Imagens dem10/Getty

A privacidade dos dados tornou-se absolutamente crucial para as empresas. E algumas empresas não medem esforços para proteger seus dados, arquivos e comunicações.

No entanto, muitos consumidores e pequenas empresas continuam a acreditar que adicionar segurança extra não compensa o trabalho extra necessário. Errado! Qualquer pessoa que se recuse ou negligencie a adoção de medidas adicionais poderá acabar no lado errado de uma violação de dados.

Além disso: Os melhores serviços de hospedagem de e-mail de 2025: testado por especialistas

Digamos, por exemplo, que você inclua informações confidenciais em um e-mail inocente, apenas para descobrir que um malfeitor interceptou a mensagem, leu o conteúdo desse e-mail e extraiu as informações para algum propósito nefasto.

Você não quer isso. Mesmo que exija um pouco mais de trabalho de sua parte, estar seguro é muito melhor do que lamentar.

O que você faz? Você criptografa seu e-mail (ou o e-mail que contém informações confidenciais).

O que você vai ler:

memória virtual

O que é criptografia de e-mail?

A criptografia de e-mail é uma forma de restringir um e-mail de forma que apenas o destinatário possa lê-lo. Isso funciona por meio de pares de chaves de criptografia da seguinte forma:

- O destinatário cria um par de chaves GPG (composto por uma chave pública e uma privada) e envia a chave pública para você.
- Você importa a chave pública para o seu chaveiro.
- Em seguida, você envia uma mensagem para o endereço de e-mail do destinatário (associado à chave recém-importada).
- O destinatário recebe o e-mail e pode lê-lo porque possui a chave privada que corresponde à chave pública que você importou.

Se o e-mail for interceptado no caminho, ele não poderá ser lido sem a chave privada correspondente. Isso, é claro, traz à tona uma questão crucial que nunca pode ser suficientemente enfatizada: ***nunca compartilhe sua chave privada com ninguém.***

Sim, adicionar criptografia ao e-mail adiciona etapas extras ao seu processo, mas ao lidar com informações confidenciais, essas etapas extras valerão o esforço.

Como cada cliente de e-mail faz isso de maneira diferente, demonstrarei o uso do aplicativo Thunderbird de código aberto. Também demonstrarei como criar sua chave GPG (usando GnuPG), para que você possa ajudar seus destinatários a gerar os pares de chaves necessários e enviar a você suas chaves privadas.

Veja como funciona.

Como criptografar seu e-mail

Serão feitas as seguintes perguntas (resposta com os padrões):

- Selecione que tipo de chave você deseja:
- Qual tamanho de chave você deseja?
- A chave é válida para?

Além disso: esse truque simples do Gmail me deu mais 15 GB de armazenamento gratuitamente – e não perdi nenhum arquivo

Quando solicitado, digite y para verificar a criação da chave. Em seguida, você deverá adicionar um nome real, um endereço de e-mail associado à chave e um comentário opcional. Finalmente, você deverá digitar e verificar uma senha para o novo par de chaves. Depois disso, sua chave está criada e pronta para exportação.

Em seguida, precisamos exportar a chave pública para que ela possa ser enviada à pessoa que deverá enviar a você um e-mail criptografado. Para exportar a chave, emita o comando:

Mostrar mais

```
gpg --export -a "EMAIL" > public_key
```

Onde EMAIL é o email associado à chave que você acabou de gerar. Depois de gerar o arquivo (chamado public_key), envie-o para a pessoa que criptografará o e-mail para você.

A seguir, precisamos importar a chave pública que foi enviada a você. Abra o Thunderbird, clique no botão Menu e clique em Configurações da conta.

Além disso: cinco razões pelas quais o e-mail nunca morrerá

Na barra lateral esquerda, clique em Criptografia ponta a ponta e depois clique em Gerenciador de chaves OpenPGP.

Mostrar mais

Obtendo acesso ao gerenciador OpenPGP no Thunderbird.

Captura de tela de Jack Wallen/ZDNET

Clique em Arquivo > Importar chave pública do arquivo e selecione Todos os arquivos no menu suspenso no canto inferior direito da janela.

Mostrar mais

Importando a chave pública do OpenPGP Key Manager.

Captura de tela de Jack Wallen/ZDNET

Localize o arquivo que você salvou (a chave pública do destinatário que receberá seu e-mail) e clique em Abrir. Na janela resultante, selecione Aceito (não verificado) e clique em OK. A chave será importada e estará pronta para uso.

Mostrar mais

Importar a chave de Henry Jekyll pode não ser a melhor ideia, mas vou em frente.

Captura de tela de Jack Wallen/ZDNET

Feche o Key Manager e volte para a janela principal do Thunderbird. Redija uma nova mensagem para o endereço de e-mail associado à chave de criptografia e, em seguida (na janela de composição de e-mail), clique no menu suspenso Segurança e clique nas caixas de seleção Exigir criptografia e Assinar digitalmente esta mensagem.

Além disso: o cliente de e-mail Thunderbird finalmente chegou ao Android e valeu a pena esperar

Envie a mensagem normalmente e ela será criptografada de forma que a única pessoa que possa descriptografá-la seja o proprietário da chave privada que corresponde à chave pública que você importou.

Mostrar mais

Criptografando e assinando seu novo e-mail.

Captura de tela de Jack Wallen/ZDNET

E é assim que funciona a criptografia de e-mail. Espero que isso seja muito mais fácil do que você esperava e que o inspire a começar a usar essa camada extra de segurança em suas comunicações por e-mail.

Existe uma diferença entre e-mail seguro e criptografado?

Sim. E-mail seguro refere-se à segurança da conexão usada para enviar e receber e-mail (com cada etapa do caminho sendo segura), enquanto e-mail criptografado é quando o conteúdo do e-mail é criptografado, de forma que apenas o destinatário pretendido possa ler o conteúdo.

Você pode criptografar e-mail gratuitamente?

Sim. Com ferramentas como OpenPGP e Gpg4win, você pode criptografar e-mails gratuitamente em seu cliente de e-mail local (como Thunderbird e Outlook).