Segurança é o tchan!

Aprenda a utilizar programas de criptografia

A revista Exame avisou: email não é seguro. E qual é a novidade? Agora recomeça aquele papo gasto de que a Internet não é segura. E desde quando é seguro entregar seu cartão de crédito na mão de alguém para pagar uma coisa numa loja? Algumas pessoas ainda não perceberam que a vida na Net não é essencialmente diferente do dia-a-dia.

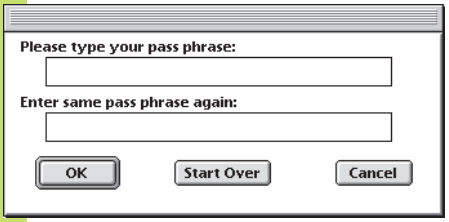
E como tornar as coisas seguras? Existe segurança, hoje em dia? Bom, o conceito de segurança mudou um pouco de uns tempos para cá. A gente pode chamar de segura a informação que custa mais caro para ser adquirida do que realmente vale, ou quando sua interpretação é mais demorada que seu período útil.

Criptografia tem tudo a ver com isso. Um arquivo bem criptografado pode levar alguns séculos para ser aberto nos computadores mais rápidos do mundo. Ou seja, apesar do código sempre poder ser quebrado, o tempo teórico para isso é tão grande que torna a espionagem inviável e, conseqüentemente, seguro o que foi criptografado. Para se ter uma idéia, uma chave (senha) de 1024 bits levaria 300 bilhões de anos para ser quebrada em um típico computador desktop que executa 1 milhão de instruções por segundo.

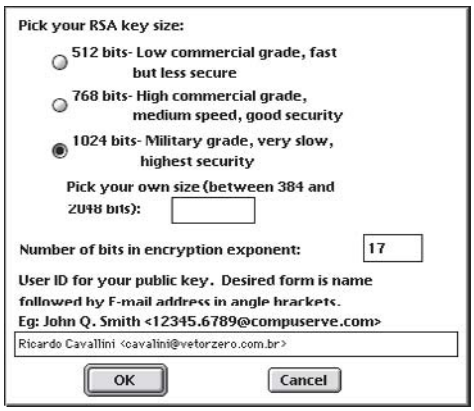
PÚBLICA E PRIVADA

Se você fechar algo com uma chave, ao passá-la para o seu recipiente a segurança toda vai pro saco, porque algum hacker pode interceptá-la. É aí que entra o conceito de chave pública e privada. Quando você cria uma chave para você, ao mesmo tempo cria uma segunda, de tal modo que uma chave só fecha e a outra só abre. Dessa forma, você pode espalhar para todo mundo que queira lhe mandar alguma coisa a chave que fecha (pública), porque com ela os outros só podem encriptar os arquivos, e somente você pode abri-los com a chave privada correspondente. Mas criptografar não significa simplesmente estar seguro. Existem vários níveis de criptografia (quanto maior o número da chave, mais segura), e aí é que entra a sacanagem política.

Como todo governo que se preza, o governo americano adora meter o bedelho na vida do seu cidadão. Assim, ele e muitos outros (francês, russo, chinês etc.) adotaram políticas rígidas restringindo o uso e a exportação de criptografia. A Netscape, por exemplo, só pode vender servidores de criptografia para fora dos EUA com o tamanho da chave máximo de 40 bits. Exportar o código integral para fora é expressamente proibido pelo governo americano, porque legalmente ele é classificado na mesma categoria da munição bélica. A justificativa do governo para restringir a criptografia é que ele precisa ter o poder de abrir as chaves na luta contra a pornografia infantil, terrorismo e tráfico de drogas, da mesma forma que pode abrir contas bancárias e grampear telefones. Mas isso é um motivo cretino. É o mesmo raciocínio de proibir a venda de armas para civis a fim de evitar que traficantes comprem armas. Qualquer um sabe que os traficantes vão continuar comprando armas, e as melhores.



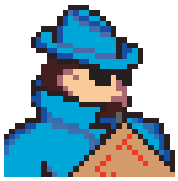
Para escrever sua senha utilize algo como uma frase misturando caixa alta e baixa, letras e números



Escolha o tamanho da chave que você vai querer e preencha o campo de baixo com informações pessoais

PRIVACIDADE LEGALZINHA

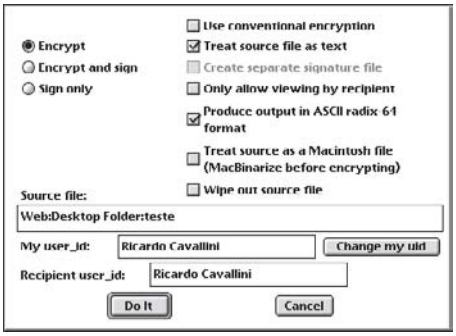
A bagunça aumentou quando um cara chamado Phil Zimmermann (dono da Pretty Good Privacy Inc. ou simplesmente PGP) jogou na Internet um programinha gratuito que criptografa arquivos em várias plataformas, com chaves de até 2048 bits.



O governo americano não gostou nada e abriu um processo contra Zimmermann. Mas você não tem nada com isso. Exportar é que é ilegal. Você, que é usuário final, pode usar o programa sem medo, já que o Brasil não tem leis contra o uso de criptografia.

E apesar de utilizar uma tecnologia que demorou para ser amadurecida, o fato do programa ser gratuito não quer dizer que ele seja pior ou menos seguro que um programa comercial. Muitas vezes as empresas optam por usar um programa gratuito que disponibiliza seu código, para ter certeza de que os seus autores não têm uma "porta dos fundos" para poder ler as informações encriptadas com ele. Mesmo com criptografia segura, uma empresa com más intenções poderia gerar uma segunda chave privada invisível a que o fabricante do programa tivesse acesso. Difícil de acontecer, mas, se você está criptografando, é porque quer algo realmente seguro. Hoje em dia existem diversas aplicações para criptografia. Você pode criptografar arquivos, discos e informações que

Para criptografar seu arquivo é só escolher Encrypt/Sign ou Conventional Encrypt (menu file), escolher qual a chave (já que você pode ter várias chaves) e mandar bala



Você ainda tem algumas opções como exterminar o arquivo original do seu Mac (Wipe Out source file)

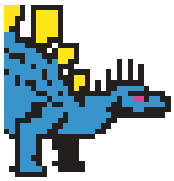
passam pela Internet, como vídeo, som, formulários etc.
Home banks podem checar se você é quem diz ser e garantir que os valores virtuais que você transmite cheguem intactos. Seus emails podem ser mandados com garantia de que somente vão ser lidos por quem você quer, e você pode mandar seu número de cartão de crédito sem ter medo de um hacker interceptá-lo no meio do caminho.

PASSO A PASSO

O PGP não chega a ser difícil de usar. A primeira coisa a fazer, depois de abrir o programa (é claro), é gerar uma chave privada para você (menu Key, item Generate Key). Escolha o tamanho da chave e preencha o campo de baixo com informações pessoais suas, algo como nome e email.
Depois disso, você precisa digitar sua senha. Lembre-se de que você não está abrindo conta no Bradesco, portanto nada de colocar nome do filho, RG ou data de nascimento; prefira uma frase misturando caixa alta e baixa, letras e números.
Na hora de gerar a chave vem a parte mais legal: você tem que digitar algumas teclas randomicamente. Nessa hora, bata no seu teclado com vontade, até ele pedir pra parar.
Depois de gerada a sua chave, copie os arquivos pubring.pgp e secring.pgp para um disquete e guarde com carinho. Nem pense em esquecer sua senha; lembre-se de que, se você perder a chave, nem mesmo o Stephen Hawking vai poder abrir seu arquivo.
Para distribuir a chave pública, você pode dar um comando Asciify na sua chave pública (arquivo pubring.pgp) para transformá-la em formato texto, e pode então mandá-la via email.
Para encriptar seu arquivo, é só escolher Encrypt/Sign ou Conventional Encrypt (menu File), escolher qual a chave (você pode ter várias chaves) e mandar bala.
Para decriptar, é só dar um Open/Decrypt, escolher o arquivo e digitar a sua senha, é claro.
Para facilitar toda essa zona, você pode usar o FileCrypt, uma extensão de sistema que coloca mais um menuzinho no Mac para encriptar e decriptar seus emails e arquivos de texto no Finder, Netscape, Eudora e Claris Emailer. Tudo fácil e rápido como comprimir um arquivo no DiskDoubler.

ESTENOGRAFIA

Mandar arquivos criptografados garante que ninguém vai abrir o que você fechou, mas não garante que ninguém perceba que você está usando criptografia. E o que fazer em países ou empresas onde o uso da criptografia é proibido? A resposta é a estenografia, um método



para camuflar uma informação dentro de outra. No Mac você pode usar o simples e prático Stego, da autoria de Romana Machado, que é engenheira de software, escritora, especialista em criptografia e, por mais incrível que pareça, modelo profissional.
No Stego, é só dar um open em uma imagem Pict, dar "Steg" no menu File e escolher o texto que quer incluir, e pronto. Mas lembre-se de que, se alguém souber do seu truque, vai poder dar um "Unsteg" e descobrir o que tem dentro. Portanto, criptografe antes de camuflar a sua informação. M

RICARDO CAVALLINI
É consultor de computação gráfica nas áreas de DTP e Interactivity.
web: http://www.impex.com/cavallini

ONDE ENCONTRAR

Pretty Good Privacy Inc. Home Page:
http://www.pgp.com/
FAQ PGP 2.6.3i:
http://www.ifi.uio.no/pgp/FAQ.shtml
EzStego Web Site:
http://www.stego.com
Romana Machado Erotic Site:
http://www.glamazon.com/
Crypto-Log: Internet Guide to Cryptography:
http://www.uni-mannheim.de/studorg/gahg/PGP/cryptolog1.html
FileCrypt:
http://www.highware.com/filecrypt/

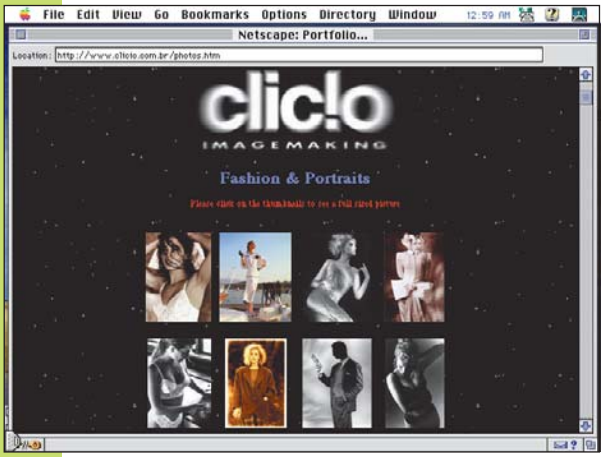
Sites da Hora

TONY DE MARCO

Peek of the Week

http://www.glamazon.com

"Procurando por fotos eróticas com um toque pessoal? Eu sou uma desenvolvedora de software e Web designer, mas faço hora extra como uma modelo glamurosa." Assim começa a home page de Romana Machado, criadora do Stego e musa dos macmaníacos. As imagens ao lado são gratuitas; se você quer ver algo mais íntimo, use o First Virtual Bank e pague US$ 10 por uma coleção de fotos ou US$ 35 para ver todas as reveladoras imagens. Romana quebra preconceitos ao apresentar seu inquietante conjunto de cabeça e corpo.



Clicio

http://www.clicio.com.br

Autor das capas mais gatinhas da MACMANIA, Clicio agora está com endereço próprio para mostrar seu trabalho. São fotos de moda, produtos, colagens digitais e informações sobre um fotógrafo que adora Macs. Caçando links sobre fotografia? Conheça esta página e passe seus dias consultando os milhares de sites comentados.

Guloseimac

http://www.solar.com.br/~rubem/GuloseiMac.html

O consultor legislativo Rubem Amorese oferece aos macmaníacos utilitários, arquivos, templates e outras guloseimas. As informações que acompanham cada link estão na seguinte ordem: nome, tamanho, compactador utilizado e breve descrição do arquivo. Atenção: todos os arquivos estão "binexados". Isso quer dizer que você precisa de um descompactador e decodificador de BinHex (como o StuffIt) para poder utilizá-los.