



Em destaque

A "Engenharia Social"

Mais +

[English version](#)



Princípios básicos de segurança

"XP Antivirus 2008" - Embuste em forma de anti-vírus

Mais +



NOVO

Panda Antivirus Pro 2009
protecção mais simples, rápida e intuitiva para o seu computador.
Licença de 2 anos para 3 computadores.

© Panda Security 2008

Visite a área de Shopping em www.millenniumbcp.pt!



Em destaque

A "Engenharia Social"

O que é a Engenharia Social?

Através das chamadas acções de *phishing*, são solicitadas informações de carácter pessoal e confidencial, fazendo-se os *phishers* passar por empresas ou organizações com as quais o receptor das mensagens terá, provavelmente, algum tipo de relação.

É o caso das mensagens enviadas aos clientes de bancos, solicitando a actualização de dados relativos às suas contas bancárias, através da introdução de informação privada/confidencial, com o objectivo de obterem essa informação para uma eventual utilização maliciosa. Estas mensagens contêm, na sua maioria, avisos de consequências negativas caso não haja resposta às mesmas. A estas técnicas de ameaça e persuasão, dá-se o nome de "Engenharia Social".

Inseridas nas diversas formas que a "Engenharia Social" pode assumir, estão as "ofertas" de dinheiro ou comissões em troca da realização de determinadas operações por internet.

São vários os casos publicitados em que são propostas comissões por movimento da conta pessoal (ex: transferências) mas com propósitos fraudulentos.

Que cuidados deverá ter?

Para evitar este tipo de fraudes, deverá ter em conta as seguintes precauções:

- Caso receba um e-mail a pedir informação pessoal ou financeira, não responda nem clique no link da mensagem. Por norma, empresas credenciadas nunca solicitam este tipo de informação por correio electrónico, como é o caso do Millennium bcp;
- Seja cuidadoso a aceitar qualquer tipo de negócio que lhe seja proposto por email, independentemente do remetente, certificando-se da proveniência desse email. Caso tenha dúvidas, contacte as autoridades;
- Verifique regularmente os movimentos das suas contas bancárias.

[Topo](#) 



Princípios básicos de segurança

XP Antivirus 2008 - Embuste em forma de anti-vírus

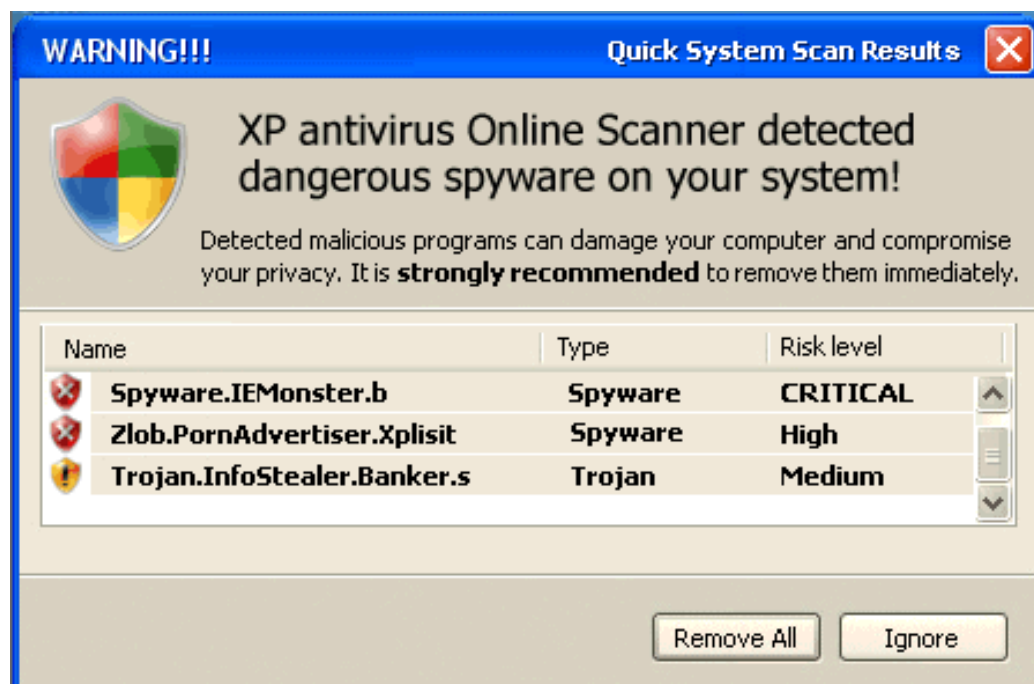
XP Antivirus 2008 - porque é importante prevenir antes de remediar

Nas últimas semanas temos assistido a um tipo de ataque cibernético ao comum utilizador, que se distingue dos restantes pela sua forma estruturada, bem pensada e que, infelizmente, tem afectado muitos, em especial os utilizadores domésticos.

Este vírus tem como objectivo, literalmente, roubar os utilizadores. Por isso, vale a pena perceber um pouco mais como funciona e, acima de tudo, como nos podemos proteger deste e de outros vírus que tenham esta forma de actuação.



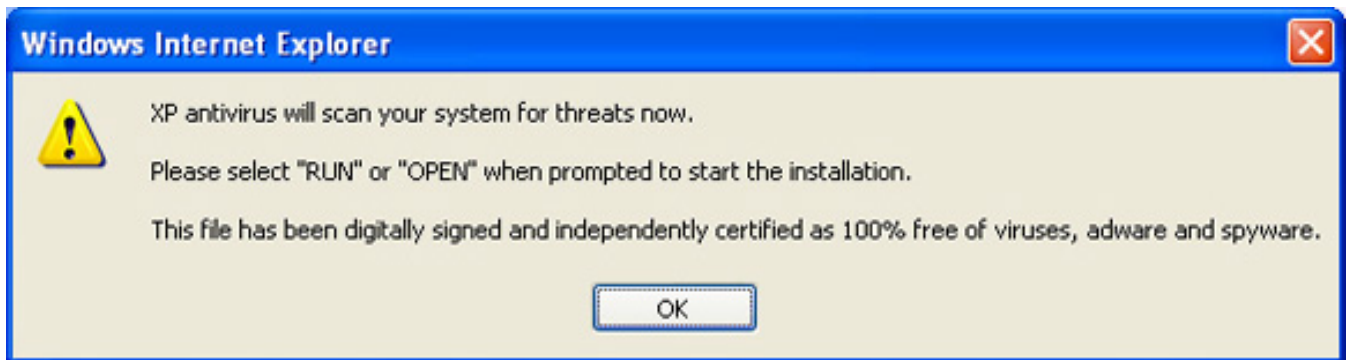
A técnica de propagação é baseada na navegação em sites infectados. A conjugação deste comportamento com uma protecção ineficiente no PC que está a ser utilizado, faz com que apareça uma mensagem como a que abaixo se encontra:



É interessante a perversidade por detrás deste tipo de ataque. O próprio vírus passa por um anti-

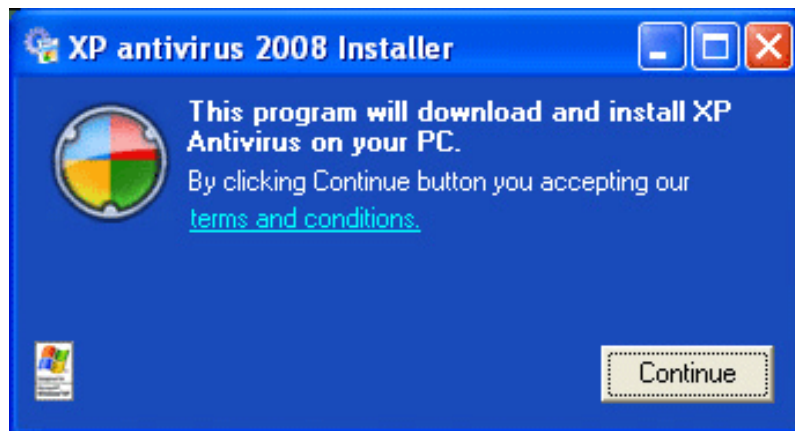
vírus! Esta mensagem, a indicar que o PC está infectado, vai assustar o utilizador e a probabilidade de este escolher a opção **Remove All** é elevada. Mas, neste caso, é irrelevante porque toda a página é apenas uma imagem que tem uma hiperligação que vai despoletar um download. Quando o aviso aparece, a parte de trás fica a cinzento, como se fosse o Vista **User Account Control (UAC)**. E nem todos os ecrãs que apareçam com o fundo a cinzento são sinónimo de que podemos confiar no que lá se encontra!

Como seria de esperar, o utilizador fica alertado que o seu PC está infectado. A forma como essa informação aparece é bastante credível porque se trata do resultado de um GIF animado. O passo seguinte é enviar o utilizador a um site - na altura em que este teste foi efectuado o site era vírus-securityscanner.com (neste momento este site já está inactivo). Não nos podemos esquecer que os criminosos mudam muito facilmente de domínios e de provedores, por isso, a nossa principal preocupação deverá ser nunca baixar as guardas. Na fase seguinte, o pretensu anti-vírus oferece um *scan* gratuito ao PC, no entanto, para tal é necessário instalar algo no PC:



Estamos perante profissionais! Eles sabem que quantos mais avisos o utilizador recebe, menos atenção presta aos mesmos e quer, acima de tudo, resolver aquela situação o mais rapidamente possível. Para tal, acabam por clicar em tudo o que parece ajudar nesse sentido.

O passo seguinte leva à instalação, mostrando mesmo o *Windows compatibility logo* e, inclusivamente, uma hiperligação para os termos e condições.



Se seguirmos os termos e condições aparece um texto bastante bem escrito, tal como seria de esperar de uma entidade idónea, ao ponto de ter um site de suporte *online*!

Chegando a este ponto, a dúvida está criada: se o anti-vírus instalado no PC não detectou estes vírus, então vale a pena comprar este anti-vírus. E é exactamente este o objectivo, levar os utilizadores à compra.

XP antivirus protection - Official web site - Windows Internet Explorer

http://www.xpantivirus.com/support.php

XP ANTIVIRUS protection

Not satisfied with your current Windows antivirus software ?

Make the switch to XP antivirus Protection and enjoy your system work without any influence of spyware and viruses

Solutions for:

- Home and Home Office
- Small and Medium Business
- Enterprises
- Technology licensing

TRY FREE BUY NOW

VIRUS WATCH

latest Virus Alerts

- W32.Trojan.Downloader.s
- W32.Backdoor.j
- Worm.Chernobyl6.a
- W32.FileDeleter.E2.b
- Worm.Trojan.OfficeWorm.k

latest Threats

- Spyware.Wather.ic
- Spyware.CreditCard.er.y
- Adware.Clicker.P2.e
- Adware.TrojanFactory.f
- Spyware.Zlob.d

Seguindo a opção *Buy Now* o sistema irá pedir \$49,95. Se o utilizador não tomar qualquer iniciativa, será bombardeado com mensagens do género:

XP Antivirus 2008 - Threats detected

WARNING! 66 infections found!!!

Unwanted software (malware) or tracking cookies have been found during last scan. it is highly recommended to remove it from Your computer.

- ✗ Lost Documents and Settings
- ✗ Permanent Data Loss
- ✗ System not starting up
- ✗ System Slowdown and Crashes
- ✗ Loss of Internet Connection
- ✗ Infecting other computers on your network

Remove all threats now Continue unprotected

Este tipo de *malware* é deveras perturbador. Por isso chamamos à atenção, uma vez mais, para pontos que são críticos na protecção do seu PC, especialmente o seu PC de casa:

- Tenha um anti-vírus actualizado, de um fabricante conhecido. Ter um anti-vírus só não chega, o mesmo deverá estar actualizado pois uma ferramenta destas desactualizada transmite a falsa sensação de estar tudo sob controlo;
- Não navegue em sites de origem duvidosa; deverá ter o mesmo nível de preocupação no mundo digital que tem no mundo físico. Tenha atenção quando navega pela Internet;
- Não aceite como de confiança tudo o que lhe oferecem, infelizmente existem muitas pessoas que querem tirar partido da ingenuidade dos outros e não olham a meios para o conseguirem.

Como em tudo na vida, mais vale prevenir do que remediar, este é apenas mais um caso onde esta velha máxima continua muito actualizada.

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 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, 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

Se não pretende receber este tipo de informação via e-mail ou se pretende alterar o seu endereço electrónico, aceda a 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



Highlights

"Social engineering"

[More +](#)

[Versão portuguesa](#)



Basic security principles

Malware scam in the guise of "XP Antivirus 2008"

[More +](#)



Highlights

What is social engineering?

Through what is called "phishing", personal and confidential information is solicited. "Phishers" pose as companies or organisations with whom the receiver of these messages might have some sort of connection.

This occasionally happens to bank clients, who receive messages asking them to update bank account details and enter private/confidential information, which will later be used for ill purposes. These messages most often contain warnings of the negative consequences which are to follow if they are not replied to. "Social engineering" is the name given to these techniques of threat and persuasion.

Examples of "social engineering" include an alleged offering of money or commissions in exchange for certain operations which victims must make over the internet.

There are several cases where commissions are offered per transaction on your personal account (e.g. transfers), with fraudulent intent.

What precautions should I take?

To avoid this type of fraud, you should keep the following in mind:

- If you receive an email requesting personal or financial information, don't reply and don't click on links in the message. As a rule, certified companies (such as Millennium bcp) never request this type of information over the internet.
- Think twice before accepting any kind of deal you are offered over the internet, regardless of the sender. You should check from where the email really comes from. If in doubt, contact the authorities;
- Check your bank account statements on a regular basis.

Top 



Basic security principles

Malware scam in the guise of "XP Antivirus 2008"

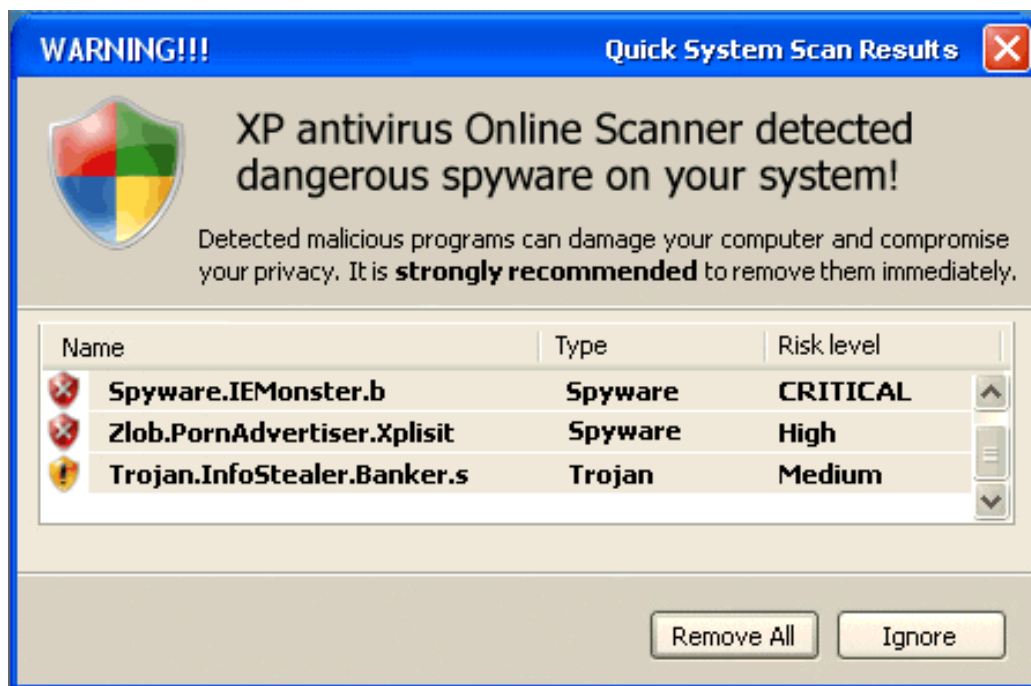
XP Antivirus 2008 - because it's better to be safe than sorry

Over the past weeks a new type of cybernetic attack has been unleashed on the common user. It's different from most: well planned and thought out, it has unfortunately affected many people, in particular home users.

The goal of this virus is to - literally - rob users. That's why it's worthwhile to learn a bit about how it operates and, above all, how you can protect yourself against it and other similarly operating viruses.



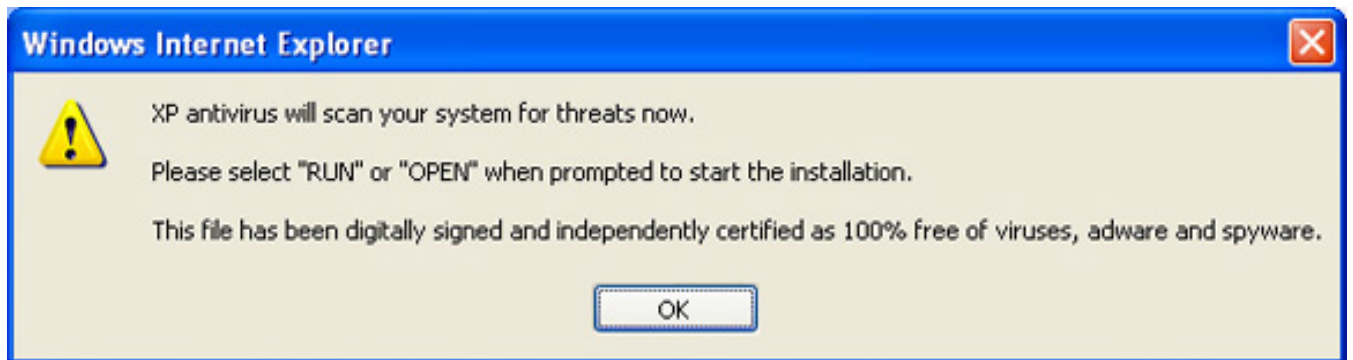
The way it propagates is based on users surfing in infected sites. If users run enter these sites and their PCs are poorly protected, the following message might pop up:



This kind of attack is especially insidious. **The virus is itself posing as an antivirus!** Users receiving a message stating that their PC is infected will most likely get scared, and the odds are they click on

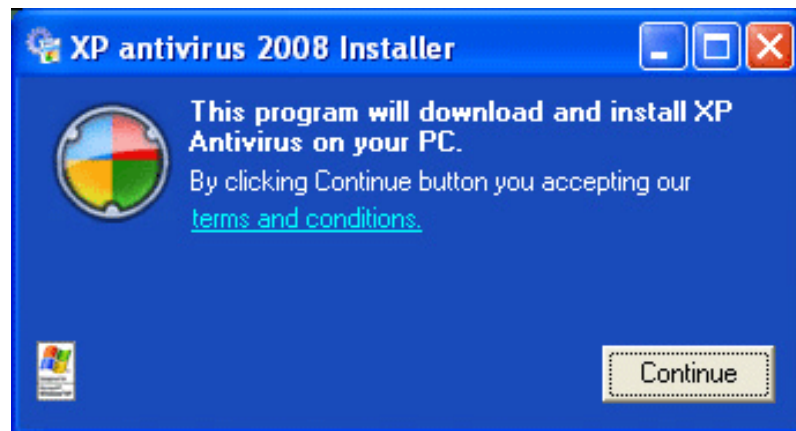
Remove All. In this case, however, it's indeed irrelevant where you click, since the entire page is simply an image with an underlying hyperlink which will trigger a download when clicked on. When the warning pops up, the background becomes gray, as if it were Vista's **User Account Control (UAC)**. (Not all screens of gray background are to be trusted!)

As expected, users are told their PC is infected. The way this information is graphically displayed is quite credible, since it's in the form of an animated GIF. The next step is to send users to a site - at the time this test was run the site was virus-securityscanner.com (which has meanwhile been taken offline). We must keep in mind that web criminals can easily switch domains and servers. Our main concern must thus be never to drop our guard. In the following stage, the alleged antivirus offers to scan your PC free of charge. You are, however, asked to install something on your PC:



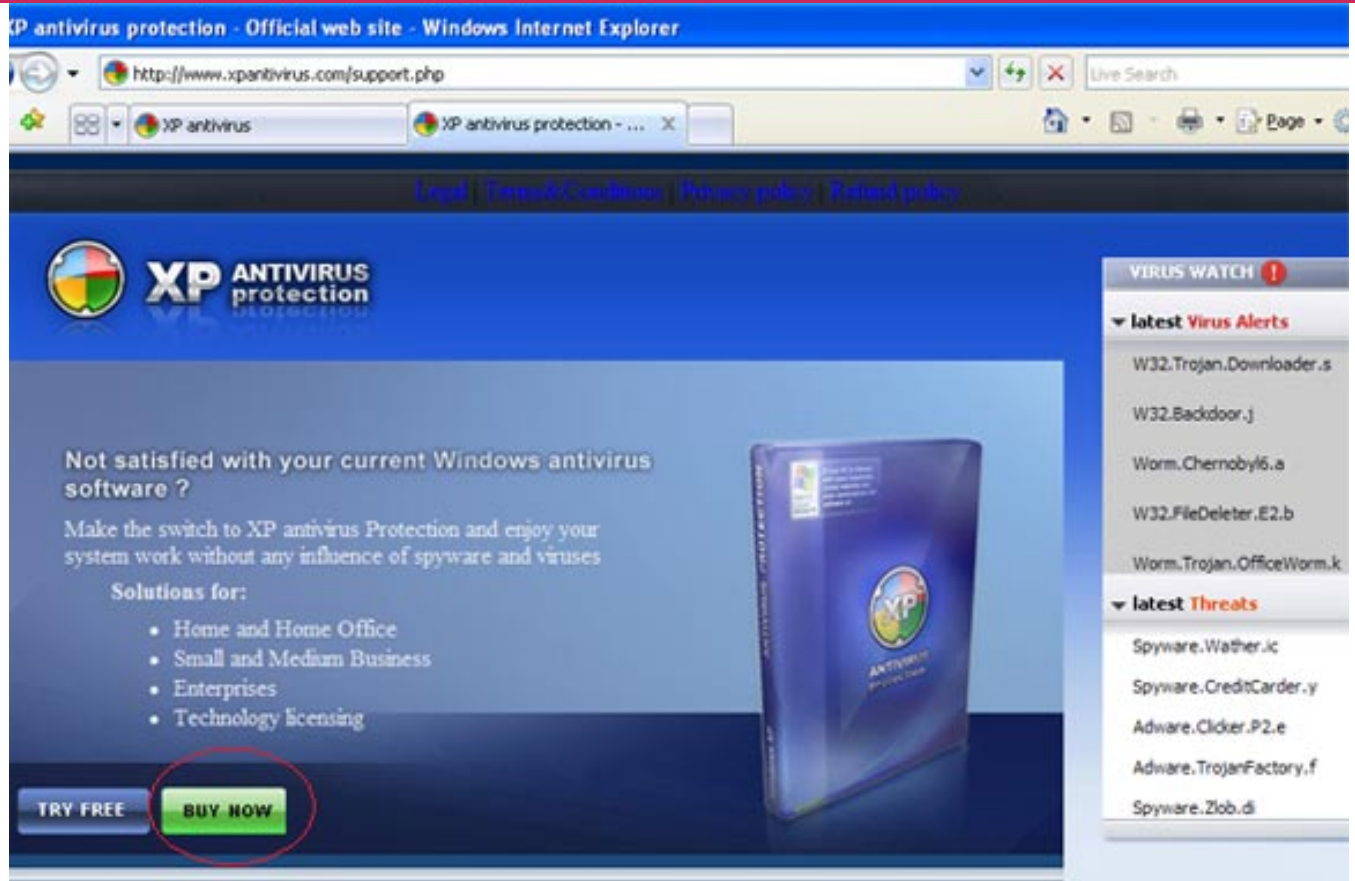
We're looking at pros here! They know that the more warnings users receives, the less attention they pay to them and above all just want to solve their predicament as soon as possible. So they end up clicking on the first and apparently most obvious solution to the problem at hand.

The next step is the installation. There is even a Windows compatibility logo and a hyperlink to terms and conditions.



If we click to read the terms and conditions, a rather well-written text comes up, just like you'd expect from a trustworthy entity - it even has an online support page!

At this point, doubt has settled in: if the antivirus I have on my PC hasn't detected this virus, then I should probably buy this one... That's precisely what they're after - that you purchase the posing antivirus.



If you click on *Buy Now* the system will ask for \$49.95. If you don't do anything, a bombardment of messages such as this one follows:



This kind of malware is very unsettling. That's why we feel it's important to, once again, call your attention to certain steps you should take to protect your PC, especially your home computer:

- Buy reliable antivirus software and keep it updated. Having an antivirus isn't enough - it must be up-to-date. An out-of-date antivirus conveys the false impression that everything is under control;
- Don't surf in sites of doubtful origin; you should be as worried with the digital world as you are with the non-digital world. Be wary when surfing the internet;
- Don't trust everything you're offered. Unfortunately there are many people without scruples in the world wanting to take advantage of others.

As with everything else in life, it's better to be safe than sorry. This is just another case where this old saying is still very up to date.

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 www.millenniumbcp.pt or dial 707 50 24 24.

These emails do not grant direct access to 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

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 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

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