Como tornar o uso do drive mais seguro

O armazenamento de dados na nuvem se tornou tão popular quanto os dispositivos de armazenamento externo – há quem diga que a nuvem está superando essas outras unidades. Isso se dá pela rapidez, velocidade e acessibilidade como principais vantagens. Já as unidades físicas (pen drives, HDs externos etc.) devem ser transportadas e só podem ser acessadas se estiverem conectadas a um dispositivo compatível, podendo ser esquecidas ou até mesmo perdidas.

O Google Drive, por exemplo, é um espaço de armazenamento em nuvens de arquivos, mas não se resume a isso. Além de guardar seus documentos de maneira organizada e acessível, ele é responsável por manter seus arquivos sincronizados entre diferentes máquinas e a internet. Com ele, é possível que você acesse seus documentos por um computador, tablet ou smartphone, basta ter conexão com a internet. Também há a possibilidade de compartilhar seus arquivos e tornar outras pessoas colaboradoras, atualizando sempre o documento para a versão mais recente.

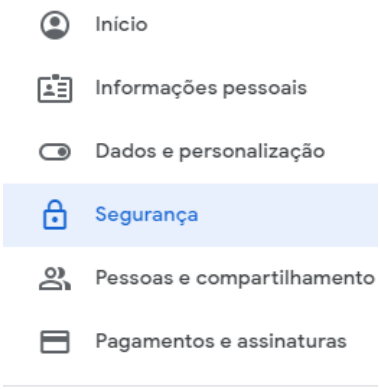
Apesar da nuvem ter várias vantagens, deve-se atentar a segurança dos dados armazenados nela. Abaixo estão listadas algumas medidas que podem ser tomadas para armazenar dados com mais segurança nesse tipo de serviço.

Verificação em duas etapas

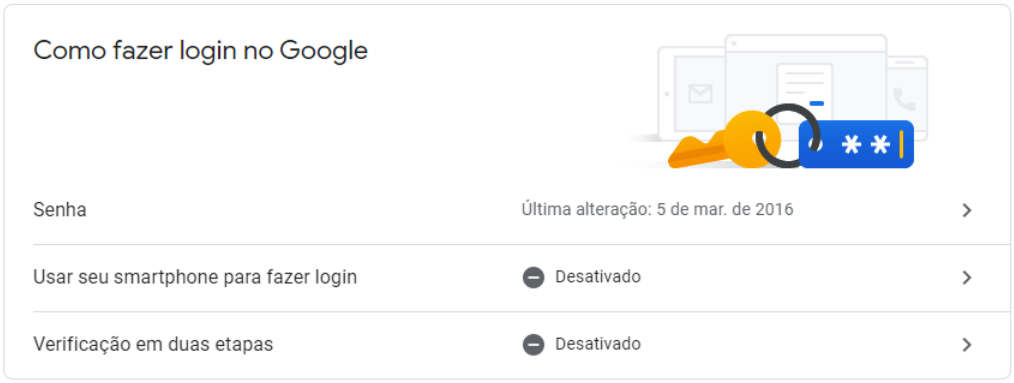
A maioria dos usuários protege suas contas usando apenas a senha, no entanto esse não é um método infalível. É aí que entra a autenticação de dois fatores. Este é um processo de segurança que só permite que uma pessoa acesse à sua conta caso consiga comprovar sua identidade duas vezes, adicionando uma camada extra de segurança à sua conta. Ou seja, utilizando uma senha e um token, que pode ser enviado por telefone, por exemplo. A ativação deste critério reduzirá a possibilidade de hackers conseguirem acesso às suas informações.

Para ativar a verificação em duas etapas na sua conta, siga os passos abaixo:

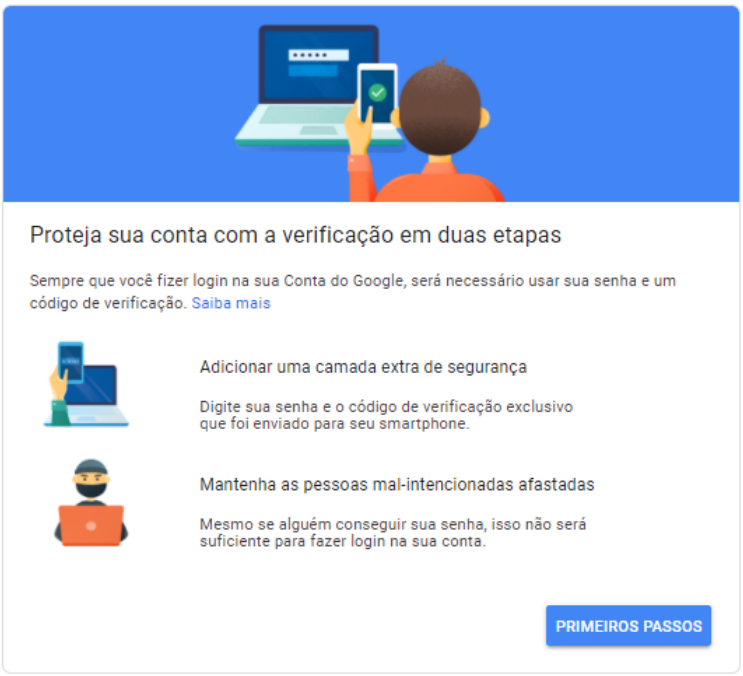
1. Abra sua conta do Google;
2. Clique em gerenciar sua conta;
3. No painel de navegação, selecione Segurança



4. Em “Como fazer login” selecione Verificação em duas etapas



5. Selecione Primeiros passos



6. Siga as próximas etapas exibidas na tela

Criptografia dos dados

Embora os dados em diversos serviços do G Suite sejam criptografados, tanto em trânsito quanto em repouso, é possível criptografar qualquer arquivo antes de enviá-lo para a nuvem. Com a criptografia implementada, mesmo se um atacante conseguir seu disco ou se o conteúdo for propagado pela internet, os dados seriam inúteis sem a chave de descriptografia.

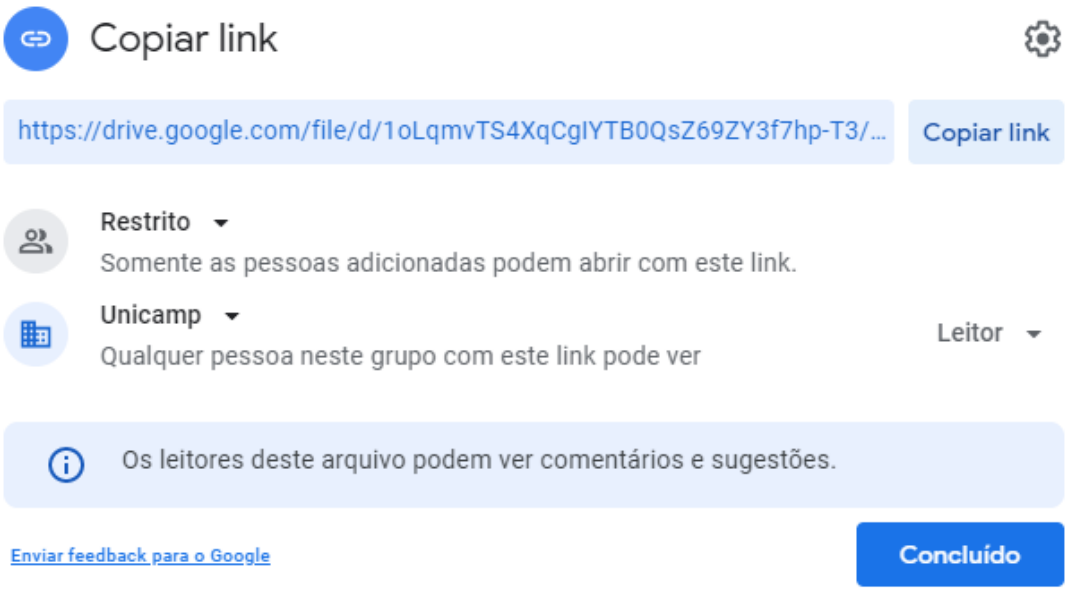
Usuários do Windows 10 Pro tem a opção de criptografar um arquivo sem softwares adicionais. Para isso basta seguir os passos abaixo:

1. Clique com o botão direito do mouse no arquivo ou pasta em questão e selecione “Propriedades”.
2. Selecione o botão Avançado e marque a caixa de seleção “Criptografar o conteúdo para proteger os dados”.
3. Selecione “Ok” para fechar a janela “Atributos Avançados”, selecione “Aplicar” e, em seguida, selecione “Ok”.

Configuração das permissões

Como os arquivos na nuvem pode ser compartilhados e ter diversos colaboradores, é necessário pensar sobre quais tipos de permissões estão sendo concedidas às pessoas com quem se compartilha os arquivos.

É possível compartilhar arquivos e pastas convidado as pessoas através de um link ou e-mail, podendo atribuir as funções de leitor, comentarista ou editor. O leitor pode ver os arquivos, enquanto aquele que tiver permissão de editor pode organizar, adicionar e editar arquivos. Também é possível compartilhar o arquivo apenas para quem tenha o domínio na organização, neste caso na Unicamp, como mostra a figura abaixo:



No exemplo acima, somente as pessoas com o domínio da Unicamp poderão acessar o documento, além disso, somente pessoas adicionadas podem acessá-lo. Ou seja, não basta ter o link e domínio da Unicamp, é necessário também ter sido convidado(a) por um dos colaboradores do arquivo para poder vê-lo, comentá-lo ou editá-lo.

As permissões podem ser editadas posteriormente, portanto, você pode restringir o acesso excluindo o usuário da lista de contas autorizadas a acessar o documento.

Quando uma pasta for compartilhada, todos os arquivos dentro dessa também serão, mas o contrário não se aplica. Caso uma subpasta seja compartilhada, a pasta de origem não será compartilhada automaticamente. Isso também se aplica à arquivos, o usuário pode compartilhar um arquivo de uma pasta sem compartilhar a pasta inteira. Essa função é muito útil, mas é necessário ter sempre atenção para compartilhar o conteúdo necessário.

Antes de compartilhar qualquer arquivo, o usuário deve ter certeza de que este ato não estará em desacordo com os pilares da Lei Geral de Proteção de Dados. Eles consistem na integridade de dados, ou seja, seus arquivos não devem conter informações adulteradas; na confidencialidade, seu arquivo só pode ser compartilhado com pessoas autorizadas; e na disponibilidade, quando necessário, a informação deve estar disponível. Caso esses três requisitos sejam satisfeitos, você poderá compartilhar o conteúdo desejado, lembrando-se sempre das recomendações de compartilhamento no drive.