entidade em questão e qual a sua política de funcionamento.
3. **Confirme os procedimentos** para reclamação, devolução, garantia e outras informações para sua protecção.

4. **Verifique as medidas de segurança** que o *site* adoptou para garantir a privacidade dos seus dados, principalmente em casos em que tenha de introduzir dados pessoais e/ou confidenciais.
5. **Não faculte dados** que não sejam essenciais à compra que está a realizar. Desconfie se lhe forem pedidos dados que nada tenham a ver com a compra em questão.
6. **Guarde o comprovativo** da sua compra bem como o nome do *site* e a referência da mesma para que a possa indicar em caso de necessidade.
7. **Guarde e-mails e/ou mensagens** que tenha trocado com o fornecedor no âmbito da compra ou onde tenham sido discutidas as condições.
8. **Confirme a existência de despesas adicionais** como taxas ou custos de envio, assim como os prazos de entrega ou de execução dos serviços adquiridos.
9. **Exija facturas**, sempre que possível, para comprovar que o produto é fidedigno e não foi roubado. Este documento serve muitas vezes de garantia do produto em caso de necessidade de troca ou devolução por defeitos de fabrico, por exemplo.
10. **Se desconfia que o computador pode estar infectado com vírus** não efectue compras *online* já que ao realizar a transacção necessitará de introduzir dados confidenciais.
11. **Evite as compras através de mensagens de e-mail** com promoções fantásticas. Tenha em atenção que os endereços ou anexos incluídos na mensagem podem levar a páginas falsas onde o objectivo é a obtenção dos seus dados pessoais e confidenciais (acções de *Phishing*). Desconfie sempre de *e-mails* que solicitem a confirmação dos seus dados sem motivo aparente ou por supostas verificações de segurança.
12. **Não faculte os seus dados de registo a terceiros**, mesmo que se apresentem como funcionários de entidade fidedignas.
13. **Utilize passwords complexas** compostas, sempre que possível, por letras maiúsculas e minúsculas, números e caracteres especiais. Não utilize datas de nascimento ou outras referências pessoais já que essas são as primeiras que terceiros, com intenções maliciosas, tentam utilizar.
14. **Verifique a reputação do vendedor** em *sites* de leilões em que normalmente os valores dos produtos são mais baixos. Veja os comentários feitos por outros usuários e os produtos que este vendedor já vendeu/promoveu, desconfiando sempre que os valores estejam muito abaixo do mercado.
15. **Não use computadores públicos** (como os cibercafés) para efectuar compras *online*, já que estes equipamentos podem estar infectados com vírus ou estar a ser alvo de vigilância por terceiros.
16. **Verifique sempre que o site em questão utiliza SSL**, um certificado de segurança onde os dados enviados pelo seu computador até ao servidor da entidade são encriptados (codificados). Para efectuar esta verificação confirme que o endereço inicia com <https://> em vez de <http://>.
17. **Opte por meios seguros de pagamento** ao realizar as suas compras *online* como o pagamento à cobrança ou, por exemplo, o serviço MBNet onde os dados do seu cartão nunca são facultados aos fornecedores.
18. **Tenha especial atenção aos produtos mais procurados** e valorizados nas vendas *online* como, por exemplo, MP3, Consolas de Jogos, Telemóveis, entre outros. Estes produtos são os mais utilizados nas tentativas de fraude *online*.
19. **Desconfie sempre de ofertas espectaculares**, promoções imperdíveis e valores muito abaixo do mercado, sobretudo em situações em que a entidade não lhe seja familiar.

Manter-se informado sobre temas de segurança informática é fundamental. Encontrará alertas de segurança e vários artigos sobre estas temáticas na *Internet*.

**A Segurança das suas Compras *Online* depende muito de si!**



## Princípios básicos de segurança

### Crie palavras-passe fortes

Ter palavras-passe fortes é dos passos mais importantes para o ajudar a efectuar transacções mais seguras.

#### Pontos essenciais para a criação de palavras-passe fortes: comprimento e complexidade

A palavra-passe ideal deve ser longa e constituída por letras, pontuação, símbolos e números.

Ao criar a sua palavra-passe, considere:

- Sempre que possível, utilize pelo menos 14 caracteres ou mais;
- Quanto maior a variedade de caracteres da sua palavra-passe, melhor;
- Utilize todo o teclado, não apenas as letras e os caracteres que utiliza ou vê com maior frequência.

#### Palavras-passe comuns a evitar

Os cibercriminosos utilizam ferramentas sofisticadas que podem decifrar palavras-passe com rapidez. Por isso evite criar palavras-passe utilizando:

- Palavras de dicionário em qualquer idioma;
- Palavras escritas de trás para a frente, erros comuns e abreviaturas;
- Sequências ou caracteres repetidos. Exemplos: 12345678, 222222, abcdefg ou letras adjacentes no teclado (qwerty);
- Informações pessoais. O seu nome, aniversário, número da carta de condução, número do passaporte ou informações similares.

#### Crie uma palavra-passe forte de que se consiga lembrar facilmente

Existem muitas formas de criar uma palavra-passe longa e complexa. Apresentamos-lhe aqui um exemplo que pode facilitar a sua memorização:

Que fazer	Sugestão	Exemplo
Comece com uma frase ou duas (cerca de 10 palavras no total).	Pense em algo importante para si.	As palavras-passe longas e complexas são bem mais seguras.
Transforme as suas frases numa fileira de letras.	Utilize a primeira letra de cada palavra.	applecsbms (10 caracteres)

Adicione alguma complexidade.	Coloque em maiúsculas apenas as letras da primeira metade do alfabeto.	AppLECsBMs (10 caracteres)
Aumente o comprimento com números.	Introduza dois números que sejam importantes para si entre as duas frases.	AppLEC68sBMs (12 caracteres)
Aumente o comprimento com pontuação.	Coloque um sinal de pontuação no início.	?AppLEC68sBMs (13 caracteres)
Aumente o comprimento com símbolos.	Coloque um símbolo no final.	?AppLEC68sBMs" (14 caracteres)

### Teste a sua palavra-passe com um verificador de palavras-passe

Um verificador de palavras-passe avalia, automaticamente, a força da sua palavra-passe. Para saber se é realmente segura, visite o Centro de Protecção e Segurança da Microsoft® e escolha a opção "Segurança do PC" e, na coluna que surge à esquerda, seleccione a opção "Crie palavras-passe fortes".

Fonte: Microsoft®

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 o site do Millennium bcp ou ligue para o número de telefone 707 50 24 24 (Atendimento Personalizado 24 horas).

**Estes e-mails não permitem o acesso directo ao site do Millennium bcp, 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 site do 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 ao site do Millennium bcp e escolha as opções: Contas, Personalização, Dados Pessoais, e posteriormente, Criar / Alterar endereço de e-mail.

Banco Comercial Português, S.A., Sociedade Aberta com Sede na Praça D. João I, 28, Porto, o Capital Social de 6.064.999.986 Euros, matriculada na Conservatória do Registo Comercial do Porto sob o número único de matrícula e de pessoa colectiva 501 525 882.

\* Alguns serviços de e-mail assumem, automaticamente, links em certas palavras, sem qualquer responsabilidade por parte do Millennium bcp.

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

707 50 24 24 / 91 827 24 24 / 93 522 24 24 / 96 599 24 24  
Atendimento personalizado 24 horas



## Highlights

This Christmas go shopping online with Safety!

[More +](#)



## Basic security principles

Create strong passwords

[More +](#)

[Versão portuguesa](#)



## Highlights

### This Christmas go shopping online with Safety!

Shopping online is more and more common among cybernauts. It is so simple and comfortable that this sort of service is really booming.

Buying out of the comfort of your home allows you to pick and choose the items you want at your own pace and purchase that really suits your needs. But just as when shopping at a store or supermarket, we need to take some measures so that unpleasant surprises don't ruin our day!

So take the following tips into account when shopping online:

1. **Look for information on the company on the internet** - To confirm the company is real, look it up using search engines. Try to get references from friend or family members who may have already made purchases from that company, or inquire in discussion forums, for example, that there are no repeated complaints about the company.
2. **Check the physical address** of the supplier, i.e. if there are telephone, email or fax contacts, etc. Be wary of websites that only provide mobile phone contacts. Before making the purchase, confirm that the contact provided really matches the company and check their terms of use.
3. **Get acknowledged with their procedures** regarding complaints, returns, guarantees and other information that may serve to protect you.
4. **Check the security measures** the website has adopted to ensure your details remain undisclosed, especially if you are required to enter personal and/or confidential details.
5. **Do not provide details** that are not essential to the purchase you are making. Be suspicious if you are asked for details that do not concern the purchase in question.
6. **Keep the proof of transaction** and its reference, as well as the website's name for future use, if necessary.
7. **Store emails and/or messages** you may have exchanged with the supplier.

8. **Check if there are additional charges**, such as taxes or shipping costs, as well as delivery or execution times for the acquired services.
9. **Demand an invoice** whenever possible to ensure that the product is trustworthy and has not been stolen. This document can often be used as a product guarantee if you need to exchange or return it due to manufacturing faults, for example.
10. **If you suspect your PC may already be infected with a virus**, do not shop online because you will need to enter confidential details to carry out the transaction.
11. **Avoid shopping from email messages** containing fantastic offers. Keep in mind that the addresses or attachments included in the message may direct you to fake webpages, which are designed to collect your personal and confidential details (phishing). Always be wary if you receive emails asking you to confirm your details for no apparent reason or on account of supposed security checks.
12. **Do not give out your access codes to other people**, even if they present themselves as employees of trustworthy organisations.
13. **Use complex passwords** made up of, whenever possible, lower and upper cases, number and special characters. Do not use birth dates or other personal references since these will be the first things others will use to try to figure out your password.
14. **Verify the seller's reputation** whenever buying at online auctions, where products are cheaper. Read comments from other users and check the products the seller's sold/promoted. Be suspicious if values are way under market price.
15. **Do not use public computers** (e.g. in cybercafés) to shop online. They may be infected with viruses or under someone's surveillance.
16. **Always check that the website uses SSL**, a security certificate whereby data sent by your computer to the company's server is encrypted (encoded). To check this, confirm that the address starts with `https://` instead of `http://`.
17. **Opt for secure means of payment** when shopping online, such as payment on delivery or, for example, the MBNet service, where card details are never given to suppliers.
18. **Pay special attention to products that are highly popular** and valued in the world of online sales, such as mp3 players, games consoles, mobile phones, etc. These products are the most targeted for online fraud.
19. **Always be wary of spectacular offers**, promotions you simply can't miss out and prices much below market price, especially when you are not familiar with the company in question.

**Shopping Online with Safety depends a lot on you!**

Consult our Newsletter and other Security themes on the Millennium bcp website.

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

Top 



Basic security principles

Create strong passwords

Having strong passwords is one of the most important steps towards making online transactions safer.

### Essential points for creating strong passwords: length and complexity

The ideal password must be long and made up of letters, punctuation, symbols and numbers.

When creating your password consider:

- Whenever possible, use at least 14 characters or more;
- The wider the variety of characters in your password, the better;
- Use the whole keyboard, not only the letters and characters you most often use and see.

### Common passwords to avoid

Cybercriminals use sophisticated tools to decipher passwords quickly. So avoid creating passwords that use:

- Words from a dictionary of any language whatsoever;
- Words written in reverse, common errors and abbreviations;
- Sequences or repeated characters. E.g.: 12345678, 222222, abcdefg, or adjacent letters on the keyboard (qwerty);
- Personal information. Your name, birthday, driving license no., passport no. or similar details.

### Create a strong password you can easily recall

There are many ways of creating a long and complex password. Here's an example that might make a password easier to remember:

What to do	Tip	Example
Start with a sentence or two (about 10 words total).	Think of something that's important to you.	I think that long and complex passwords are far safer.
Transform your sentences into a string of letters.	Use the first letter of each word.	ittlacpafs (10 characters)
Add some complexity.	Change only the letters from the first half of the alphabet into capital letters.	IttLACpAFs (10 characters)
Increase the length with numbers.	Enter two numbers that are important to you into your password.	IttLACp68AFs (12 characters)
Increase the length with punctuation.	Place a punctuation mark at the beginning.	?IttLACp68AFs (13 characters)
Increase the length with symbols.	Place a symbol at the end.	?IttLACp68AFs" (14 characters)

### Test your password with a password checker

A password checker automatically verifies the strength of your password. To see if it is really safe, visit

the Microsoft® Safety and Security Center, click on the "PC Security" tab and then on "Create Strong Passwords" on the left-hand column.

Source: Microsoft®

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 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.*

*Banco Comercial Português, S.A., Sociedade Aberta com Sede na Praça D. João I, 28, Porto, o Capital Social de 6.064.999.986 Euros, matriculada na Conservatória do Registo Comercial do Porto sob o número único de matrícula e de pessoa colectiva 501 525 882*

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

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

707 50 24 24 / 91 827 24 24 / 93 522 24 24 / 96 599 24 24  
24 hours Personalized Service