Manual básico segurança para leigos

Sumário

1. Introdução

A maioria das pessoas tem medo ou se sentem inseguras na internet, com medo de cracker's (hacker's do mal) . Com o intuito de esclarecer essas pessoas estou escrevendo este artigo. Na internet temos grandes facilidades, comunicação , agilidade, compras pela internet, movimentação bancaria, etc, seria uma pena não poder usufruir de tais facilidades.
Existem riscos é claro, porém a maioria deles é causada por comportamento de risco dos usuários. Não é nenhum bicho de sete cabeças se manter seguro. Esse manual é destinado à usuarios de WindowsXP, mas a maioria das regras de segurança podem ser aplicadas a outros Windows e mesmo ao Linux, a difrença é que usuarios Linux ao invés de preocupar com antivirus tem que se preocupar com atualização de sistema e firewall.

2. Senhas

Assim como sua casa, seu computador precisa ter uma chave para acessa-lo. Caso você ache mais fácil deixar a porta aberta para você não ter necessidade de chaves, o ladrão também ira gostar disso. Agora o maior problema esta na escolha da senha, existem senhas boas e senhas ruins. As senhas ruins são aquelas que podem ser imaginadas facilmente , por que muita gente usa igual ou que alguns programas de cracker podem descobrir com relativa facilidade. Exemplo de senhas muito ruins:

-senha
-a1b2c3d4
-123456
-54321
-abcdefgh
-”mesmo que o login”: usuário: joao senhas: joao

As senhas acima são as piores, uma outra péssima escolha pra senha são nomes relacionados a você, que uma pessoa qualquer que o conheça possa desvendar. Exemplo:

-nome da namorada/esposa
-nome do filho/filha
-nome do time
-nome do carro que gosta
-preferências religiosas
-data de aniversário

Você deve estar pensando: “Então não posso usar um nome que eu tenha facilidade de lembrar.” Na verdade pode, contanto que seja algo bem grande, por isso é melhor para fazer sua senha uma frase:

-minha “nome da namorada” e muito bonita
-o nome do meu cachorro e toto

-meu time e o melhor de minas
Frases grandes podem ser fáceis de lembrar e se tornam boas senhas, pois são muito difíceis de serem quebradas por programas destinados a roubar senhas. Outro tipo de senha boa é a que mistura letras e números:

-2w9x8dk1
-5ffg9cps
-00s32m5

Porém esse tipo de senha é bem mais difícil de decorar.

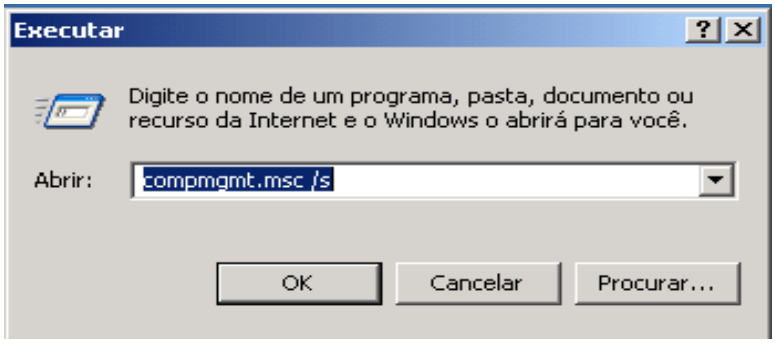
A escolha do nível de segurança da senha, depende do que ela protege. Senhas de banco por exemplo tente colocar sempre senhas bem grandes e se puder decorar misture números . Porém a senha para acessar o seu computador pode ser mais simples, mas evite senhas ruins , com menos de 8 caracteres.

2.1 Definindo senha no Windows

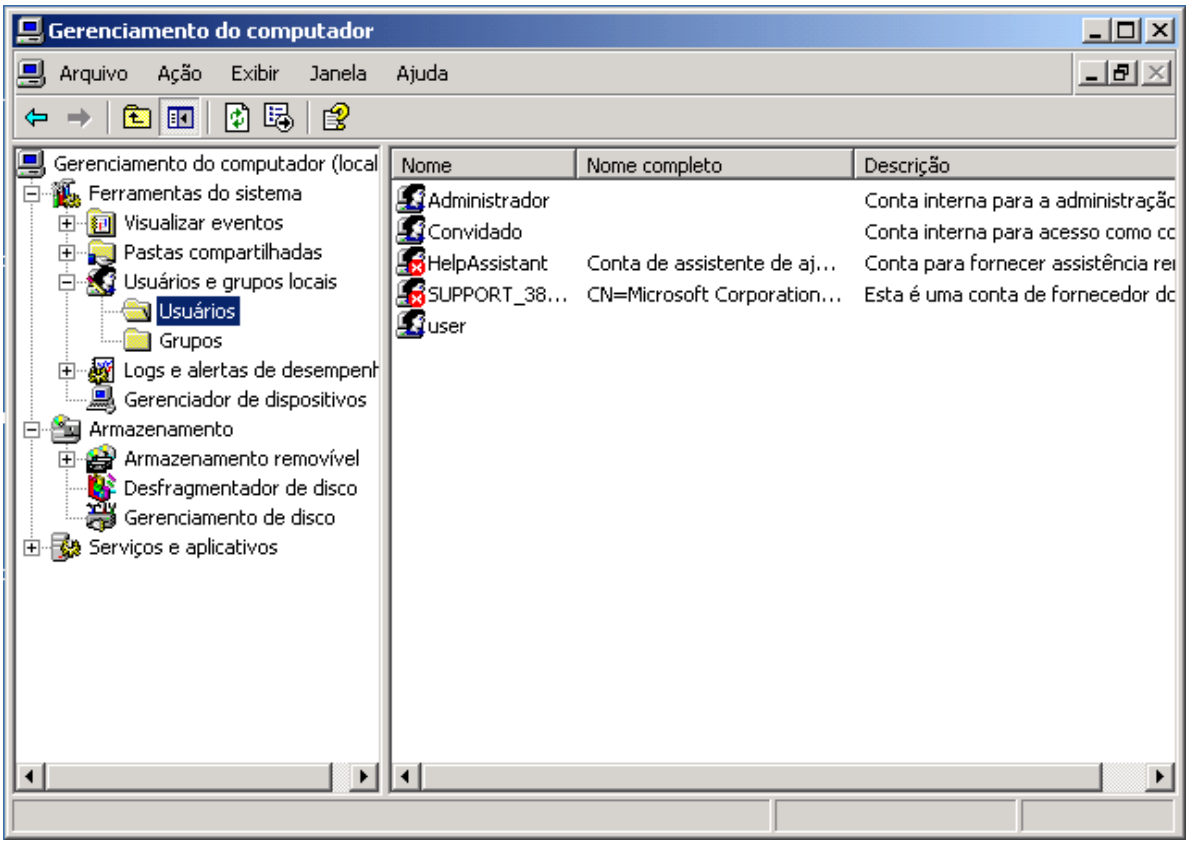
Agora como colocar a senha no sistema? Primeiro vamos ver como fazer isso no Windows XP:

Vamos usar um atalho para acessar o gerenciamento do computador, vá em iniciar, depois na opção executar, dentro da caixa que ira aparecer digite “compmgmt.msc /s”.

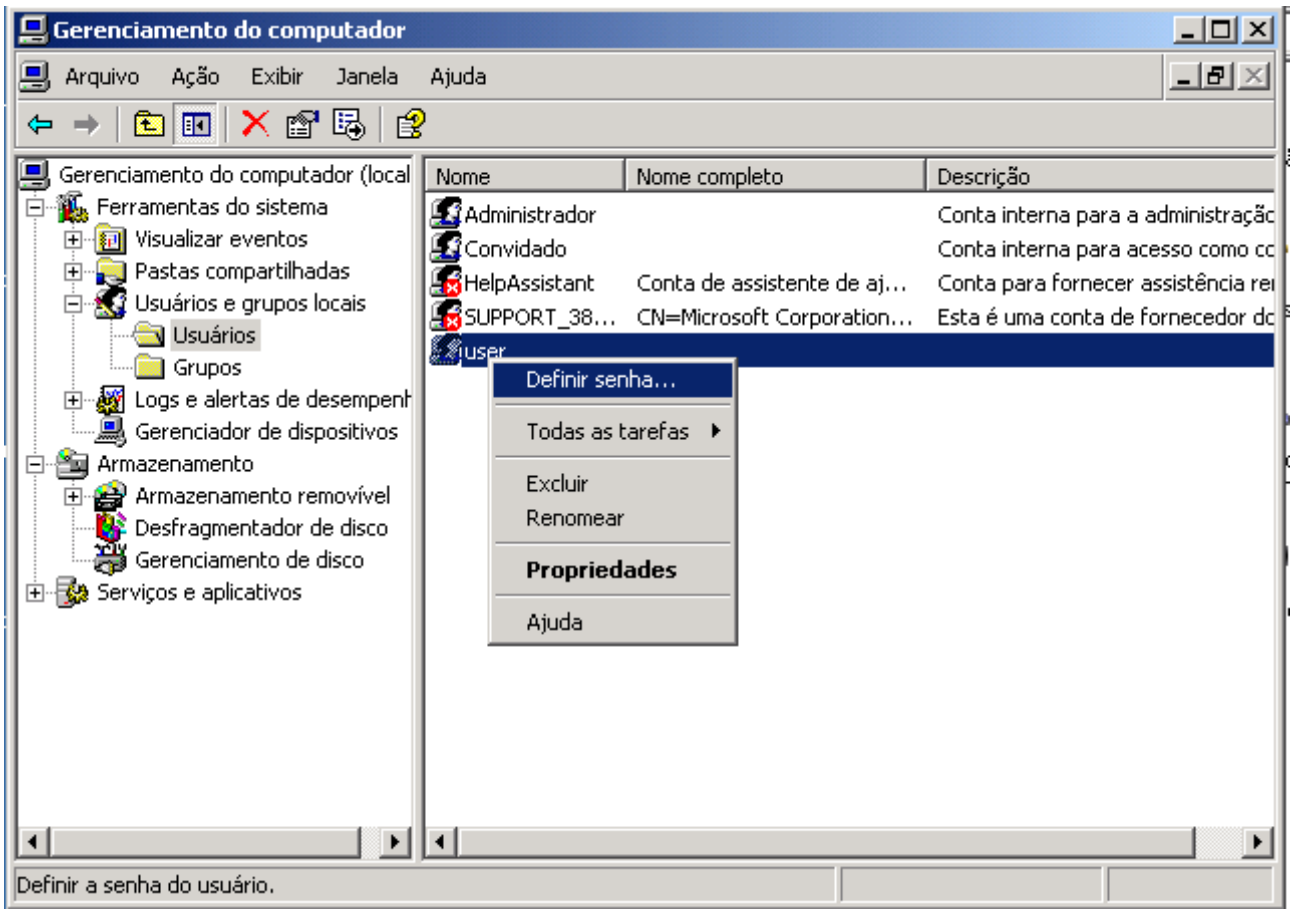
Depois de digitado esse comando iremos entrar na parte do sistema aonde faremos o gerenciamento do computador:



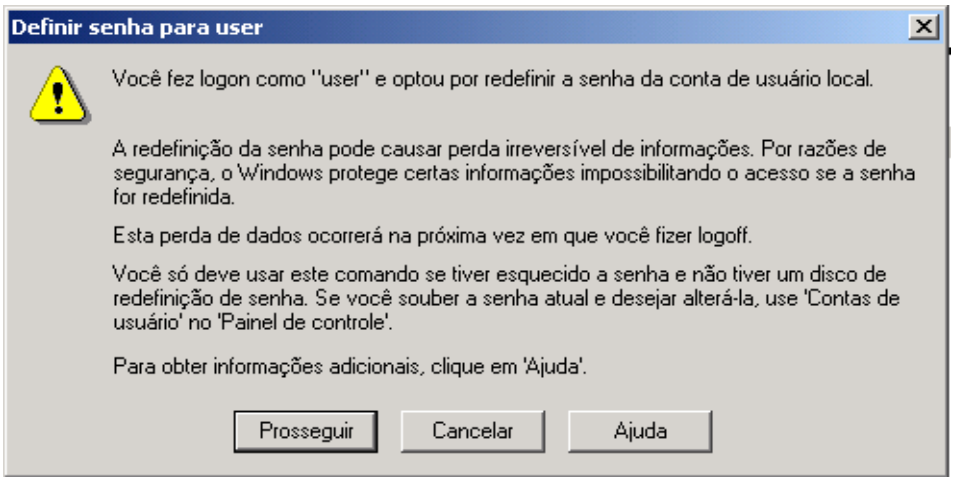
Depois de digitado esse comando iremos entrar na parte do sistema aonde faremos o gerenciamento do computador:



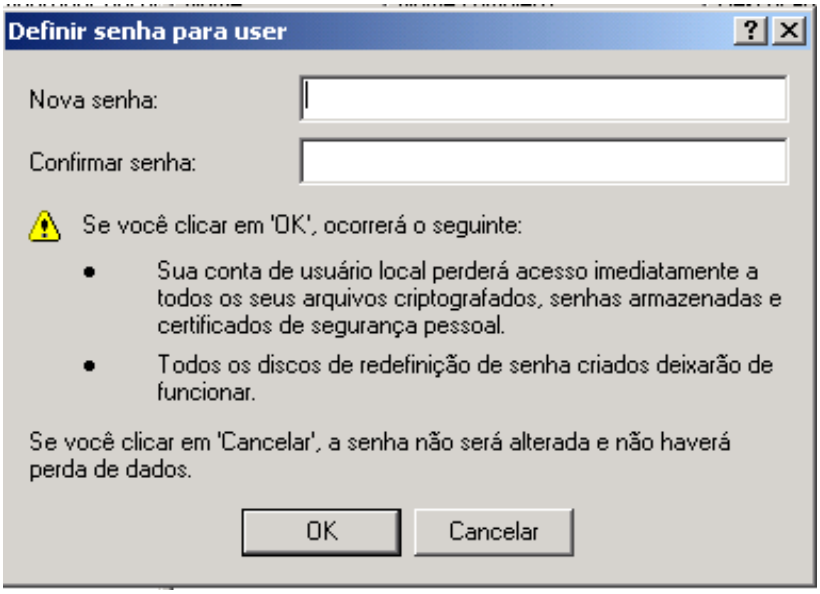
Dentro dele iremos na opção Usuários e grupos locais, depois na opção Usuários, ao lado direito serão listados todos os usuários da maquina. Usuário administrador é uma conta administrativa que toda a maquina Windows tem para gerenciar todos os outros, tem todos os poderes e privilégios, então não adianta nada colocarmos senha em nosso usuário se não colocarmos senha neste. Os usuários convidado, HelpAssistant e SUPORT são usuários do sistema, normalmente desativados e que servem para atividades especificas. Não há necessidade de se preocupar com eles, só não tente ativa-los. Para alterar a senha é muito simples, click com o botão direito sobre ele e ira aparecer a opção definir senha:



Aparecera uma mensagem de alerta, que avisa quanto os problemas de alterar a senha , porém para atividades normais não há risco algum, principalmente se a maquina ainda não tem senha. Apenas click em prosseguir.



Agora apenas coloque a senha desejada no usuário, e depois redigite a senha para confirmar, lembre-se de definir uma senha para cada usuário da maquina, principalmente o administrador.



Além de senha do sistema, você precisa colocar senhas seguras em seu e-mail e contas de banco, ou sua conta que usará para comprar na internet. O procedimento para alterar o senha vai depender de cada provedor de serviço. Você terá de entrar em contato com ele para que haja o esclarecimento de tais procedimentos, porém o mais importante é você saber quando uma senha é ruim, ou quando uma senha é boa.

3. E-mail

3.1-Spam

Em questão de e-mail, vale aquela regra que sua mãe te ensinou quando você era criança, **não converse com estranhos.** E-mails de origem desconhecida, são geralmente a maior porta para ***trojans, worms ou vírus** e conseqüentemente invasões. Esses e-mails são conhecidos por Spam. Um Spam é criado para vários propósitos, como vender produtos, infectar maquinas, derrubar servidores, invasão de maquinas, ou seja são realmente inconvenientes.

*trojan e worm são softwares que se instalam na sua maquina com intuito de algum malefício. No Caso do trojan, também conhecido como cavalo de Tróia , o mesmo vem dentro de algum outro software útil, ou seja disfarçado de presente, igual ao cavalo de Tróia.

3.2-Como conseguem nosso e-mail?

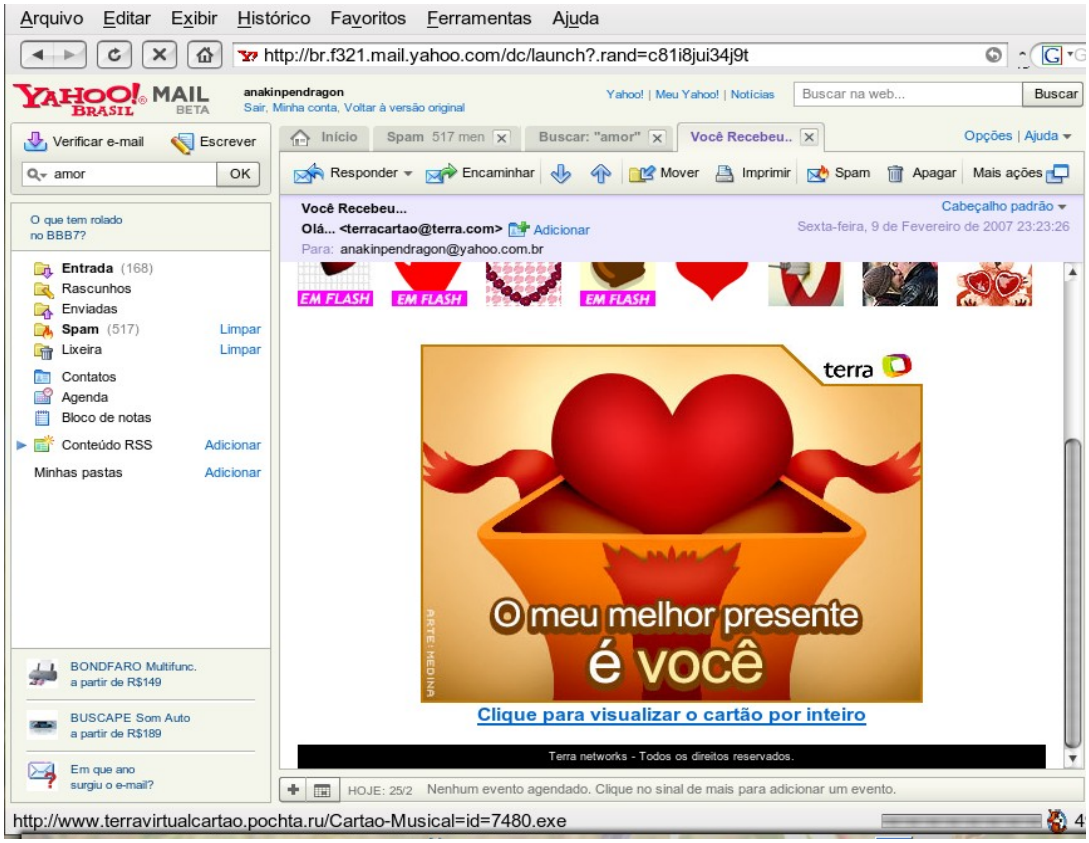
Existem varias formas, ou por meio de um trojan já instalado na sua maquina, ou por algum cadastro que você fez em algum site que não possuía segurança,etc. O que sabemos é que hoje em dia é muito difícil não receber um Spam, por que se você tiver um amigo com a maquina infectada e ele tiver no catalogo de endereços você listado, já é possível que obtenham seu endereço.

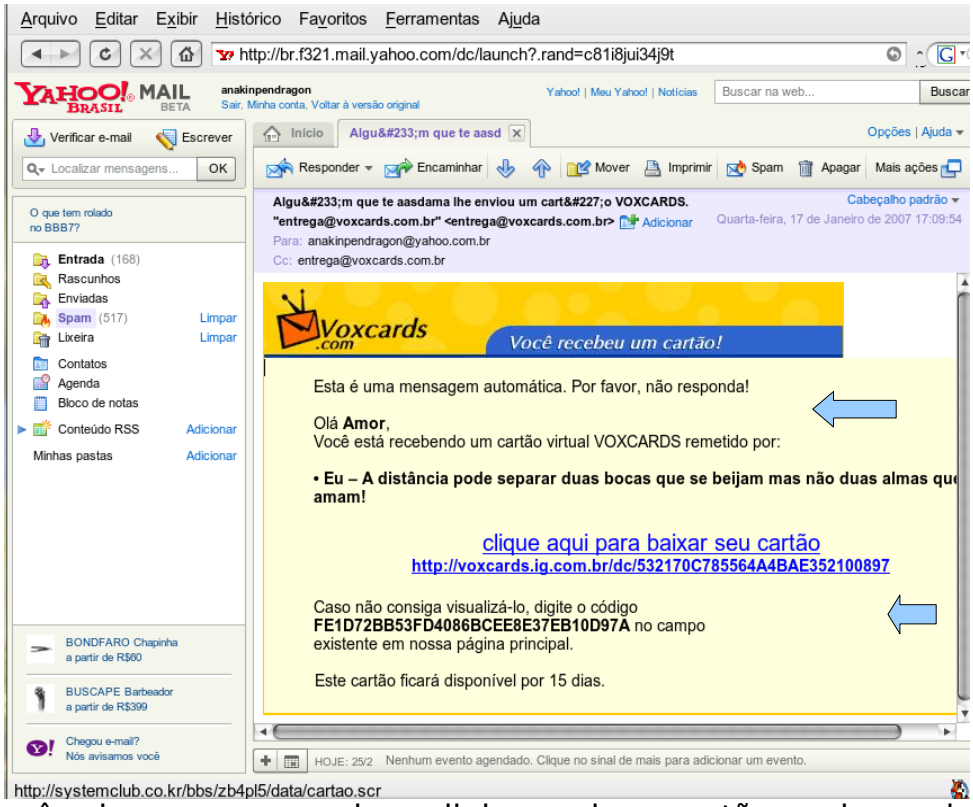
3.3 Nunca responda um Spam!

Responder um Spam é a confirmação de que seu e-mail realmente existe e conseqüentemente vão te mandar mais porcaria.

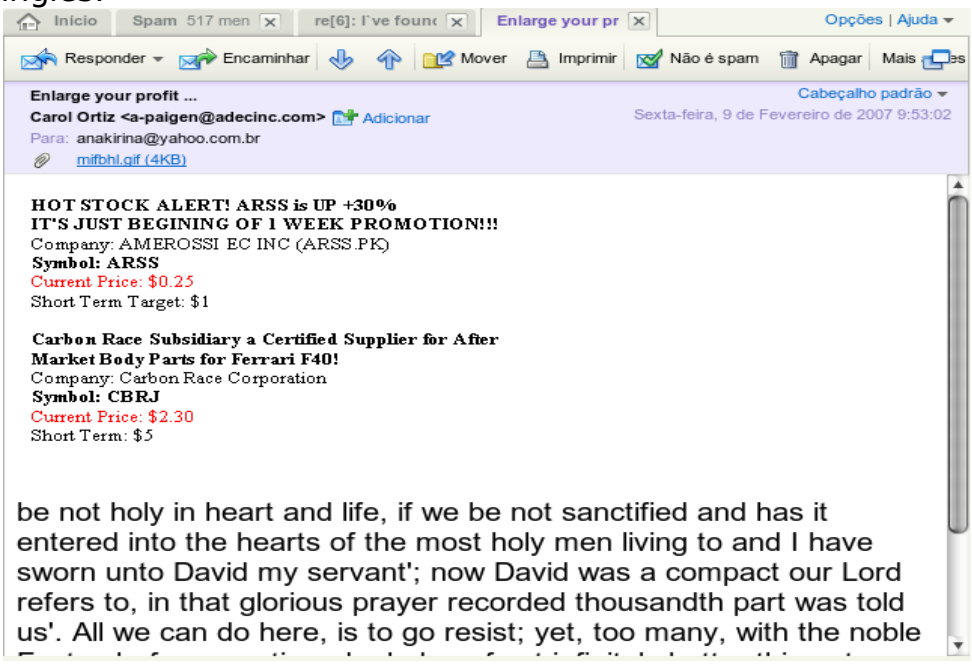
3.4 Como identificar um Spam?

Bom se você receber um e-mail em inglês ou outra língua que você não fale, e todos saibam que você não fala, automaticamente você já pode considerar um Spam. Se vier de alguém que você não conhece, também é bem provável que seja um Spam. **Conto do vigário** , desconfie de qualquer proposta ou promoção, principalmente se oferecer coisas de graça, alguém lembra do conto que a nokia ia dar um celular de graça pra quem repassasse o e-mail que recebeu para 20 amigos? Alguém recebeu? Aproveitam muito da curiosidade dos outros, e-mail com as fotos de mulher pelada, big brother, o que estiver na moda desconfie. E-mails de amor, sem que a pessoa se identifique, ou sequer na mensagem fale seu nome ao menos uma vez, é bem provável que esteja infectado. Veja o exemplo de dois spams muito bem feitos.





Quando você coloca o mouse sobre o link para ir ao cartão, na barra de status do navegador você pode ver o endereço da pagina para onde ele aponta(na parte inferior do navegador). No caso ao invés de apontar dentro da pagina para um arquivo .htm,html, php, asp, cgi, que são os padrões normais de paginas da internet ele aponta para um arquivo 7480.exe e no cartão de baixo para cartão.scr. Esses arquivos são arquivos que contém programas para windows, que no caso se destinam a infectar sua maquina. Perceba como a mensagem é genérica, de forma que o e-mail sirva para qualquer pessoa, inclusive homem ou mulher. Ou seja da pra perceber que é uma mensagem automática, feita para infectar o numero maior da maquinas possíveis. No geral a maioria dos spams estão em inglês:



3.5 Anexos

Os anexos são os arquivos que vem junto ao e-mail. Geralmente mandamos documentos e fotos junto dos e-mails. Porém se vier certos tipos de arquivo junto ao seu e-mail evite abri-los. Os arquivos que podem vir contaminados são os arquivos executáveis de programas, com a extensão **“.exe”, “.pif”, “.scr”, “.bat” .** Mesmo que o e-mail venha de uma pessoa confiável, se ela estiver infectada , o computador irá enviar esses e-mail contaminados para seus conhecidos, sem que ele saiba. Recebendo e-mail com esses arquivos infectados, avise seu amigo para que ele tome as providencias para se desinfectar.

Antigamente havia muita preocupação com arquivos de documentos como arquivos **.doc,** por causa dos vírus de macro. Os vírus de macro são programas inseridos dentro desses documentos, que aceitam algumas linguagens de programação para automatizar tarefas. Atualmente eles são muito raros e não chegam a preocupar como faziam há muitos anos atrás. Um anti-vírus atualizado já dá conta de resolver o problema desses arquivos.

4. Navegando

Navegar na internet além de ser algo agradável, pode ser instrutivo. Temos sites cheios de noticias como portais Terra, Uol. Temos na internet sites recheados de conhecimento como a enciclopédia colaborativa Wikipedia (http://pt.wikipedia.org/) . Sites de compras, moda, receitas, tecnologias, etc. No geral esses sites não representam perigo nenhum. O problema na internet é você ir à lugares obscuros, lugares aonde se cometem crime e prostituição on-line. Sites que geralmente não deixaríamos nossos filhos freqüentarem são os lugares perigosos.

Por exemplo, um site como o terra tem uma serie de profissionais de segurança e um bom nome a zelar, então não é de lá que você vai pegar um vírus, mas por outro lado, se você acessa um site aonde tem as ultimas fotos da playboy de graça, sendo que no site da playboy o acesso é pago, pode estar caindo em uma armadilha. Qualquer site que cometa um crime, não é um site confiável. Evite sites que ofereçam de graça, pornografia, *programas que são pagos oferecidos gratuitamente ou *cracks para destrava-los, musicas e filmes protegidos por direitos autorais distribuídos de graça também são usados como chamarisco para esses sites.

Resumindo, entre em sites que estão dentro da legalidade e você dificilmente terá problema. Entre em sites de criminosos por sua propia conta e risco, não se pode confiar em quem comete crimes.

*crack em informática é um programa que faz um programa shareware (que tem sua função limitada, ou funciona por um determinando tempo) ou um programa que não foi adquirido de forma licita funcionar plenamente.

*Programas são um conjunto de instruções para o computador, que no caso vem armazenado em um arquivo ou um conjunto. Estão nessa categoria então os utilitários como pacote office, anti-vírus, jogos, etc.

5.Prevenindo e remediando

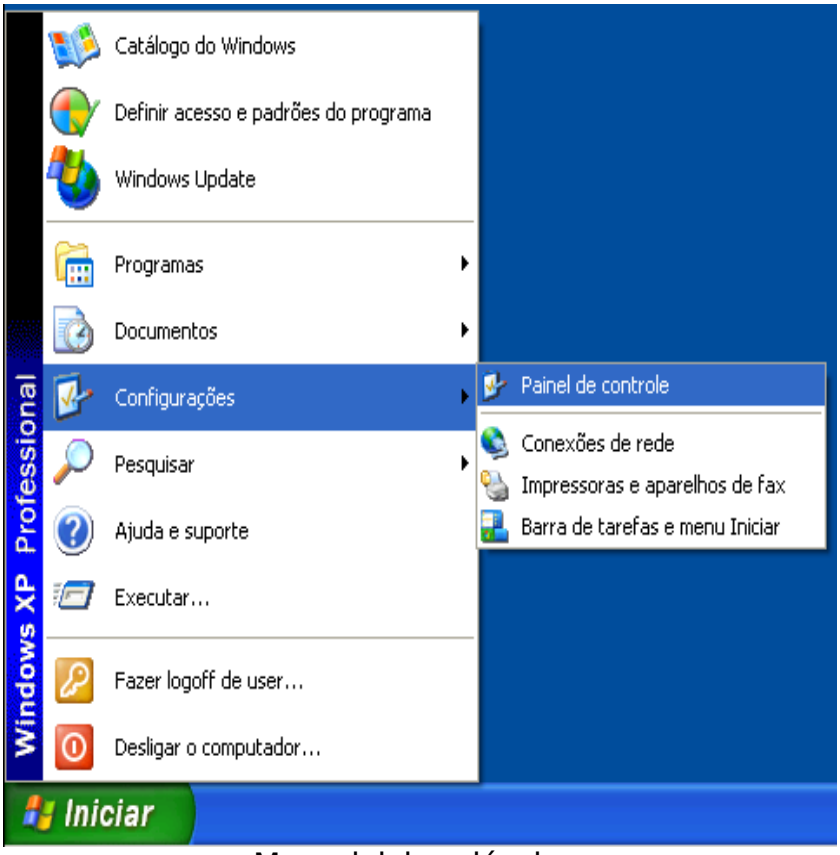
Programas de computador costumam ter falhas, que são utilizadas para invadir e infectar um computador. Resolvemos esses problemas quanto a falha de segurança de três formas, atualizando o programa pela versão mais nova que contém correção para o problema, um bom anti-vírus atualizado, ou um firewall. Obviamente o ideal é ter as três soluções.

5.1 Atualizações de segurança

A Microsoft disponibiliza a solução conhecida como Windows Update. O windows update pode ser utilizado de duas formas, automaticamente e manualmente. Se estiver marcado a opção automática, a vantagem é que você não precisa se preocupar, as atualizações serão feitas sem necessidade de sua intervenção, por outro lado, sua maquina pode sofrer de lentidão na hora em que ele estiver fazendo o processo ao mesmo tempo em que você trabalha. Se fizer o Windows update manualmente você terá que lembrar periodicamente de fazer o processo, mas como poderá escolher a hora em que será feito, pode escolher uma hora em que não esteja usando o computador para outras tarefas , assim não o prejudicando. Windows pirata não tem direito a atualização.

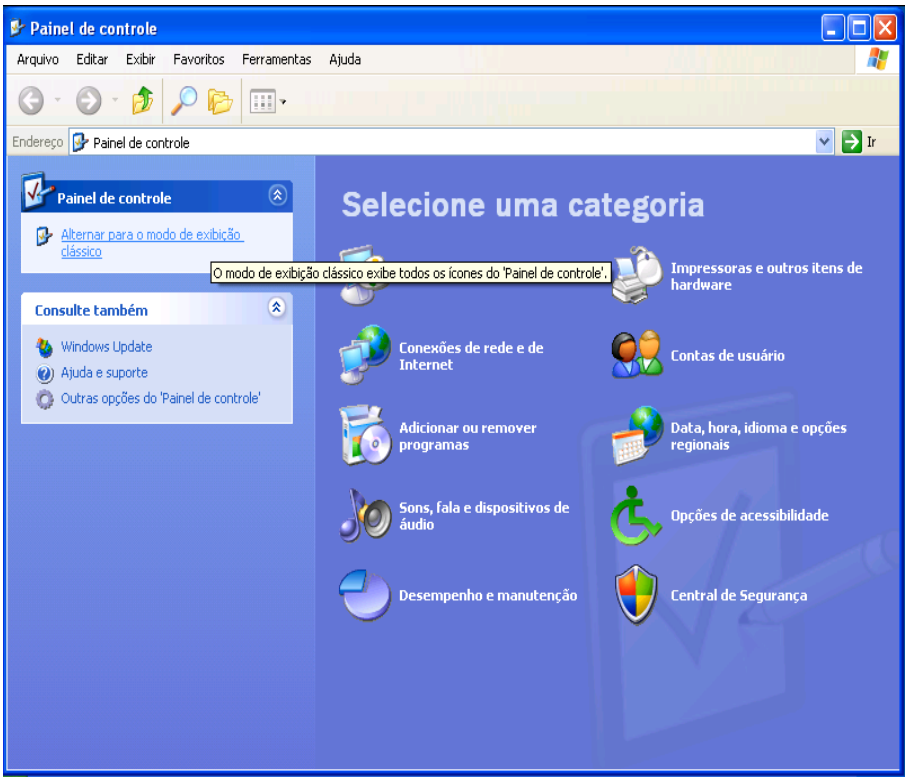
Vamos primeiro ao método mais simples, que é o automático . Primeiramente entraremos no painel de controle. Vá no menu iniciar, depois em painel de controle, ou se o menu iniciar estiver no modo clássico, vá em iniciar, configurações, depois em painel de controle.

Menu iniciar moderno

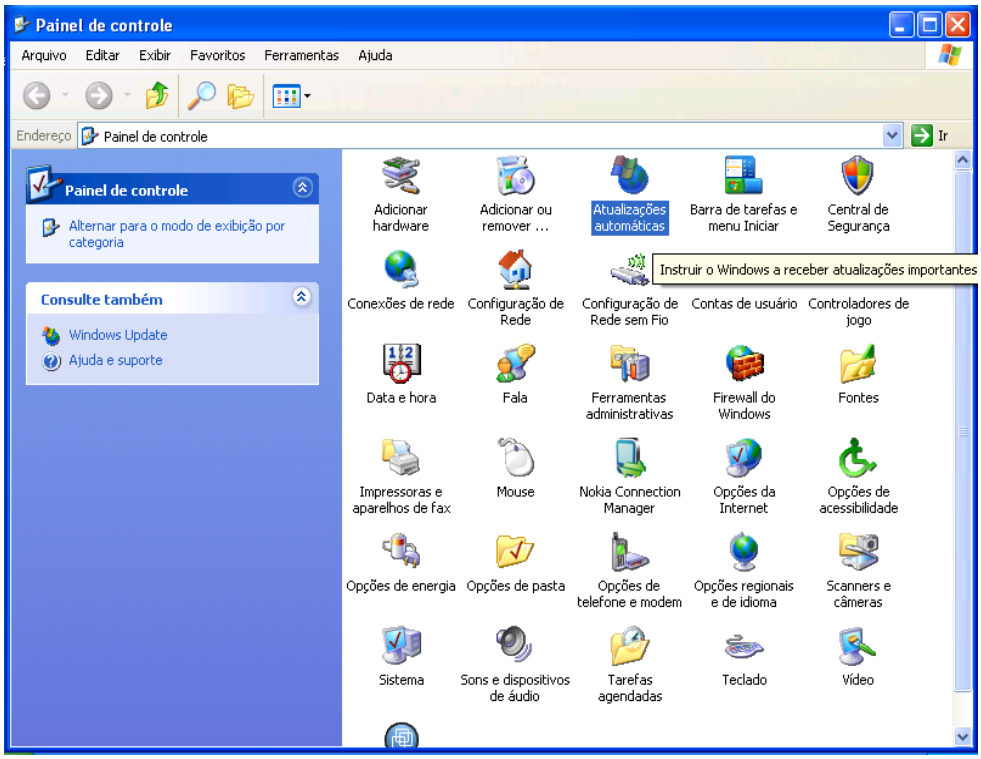


Menu iniciar clássico

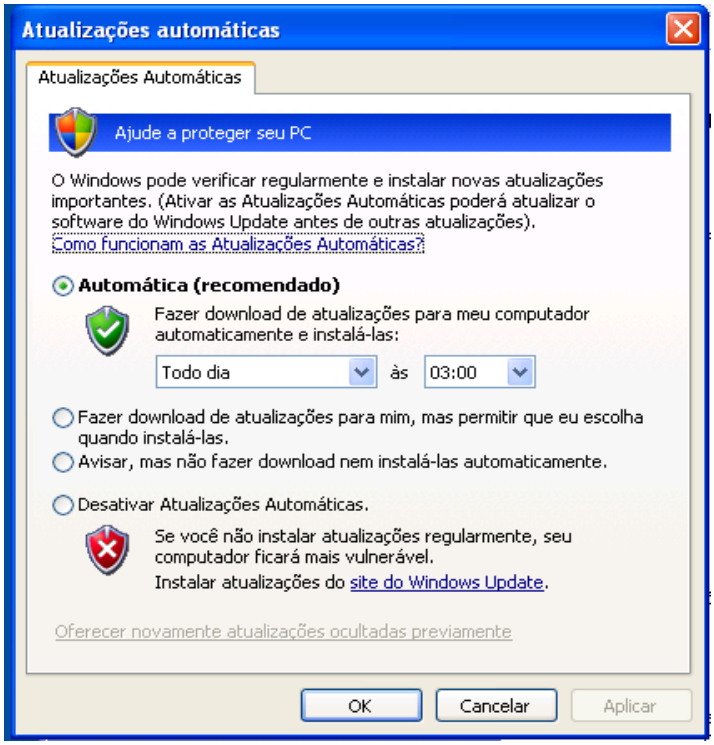
Depois dentro do painel de controle, vá ao lado esquerdo em “alterar para modo de exibição
clássico”



Já no painel de controle clássico vá em “atualizações automáticas”:



Caso já não esteja marcado , marque a opção “automática ”.

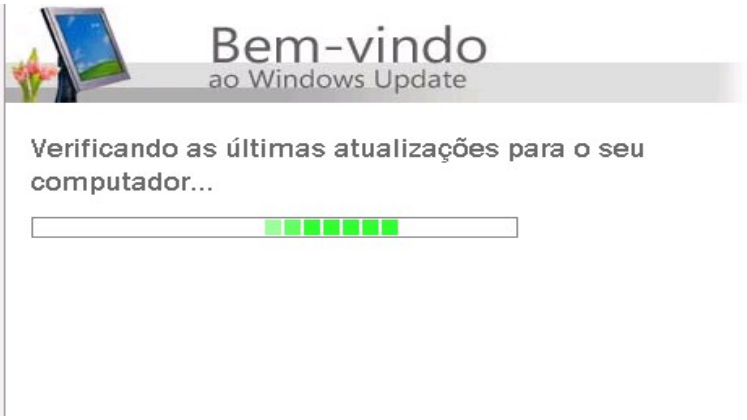


Caso queira fazer as atualizações manualmente, você deve ir na opção “desativar atualizações automáticas”.

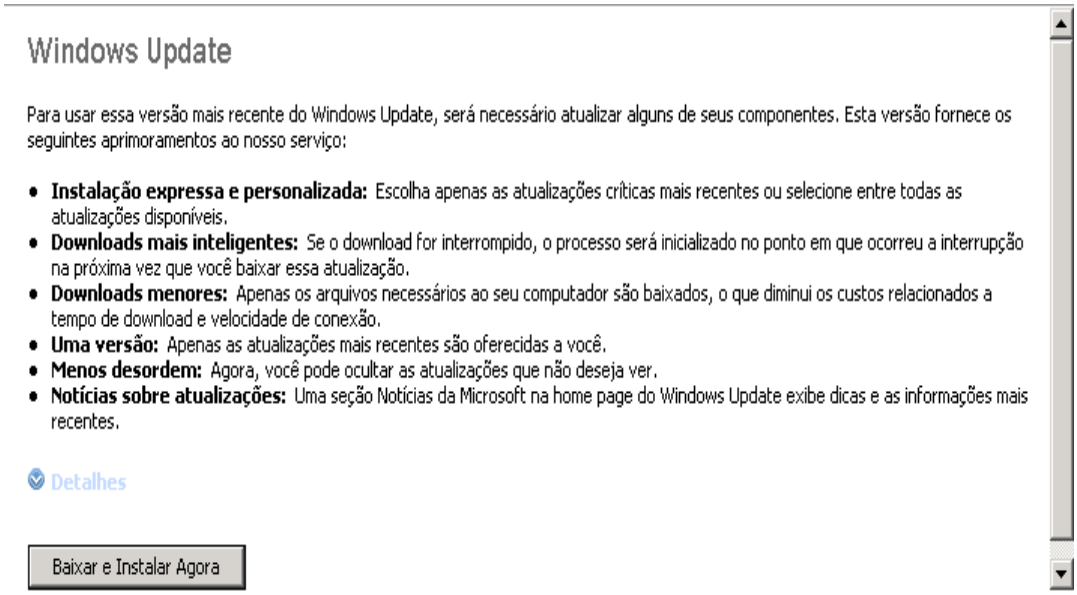
Para atualização manual, abra o internet explorer(não serve outro navegador) e entre no seguinte endereço:
http://www.windowsupdate.com

Você pode escolher entre atualização expressa ou personalizada,a expressa fara todas as atualizações de segurança necessárias. Na atualização personalizada você pode escolher o que será instalado. Recomendo usar a **expressa.**

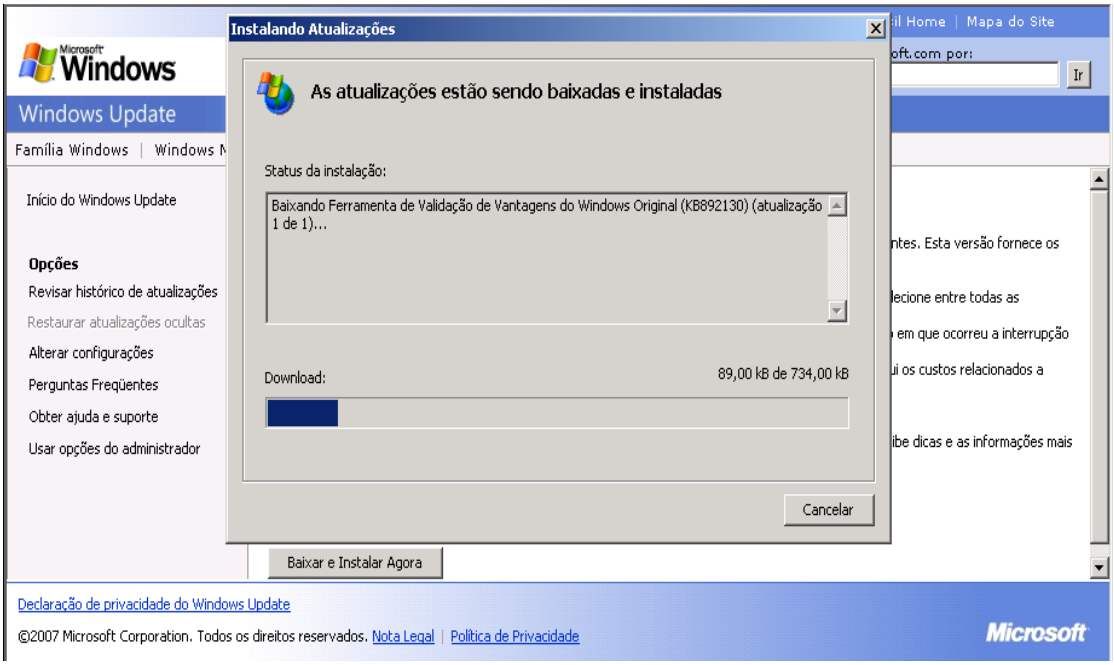
Agora o windows update ira verificar as atualizações disponíveis .



Após terminar de verificar quais atualizações estão disponíveis aparecerá a opção de baixar e instalar as atualizações.



Por ultimo será baixado as atualizações, porém elas só entram em vigor após o reiniciarmos o computador .



5.2 trojans, vírus worms

Desde os primórdios da informática existem programas destinados a danificar o nosso trabalho e nosso software. Esse tipo de software chamado de Malware (O termo Malware é proveniente do inglês Malicious Software) engloba os famosos vírus, trojans e worms.

O vírus é um software que entra dentro do código de algum outro programa , sendo que quando este programa é executado as funções do vírus também são, sendo uma função básica do vírus sé reproduzir.

Trojan , ou trojan horse, que em português significa cavalo de Troia , segue o mesmo roteiro da historia de roia. Um programa útil, que vem como presente, porém depois que você o instala na maquina, ele se aproveita e executa suas funções maliciosas sem que você se dê conta. Por exemplo o software Kazaa original vinha com um trojan embutido, pois monitorava certas ações dos usuários e os enviava de volta ao criador do software. Existe um outro programa que instala do nada (aproveitando-se de brecha no sistema operacional) é o HBTools. Ele coloca um utilitário para ver como esta o clima e também introduz melhoramentos visuais no internet explorer. Porém o mesmo também monitora as suas ações e envia para o fabricante de software. Algumas categorias de Trojan são conhecidas como spyware(software espião).

Worm é um programa completo que se instala em sua maquina que tem alguma função maliciosa. Ele dificilmente será detectado só de olhar o comportamento da maquina. As vezes ele usa arquivos com nomes parecidos com os do windows para confundir os usuários.

Para finalizar a explicação, vamos aos riscos que o usuário infectado corre:

-Danificação de programas e dados
-Monitoramento de suas ações
-Invasões
-Infecção de outras maquinas a partir da sua
-Roubo de senhas
-Perda do controle da maquina (maquina zumbi)

Os últimos riscos são os piores, pois se for roubada a senha do seu banco pode haver o risco de roubo. Caso a sua maquina se torne uma maquina zumbi, o cracker pode usa-la remotamente para atacar outras maquinas, fazer invasões entre outros crimes virtuais, porém pelo rastro que as transações deixarão vai parecer que a invasão saiu realmente da sua maquina.

Agora que você se assustou um pouco, vamos a parte boa da historia, se você tiver suas atualizações de segurança em dia, um anti-vírus atualizado , um anti-trojan e estiver seguindo as dicas do meu tutorial, as chances de você ser pego desprevenido são mínimas.

Existem varias opções de anti-vírus no mercado. Existem os pagos como o Norton Antívirus(www.symantec.com.br),Macafee(www.mcafee.com.br).
Também existem produtos gratuitos para uso residencial como o AVG (www.grisoft.com) e o Avast (www.avast.com). As versões pagas são muito melhores em questão de numero de vírus que podem pegar, fora o suporte que você vai ter do fabricante, por outro lado tem uma desvantagem, são muito mais pesados que os gratuitos, podendo fazer uma maquina mais antiga ficar lenta e as vezes até travar.

Os programas anti-vírus costumam pegar trojans e worms também, porém um dos programas que tem se mostrado mais eficiente para remoção dos mesmos é um programa gratuito chamado Spybot:
(www.safer-networking.org/en/index.html)
Outro bom programa para remover trojans é o Adware:
(http://www.lavasoft.de/software/adaware/).

Resumindo, o interessante é ter sempre um anti-vírus atualizado e um anti-trojan, também atualizado. Os antitrojan que eu recomendei são de uso manual, já os Antívirus funcionam de forma automática, ou seja o Antívirus, se tiver conexão com internet se atualizara sozinho e detectara os vírus quando chegarem, os antitrojan exigem que você faça isso manualmente, mas existem antitrojans automáticos também, que geralmente pesam um pouco mais a maquina, a própria grisoft, criadora do AVG possui um, porém não o testei e não posso falar de sua eficácia.

5.3 Firewall

Firewall é um programa que tem por função filtrar o que pode entrar e sair da sua maquina. Tem mais funções que isso, mas pela parte de segurança a função de filtro é que nos interessa. O WindowsXP a partir da versão com Service Pack 2 (segundo pacote de atualizações) já vem com um firewall integrado. O firewall não é inteligente a ponto de saber o que é um acesso de vírus, ou acesso do internet explorer, então ele tem algumas regras básicas pré-definidas, então se você tentar usar u programa que não esta pré definido como seguro ele ira perguntar se você quer permitir o acesso desse programa.

Se o programa que estiver pedindo permissão de acesso para internet foi instalado por você, click em desbloquear e o programa vai ter acesso à internet. Caso apareça essa tela com um programa desconhecido pedindo acesso à internet, então pode ser um vírus na sua maquina, na duvida pergunte à um profissional de informática, ou mande bloquear o acesso clicando em manter bloqueado.

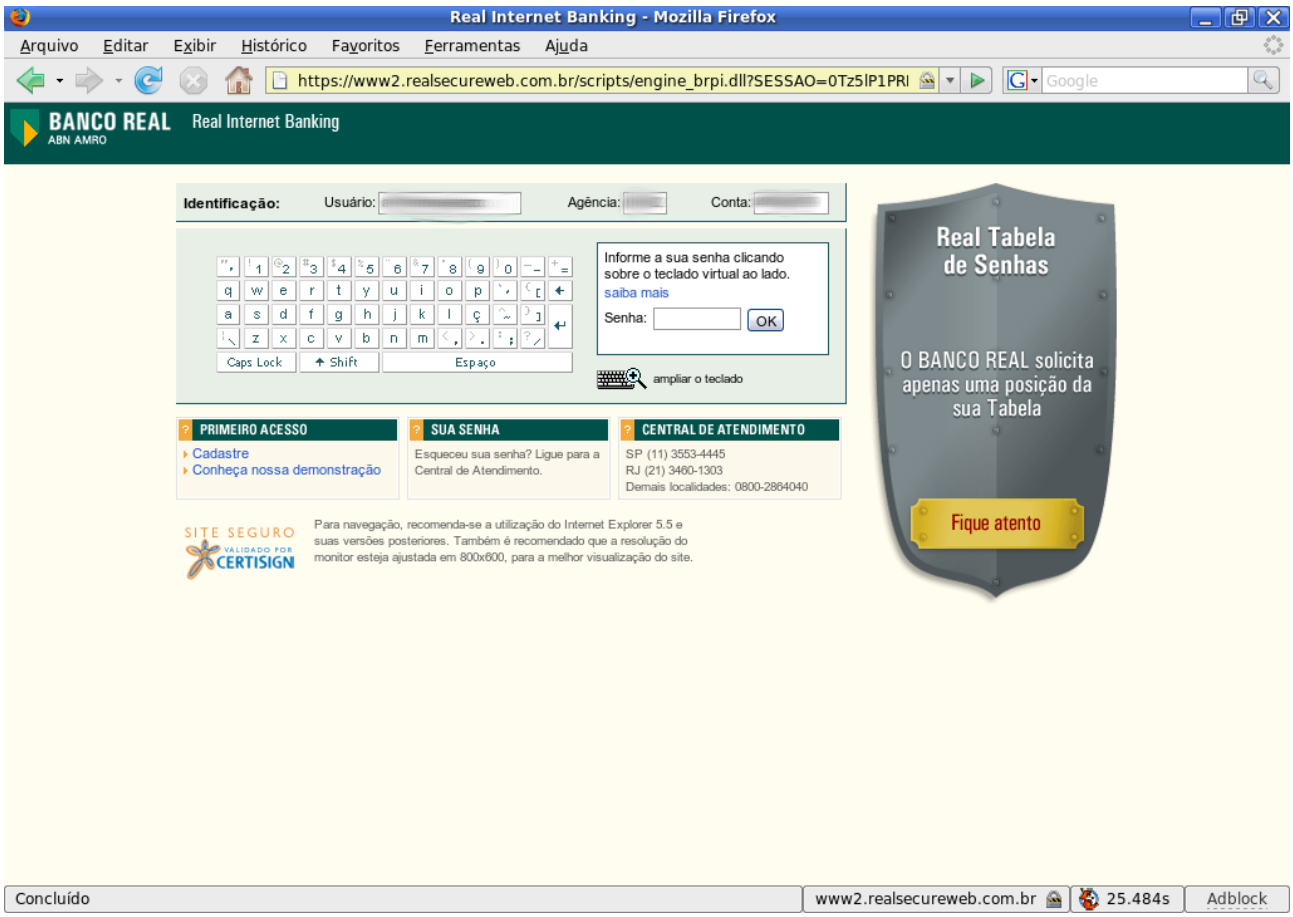
Além de soluções de firewall como a integrada do Windows XP temos também soluções separadas, como o Norton Internet Security, geralmente as soluções de firewall que não são do propio sistema operacional costumam ser bem mais pesadas, porém tem um conjunto de regras mais eficientes. Mas no geral a solução do propio windows já é satisfatória.

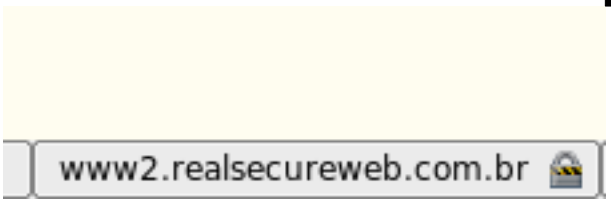
6. Banco pela internet

O acesso ao banco pela internet traz muito comodidade. Podemos ver nosso saldo, fazer transferências, pagar contas, recarregar celular, etc , sem precisarmos sair de casa. No geral quem faz os maiores investimentos em segurança são os bancos. Para acessar um banco com segurança, precisamos usar uma maquina segura, pois o banco tem um site seguro, o grande risco esta no propio computador que pode estar sendo monitorado. É claro que se você seguiu os passos que eu passei até agora você tem um computador relativamente seguro. Então vão algumas dicas para você acessar o banco se sentindo tranqüilo:

-Acesse ao banco do seu computador que você mantem seguro, ou no computador de alguém que você saiba que também mantem o computador seguro. Se você acessar um banco de um computador de uma Lan House, ou de alguém que possa estar infectado não há segurança.

-Em casos raros crackers conseguem trocar a pagina do banco por uma pagina deles, aonde você deve reparar em certas coisas mais comuns, por exemplo, a maioria dos banco não pedem usuário,senha, numero da conta na mesma tela. Outra coisa é o cadeado que é usado em algum site que tem comunicação de forma segura, criptografada. Você pode achar o cadeado no canto da tela do navegador.





Se o site não aparecer esse cadeado na parte do site aonde você tem que colocar a senha com certeza o site é falso.

-Você sempre terá de digitar sua senha no teclado virtual, que evita rastreamento de teclado por software espião, se o site não tiver mais teclado virtual também será um site falso.

-O banco nunca vai pedir sua senha por e-mail, por telefone, ou em outro qualquer lugar que não seja no site.

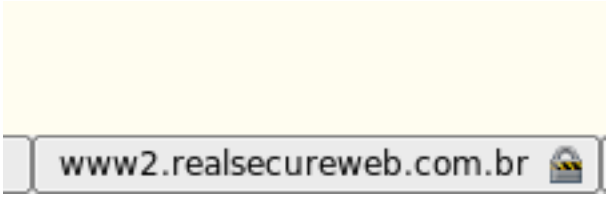
Paginas falsas além de serem raras, geralmente o propio banco as tira do ar em pouco tempo.

7.compras pela internet

O mundo maravilhoso das compras pela internet, sem sair de casa, buscas rápidas ao invés de ficar rodando horas fazendo pesquisa preço. Além de preços muito convidativos. A preocupação de comprar pela internet é a mesma que nós temos de comprar em qualquer lugar, picaretas, vendedores desonestos. Além disso alguns empresas também podem ser honestas, mas não terem segurança adequada no site. Em alguns sites a gente paga um pouco mais caro, justamente pela segurança que eles tem. Se você comprar em sites como www.americanas.com.br, www.submarino.com.br você tem certeza de comprar em sites com tradição de vendas pela internet e muitos clientes satisfeitos. Inclusive a segurança de devolução do produto que será buscado em sua casa em caso de defeito ou simplesmente por que você se arrependeu da compra (obviamente dentro de um prazo curto). Sites de grandes empresas costuman ter um bom investimento em segurança, pois vale uma lei do comércio : Cliente satisfeito faz propaganda para outras 4 pessoas, insatisfeito faz para 20 ou 40. Isso não quer dizer que você não pode comprar de sites menores, que costumam ter até preços melhores, mas se um site for menos conhecido e você conhece um cliente satisfeito do site isso já ajuda bastante.

Existem sites especializados em pesquisa de compras pela internet como o www.bond**faro**.com.br/ e o http://www.buscape.com.br/ . O interessante é que neles além de você pesquisar aonde pode encontrar um produto, pesquisar quem tem o menor preço, os usuários do site podem deixar suas impressões sobre o produto e sobre a loja virtual aonde compraram.

É preciso verificar sempre se aonde pedir qualquer dado confidencial se no site aonde você esta comprando tem aquele cadeado, igual no site de banco, esse cadeado garante que os dados estão sendo transmitidos de forma segura.



Geralmente temos como forma de pagamento nestes sites o cartão de credito e boleto bancário, alguns sites menores também trabalham com deposito em conta bancaria. Não aconselho o deposito em conta bancaria, pois o mesmo não é prova pagamento de um produto ou serviço. Sendo mais seguro o pagamento por cartão de credito e boleto.

Se de tudo ainda assim não se sentir seguro na compra por um site, por que não tem nenhuma referencia se o site é bom ou ruim, ao invés de comprar por cartão de credito, compre por boleto bancário, pois o mesmo é um bom documento para correr atrás de seus direitos em caso de problemas, junto ao procon. Ou então não compre nada muito caro desse site para testar o serviço.

8.Orkut

O Orkut é uma forma de comunicação e deixar sua vida pessoal publica. Informações encontradas no orkut . Qualquer pessoa pode acessar o seu perfil, ler suas mensagens curtas (também conhecidas por scraps). Dependendo das informações que você deixa no Orkut pode acontecer desde uma briga de namorados até um falso seqüestro.

Imaginem, aquela antiga paquera deixa uma mensagem no seu orkut dizendo que esta com saudades, e sua nova namorada entra lá, adeus novo namoro, isso por que no orkut não existe privacidade.

Ou então, você tem dados importantes que podem te identificar e uma foto para te descrever. Facilmente pode se fazer um falso seqüestro .

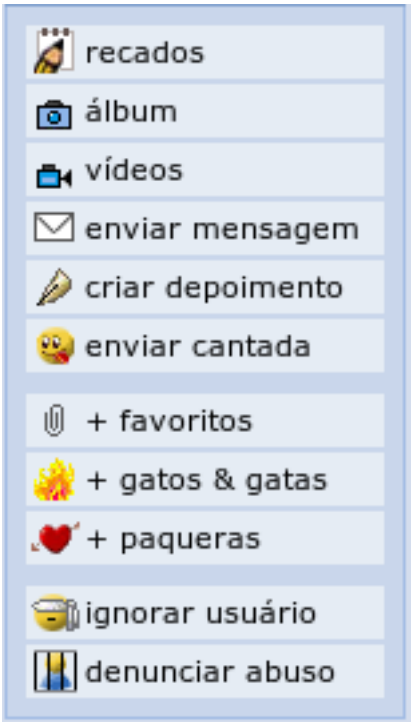
Não existe forma de se estar 100% seguro da sua privacidade dentro do orkut, assim como não dá pra fazer isso em nenhum lugar publico como na rua, mas alguns bons hábitos podem tornar o uso do orkut mais seguro.

Primeiramente não coloque dados importantes no orkut! Endereço, telefone, seus gostos, hábitos, lugares que freqüenta, etc. Deixe apenas cadastrado seu nome (primeiro nome) ou então apelido. Fotos, quando tiverem legenda, não seja especifica. Por exemplo, “festa da Natalia”, e não “festa no dia 21 de janeiro 2007 na casa da natalia BH/Belvedere”. Se deixar seu e-mail visível no orkut com certeza você recebera propaganda no seu e-mail.

Eu sinceramente prefiro o e-mail para receber mensagens, pois é muito mais seguro, mas se como eu seus amigos resolveram que só vão se comunicar pelo orkut, então leia suas mensagens e depois apague, ninguém precisa saber das mensagens que são destinadas a você.

Se receber mensagens com um link, tipo, clique aqui para ver as fotos, ou clique aqui para qualquer coisa, se for de um amigo seu, pergunte a ele se realmente enviou essa mensagem. Alguns vírus são enviados dessa forma por pessoas que tem sua maquina infectada.

Se receber propaganda, coisa ilegal no orkut, pedofilia, ou alguém usando sua foto você deve denunciar o abuso,existe uma parte do orkut aonde você pode fazer isso no canto esquerdo da tela.



Além de poder denunciar o abuso é possível ignorar um usuário inconveniente.

Resumindo, o Orkut é um local publico e assim como na rua você não deve confiar em qualquer pessoa.

9. Conclusão

A internet é um lugar inseguro como qualquer lugar publico. Mas não deixamos de ir no supermercado, a balada ou ao banco por que existem riscos no caminho. Não é tão difícil se manter seguro, é claro que se você seguir esses passos mínimos você estará bem mais seguro. Porém não posso garantir de forma alguma que estará 100% seguro pois novos golpes estão sempre sendo lançados. Mas as regras para se estar seguro na internet são as mesmas da vida social, não freqüente lugares mal freqüentados, não confie em estranhos, vá a lugares bem freqüentados e que tem segurança e dificilmente acontecerá alguma coisa ruim. A internet chegou para ficar e o custo beneficio dela é muito boa para deixarmos de incorporar seus benefícios a nossa vida.

10. Sobre o autor

Alexandre da Silva Costa - Técnico em Informática e Profissional em Linux, aluno do curso de Tecnologia da Informação do Centro Universitário de Belo Horizonte - UNI-BH
Sugestões e criticas podem ser enviadas para
anakinpendragon@gmail.com