EDIÇÃO LIMITADA • EDIÇÃO LIMITADA • EDIÇÃO LIMITADA

Windows Vista™ A Revista Oficial

ESPECIAL SEGURANÇA

Segurança total

- Saiba como configurar as portas do Firewall do Windows Vista
- Torne seu laptop inexpugnável com o Bitlocker
- Aprenda a usar o Windows Defender
- Deixe o Vista automatizar suas cópias de segurança
- Conheça o recurso de cópia de sombra
- Saiba como proteger seus dados pessoais com o Vista

Navegue seguro com a proteção

ANTI PHISHING

do **Internet Explorer 7**

MAIS PROTEÇÃO PARA VOCÊ

GARANTA UMA NAVEGAÇÃO MAIS SEGURA NA INTERNET E PROTEJA SEUS FILHOS DE CONTEÚDOS INADEQUADOS

CRIANÇAS

Deixe o acesso delas mais seguro

→ Conheça os recursos de segurança do Windows Vista

→ Dicas para usuários domésticos e corporativos

UAC Conviva pacificamente com o Controle do Usuário

PROMOÇÃO

O SEGREDO MICROSOFT

Os prêmios não são segredo.
Você pode ganhar:
Windows Vista, Office, Xbox 360, teclado, mouse, games, notebook Megaware, celular LG e Fiat Punto com tecnologia Blue&Me.

São 4 cofres esperando por você.
Cumpra as tarefas e siga as instruções.
O primeiro a desvendar o segredo ganha os prêmios.

Acesse o site e participe:
www.osegredomicrosoft.com.br

Microsoft®
Seu potencial. Nossa inspiração.®

Consulte o regulamento completo no site www.osegredomicrosoft.com.br. Promoção válida de 14/5/2008 a 30/6/2008 ou até se todos os cofres forem abertos. Fotos ilustrativas. Confira a lista completa de prêmios no site do promoção. CA 14884 de 13/05/2008.

Windows Vista A Revista Oficial

Diretor Editorial: Alessio Fon Melozo
Diretor Comercial: René Cassettari
Coordenador Editorial: Hudson de Almeida

REDAÇÃO
Editor: Heinar Maracy
Editor de Arte: Luciano Hagge Dias
Reportagem: Rodrigo Martin, Fábio Zemann (estagiário), Henrique Ulbrich
Assistente de Arte: Rubens Ishara (estagiário)
Tradução: Julia Vidili
Revisão e checagem: Sirlene Farias
Capa: Sérgio Bergocce (arte)

MULTIMÍDIA
Coordenador multimídia: Tiago Reis
Seleção de conteúdo: Marcel Lage e Thiago Ferreira

COLABORADORES
André Gurgel, Abel Alves, Raul Oliveira, Flávio Xandó, Bia Kunze

PUBLICIDADE
Gerente: Alexandre Cassettari
e-mail: acassettari@digerati.com.br

ATENDIMENTO AO LEITOR – SUPORTE
Horário de atendimento: das 9 às 18h
e-mail: atendimento@digerati.com.br, suporte@digerati.com.br, tel.: (11) 3217-2626

EDIÇÕES ANTERIORES
Atendimento a jornaleiros: (11) 3648-9090
Televendas: (11) 3648-9090
e-mail: vendas@digerati.com.br, fax: (11) 3217-2616
Site: www.lojadigerati.com.br

CONTATO
Redação: R. Haddock Lobo, 347, 12º andar, São Paulo – SP, CEP 01414-001, Tel.: (11) 3217-2600, Fax: (11) 3217-2617
Representante comercial nos EUA: USA-Multimedia Tel.: +1-407-903-50000, Ramal: 222
e-mail: info@multimediausa.com
Marketing: (11) 3217-2600
e-mail: marketing@digerati.com.br,
Circulação: (11) 3217-2719
e-mail: circulacao@digerati.com.br

DIGERATI

Windows Vista – A Revista Oficial (ISSN 1981-0296) é uma publicação da editora Digerati.
Distribuidor exclusivo para todo o Brasil: Fernando Chinaglia Distribuidora S.A.
Tel.: (21) 2195-3200
Distribuidor para Europa e América Latina: Malta Internacional +55 11 3284 6444
Impressão: Bandeirantes

DIGERATI É UMA EMPRESA DO GRUPO DOMO

GRUPO DOMO

Presidente: Alessandro Gerardi
Conselho editorial: Alessandro Gerardi, Luís Afonso G. Neira, Alessio Fon Melozo, William Nakamura

IVC ANER FIPP MPA

Future

"Windows Vista: A Revista Oficial" é publicada pela Digerati sob licensa da Future plc no Reino Unido. Se você está interessado em se tornar um licenciador, por favor contate Tim Hudson, Head of International Licensing, em +44 (0) 1225 442244 ou tim.hudson@futurenet.co.uk.

Bem-Vindo

Quando a Microsoft iniciou o desenvolvimento do Windows Vista , por volta de 2002, uma de suas principais preocupações era proporcionar aos usuários um sistema mais seguro. O Windows Vista trouxe uma pequena "revolução" na empresa. Houve praticamente uma paralisação em todos os projetos visando a implantação da filosofia "Trustworthy Computing" (Computação Confiável), no novo sistema e no Windows Server 2003.

O conceito por trás dessa filosofia é que "o sistema não deve falhar", seja no aspecto funcional ou segurança. Na verdade um se relaciona diretamente com o outro. Se há brechas de segurança muito provavelmente o ambiente irá sofrer e consequentemente pode até parar. Os pilares básicos sobre os quais se ergue este direcionamento são: Segurança, Privacidade, Confiabilidade e Integridade nos Negócios. O conceito de computação confiável gerou tecnologias como o Bitlocker, Controle de Conta de Usuário, Windows Service Hardening e o controle anti-phishing do Internet Explorer, entre outras, que tornaram o Vista o sistema operacional mais seguro da história da informática. Preparamos este pequeno guia para você conhecer melhor esses recursos e aproveitar melhor seu sistema operacional, para poder trabalhar, navegar na internet e se divertir.

Aproveite essa edição muito especial de Windows Vista - A Revista Oficial e acompanhe nossas edições regulares nas bancas. Visite também o site especial de segurança da Microsoft: www.windowsvista.com.br/seguranca

Heinar Maracy, Editor
Email **editor@revistawindowsvista.com.br**

WINDOWS VISTA - A REVISTA OFICIAL É PUBLICADA NOS SEGUINTES PAÍSES:
Reino Unido · EUA · França · Itália · Croácia · África do Sul · Holanda · Bélgica · Austrália · Portugal · Espanha · Rússia · Brasil · Alemanha · Ucrânia

SEGURANÇA

Seguro morreu de velho, diz o ditado. Para seus dados morrerem de velhice e não roubados ou perdidos, separamos aqui nesta seção algumas dicas básicas de proteção.

NESTA EDIÇÃO

WEB SEGURA

Tranque seu Internet Explorer

O browser é a principal porta de entrada de vírus e malwares. Aprenda a se proteger deles.

Por Flavio Xandó

O Internet Explorer, bem como qualquer browser, têm pontos de fragilidade, pois o usuário visita sites dos mais variados tipos. Estes sites podem ou não serem "bem intencionados". Podem ser armadilhas como simulações de sites de bancos ou mesmo sites que sugerem que se instale um Active-X para "melhorar a visualização", mas na verdade

NAVEGAÇÃO SEGURA Um dos esquemas usados pelo IE é a Virtualização do Registro e do Sistema de Arquivos

PROTEÇÃO Fique atento à indicação de ativação do modo protegido na barra inferior

são programas altamente maliciosos e perigosos para o usuário.

O mecanismo "anti-phishing" do IE 7 do Vista faz um bom trabalho na análise e validação de sites como seguros. Quando o site sendo visitado é perigoso, uma tarja vermelha informa isto para o usuário. Se o site é desconhecido ou não pode ser validado, um sinal de exclamação "!" é exibido no rodapé da tela, pedindo atenção e cautela.

O Internet Explorer do Vista inclui um recurso que lhe é único, o chamado "modo protegido". Não deixe de usá-lo desta forma!! Verifique no rodapé do IE se ele está ativado! Ele roda em um contexto de baixíssimo privilégio, que impede programas, sites e outros objetos acionados durante a navegação criem ou alterem arquivos ou configurações. Isso diminui muito o risco de violação da máquina do usuário.

Um dos mecanismos usados pelo tal modo protegido do IE é a Virtualização do Registro e do Sistema de Arquivos, que vale para o IE e para alguns outros tipos de programas. Estes podem tentar escrever em áreas "perigosas" do sistema como certas chaves do Registro ou pastas especiais do sistema. Quando o Vista identifica um programa com estas características possibilita que ele seja rodado no modo "file/registry virtualization". Assim os programas rodam em um ambiente que julgam ter tanto o Registry quanto as pastas críticas sob seu domínio, mas na verdade são cópias virtualizadas para proteger o sistema. Essa forma de uso traz uma pequena degradação no desempenho daquele programa mas ao menos pode ser rodado de forma transparente e segura ao mesmo tempo. O site que possua algum programa malicioso ou mesmo um link que seja aberto inadvertidamente pelo usuário não afeta o IE de verdade, mesmo que execute o código perigoso: o modo protegido "engana" o programa, fazendo-o pensar que assumiu o controle do PC e o infectou, quando isso de fato não aconteceu.

Para ter certeza de que você está mesmo sendo defendido pelo tal modo protegido olhe na linha de status do IE (como na figura). Caso esse mecanismo de defesa não esteja ligado, basta clicar duas vezes sobre aquele local (duplo clique) e abrir a tela que ativa o recurso.

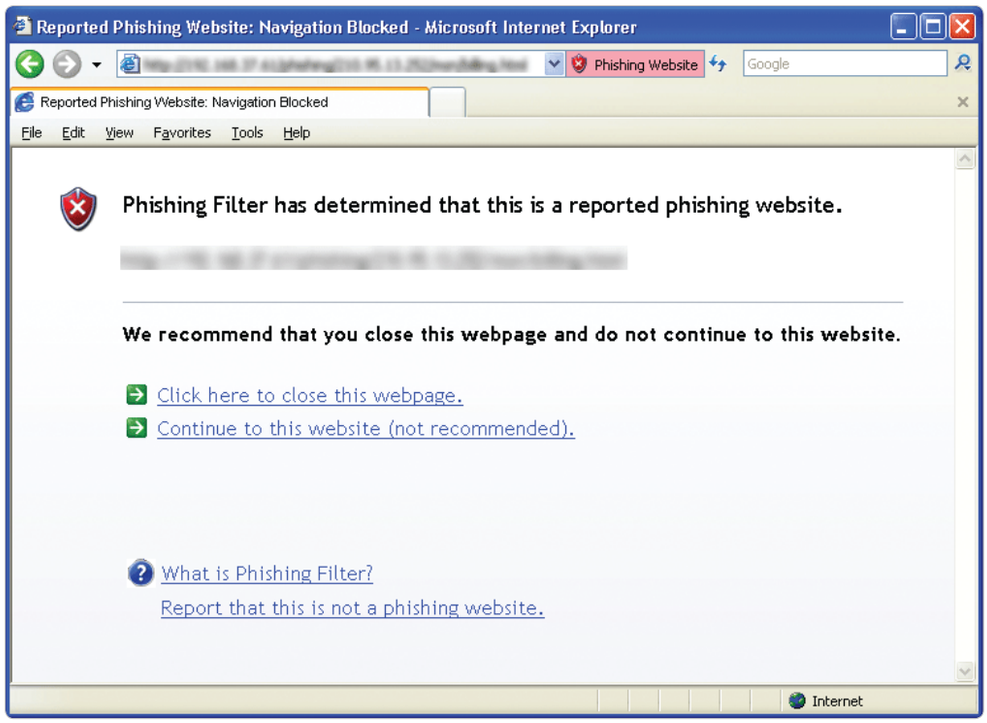
Um reforço muito importante do IE 7 é o seu mecanismo ANTI-PHISHING. Os astutos gatunos virtuais têm uma criatividade gigante quando o assunto é tentar lesar as pessoas fazendo-as pensar que estão acessando um site legítimo, quando na verdade um determinado site acessado é uma armadilha. Seja para capturar dados ou mesmo para induzir a pessoa a instalar um programa altamente nocivo em sua máquina, sites malignos disfarçados de sites reais são usados pelos malfeitores. Eles usam uma técnica chamada de engenharia social que na verdade é a "arte do convencimento". De toda forma o mecanismo de proteção do IE para isso é o Anti-Phishing, que segundo os número da Microsoft já bloqueou mais de 1.2 milhões de acessos a sites perigosos.

A forma como a Microsoft identifica um site de phishing é variada. Desde um banco de dados consultado online toda vez que se visita um site, como a formação do nome do site (URL), etc. O importante é sempre se valer de todos estes mecanismos de proteção.

NÍVEL Você pode definir o nível de segurança dos sites que você visita frequentemente

Caçando bandidos

O IE7 tem uma opção para você denunciar sites de phishing. Clicando na mensagem de aviso (ou indo no menu Ferramentas), você abre um menu onde pode selecionar um link para abrir o processo de denúncia. Pouco tempo após a denúncia, o site é avaliado e adicionado a lista de sites malvados no servidor.



PHISHING Internet Explorer denuncia um site de Phishing e pede providências

Abrindo portas no Firewall do Vista

ATENÇÃO!
Não fique vulnerável
Apesar de ser muito mais simples desligar totalmente o Firewall do que somente abrir a porta necessária, nunca faça isso! O seu computador vai ficar muito vulnerável e poderá ser acessado por outro na Internet.

Configurar o Firewall do Windows Vista não é nenhum bicho de sete cabeças

Por Abel Alves

O Firewall do Windows Vista foi um dos programas que mais avançaram em relação à versão existente no Windows XP. No Windows Vista, o Firewall é bem mais avançado e completo. Ele permite, por exemplo, regras mais detalhadas e controle do tráfego de saída, além de ter um novo Painel de Controle e de suportar o protocolo IPv6.

Muitos usuários não sabem para que serve o Firewall, então é bom lembrar: o Firewall é um programa que protege nosso computador contra acessos indesejados. Por exemplo, quando estamos navegando na rede, o Firewall impede que nossa máquina seja invadida. O Firewall do Vista pode ser acessado por meio da seqüência **Iniciar ➜ Painel de Controle ➜ Segurança ➜ Windows Firewall**.

O Firewall do Vista procura ser o mais discreto possível e não atrapalhar o funcionamento dos outros programas que rodam na máquina. Entretanto, alguns programas não funcionam corretamente por causa dessa proteção feita pelo Firewall. Exemplos típicos são os programas P2P, como o Emule, Bit-torrent, etc. No caso específico desses programas, eles até funcionam, mas o Firewall impede um melhor desempenho na troca de arquivos. Só que existem programas que nem chegam a funcionar! Nesses casos, quase sempre, é apresentada uma mensagem reclamando do Firewall.

Então, pode ser necessário abrir uma porta do Firewall para ser utilizada pelo programa. Neste ponto, é importante lembrar que essa porta aberta é uma brecha na segurança de seu micro, e que você só deve permitir essas exceções no caso de conhecer bem e confiar no programa que pede a abertura da porta. De uma maneira geral, pode ficar tranqüilo com os programas P2P mais conhecidos, porém desconfie de programas que nunca ouviu falar e que pedem para abrir portas no Firewall.

Se você acha que trabalhar com o Firewall do Vista é complicado, fique tranqüilo! Abrir portas nele é muito simples. Basta seguir os passos do nosso tutorial.

Como abrir portas no firewall

Só faça isso se você tiver certeza absoluta do que está fazendo. Uma porta aberta é uma brecha de segurança

1 .ACESSE O FIREWALL Por meio da seqüência **Iniciar** > **Painel de Controle** > **Segurança** > **Windows Firewall**, acesse o Firewall do Vista.

2 ABRA A PORTA Para abrir uma porta no Firewall, basta clicar na opção **Permitir um programa pelo Firewall do Windows**, que aparece na janela do Firewall. Depois da confirmação do UAC (Controle de Conta do Usuário), vai aparecer uma outra janela em que podemos alterar as configurações do Firewall.

Opinião de especialista

Gabriel Menegatti, responsável pela área de tecnologia da F-Secure, dá dicas de segurança para pequenas e médias empresas

1 Esteja atento a todos os alertas de segurança e atualizações disponíveis em update.microsoft.com.

2 Mantenha um controle muito rígido dos softwares e, principalmente, dos plug-ins instalados na rede. A maioria dos ataques não acontece mais por falhas no sistema operacional, mas sim por vulnerabilidades existentes em softwares que o administrador da rede nem sabe que estão instalados.

3 Tenha um bom antivírus e, principalmente, mantenha-o atualizado. Hoje em dia, ficar sem uma atualização mais recente pode significar uma grande possibilidade de infecção.

4 Tenha um firewall em todos os servidores e estações de trabalho. A maior parte dos incidentes por infecção ou invasão é proveniente de dentro da rede corporativa.

5 Tenha uma solução de detecção de rootkit integrada ao antivírus em cada computador ou servidor da rede. Hoje em dia, uma das maiores ameaças é representada pelos rootkits, que escondem os vírus, impossibilitando as soluções de segurança comuns de removê-los.

6 Crie processos e regras para a utilização e atualização das senhas utilizadas na rede. Isso impossibilita que alguém crie uma senha muito fácil ou que a mesma tenha validade por muito tempo.

7 Caso a empresa possua usuários que se conectem remotamente, ou que simplesmente utilizem notebooks, verifique quais são os níveis de acesso à rede de alguém que se conecta remotamente e se essa pessoa utiliza uma conexão segura (VPN). Crie regras para que somente computadores protegidos possam se conectar novamente à rede corporativa: isso impede que alguém que ficou muito tempo sem se atualizar retorne à rede trazendo riscos para a mesma.

8 Caso a empresa utilize wireless, ative a encriptação de dados na rede e desabilite a "auto-promoção", isto é, desabilite a função de broadcast do SSID, que divulga constantemente a existência de sua rede wireless para dispositivos que estiverem dentro do sinal de alcance. Determine quais dispositivos podem usar sua Wi-Fi, ativando os filtros por endereço MAC. Bloqueie portas inúteis, somente deixe habilitado o que está em utilização e possui algum controle. Por fim, modere o sinal habilitado, possibilitando, assim, que outras áreas ou empresas não tentem utilizar o seu sinal wireless.

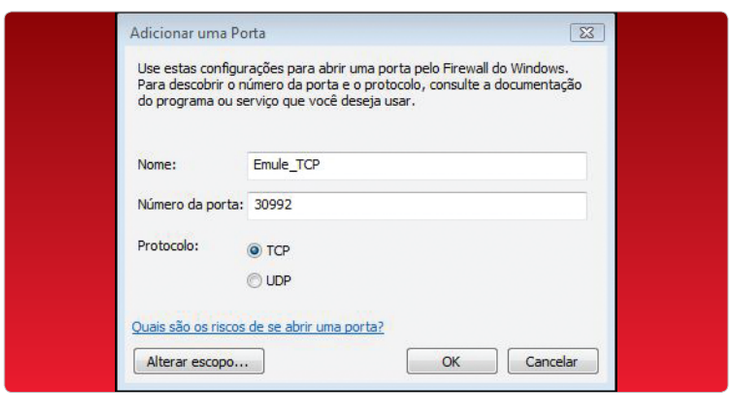
9 Nunca abra anexos com arquivos executáveis recebidos via email, mesmo que pareçam ser de dentro da empresa. Hoje em dia, são muito comuns os ataques personalizados (Target Attacks), que se passam por alguém de dentro da empresa.

10 Tenha muito cuidado ao abrir links enviados via email, pois não é mais necessário baixar algum arquivo para que você possa ser infectado. Somente visitando uma página web, você já pode ser infectado.

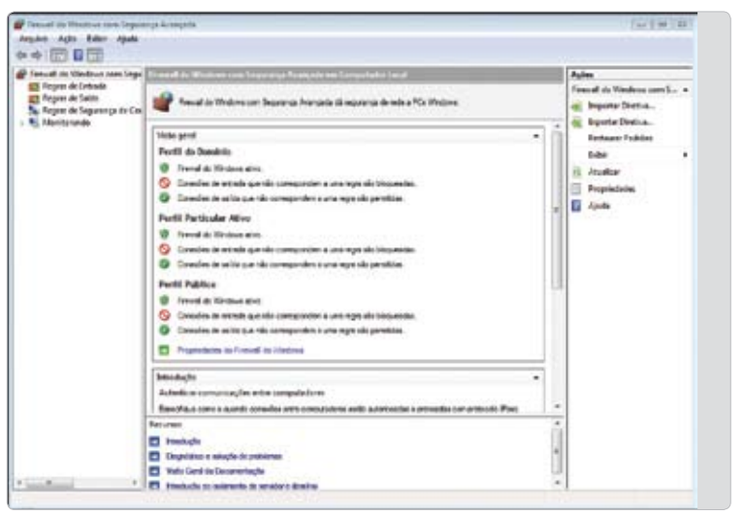
11 Não utilize a mesma senha que utiliza em sites bancários em outros sites com menos importância. Você nunca sabe quem são os donos do site e quais são suas políticas de privacidade/sigilo de informações.

12 Saiba que seu banco nunca enviará um email solicitando sua senha. Se receber alguma oferta vinda pela Internet e a mesma parecer boa demais para ser verdade, desconfie.

13 Por fim, TENHA MUITO bom senso na navegação, na instalação de novos softwares e nas informações que você compartilha dentro da empresa (intranet) ou na Internet.



3 ADICIONE Clique no botão **Adicionar porta** para fazer aparecer uma outra janela, na qual devemos preencher um nome para identificar a porta que não será monitorada (em geral, usa-se o nome do programa que exige a abertura da porta), o número da porta que deve ser aberta (o programa que exige a abertura da porta normalmente diz o número da porta que deve ser aberta) e o tipo de protocolo a ser usado (TCP ou UDP).



4 DETALHE Clicando no botão **Alterar escopo**, podemos escolher quais os computadores em que a porta aberta no Firewall do Vista vai ser válida.

Tenha um laptop inexpugnável

Aprenda a utilizar os recursos de criptografia e segurança do Bitlocker.

Por Flávio Xandó

O problema é antigo. Mas antes era bem menos crítico. Ter um computador subtraído, sendo um computador de mesa ou um notebook, significa que arquivos pessoais serão levados junto. Normalmente os amigos do alheio visam lucro rápido, a venda do equipamento. Mas aquilo que no passado parecia coisa de "filme de agente secreto", hoje em dia é muito real: roubo premeditado de informações. Existem variações insanas deste crime como seqüestro de informações. Roubam um notebook e pedem dinheiro em troca da devolução do mesmo. Claro que para praticamente todas as pessoas o valor do equipamento em si é mínimo perto do valor das informações perdidas ou repassadas para outras pessoas que poderiam usá-las contra você mesmo ou contra a empresa que se trabalha. Se a pessoa foi roubada ou danificou irremediavelmente o notebook (ou o HD de seu desktop) e não há backup, não há esperança. Mas se o equipamento caiu em mãos erradas, para isso, o Vista tem uma ótima solução.

Em algum momento você já deve ter ouvido falar sobre criptografia ou codificação de dados. Não se preocupe com os detalhes desta tecnologia. O que interessa é que uma palavra, frase ou texto inteiro, quando criptografado é representado de uma forma completamente ininteligível. Algo como "Revista Windows Vista" viraria "Be^O_bK GQ\dYgWVY[Xa". Este é só um exemplo pois há milhares de técnicas para codificar os dados, algumas mais simples e outras muito mais sofisticadas. O problema é que quanto mais complicado o processo de codificação de dados, mais lento é para realizá-la. Ao mesmo tempo muito mais difícil é para alguém tentar "quebrar" esta proteção. Por isso que até pouco tempo atrás só havia soluções para codificação segura de fato para arquivos e pastas e não de um disco inteiro.

Computadores mais modernos, além de contarem com processadores duplos, quádruplos, bem mais rápidos, podem ter um componente de hardware especializado em criptografia e segurança chamado TPM (Trusted Platform Module). Este garante que os arquivos fundamentais do processo de boot não foram modificados indevidamente por algum agente externo (ou alguém tentando driblar a segurança). Somente após a digitação de uma senha ou a inserção de uma "USB-KEY" (um pendrive que contém uma senha adicional) o sistema se é iniciado e os dados poderão ser usados. Se o disco rígido for removido e usado em outro computador ele não funcionará pois está codificado. Só funciona na máquina original, com toda a segurança da senha e do USB-KEY.

Máquinas sem o chip TPM podem usar o recurso Bitlocker mas terão uma camada a menos de proteção que é a verificação "pré-boot" dos arquivos de sistema e uma pequena redução no desempenho, uma vez que o chip TPM também pode ajudar no processo de codificação/decodificação dos dados. Se for necessária a troca do disco rígido para outro PC este obrigatoriamente precisará rodar o Vista (Ultimate ou Enterprise) e com a senha e o USB-KEY uma "reativação" deste disco será efetuada na nova máquina.

Um cenário importante é a reutilização de PCs, principalmente em empresas (mas para pessoas físicas também). Os discos mesmo após formatados podem ter seus dados lidos sem problema algum usando softwares como GetBackNTFS ou OnTrackRecovery por exemplo. Se o disco tiver sido usado com Bitlocker não há chance alguma de recuperar a informação, seja pela troca ou venda do PC. Por outro lado formatações acidentais e deleções desastradas de dados vitais também são mais críticas. Manter os backups em dia é fundamental!

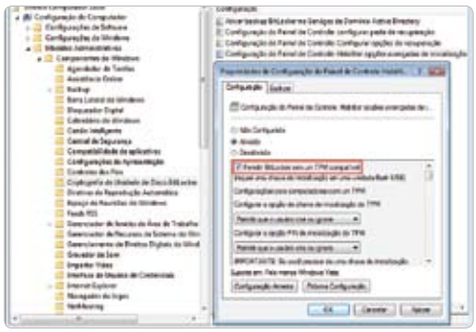
Se ocorrer perda ou desastre com o USB-KEY, ou troca de placa mãe, Bios ou algo assim, um volume protegido com o Bitlocker pode ser recuperado somente com uma senha de 48 dígitos, gerada na hora da instalação e preservada pelo Administrador. Na versão Enterprise do Vista, é possível ter no Active Directory um repositório destas senhas de Bitlocker muito bem protegidas e só acessadas pelo Administrador. Para digitar a senha se usam as teclas de função de F1 a F10 e não os números. Usuários não corporativos recuperam a senha "mestre" pelo painel de controle (após todo o crivo de segurança do Vista, USB-KEY, etc.).

Existem duas situações, com duas variações. Uma quando a máquina é nova e outra quando vai ser formatada. Quando a máquina tem o chip TPM e quando não tem. Na máquina nova o disco deve ser particionado em dois volumes. Um com pelo menos 1.5 Gbytes e o segundo volume com todo o resto do espaço disponível. A primeira partição será a de boot do sistema e a segunda conterá o Vista propriamente dito e todos os dados do usuário.

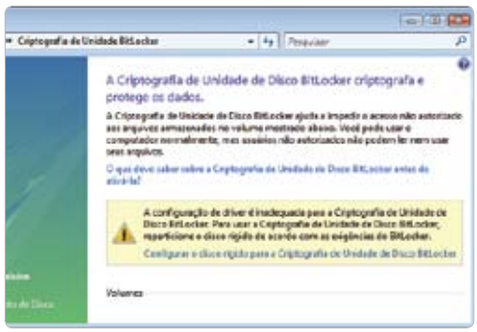
Vamos fazer o caso mais "difícil" que é sem TPM e com a máquina já formatada, sem a estrutura de discos exigida pelo Bitlocker.

Habilitando o Bitlocker em seu PC

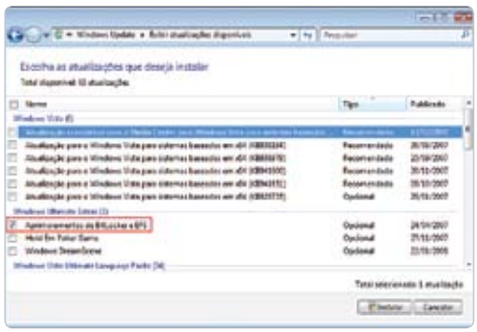
Mesmo sem o chip TPM é possível utilizar o sistema



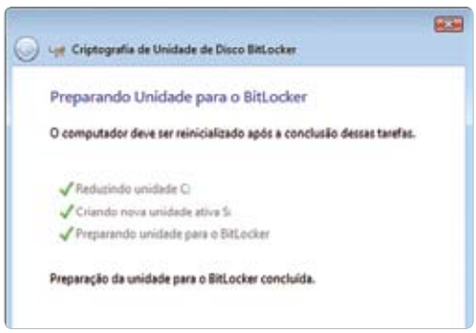
1 BITLOCKER SEM TPM Execute o GPEDIT.MSC e modifique o seguinte: Configuração do Computador / Modelos Administrativos / Componentes do Windows / Criptografia de Unidade de disco Bitlocker. No Painel de Controle **Habilitar opções avançadas de Inicialização** ative a opção avançada Permitir Bitlocker sem um TPM compatível.



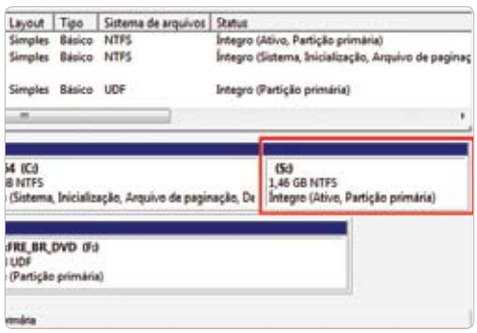
2 PARTICIONAMENTO ERRADO No menu do Vista digite Bitlocker que aparecerá a opção Criptografia de Unidade Bitlocker. Como a máquina já estará formatada com uma única partição C: o programa alertará sobre a incompatibilidade.



3 FERRAMENTAS AVANÇADAS A Microsoft criou uma ferramenta para contornar esta incompatibilidade. No Windows Update existe uma opção para instalar um programa que resolve o problema. Selecione Aprimoramentos de Bitlocker EFS no Windows Update e faça o download.



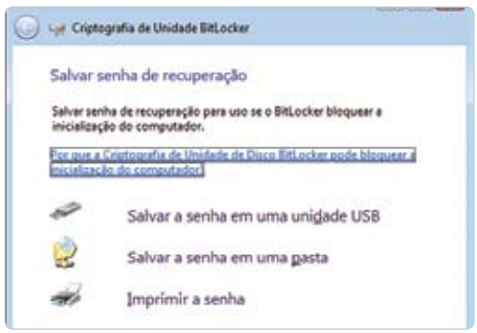
4 REPARTICIONAMENTO Após o download você deve executar pelo menu do Vista o programa Ferramenta de preparação de Unidades de Disco Bitlocker. Automaticamente um reparticionamento do disco rígido será feito.



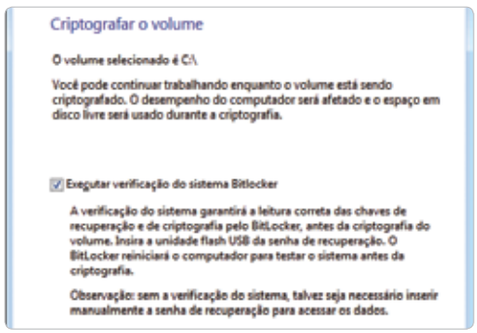
5 PARTIÇÕES PRONTAS Será criada uma partição de 1.5 Gb primária de inicialização necessária para o BitLocker funcionar e o resto, o próprio Vista e todos os dados do usuário serão mantidos na outra partição

6 CRIPTOGRAFAR Após o término e um necessário boot em seu sistema chame novamente o programa Criptografia de Unidade Bitlocker no menu do Vista. Lembre-se, tenha em mãos um pendrive pronto, pois será nele que a "chave" de ativação será gravada. Clique em **Ativar Bitlocker**.

7 AUTENTICAÇÃO Como o PC (neste exemplo) não tem TPM o uso do pendrive é obrigatório. Se tivesse chip TPM haveria a possibilidade de escolher entre PIN (senha numérica), USB ou sem chave alguma. Já sem TPM só com pendrive USB que será a "chave do carro" para ligar o seu PC.



8 CONTRA-SENHA Existe uma "contra-senha" especial para ser usada somente no caso de perda do pendrive ou caso ele seja avariado. Sem esta outra senha os dados estarão irremediavelmente perdidos. O Vista oferece a opção de salvar esta senha mestre em outro pendrive ou mesmo imprimi-la.



9 TESTE O PENDRIVE O Vista ainda oferece uma opção de "verificação" do pendrive USB. Não desative esta checagem!! Caso o pendrive USB não possa ser lido a criptografia não é feita. Depois da criptografia executada, o uso do PC acontecerá de forma natural e transparente, mas com o disco rígido já protegido.

Redes abertas só se precisar e quando precisar

Aprenda a usar o Windows Defender e o Windows Firewall para proteger sua rede.

Por Flavio Xandó

Em épocas não tão distantes assim, quando Windows 98 e Milenium eram muito populares, uma rede era algo absolutamente escancarado. Qualquer um entrava em qualquer computador a qualquer hora. Senhas eram opcionais e criá-las era tarefa quase "escondida". No XP houve uma boa melhora, mas mesmo assim algumas opções ainda eram bem "abertas". A começar pela possibilidade de ser descoberto na rede.

Quando uma placa de rede é detectada e configurada o Vista pergunta qual o tipo de rede: Doméstica, Trabalho ou Pública. Em redes públicas (hotéis, centros de convenção, lan-houses, etc.) o PC não pode ser "visto" de forma alguma, pois pode haver pessoas mal intencionadas na vizinhança e que se descobrem o nome/IP da máquina podem tentar invadi-la.

Além disso, uma grande mudança aconteceu nos "serviços" de rede, ou seja, aqueles componentes críticos que fazem acesso a redes pelo Vista. Eles usam uma conta "interna" com baixo privilégio e que não tem acesso por si à rede completa. Antes (2000 ou XP) alguns serviços de rede eram muito poderosos e tinham até mais poder de acesso que a senha do próprio usuário logado.

Essa mudança reduz drasticamente ou mesmo zera a ocorrência de infecções que se propagam pela rede "na surdina". O componente Windows Defender, que é um download opcional no Windows XP, faz parte do Vista. Ele defende o ambiente contra spywares e programas afins. Também é pré-instalado e ativado por padrão.

Ao escolher rede Doméstica ou Trabalho o PC é "visível" na rede, mas mesmo assim um grande conjunto de opções podem ser "ativadas" ou "inativadas". Logo após a instalação do sistema operacional o usuário responde a uma pergunta sobre a configuração da rede.

O Windows Firewall foi completamente revisto e refeito. A começar ele está ativo (padrão) na instalação do Windows. Na aparência básica ele é "igual" ao do XP para não trazer dificuldades aos usuários, embora com muito mais opções de bloqueios e desbloqueios. Mas nos bastidores ele é muito diferente. Na sua forma avançada, acessado em Ferramentas Administrativas/Firewall do Windows com Segurança Avançada, ele usa o MMC

Acione o Windows Defender

Proteja seus computadores contra ameaças online

1 CHAME Digite Defender no menu Iniciar do Vista. Quando o ícone aparecer (pode demorar uns segundinhos, dependendo de como está o banco de dados de pesquisa) clique nele para chamar o programa.

2 VERIFIQUE Na tela inicial sabemos quando foi feita a última verificação, a data das vacinas e a hora agendada para a inspeção automática do sistema. Clique na opção ferramentas e em seguida em **Opções**. Recomenda-se mudar o padrão Verificação Rápida para Verificação Completa, principalmente se for executada por exemplo de madrugada (sem atrapalhar o usuário).

3 VERIFICAÇÃO COMPLETA Na verificação simples somente os arquivos de sistema e programas são analisados. Na verificação completa, como o nome sugere, todos os arquivos são analisados, portanto muito mais rigorosa. Existem spywares que de modo muito esperto se escondem em inocentes arquivos comuns, por isso esta forma é mais segura (embora mais lenta).

Rede pública ou particular?

Seguindo nosso tutorial, você vai conseguir criar sua rede de acordo com o tipo dela. Mas quais as diferenças de cada um destes tipos de rede? Ao contrário do que poderia parecer (pelos próprios nomes), a rede PÚBLICA é aquela rede fora do controle do usuário, na qual não se deseja ser visto ou ter sua estação descoberta por outros computadores. Assim o usuário deseja somente usar os serviços da rede sem risco de ser molestado. Exemplo, uma rede Wi-Fi de aeroporto. Já a rede chamada PARTICULAR encontra-se em um ambiente restrito, controlável e sem riscos evidentes, no qual seu computador pode ser descoberto pelas outras estações e assim remover compartilhar recursos.

Console 3.0, adequado para seus novos recursos. É fácil criar novas regras e estas são muito mais poderosas. Este console não é para usuários finais, pois é um Firewall de primeira classe com todas as possibilidades de criação de regras de entrada, regras de saída, monitoração, etc. É brilhante, não fica atrás de qualquer Firewall, mesmo os tão falados Firewall em Linux, mas com a grande vantagem de ser gerenciado em ambiente gráfico.

Windows Defender

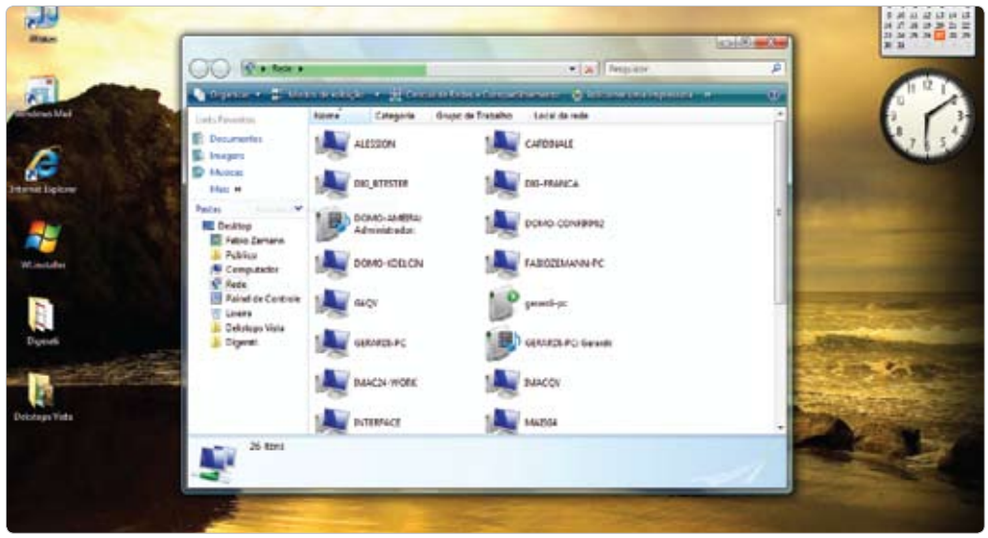
Como o nome sugere o Defender é um componente essencial do Vista que monitora a máquina contra spywares. Estes são softwares "maliciosos" muito perigosos que podem ser encontrados desde anexados em e-mails, com links em páginas e também em mensagens. Visam espionar o usuário seja para bisbilhotar seus hábitos de navegação como roubar senhas de bancos para roubá-lo.

O Defender não é antivírus, que não deve ser esquecido no Vista (instale um de sua preferência). Ele complementa o antivirus que nem sempre tem a capacidade de olhar por esta categoria de ameaças (spywares).

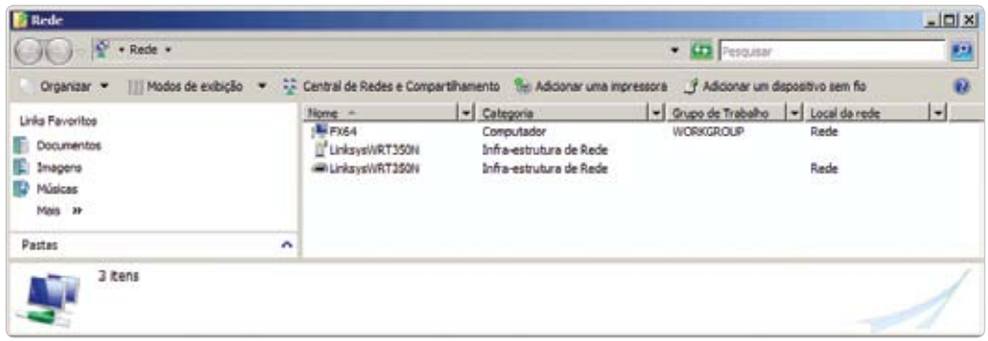
O Defender funciona de forma automática, monitorando as ameaças não sendo necessário configurá-lo, pois ele vem ativado automaticamente após a instalação do Vista. Porém algumas opções podem ser alteradas como horário que se executa uma varredura extra no sistema, atualização das "vacinas", bem como ordenar uma varredura manual no sistema.

Escolha seu tipo de rede

Saiba como adequar a segurança de sua rede

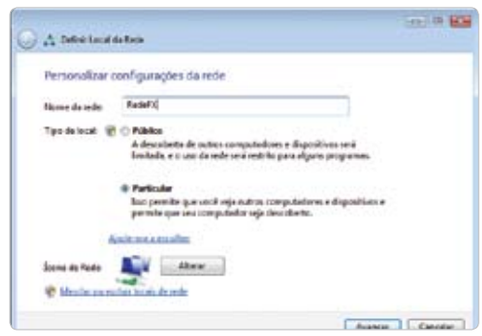


1 LIGUE A REDE No menu do Vista selecione a opção Rede. Você verá os computadores na sua rede.



2 ATIVE A DESCOBERTA Caso não se veja os computadores da rede, seu Vista está configurado com a opção **Desativar Descoberta de Rede**, que por privilegiar a segurança (mas não exatamente a usabilidade) vem assim como padrão. Para ativar a descoberta de rede clique em **Central de Rede e Compartilhamento**.

3 LIBERE OPÇÕES Aqui você vê cada tipo de acesso que pode ou não pode ser individualmente ajustado. Opções como se o PC pode ou não compartilhar arquivos e pastas podem estar ligadas, mas se um compartilhamento formal não for feito ninguém acessa o PC; analogamente se impressoras podem ser compartilhadas; se o PC é visível na rede, etc.



4 ESCOLHA O TIPO Existe outra aspecto da rede a ser configurada que é o conceito de pública e particular. Na tela **Central de Rede e Compartilhamento** clique em personalizar. Escolha o tipo de rede para definir a segurança necessária (ver Box Rede Pública ou Particular?)

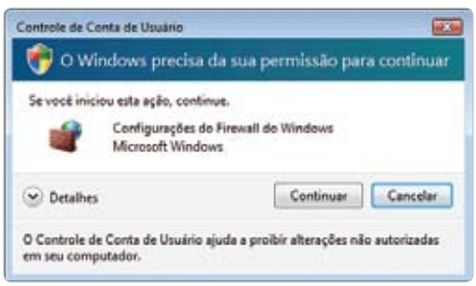
Aqui ninguém entra!

O Controle de Conta de Usuário (UAC) trabalha para que ninguém (ou qualquer ameaça) rode programa algum no seu PC sem que você saiba!

Por Flavio Xandó

Ao começar a usar o Windows Vista, alguns usuários estranham a presença de telas solicitando confirmações e autorizações que não existiam no Windows XP. Pode-se dizer que apesar de aparentemente "chatas" são fundamentais na estratégia de proteção. No Windows XP, por exemplo, um usuário pode ser Administrador ou Usuário Limitado. Fora ambientes corporativos, nos quais políticas de segurança forçam o usuário a ter menos prerrogativas, no ambiente de pequenos e médios escritórios e principalmente em casa, todos se promovem a Administrador. O perigo nasce aí. Por causa da arquitetura do Windows XP (imagine os sistemas operacionais mais antigos então), processos benignos e malignos herdam da sessão do usuário todos os seus privilégios. Programas podem ser instalados à revelia do dono da máquina, sub-repticiamente, áreas críticas alteradas, etc. Por outro lado o usuário comum (não administrador) não tem privilégios suficientes nem para trocar o fuso horário (em caso de viagem) ou a hora do computador, muito menos instalar um driver de impressora.

Na prática, no XP, o Administrador é muito mais poderoso que seria necessário enquanto o usuário comum é desprovido de capacidades básicas (por isso todos se promovem no XP a administrador). A estratégia usada no Vista teve bom senso, embora custe um certo nível de policiamento (ou burocracia para alguns). Quando uma ação crítica, que comprometa a integridade ou segurança é executada por um Administrador, o Vista interrompe o usuário e o informa da ação sendo executada e solicita uma confirmação. Se o usuário não for administrador, a senha do administrador daquele PC é solicitada para que a tarefa se complete. Esta segunda forma foi chamada originalmente de "Over the shoulders" (sobre os ombros). Mimetiza a ação de um supervisor que vem ao socorro de seu funcionário e autoriza com sua senha determinada ação.



ATENÇÃO Administrador sendo alertado de uma ação crítica

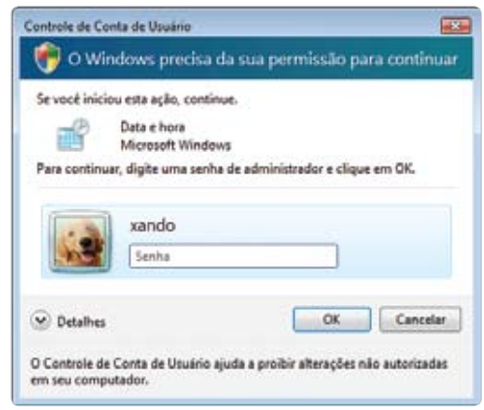
Isso é importante, pois desta forma um programa mal intencionado não realizará nada sem consentimento explícito de seu usuário (administrador ou não). Spywares por exemplo tentam interromper os serviços de antivírus e o fazem sorrateiramente no XP, mas não mais no Vista. Na essência esta descrição toda é o que faz o UAC ("Controle de Conta de Usuário").

Por outro lado várias ações que o usuário comum não realizaria antes estão disponíveis para ele, como desfragmentar discos, conectar-se a rede sem fio com criptografia, instalar controles Active-X ou periféricos previamente autorizados pelo administrador, realizar as atualizações críticas do Windows, etc. Foi uma troca. Um pouco mais de liberdade, mas um pouco mais vigiada. Uma decisão errada, autorizar a execução de um programa maligno, ainda pode ser feita, mas jamais sem que o usuário tenha autorizado explicitamente.

Privilégios somente para quem precisa

Mas e se o usuário mesmo com todos os alertas e solicitações de autorização permitir a execução de um programa maligno?

"Windows Service Hardening" é a resposta. Analogamente ao Controle de Conta de Usuário, a execução dos Serviços



PERMISSÃO Usuário comum solicitando uma permissão do administrador para ação crítica

do sistema também tem formas diferentes de conferir poderes às aplicações. Enquanto no Windows XP o "Local System Account" utilizado pelos serviços é pleno e poderoso, no Vista existem outras contas de usuário do sistema :

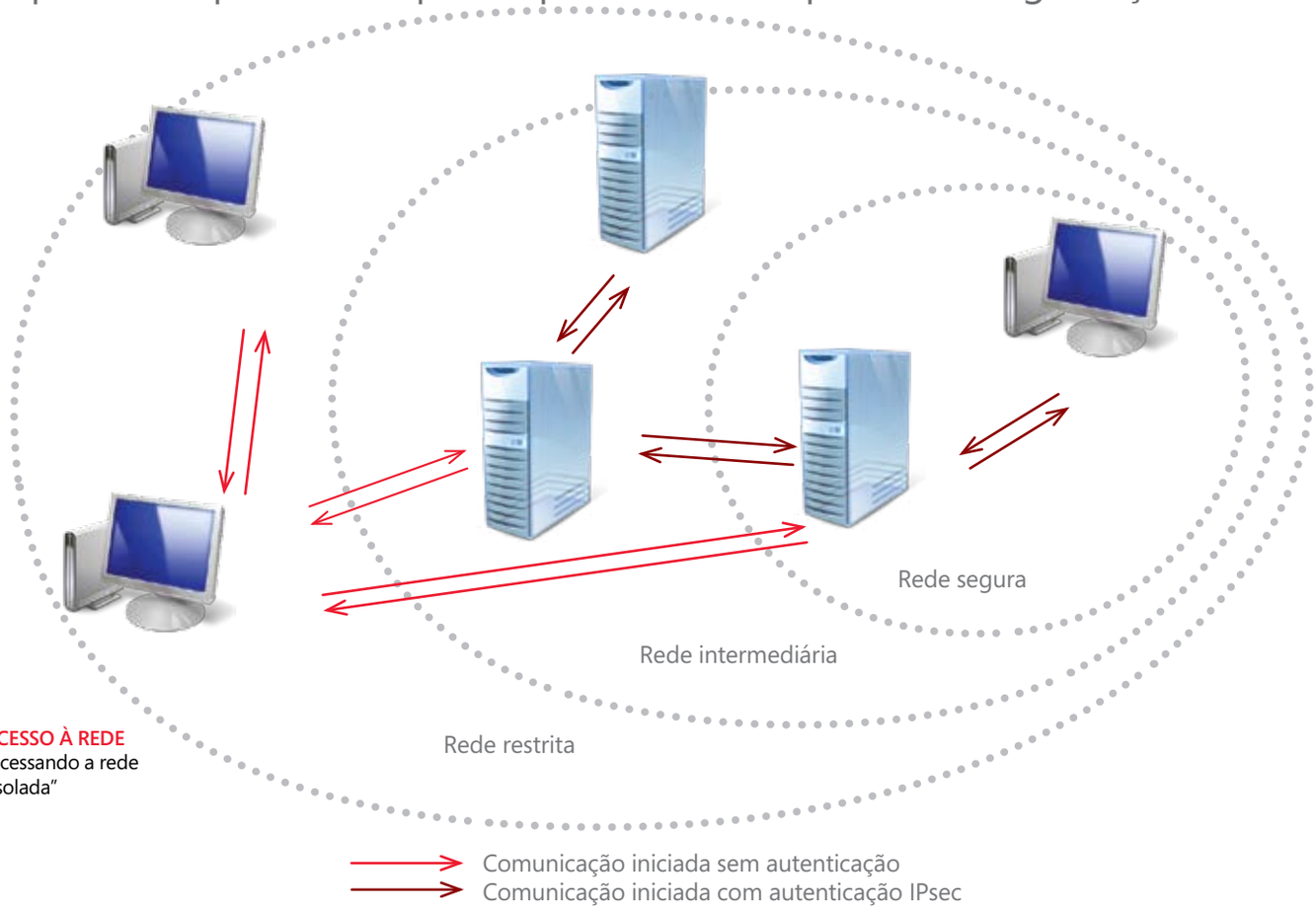
- "Network System Account", que é limitada em privilégios mas usada para serviços que precisam ter acesso à rede
- "Local Service Account", que é usada pelos serviços que somente precisam ter acesso à própria máquina.

Dessa forma as contas são limitadas nos privilégios básicos e somente têm autorização para atuar no escopo permitido. Devido ao grande número de "serviços" rodando simultaneamente, os "System accounts" podem ser aproveitados por usuários mal intencionados para instalar e executar código indesejado na máquina. Não é de admirar que tais "serviços" sejam o alvo principal de ataques de "malwares" como os recentes Blaster, Slammer e Sasser.

Essencialmente a estratégia denominada "Services Hardening" consiste em reduzir os privilégios dos "serviços" ao grau mínimo indispensável e limita seu raio de ação à máquina ou à rede. Todos os serviços do sistema operacional foram sujeitos a uma

Proteção de acesso à rede

Uma rede paralela separa as máquinas que não têm requisitos de segurança



PROTEÇÃO DE ACESSO À REDE
Visão do cliente acessando a rede segura ou "rede isolada"

forte análise sob esta ótica e excluídos quaisquer privilégios desnecessários – como, por exemplo, a possibilidade de "depurar" código, que pode ser explorada por programas mal intencionados (entre tantos outros perigos).

Na prática estas medidas não visam impedir a entrada de códigos perigosos e sim dificultar a ação de um malware e limitar o potencial de causar danos de um serviço eventualmente comprometido. A Microsoft encoraja os desenvolvedores independentes a aplicar as mesmas diretivas aos serviços por eles criados. Muitos dos serviços que rodam na máquina são feitos por terceiros para darem suporte a seus programas, como antivírus, rotinas de reconhecimento de periféricos, etc. Assim, tais serviços serão mais seguros ao rodar sob Vista.

PC suspeito? Isole-o da rede!

O Vista traz uma novidade, um recurso de auto monitoração que amplia muito o nível de segurança em rede, principalmente nas empresas. É a tecnologia chamada "Proteção de Acesso à Rede" (Network Access Protection). Um conjunto de políticas de segurança podem ser definidas como por exemplo :

- Existência de antivírus atualizado
- Windows Firewall ativado
- Vacinas do Windows Defender em dia
- Atualizações críticas de segurança

aplicadas ao sistema operacional

Entre muitas outras. A não observância destas condições impede determinada estação de trabalho de entrar na rede. Nas redes corporativas uma rede "paralela", que serve para isolar as estações de trabalho com esta falta de requisitos de segurança. Assim a única tarefa que estas máquinas conseguirão realizar é se ajustarem às políticas de segurança para só depois terem acesso à rede "real" e completa da empresa.

O recém lançado Windows Server 2008 é um ambiente especialmente pronto para trabalhar com todos estes controles pois consegue administrar, inspecionar e gerenciar estas situações dos sistemas operacionais das estações de trabalho.

Na empresa isto é particularmente muito importante quando um notebook de funcionário, que após passar um ou mais dias fora da empresa, retorna com alguma configuração fora dos padrões de segurança definido (Firewall desativado por exemplo). A mesma coisa se aplica para o caso de algum "visitante", cliente, fornecedor, que tente entrar na rede da empresa. Será submetido ao mesmo crivo.

No caso de Vista mais Windows Server 2008 pode ser inclusive feita de forma automática o "conserto" dos pontos que impedem o uso da rede. Atualizações críticas são instaladas, firewall religado, vacinas do Defender atualizadas, etc. visando restabelecer as condições mínimas que farão permitir o uso da rede.

Além do Vista que já tem o recurso, o Windows XP Service Pack 3 terá condições de ser também policiado e bloqueado caso seu status de segurança esteja aquém do necessário.

Esta arquitetura é bastante elaborada e pode ser tão complexa quanto for necessário. Para grandes empresa, com redes muito grandes, servidores poderão ser dedicados à função de "bloqueadores" (que consistem as políticas de segurança), os "remediadores" (servidores de atualizações de segurança), etc.

Backup sem stress

Saiba como o Windows Vista pode agilizar suas cópias de segurança.

Por Abel Alves

Você já imaginou se, de uma hora para outra, todo o conteúdo do disco rígido desaparecesse? Um pesadelo, não é mesmo? Pois saiba que isso não é tão improvável. Um simples vírus de computador pode causar esse tipo de estrago. Além disso, apesar dos discos rígidos estarem mais confiáveis do que nunca, eles também podem falhar. E, se isso acontecer, grande parte dos arquivos armazenados no disco estará perdida. A possibilidade de ter que reinstalar todos os programas na máquina já assusta, mas o problema maior é a perda dos arquivos pessoais, que não podem ser recuperados com uma simples reinstalação. Como podemos nos prevenir contra essa catástrofe? Simples: fazendo um backup de nossos arquivos.

O processo de backup consiste simplesmente em copiar arquivos de um meio de armazenamento (HD, CD-ROM) para outro (HD externo, disquete, Zip drive, CD-R, DVD-R, etc.) de modo que, se houver falha na mídia original, a informação estará segura no segundo local utilizado. Dessa forma, se um vírus contaminar seu micro e apagar todos os arquivos, você conseguirá recuperá-los por meio da restauração do backup.

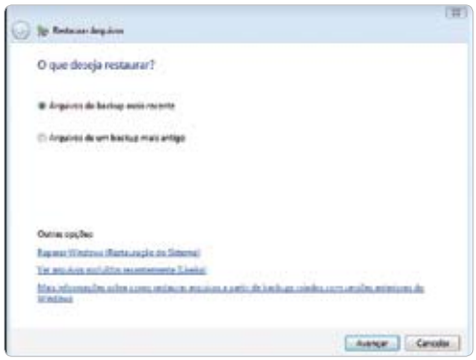
Infelizmente, a maioria das pessoas só lembra do backup quando já é tarde demais. Todo usuário precavido deve fazer backup periódico de seus arquivos. Inclusive porque essa tarefa é facilitada por vários programas. A Microsoft decidiu facilitar ao máximo a realização de backups no Windows Vista e mesmo os usuários leigos não terão dificuldades para realizar o procedimento.

O programa de backup e restauração do Windows Vista é, de longe, o mais simples para o usuário leigo que já vimos a Microsoft fazer. Mas, para um usuário mais avançado, ele peca num ponto importante: não permite que o usuário saiba QUAIS são os programas incluídos no arquivo de backup! Será que, marcando as caixas da figura, todos os meus documentos serão gravados? Será que um documento "escondido" em uma pasta de sistema será incluído no backup? E se eu possuir algum programa executável que baixei da Internet e desejo fazer backup? Simplesmente não dá para saber essas respostas! (Aliás, fizemos um teste e descobrimos que ele NÃO fez backup de um executável que baixamos da Internet e colocamos no desktop).

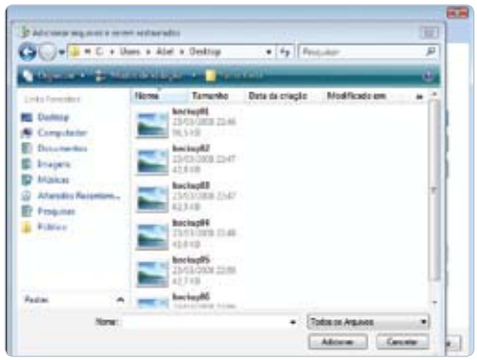
Para grande parte dos usuários, o backup do Windows poderá ser útil, principalmente pela facilidade e automatização. Mas os usuários mais avançados ainda vão precisar recorrer a soluções de terceiros.

Restaurando seu backup

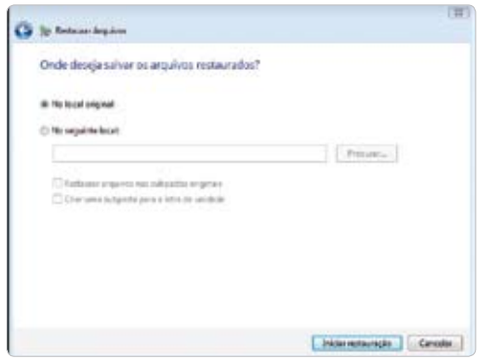
A restauração do backup não é tão automatizada quanto a sua criação. Comece clicando na opção **Restaurar Arquivos** do Painel de Controle, em Sistema e Manutenção.



1 ESCOLHA Escolhemos qual o arquivo de backup a ser restaurado. O último a ser realizado ou algum anterior:



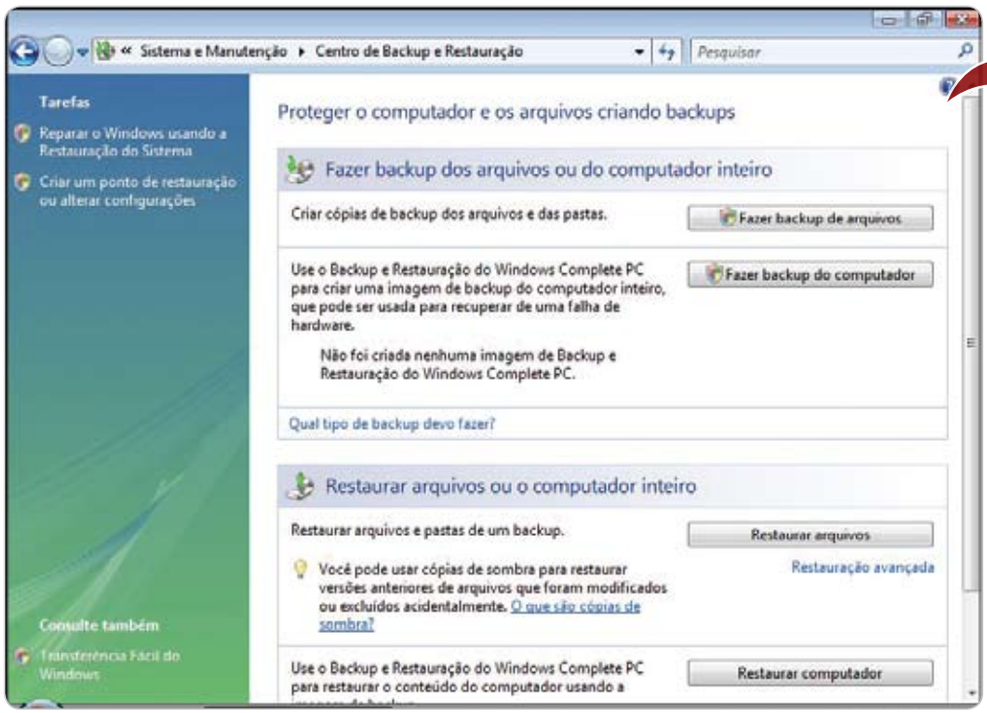
2 SELECIONE Selecionamos quais os arquivos que desejamos restaurar. Basta clicar no botão **Adicionar arquivos...** ou no **Adicionar pastas...**



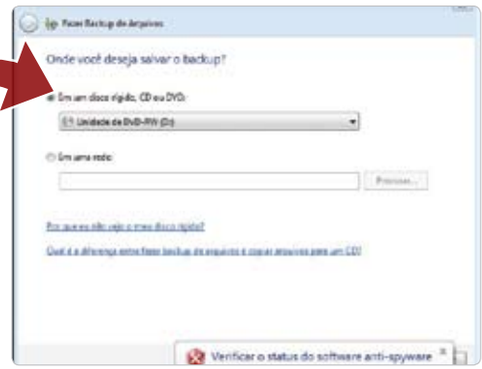
3 DEFINA O LOCAL Com os arquivos desejados já selecionados, basta escolher onde restaurar os arquivos: no local original ou num local específico.

Backup no Vista

Siga esses passos e garanta a segurança dos seus dados



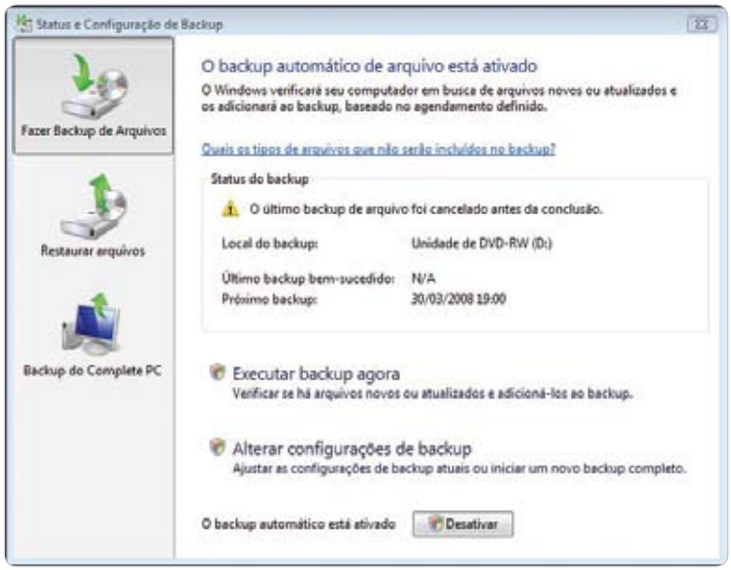
1 PAINEL DE CONTROLE Entre no Painel de Controle e, no item Sistema e Manutenção, clique em **Fazer backup do computador**.



2 BACKUP PESSOAL Como você quer apenas um backup de arquivos pessoais de seu micro, clique no botão **Fazer backup de arquivos**. Depois da confirmação do controle de conta do usuário, vai aparecer a janela em que você escolhe onde quer gravar o arquivo de backup.

3 ESCOLHA OS ARQUIVOS Agora, você escolhe quais os arquivos que estarão incluídos no backup. Note que são apenas os seus arquivos pessoais. Não serão incluídos arquivos de sistema, executáveis, etc.

4 PADRÃO Se o programa está sendo executado pela primeira vez, será criada uma configuração padrão de backup na qual, além dos tipos de arquivos que serão incluídos no backup, também ficará armazenada a freqüência com que será feito o procedimento de forma automática.



5 ALTERANDO Se desejarmos alterar as configurações de backup, basta entrar no Painel de Controle e, no item Sistema e Manutenção, clicar em **Fazer backup do computador**. Notem que, na janela de backup, aparece uma opção (em azul) **Alterar Configurações**.

A sombra sabe...

Aprenda a restaurar seu sistema a uma versão anterior para recuperar arquivos apagados e resolver outros problemas cabeludos.

Por Abel Alves

"UAU"

ShadowExplorer

Se você tem a versão Home do Windows Vista e quer utilizar os recursos do Shadow Copy, baixe o freeware ShadowExplorer (www.shadowexplorer.com) que permite acessar as cópias de sombra criadas pelo sistema

Que atire a primeira pedra quem nunca errou na hora de salvar um arquivo! Explicando melhor com um exemplo do Word: Você abriu um documento importante e usou o mesmo como "base" para criação de um novo documento. Porém, na hora de salvar, clicou (sem perceber) em "Salvar" ao invés de "Salvar como..."! Às vezes, um simples "Desfazer" resolve a situação, mas existem programas e situações em que ele não funciona. Assim como o Windows XP, o Windows Vista possui um utilitário para Restauração do Sistema. Porém a versão do Windows Vista é muito mais completa! No Windows XP a Restauração do Sistema se resume basicamente à restauração dos arquivos do Windows e remoção das alterações do registro. Já no Windows Vista, a Restauração do Sistema permite também recuperar versões antigas de qualquer arquivo que tenha sido criado no micro rodando o Vista! É essa capacidade que permite aos usuários do Vista resolver problemas como aquele mostrado no início deste artigo. O Windows Vista chama estas "cópias de segurança" dos arquivos ou pastas de versões anteriores. As versões anteriores são cópias de backup (cópias de arquivos e pastas de que você fez backup usando o Assistente de Backup de Arquivos) ou cópias de sombra (cópias de arquivos e pastas que o Windows salva automaticamente como parte de um ponto de restauração). As cópias de sombra podem ser cópias de arquivos no computador ou arquivos compartilhados em um computador em uma rede. Você pode usar versões anteriores de arquivos para restaurar arquivos que modificou ou excluiu acidentalmente ou que estavam danificados. Dependendo do tipo de arquivo ou pasta, você pode abrir, salvar em um local diferente ou restaurar uma versão anterior.

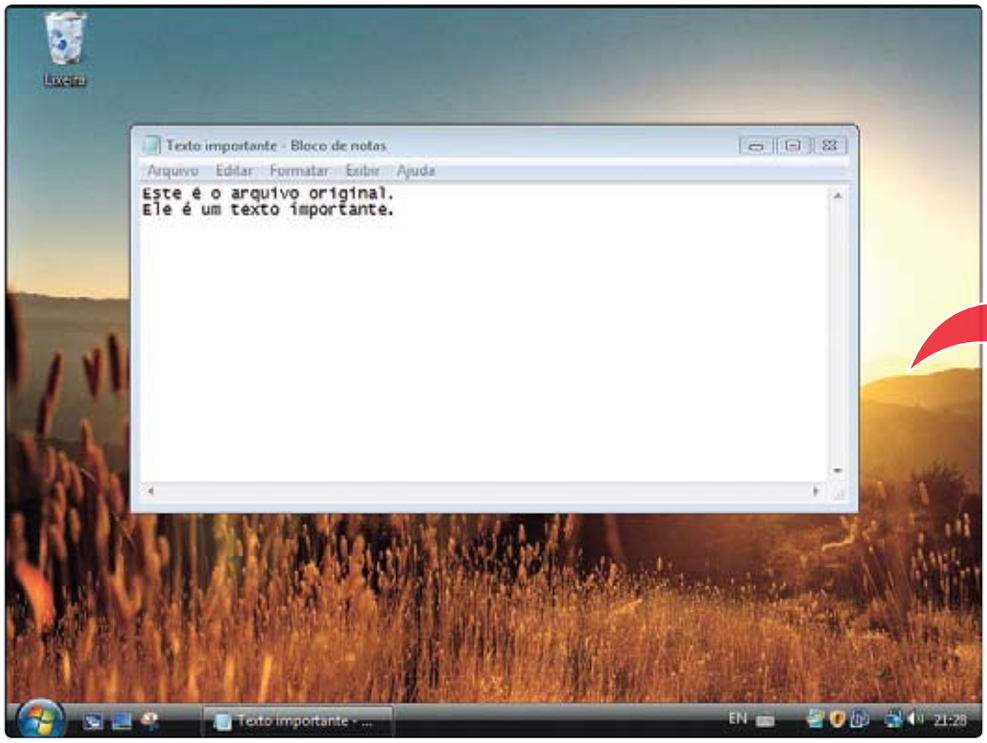
As cópias de sombra são salvas automaticamente como parte de um ponto de restauração em Propriedades do Sistema. Se a opção Proteção do Sistema estiver ativada, o Windows criará automaticamente cópias de sombra de arquivos que foram modificados desde que foi feito o último ponto de restauração, o que ocorrerá normalmente uma vez por dia. Se o disco rígido estiver particionado ou se houver mais de um disco rígido no computador, você precisará ativar a Proteção do Sistema nas outras partições ou discos rígidos. Para criar um ponto de restauração ou ativar a Proteção do sistema, clique com o botão direito do mouse em Computador e escolha Propriedades. Depois é só escolher a opção Proteção do sistema. Marque o disco ou partição onde deseja que a protecão atue ou crie um ponto de restauração clicando no botão.

É importante lembrar que o recurso de cópias de sombra só está presente nas versões Business, Enterprise e Ultimate do Windows Vista. Além disso, o recurso só funciona se já existir algum ponto de Restauração do Sistema que tenha "armazenado" a versão original do arquivo. E mais uma coisa: a cada ponto de restauração criado, uma parte do espaço em disco é usada. Para armazenar pontos de restauração, é necessário pelo menos 300 megabytes (MB) de espaço livre em cada disco rígido que tenha a Proteção do Sistema ativada.

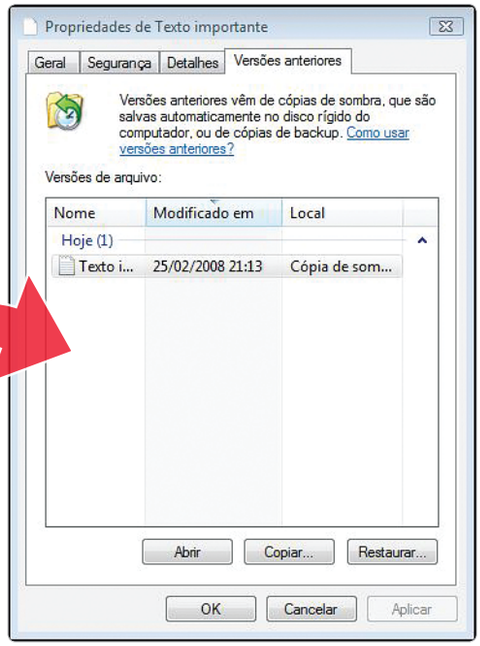
A Restauração do Sistema pode usar até 15% do espaço em cada disco. Conforme a quantidade de espaço é preenchida com pontos de restauração, a Restauração do Sistema exclui pontos de restauração mais antigos para criar espaço para novos.

Como usar as cópias de sombra

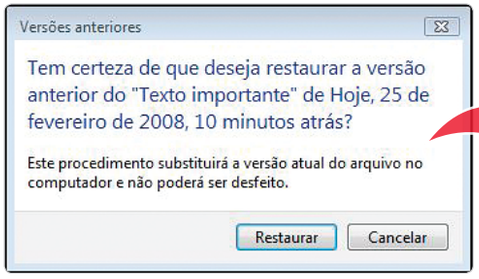
Saiba como usar esse recurso para restaurar a versão "original" de um texto importante apagado inadvertidamente.



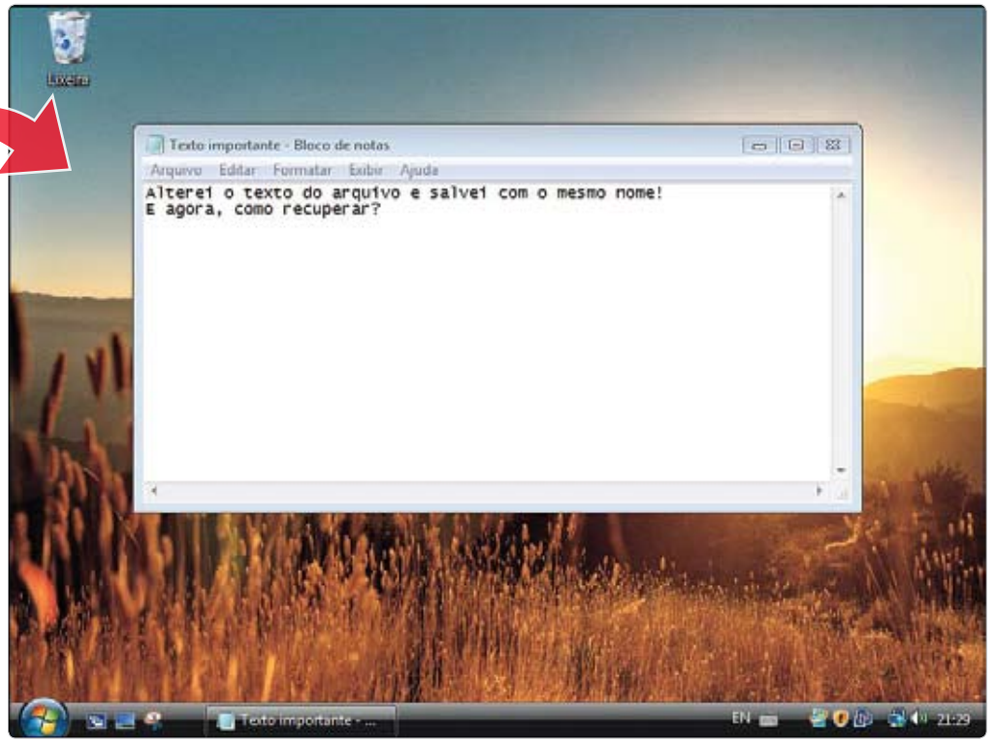
1 OPS! Você usou o texto original como base para outro documento e fez modificações. Infelizmente, na hora de salvar, se distraiu e salvou o texto com o mesmo nome do arquivo original.



2 RECUPERAR Para recuperar a versão de "backup" do texto importante, clique com o botão direito do mouse no arquivo "atual" e escolha Propriedades. Selecione a aba "Versões Anteriores".



3 CONFIRME Você verá uma lista das versões anteriores disponíveis do arquivo ou pasta. A lista incluirá arquivos salvos em um backup assim como cópias de sombras, se ambos os tipos estiverem disponíveis. Clique no arquivo ou pasta e clique em Restaurar. Na janela de confirmação, clique no botão Restaurar novamente.



4 NOTE que na janela de versões anteriores existem também as opções de Abrir e Copiar. Elas servem para verificar as versões originais (Abrir) ou restaurar a versão original dos arquivos ou pastas sem apagar a versão atual.

Proteja-se contra o roubo de identidade

"UAU"

Filtro contra phishing

Tecle Alt + O, seguido por H e C para checar rapidamente um site usando o filtro contra phishing do Internet Explorer 7 (isso se você preferir deixar o filtro automático desligado)

O roubo de identidade é uma fraude da era da Internet. Mas é possível limitar as chances desses "ataques predatórios" ocorrerem em seu PC com os recursos incluídos no Windows Vista. **Por Karl Hodge**

Paul Chapman passava os olhos pela mistura usual de folhetos de propaganda e contas durante o café da manhã, abrindo uma nova carta de uma empresa de celulares. Era uma conta de R$ 600 por ligações feitas de um telefone novo. Um telefone que ele nunca pedira nem usara... Philip Cortocoro recebeu uma mensagem em sua caixa de entrada dando-lhe as boas-vindas a um site de relacionamentos no qual ele nunca se inscrevera. Ao conferir a conta de seu cartão de crédito, descobriu que haviam lhe cobrado US$ 200 pelo privilégio.

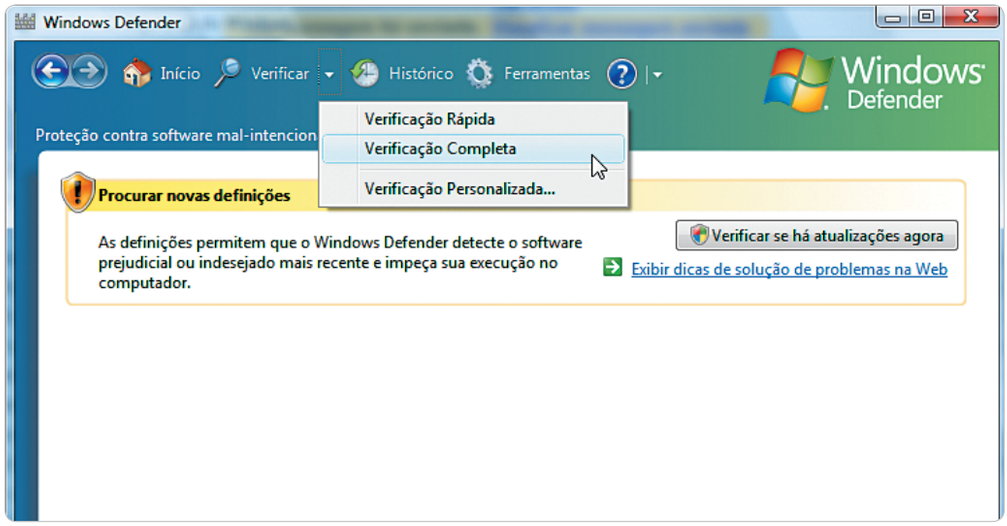
Esses dois homens foram vítimas do crime que mais cresce no mundo: roubo de identidade. Eles fazem parte dos milhares cidadãos que, anualmente, têm a identidade usada para compras fraudulentas no cartão, transações forjadas e empréstimos bancários. Uma gota no oceano em comparação aos milhões de pessoas afetadas pelo mesmo crime nos Estados Unidos. Muitas não percebem que foram apanhadas até muitas semanas ou meses depois – quando os indícios aparecem nos cartões e extratos bancários.

"Esses ladrões precisam de informações mínimas para roubar a identidade de alguém", diz Charles Rudagard, chefe do departamento de produtos e serviços da Garlik (www.garlik.com). "Para 'acessar' uma identidade, só é preciso descobrir alguns detalhes principais sobre um indivíduo: seu nome, a data de nascimento e seu endereço. Nada muito difícil de conseguir através de sites de relacionamento ou mecanismos de busca.

CONFIANÇA COMPUTADORIZADA
O Windows Vista ajuda a evitar que seus dados pessoais caiam em mãos erradas.

Como roubar uma vida

Os ladrões usam vários métodos para obter as primeiras informações. Neil Munroe, presidente do Grupo de Conscientização do Consumidor contra Fraudes de Identidade,



SPYWARE PENETRANTE O Windows Defender varre o computador em busca de programas perigosos em tempo real, impedindo ataques desde o berço e procurando spywares que tenham conseguido penetrar através da Internet.

indica um aumento nos ataques a grandes empresas – como a recente revelação de que hackers do mal roubaram os detalhes de quase 46 milhões de cartões de débito e crédito da TJX, a empresa dona da TK Maxx, uma conhecida rede de lojas de departamento do Reino Unido. "Vazamentos de dados são bastante comuns agora", conta Neil. "Os empregados podem ser subornados, enganados ou chantageados para roubar dados."

Em uma escala menor, há outros métodos da "vida real". O "mergulho no latão" - uma busca em latas de lixo atrás de contas velhas e documentos que contenham dados pessoais – é tão antigo quanto a própria fraude. O velho e bom furto também é recorrente – uma carteira batida ou um laptop roubado têm todas as informações de que um trapaceiro dedicado necessita. Atualmente, a Internet tornou o roubo de identidade um crime ainda mais atraente. "Logo que você tenha as informações certas, a Internet facilita a tarefa de usá-las remotamente", conta Maury Shenk, sócio do escritório de advocacia Steptor & Johnson.

"O anonimato da Internet permite que um criminoso arranque dados pessoais dos usuá-

CONSELHO DE AMIGO Consulte a cartilha de segurança elaborada pelo Comitê Gestor da Internet no Brasil (www.nbso.nic.br/docs/cartilha) para mais informações sobre procedimentos de segurança

"Uma carteira batida ou um laptop roubado podem conter todas as informações de que um trapaceiro dedicado necessita"

Dica do MVP
Busca de vírus

Chris Boyd - MVP, segurança

"Malware e roubo de identidade andam de mãos dadas", diz Chris Boyd, diretor de Pesquisa sobre Malware da FaceTime Security Labs. "Os sites de relacionamentos são um ótimo alvo para os criadores de malware. A opulência de informações pessoais oferecida, combinada com níveis generosos de customização pelo usuário, apresenta todas as sortes de problemas. Atualmente existem worms especializados em determinados serviços, que se espalham pela lista de contatos". Chris fala por experiência própria; ele descobriu o "Orkut Worm" ano passado, um tipo de vírus que recolhia detalhes bancários das vítimas em perfis de usuários do Orkut (www.orkut.com) convencendo os usuários a se logar por meio de links infectados. **www.facetime.com**

O roubo de identidade em números

Os ladrões de identidade atualmente lesam mais de 100,000 britânicos por ano
(fonte: www.garlik.com)

Em média, leva-se 467 dias para uma pessoa descobrir que foi vítima de fraude de identidade
(fonte: www.experian.com)

O roubo de identidade custou ao Reino Unido £1,67 milhões (R$ 6,68 milhões) em 2006
(fonte: Home Office)

97% dos lares britânicos jogam no lixo itens que podem auxiliar os ladrões de identidade
(fonte: www.stop-idfraud.co.uk)

Em 2005, identidades roubadas foram usadas para obter 3500 cartas de motorista, 1600 passaportes falsos e 2500 certificados de casamento forjados
(fonte: www.garlik.com)

25% das vítimas de roubo de identidade conhecem o ladrão
(fonte: Which)

4 milhões de pessoas no Reino Unido tiveram "alguma experiência de fraude de identidade"
(fonte: Sainsbury's Bank)

9 milhões de cidadão americanos são lesados pelo roubo de identidade a cada ano
(fonte: Larry Bridwell, www.grisoft.com)

222 casos julgados de fraude de identidade no Reino Unido em 2005 envolviam somas maiores que R$ 400.000
(fonte: www.garlik.com)

Um novo "malware" é criado a cada três minutos
(fonte: Timonthy Eades, www.sanasecurity.com)

Quem é quem

Charles Rudagard da Garlik (www.garlik.com), operadores da DataPatrol – um serviço de monitoramento que previne contra vazamentos de dados e potenciais fraudes de identidade.

Neil Munroe, diretor de Negócios Externos da Equifax (www.equifax.com), preside o Grupo de Conscientização do Consumidor contra Fraudes de Identidade.

Maury Shenk é sócio do escritório de advocacia britânico e americano Steptoe & Johnson; ele lidera o grupo europeu de tecnologia.

Geoff Sweeney, co-fundador da Tier-3, criadores do Huntsman, um sistema de gerenciamento de ameaças para ambientes corporativos e de governo.

Timothy Eades, vice-presidente de Vendas & Marketing da Sana Security, criadora de programas anti-malware para casa e escritório.

rios sem que eles saibam realmente com quem estão falando", diz o detetive Russel Day, do Met's Economic and Specialist Crime Command. Um bom exemplo disso é o "phishing": a prática de persuadir os usuários a digitar dados pessoais em sites falsos, mandando mensagens de spam para vítimas inocentes.

Geoff Sweeney, Chefe do Departamento de Tecnologia da empresa de desenvolvimento de software de segurança Tier-3 (www.tier-3.com), indica uma ameaça mais hi-tech. "Os ladrões usam uma variedade de métodos", conta Geoff, "incluindo ataques de 'malware' altamente sofisticados". Geoff dá como exemplo o Trojan Gozi, um malware que roubou os dados das transações da Secure Socket Layer – como os formulários de cartões de créditos. Descoberto em janeiro de 2007, o aplicativo era enviado às vítimas por meio de um email de spam que apresentava um link para um download falso do Internet Explorer 7. Irônico, considerando os recursos extras de segurança oferecidos pelo IE7 genuíno.

Embora o roubo de identidade seja assustador para a vítima, nem sempre a perda financeira é o maior problema. Na maioria dos casos, os bancos e empresas de cartão ressarcem as perdas. O verdadeiro incômodo é limpar a sujeira depois. "Não é como quando alguém rouba sua TV", diz Neil Munroe, presidente do Grupo de Conscientização do Consumidor contra Fraudes de Identidade. "Quando sua identidade é roubada, você não sabe se eles vão parar de usá-la."

Acesso apenas por senha

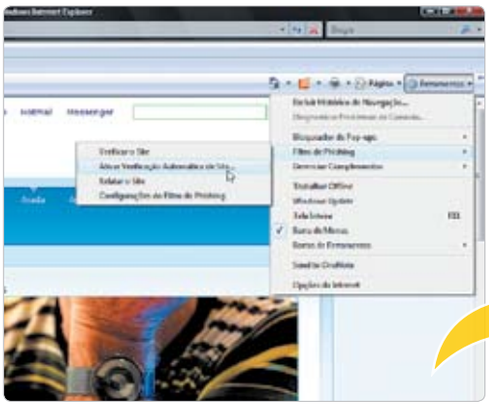
Ao adotar o Windows Vista, você já deu um passo gigante para se proteger contra fraudes de identidade; muitos de seus recursos de segurança já estão habilitados por padrão.

Dynamic Security Protection é o nome dado a uma variedade de recursos que protegem contra software malicioso como worms, vírus e sites que pescam dados. Eles vão desde o bloqueio de pop-ups até controles ActiveX opcionais para o Filtro de Phishing incluído no Internet Explorer 7. Seu navegador é conectado a um banco de dados com sites conhecidos de phishing e o programa detecta atividades fraudulentas em sites ainda não listados. Fique sabendo que o Phishing Filter fica desligado por padrão – é preciso habilitá-lo.

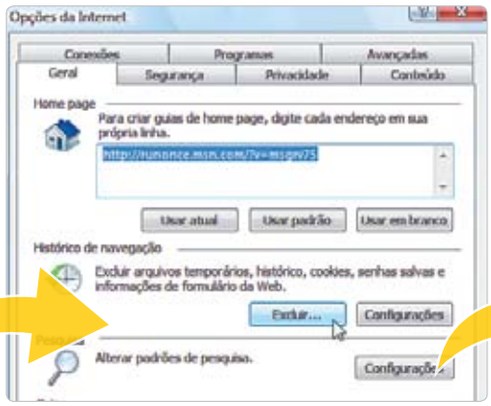
BLOQUEIO ANTIVÍRUS A Grisoft (www.avguk.com) anunciou recentemente o lançamento do AVG Internet Security 7.5

Proteja seus dados pessoais

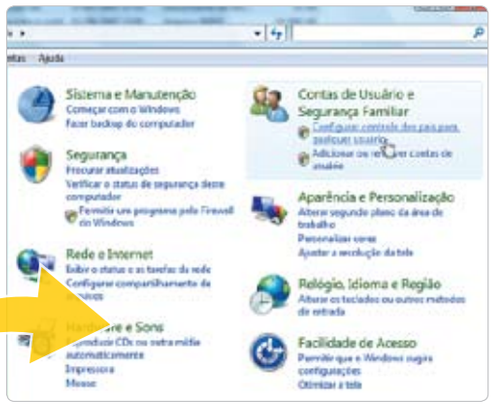
Três etapas para aumentar a segurança de seu computador



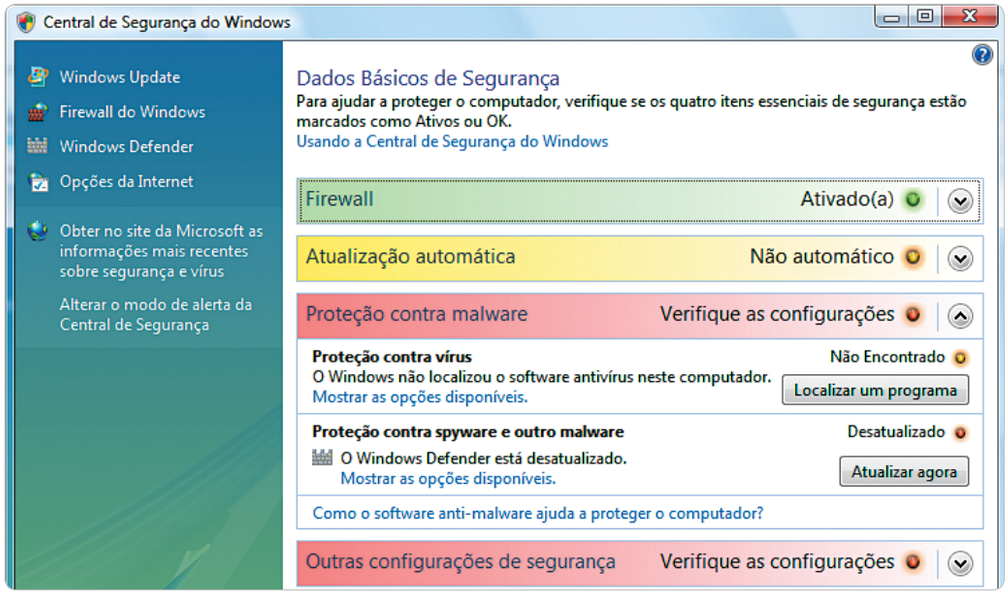
1 FUI PESCAR O Internet Explorer 7 pode detectar automaticamente sites que pescam detalhes pessoais. Vá em **Ferramentas ➜ Filtro de Phishing ➜ Ativar Verificação Automática de Site.** O filtro combina uma checagem local a uma comparação em um banco de dados.



2 DELETE SEU HISTÓRICO Vá a **Ferramentas ➜ Opções da Internet** e clique em **Excluir** na seção **Histórico de navegação** para apagar o histórico, senhas armazenadas, cookies e dados de formulário, evitando que ladrões oportunistas espiem detalhes de login.



3 AJUSTE O CONTROLE DOS PAIS Seus filhos podem entregar detalhes pessoais inadvertidamente ou permitir que um site suspeito instale malware. Vá ao **Painel de Controle** e clique em **Configurar controle dos pais** para qualquer usuário em **Contas de Usuários e Segurança Familiar** para restringi-los.



SEGURANÇA É FUNDAMENTAL A Central de Segurança do Windows Vista reúne firewall, proteção contra malware e atualizações.

"Ninguém pode acessar um drive criptografado pelo BitLocker sem a autenticação correta"

Os usuários do Internet Explorer 7 no Windows Vista têm uma camada extra de segurança, com seu Modo Protegido sempre ativado, feito para proteger contra ataques de "elevação de privilégio", nos quais programas de malware tentam mudar dados em sua máquina sem permissão.

Seu navegador trabalha em conjunto com outra novidade do Windows Vista, o Windows Defender. Essa ferramenta está acessível a partir do menu Iniciar. Por padrão, vem programada para varrer o sistema em busca de malware às 2 da madrugada todos os dias – mas é possível fazer uma checagem manual selecionando Scan sempre que desejado ou alterar o horário agendado em **Ferramentas ➜ Opções**. O Windows Defender também funciona em segundo plano enquanto você trabalha, alertando contra novas ameaças no momento em que surgem.

Se algum ladrão passar a mão em seu laptop ou obtiver acesso físico a sua máquina, a proteção contra malware não vai servir de nada. Mas proteger sua conta com uma senha, sim. Vá a Contas de Usuário no Painel de Controle e especifique uma senha para sua conta padrão. Os usuários das versões Enterprise e Ultimate do Windows Vista têm a proteção extra do BitLocker, uma tecnologia que criptografa uma partição de dados em seu disco rígido usando uma chave armazenada em um chaveiro USB ou em um Trusted Platform Module (TPM) instalado na máquina. Ninguém pode acessar um drive criptografado pelo BitLocker sem a autenticação correta, nem mesmo a polícia.

A Microsoft também está trabalhando para tornar mais seguras as transações online, com o Windows CardSpace – um sistema que armazena dados pessoais criptografados em uma "carteira de identidade" virtual. Integrados ao Windows Vista, os cartões CardSpace são exclusivos à pessoa e emitidos de maneira semelhante à dos certificados SSL. Também é possível criar seus próprios cartões. A principal vantagem é que o CardSpace elimina a necessidade de senhas, o que reduz as chances de roubo de identidade por phishing. A tecnologia é promissora, mas está em estágio inicial e exige maior apoio dos vendedores para realmente decolar.

O roubo de identidade é uma ameaça séria para todos. Mas com os recursos de segurança do Windows Vista e um pouco de bom-senso, é possível evitar tornar-se mais uma estatística.

SEGURANÇA NO LAR Visite o site www.identity-theft.org.uk da Home Office para mais conselhos sobre como defender suas informações.

7 Formas de garantir a segurança no Vista

1 Crie senhas a partir de frases. Elas deverão ser fáceis para serem memorizadas. Utilize caracteres especiais como (#$&@), letras maiúsculas e minúsculas e números. Quanto mais diversidade em sua senha, mais difícil será quebrá-la. Um bom exemplo é colocar informações como: Meu_ filho_nasceu_em_1990! ou Meu_aniversário_é_dia_25.

2 Acesse constantemente o seu Painel de controle e clique no Windows Defender. Faça uma busca por programas maliciosos e indesejados. Configure tudo para que ele esteja sempre alerta nas suas surfadas pela rede.

3 Crie uma unidade criptografada com o software Unidade BitLocker do Windows®. Esse suplemento está em Acessórios, Ferramentas de Sistema, Unidade BitLocker. Cuidado, é sempre bom ter um backup à mão.

4 Instale um antivírus. Existem muitas opções no mercado, inclusive gratuitos. Essas suítes de aplicativos contam também com firewalls mais incrementados que o do Windows. É um aplicativo essencial.

5 Cuidado com os softwares P2P, como o Emule, Kazaa, Shareaza. Além de utilizarem-se de portas diferentes das comuns para transferência de arquivos, eles costumam trafegar arquivos mascarados, ou seja, que dizem ser uma coisa que, realidade é outra. Portanto, sempre que baixar qualquer tipo de arquivo neles verifique tudo com um bom antivírus.

6 Nunca responda a spam. Você estará apenas confirmando que seu endereço de email é válido.

7 Fique de olho nos sites com Certificado Digital, aquele cadeadinho que aparece nos sites de compra. Novas versões fazem a barra mudar de cor, mas com um clique sobre ele e **exibir certificado** você poderá ver se a URL do site foi verificada por uma empresa de segurança.

Escritório à prova de crianças

É bom trabalhar em casa para ficar perto daqueles que amamos. Porém, os escritórios domésticos são cheios de riscos. Vamos descobrir como manter seus filhos – e seu PC – a salvo. **Por Gary Marshall**

Para quem tem filhos, trabalhar em casa costuma ser uma bênção – mas o equipamento de escritório pode apresentar muitos perigos para os pequenos e, sem sombra de dúvida, as crianças também podem ser perigosas para seus preciosos documentos e seu computador.

Eis aí algo que Linda Jones (do blog em inglês passionatemedia.typepad.com/kids) aprendeu do jeito mais difícil. "Sou naturalmente bagunceira, mas precisei aprender a me organizar quando comecei a trabalhar em casa. Eu me preocupava com todos aqueles cabos e tomadas em que as crianças podiam tropeçar ou enfiar o dedo e, quando minhas filhas Emily e Melissa (agora com oito anos) eram novinhas, não tinham permissão de entrar lá sozinhas", relembra. Ela costumava pegar as meninas no colo enquanto trabalhava e era o computador quem pagava o pato. "Sempre que o técnico, furioso, vinha em casa, me dava uma bronca: 'não beba nada quando estiver ao computador!' e sorríamos, concordávamos e já nos preparávamos para a próxima porcaria que seria derramada no teclado". Depois de um ano de migalhas e respingos de Nescau, o PC de Linda finalmente deu dois suspiros e morreu.

Ela acabou decidindo que computadores e crianças não são uma boa combinação e resolveu alugar um escritório fora – coisa que, certamente, Jake Ludington desejou ter feito quando seu filhinho Wyatt amarrotou um contrato importantíssimo que estava dando sopa na mesa dele. Mas, em vez de desistir, Jake decidiu-se a ajudar as outras pobres almas na mesma situação: arregaçando as mangas, partiu na arriscada missão de tornar seu escritório doméstico à prova de crianças – e, para nossa sorte, publicou seus conselhos no site www.jakeludingtron.com/child-safe-home-office. Ele descobriu que é possível realizar esse sonho – mesmo que dê um pouco de trabalho.

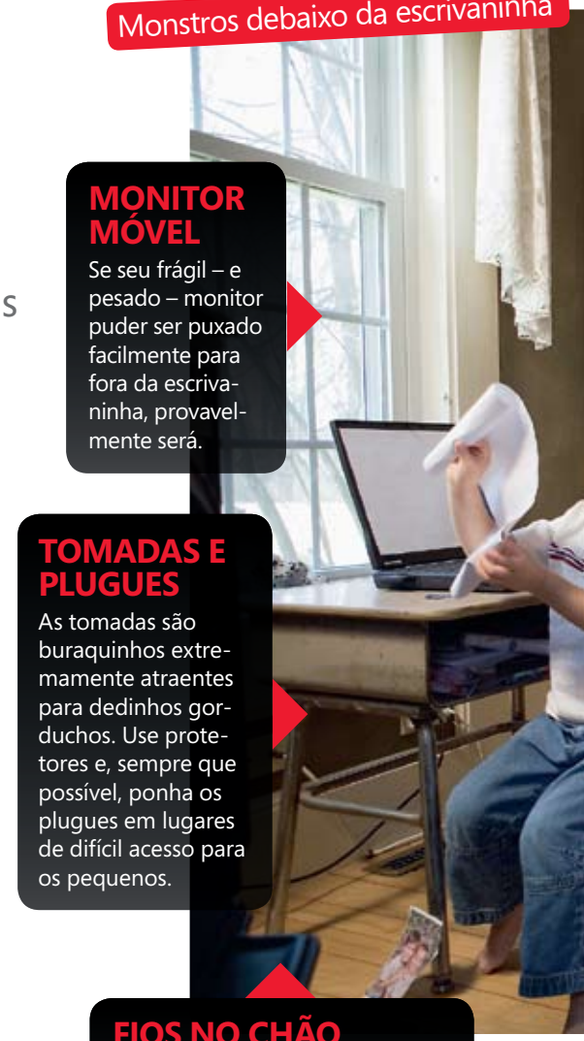
Perigos do escritório

Um dos modos mais fáceis de identificar riscos em potencial na sua sala de trabalho é engatinhar e explorar o cômodo na altura do pequeno. Se houver qualquer coisa que caia, quebre, dê choque, corte, espete ou faça tropeçar, isso provavelmente acontecerá. Engatinhar é um bom modo de identificar esses riscos.

"Logo que você tenha passado pelas coisas óbvias, como deixar objetos pontudos fora de alcance, esconder lâmpadas, armazenar apropriadamente as substâncias tóxicas e assim por diante, restará o trabalho de manter o ambiente de trabalho seguro para não precisar arrancar os cabelos mais tarde por sua falta de cuidado", explica Ludington, ressaltando que "abridores de cartas, estiletes e outros objetos afiados apresentam um certo grau de risco físico", e que não se deve esquecer de todos os cabos elétricos e tomadas.

Os conselhos online de Ludington vão desde cobrir as tomadas com dispositivos adequados até a escolha de uma cadeira

ARMÁRIOS À PROVA DE CRIANÇAS Use fechos de segurança para manter itens perigosos fora de alcance



GAVETAS DESTRANCADAS
São verdadeiras armadilhas para os dedos e, se houver objetos cortantes ou produtos de limpeza nelas, o risco é ainda maior.

PERIFÉRICOS COM FIO
Um tropeção ou esbarrada no teclado podem mandar o sistema inteiro para o chão, com seqüelas para o computador, para a criança e para o seu bolso.

MONTANHA DE PAPEL
O costume de arquivar a papelada não apenas ajuda a evitar que seu filhinho adorado transforme seus documentos em confete, como também contribui muito na organização do escritório.

PICOTADOR
A tragédia da combinação de lâminas ensandecidas e dedinhos exploradores, infelizmente, nem sempre é uma lenda urbana.

ESCRIVANINHA COM CANTOS AGUDOS
Muitas escrivaninhas têm a altura perfeita para atingir a cabecinha dos pequeninos. Se for o seu caso, use cantoneiras de borracha.

JUPITER IMAGES (UK) LTD

CANTOS MACIOS E OUTROS PRODUTOS DE SEGURANÇA PARA CRIANÇAS MOSTRADOS PODEM SER ENCONTRADOS EM WWW.BABYDAN.COM

CANTOS MACIOS Bordas afiadas e cabecinhas macias não combinam. Cantoneiras arredondadas resolvem o problema.

sem alavancas de ajuste contra as quais as crianças possam trombar. Mas não há o risco de que certos pais paranóicos possam ir longe demais? Ou será mais prudente imaginar sempre o pior? "Certamente é mais prudente... mas é melhor não exagerar", diz Ludington.

O principal conselho de Ludington é criar um ambiente repleto de "sim". Ele explica: "Trata-se de um ambiente em que você não precisa ficar o tempo todo dizendo 'não' para a criança. Acho que vi isso em algum livro sobre cuidar de crianças, mas não me lembro qual. Se você vai conviver com seus filhos em um escritório doméstico, precisa de coisas

Windows Vista para menores

Use o controle dos pais para proteger seus filhos contra a Internet

Até agora, falamos apenas dos riscos físicos, mas é óbvio que existem outros. É muito fácil encontrar coisas – ou pessoas – duvidosas online e, se seus filhos estiverem mexendo em um PC sem restrições, não é nada difícil que acabem vendo conteúdo inadequado. O outro risco é que mexam em coisas que não devem, como documentos de trabalho. Embora seja razoavelmente fácil recuperar arquivos no Windows Vista, é melhor prevenir do que lavar o carro do chefe.

A solução está nas Contas de Usuário e no Controle dos Pais. Ao atribuir a cada membro da família sua própria conta protegida por uma senha, é possível configurar o Controle dos Pais para filtrar o acesso à web ou evitar que determinados programas sejam rodados. O melhor é que os controles podem ser diferentes para cada conta, o que permite dar mais liberdade aos mais velhos. É muito fácil configurar as Contas de Usuário e o Controle dos Pais: basta entrar com a conta do administrador, abrir o Painel de Controle e seguir nosso tutorial abaixo.

CONTAS FÁCEIS Criar novas contas é brincadeira de criança: dê uma voltinha em **Painel de Controle ➜ Contas de Usuário e Segurança Familiar ➜ Adicionar ou remover contas de usuário** e crie uma nova conta.

SENHAS PARA OS PAIS Não há por que criar contas separadas se a sua própria não for protegida por uma senha – caso contrário, qualquer um poderia entrar nela e desabilitar o Controle dos Pais.

Estudo de caso: Traumas da primeira infância

Quando Pete Boston entrou para a agência de webdesign Headscape (www.headscape.co.uk), nunca tinha trabalhado em casa. "Transformamos um dos quartos em escritório", conta ele. "Decorei o quarto e comprei móveis de escritório para deixá-lo com cara de 'trabalho', para não ter sempre a impressão de que estava em casa".

Trabalhando em casa, ele pode passar mais tempo com a filhinha de um ano, Rachel. Embora o escritório não seja à prova de crianças, algumas alterações foram necessárias quando a menina começou a afirmar sua própria independência – e sua curiosidade.

"Preocupo-me principalmente com todos os fios e tomadas debaixo da escrivaninha, que é onde Rachel gosta de se enfiar quando engatinha para o escritório. Por isso, cuidei para que não fosse fácil puxar os cabos do monitor". Ele também vai mudar de lugar seu aquecedor de halogênio no inverno inglês (correspondente ao nosso verão), porque "Rachel já vai estar começando a andar até lá". De todas as coisas que estão no escritório de Pete, o aquecedor provavelmente é a mais perigosa.

Mas será que um escritório é mais perigoso do que qualquer outro cômodo da casa? "Sim e não", Pete responde. "É mais arriscado que um quarto de dormir, mas menos que uma cozinha – especialmente quando eu não estou e a porta fica aberta". Para Pete, a melhor solução é simples: "Deixe a porta fechada se você não estiver no escritório e o bebê estiver circulando por lá".

que eles possam fazer, porque eles vão querer estar com você. Dizer 'não' a cada passo deles não é nada produtivo e nem saudável para a criança".

Ele prossegue: "Providencie alternativas sólidas – como uma mesinha com papel à vontade e bastante lápis de cor – para conseguir trabalhar sem passar o tempo todo dedicando atenção negativa ao pequeno".

Trabalhe sossegado

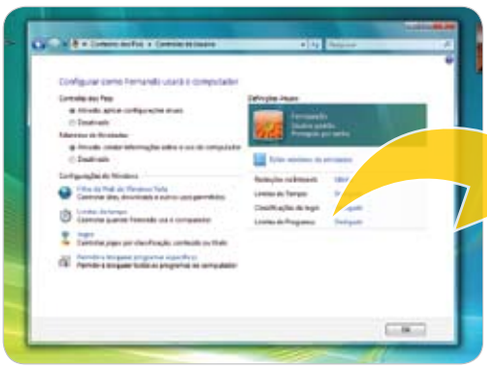
O site de busca de serviços Yell.com é famoso pelo tratamento que dá às famílias. Muitos de seus principais executivos passam a trabalhar em casa quando os filhotes chegam. Conversamos com três dessas felizardas do Yell.com: Patricia Kenar, Lynn Cormack e Alison Schillaci. Como elas se arranjam?

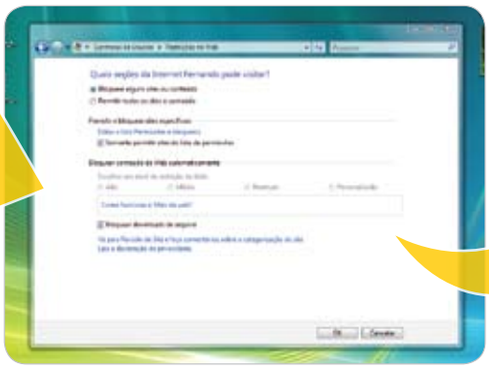
Os filhos de Lynn – Cameron (10) e Natalie (8) – são mais velhos, então "não foi preciso proteger grande coisa, já que eles já têm idade para não fazer – muita – besteira", conta ela. Não houve nenhum desastre – quer dizer, nada além da "bagunça de costume quando estou falando com um cliente: campainha, choradeira, cachorro latindo...".

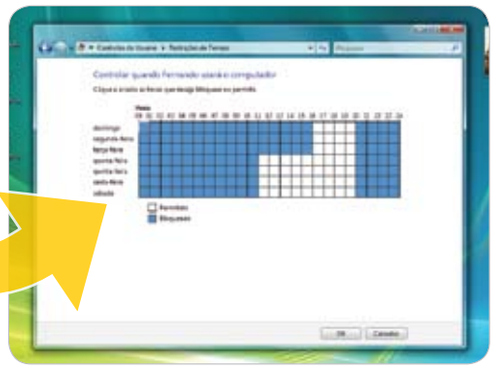
"A resposta do espertalhão é 'tranque-os para fora do escritório', mas nem sempre dá para fazer isso", conta Patricia Kenar. "Não permito que Neco (de 4 anos) entre quando

Internet segura para as crianças

Como configurar o Controle dos Pais no Windows Vista







1 CONTROLE COMPLETO Para ativar o Controle dos Pais no Windows Vista, vá ao **Painel de Controle ➜ Contas de Usuário e Segurança Familiar ➜ Configurar Controle dos pais para qualquer usuário**. Escolha a pessoa cuja conta deseja editar (configure contas separadas para cada membro da família), e aparecerá a tela mostrada na ilustração. Clique em **Controle dos pais: Ativado** para começar a montar uma conta segura para a criança.

2 VIGILÂNCIA NA REDE Além de bloquear o acesso a determinados programas, o Windows Vista inclui um filtro de Internet que impede as crianças de verem o que não devem. Clique em **Filtro da Web do Windows Vista** para escolher se prefere restringir ou bloquear sites. Para crianças pequenas, sugerimos marcar a caixa **Somente permitir websites da lista de permissão** e digitar uma lista de sites que você tenha a certeza de serem seguros. Se não estiver na lista, a criança não poderá abrir.

3 SENHOR DO TEMPO Nossa parte favorita do Controle dos Pais é o bloqueador temporal. A partir da tela principal do Controle dos Pais, clique em **Limites de tempo** para visualizar uma tabela como a mostrada acima, que divide cada dia em blocos de uma hora. Use o mouse para colorir a grade como desejar – o azul significa que o PC é ilimitado naquela hora. Se a criança tentar entrar em um horário indevido, o Windows Vista vai fazer pé firme e dizer que não.

JUPITERIMAGES (UK) LTD

NÃO É BRINCADEIRA Dê às crianças algo com que possam brincar e elas atrapalharão menos seu trabalho

estou trabalhando, mas, se estiver apenas organizando documentos ou algo assim, fazemos uma brincadeira na qual ele não pode falar comigo e fica quietinho desenhando". Ela também recomenda um portãozinho na entrada, "para que você possa vê-los, mas eles não consigam mexer em nada", e repete os comentários de Ludington sobre alternativas que sejam divertidas para as crianças: "Comprei um telefone de brinquedo e ele gosta de ficar imitando meus movimentos", ri. "É engraçadíssimo".

"Eu comprei um telefoninho e ele fica imitando meus gestos!"

"Usamos organizadores de fios e avisamos a Luke (7) e Isaac (4) sobre o perigo de mexer no picotador de papel", conta Alison Schillaci. "Deixamos que picotem documentos inúteis, propaganda e coisas assim com supervisão, por isso eles não ficam ansiosos para brincar com o aparelho... dissemos que eles poderiam perder um dedo e ele nunca voltaria a nascer. Sei que é chocante, mas achamos que é melhor ser dramático se as conseqüências podem ser ainda mais dramáticas".

"As crianças sempre querem aquilo que é proibido", observa Alison. Por isso, quando Luke tinha três anos, ela o apresentou ao Paint e ao site Cbeebies. "Ele não mexe em nada – modem, fios etc. – porque está mais interessado naquilo que pode fazer na tela". Ela descobriu que o mesmo método funciona com outros equipamentos: "Eu simplesmente demonstrava para que servia e alimentava o apetite deles para brincar com algo novo. Agora, eles nem ligam mais".

Como Jake Ludington, Alison descobriu que encher o ambiente de "sim" é um dos métodos mais eficazes de proteger os filhos. "Alimente e respeite a curiosidade de seu filho", diz ela. "Mostre como as coisas funcionam e dê um tempinho – supervisionado, no início – para que mexam no computador, deixe-os enviar um fax – isso logo cansa – e observe-os adquirir novas habilidades. Descobrimos que, quando Luke e Isaac aprendem para que servem as coisas e como funcionam, sua curiosidade diminui bastante. Quando não tentam fazer as coisas escondidos, não é preciso ter preocupações com a segurança deles".

Rapidinhas: 10 maneiras de enfrentar a ameaça do PC para as crianças

1 Engatinhe
Explore o escritório andando de quatro. Procure tudo o que possa ser puxado, empurrado ou derrubado.

2 Corte os cabos
Os teclados e periféricos sem fio não ficam presos ao PC – assim, não há risco de que mãozinhas ávidas possam derrubar o sistema inteiro no chão. É mais caro no começo, mas ajuda a poupar uma fortuna de conserto, para não mencionar as corridas histéricas ao pronto-socorro.

3 Limpe os fios
Certos cabos – de energia, de vídeo e assim por diante – são necessários. Use organizadores ou conduítes para mantê-los fora da vista e do alcance.

4 Esconda as coisas
Sejam CDs importantes ou clipes e tachinhas, se uma criança conseguir pegá-los, ela os pegará.

5 Tranque as gavetas
Travas à prova de crianças para gavetas e armários não custam muito, são fáceis de instalar e impedem que os pequenos mexam em objetos perigosos ou valiosos.

6 Cubra as tomadas
Os protetores de tomada não deixam que os dedinhos entrem em contato com a eletricidade em estado puro. Pense também em proteger os plugues conectados.

7 Mude o PC
Para crianças mais novas, drives de CD e DVD são lugares ótimos para apoiar brinquedos ou torradas com geléia. Ponha seu gabinete em um lugar mais alto para evitar um desastre melado.

8 Tampe a lixeira
Se tiver uma lixeira no escritório, uma simples tampa já impedirá o anjinho de apanhar velhos clipes, grampos e outras coisinhas que fazem dodói.

9 Mude o monitor
Os monitores, principalmente os antigos CRT, são muito pesados – e, portanto, perigosos. Mantenha o seu bem equilibrado e difícil de derrubar da escrivaninha.

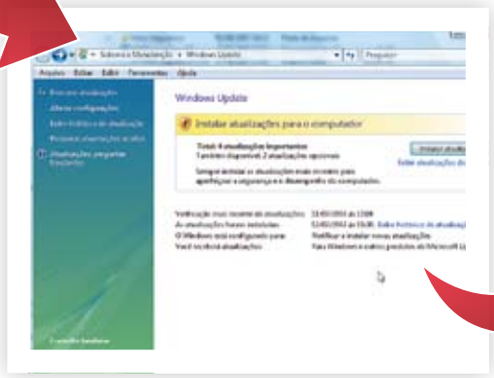
10 Abra espaço
Crie uma área para as crianças no escritório doméstico para diverti-las e, esperamos, distraí-las a ponto de esquecerem de enfiar o dedo na tomada.

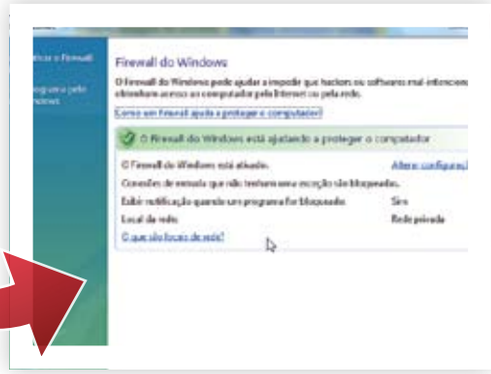
Cinco modos de deixar seu PC seguro

Pesquisas recentes mostram que um em cada 10 sites na Internet possui código malicioso, por isso é essencial proteger seu PC; a Central de Segurança do Windows ajuda a defender o seu computador. **Por James Stables**

"UAU" Atualizações automáticas

O Windows Vista atualiza automaticamente suas definições de segurança para manter seu computador continuamente a salvo de programas perigosos

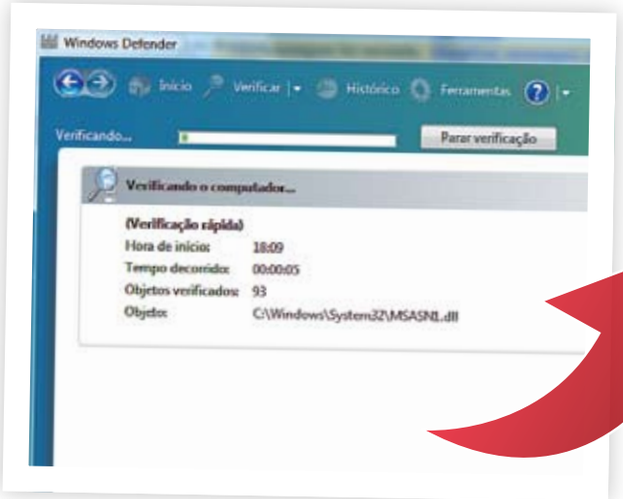


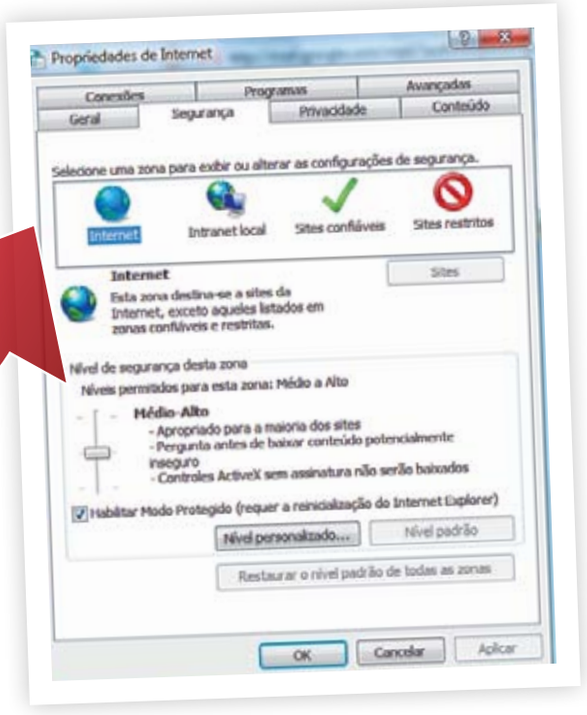


1 CENTRAL DE SEGURANÇA Se você ainda não foi lá, veja qual o seu status de segurança em **Painel de Controle ➜ Segurança ➜ Central de Segurança**. A janela principal mostra o status atual do Windows Firewall, Atualizações e Proteção contra Vírus; os problemas de segurança estão indicados em vermelho.

2 ATUALIZE Vá ao **Windows Update** na janela da **Central de Segurança** para ver quais são as atualizações essenciais ao Windows Vista. Defina se prefere que o Windows Vista baixe e instale automaticamente as atualizações ou se prefere procurá-las e instalá-las você mesmo.

3 FIREWALL O Windows Vista vem com um Firewall embutido para criar uma barreira entre você e os ogros virtuais. A partir da **Central de Segurança**, vá até a opção Windows Firewall no canto inferior esquerdo. Se tiver privilégios de administrador, pode mudar as opções de seu firewall, podendo inclusive editar as exceções ou as redes.





4 DEFENDA O Windows Defender é um aplicativo projetado para detectar spyware e malware. Clique nessa opção da Central de Segurança para varrer o PC em busca de programas suspeitos e configurar datas e horários para rodar o programa. A busca por software prejudicial (que pode vir até mesmo acoplado a outros downloads) não afeta em nada seu trabalho.

5 PROPRIEDADES Finalmente, vá direto ao onipresente e funcional menu Opções da Internet através da Central de Segurança. Aqui é possível fazer alguns ajustes menores nos níveis de segurança dos serviços de Internet e Intranet. Também dá para mexer nas configurações de privacidade, histórico do navegador e programas associados ao Internet Explorer.

RECEBA EM PRIMEIRA MÃO DICAS E NOVIDADES SOBRE ENTRETENIMENTO DIGITAL DOMÉSTICO.

Fique sempre por dentro das últimas novidades em entretenimento digital doméstico e receba dicas especiais da Microsoft assinando gratuitamente o informativo eletrônico do Windows Media Center. Para começar a recebê-lo, basta simplesmente se cadastrar no site **www.microsoft.com/brasil/hometheater**.

Escolha quando quer ver seus programas preferidos: pause TV ao vivo, agende gravações e organize-as no seu PC.

Organize sua coleção de músicas e escolha o que quer ouvir vendo a capa do álbum.

Compartilhe suas fotos digitais com quem você quiser, no conforto do sofá - ouvindo música e vendo as fotos na televisão.

Windows Media Center

Saiba tudo sobre o Vista

Windows Vista
A Revista Oficial
traz tudo o que você precisa saber sobre o novo sistema da Microsoft. Tutoriais passo-a-passo, dicas úteis, curiosidades e novidades. Tudo em uma linguagem coloquial e bem humorada.

PARA ASSINAR:

www.revistawindowsvista.com.br

DIGERATI