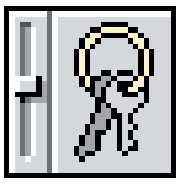
SÉRGIO MIRANDA

Chaveiro eletrônico

Guarde suas senhas num lugar seguro

A Internet invadiu a sua casa trazendo com ela banco, correio, música, literatura e até sexo para o seu computador, tudo isso possível com alguns cliques do mouse. E junto com todas essas mordomias, trouxe



um interminável amontoado de senhas para entrar nesses lugares maravilhosos. Como ficar decorando um monte de letras e números não é pra qualquer um e usar a mesma senha para tudo não é hábito saudável (sem falar em ficar escrevendo todas elas num arquivo de texto), a Apple inventou o Keychain, um painel de controle do Mac OS 9 que pode armazenar todas as suas senhas num único arquivo.

Mas você, que foi picado pelo mosquito da paranóia eletrônica, já está se coçando todo e faz a indefectível pergunta: mas esse negócio de manter todas as senhas num mesmo lugar é seguro? A resposta você vai ver já!

Guardando e trancando

Vamos partir do princípio de que você ainda não tem um Keychain. Ao acessar esse painel de controle, uma janela se abre perguntando se você pretende criar um "chaveiro". Depois, aparece uma tela pedindo um nome, uma senha e a confirmação. Essa é a única senha que você terá que memorizar daqui pra frente, por isso pense bem antes de escrevê-la. Ao clicar no OK, automaticamente será criado um chaveiro. Uma outra maneira de fazer isso é usar um programa que pergunta se você quer adicionar a senha ao Keychain. Se você não tiver criado sua senha-mestra, ele vai criá-la na hora.

Quando o Keychain abre pela primeira vez, ele está destrancado (*unlocked*). Mas, quando o computador é ligado, ele estará trancado (por motivos óbvios de segurança). Se algum programa tentar acessar o Keychain, você será avisado e uma janela pedirá a senha para destrancar. Quando não estiver usando, o melhor é trancar o programa para evitar aborrecimentos.

Você tem muitas senhas, mas sua memória é fraca? O negócio é encarar o Keychain

Com apenas uma senha-mestra, o Keychain guarda todas as suas senhas e certificados para a Internet

Chaves no chaveiro

O maior problema em relação ao Keychain é que, mesmo seis meses depois do lançamento do Mac OS 9, poucos programas são compatíveis com essa tecnologia: nem o Internet Explorer 5.0 nem o Netscape 6 trazem compatibilidade com o Keychain. Infelizmente, a aplicação mais bacana dele seria poder armazenar senhas de sites de Web (o site da Apple até diz que isso é possível, mas na prática não funciona).

Alguns dos poucos programas que já estão adequados ao novo sistema são o Anarchie (FTP) e o Eudora (email). Em ambos, o uso do Keychain facilita bastante tarefas como fazer updates de sites e baixar emails, eliminando a necessidade de lembrar várias senhas.

Mesmo sem a cooperação dos browsers, você pode usar o Keychain para guardar suas senhas de Web, de uma forma menos automática que o ideal, mas ainda assim útil.

Para isso, siga os seguintes passos:

1 Crie um documento qualquer (um arquivo de uma palavra no SimpleText).

2 Dê ao seu documento o nome do serviço que você quer guardar a senha (exemplo: Hotmail)

3 No menu File, escolha a função Encrypt. O Apple File Security irá encriptar o documento. Cheque se o quadradinho "Add to Keychain" está selecionado.

4 Coloque como senha o *login* e a senha do serviço (por exemplo, Silva/12345). Pode jogar fora o arquivo original.

Pronto, agora toda vez que você precisar lembrar sua senha, basta abrir o Keychain e dar um

Uma vez trancado, o Keychain só abre se você quiser

Get Info no arquivo Hotmail. Isso não aproveita a praticidade que o Keychain permite, mas pelo menos é um lugar seguro para guardar suas senhas. E com a vantagem de que você pode transportá-las para outras máquinas.
Com apenas um disquete (tá, você tem um iMac, não tem floppy… pode usar Zip ou o que quiser, falou?) é possível carregar suas senhas para qualquer outro computador com o Mac OS 9 e o Keychain instalado. Isso é possível porque as senhas ficam armazenadas em arquivos dentro da pasta Keychains, no System Folder. Carregue este arquivo para outra máquina, dê um duplo-clique sobre ele e pronto! Ele abrirá o Keychain. Aí é só colocar sua senha-mestra para ter acesso a todas as suas senhas secretas.

Segurança

Você continua se coçando todo, querendo saber se esse negócio é seguro ou não. Calma. Já vamos explicar.
Se você não contar para ninguém a sua senha, não há como outra pessoa abrir o seu Keychain. Isso é possível graças a um sistema de criptografia de 128 bits, o que significa que se alguém pegar sem querer (ou tiver roubado, mesmo) o seu chaveiro de senhas, será praticamente impossível usá-lo sem a senha-mestra.
E se você foi dar uma saída para arejar a cuca e esqueceu o seu Keychain aberto? Bem, não há muitos problemas, porque para fazer qualquer alteração nos settings do programa, inclusive modificar a senha principal, será preciso digitar a senha-mestra. Quem tentar mexer no seu chaveiro não poderá visualizar nenhuma das senhas guardadas, também.
Porém, muito cuidado ao desabilitar a opção de aviso toda vez que um programa ou site for utilizar os arquivos do Keychain. Se alguém fuçar no seu Mac e tentar acessar qualquer um das suas senhas, o programa ou o browser vai apenas procurar se aquela senha está armazenada e vai embora. Se muita gente gosta de mexer no seu computador, é preferível digitar aquela única senha algumas vezes a correr o risco de alguém descobrir o que você anda escondendo.

Aqui você vê a senha que esqueceu

Dicas para uma boa senha

Muito cuidado na hora de escolher sua senha-mestra. Aqui vão algumas dicas:
1 Não repita uma senha já existente (como a da conta do seu webmail, por exemplo).
2 Misture letras e números, mas não use datas que podem ser facilmente adivinhadas (seu aniversário, essas coisas).
3 Não componha sua senha com informações pessoais, como por exemplo o nome do cachorro, da namorada.
4 Não use palavras tiradas a esmo do dicionário.
5 Não conte para ninguém nem a escreva num papel escreva num papel ou num arquivo no desktop.
6 Use letras maiúsculas e minúsculas aleatoriamente, porque ela terá sempre de ser digitada dessa maneira.
7 Use a "Língua do Prince", trocando letras por números com formas parecidas (A por 4, E por 3, I por 1, S por 5, G por 6). Dessa forma você obtém combinações esdrúxulas, mas facilmente memorizáveis, tal como M4CM4N14 ou 8R4S1L.
8 Pegue as primeiras letras das seis primeiras palavras de uma música. No caso do Hino Nacional, seria ODIAMP.
9 Crie combinações de tecla que podem ser lembradas pela maneira como são digitadas, não pelo conteúdo. Exemplo: 7u8i9, que forma um W na hora em que você digita. Experimente várias combinações.

Arquivos confidenciais

O **Apple File Security** é um programa que transforma arquivos comuns em confidenciais. Com um sistema de algoritmos extremamente complexos, criado por Richard Crandall, que trabalhava na NeXT, esse programa era o que faltava para esconder textos importantes (ou aquele "nu artístico" que você baixou da Internet) de bicões. Todo o processo é muito simples e intuitivo. Você pode simplesmente clicar num arquivo (observação: não é possível encriptar aplicativos ou pastas, apenas arquivos), ir ao menu File e escolher Encrypt. Quer mais? Clique segurando a tecla Control e escolha Encrypt no menu contextual. Escolha uma senha (chamada aqui de *passphrase*). Ninguém além de você poderá acessar esse arquivo. Mais fácil, impossível.

Encriptar é outra solução rápida e fácil

Se você quer encriptar vários arquivos de uma só vez, a única maneira é usar o StuffIt para comprimi-los em apenas um arquivo e depois encriptá-los com o Apple File Security. O AFS, além de encriptar, também comprime os arquivos, economizando espaço em disco. Como já dissemos, é possível colocar esse arquivo encriptado no seu Keychain; assim, não será preciso ficar lembrando qual senha você colocou nele.
Agora, os pequenos problemas...
Toda vez que você encripta um arquivo, ele é deletado e transformado num arquivo do AFS. Até aqui tudo bem, pois por medidas de segurança é melhor ficar apenas com o arquivo encriptado. Porém, qualquer mané pode, com um Unerase da vida, encontrar seu arquivo original e recuperá-lo. Daí, meu amigo, não tem choro nem vela, sua privacidade foi pro saco.
Mas, calma, rapaz! Não há motivo para pânico. Para isso existem programas que podem limpar definitivamente os arquivos deletados do seu HD, como por exemplo o WipeInfo do Norton Utilities – que além de deletar, grava "brancos" sobre o arquivo (de maneira que, mesmo que o documento seja "ressuscitado", seu conteúdo estará vazio). M