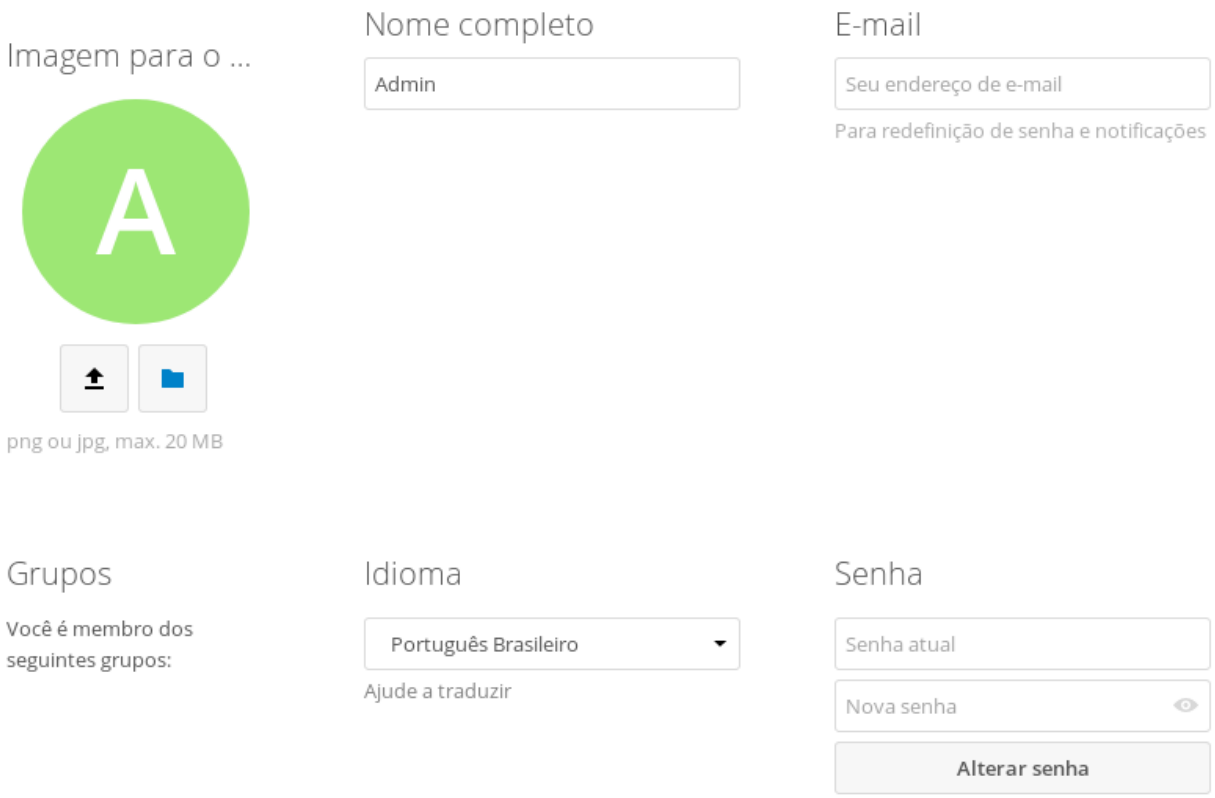
INTRODUÇÃO RÁPIDA AO GIBBERFISH

Olá! Estamos focados em garantir sua privacidade e segurança, mas, para isso, precisamos da sua colaboração. Abaixo, algumas sugestões iniciais.

PERFIL

Se esta é a primeira vez que você entra tire alguns minutos para preencher seu perfil e aproveite para alterar sua frase secreta Clique em ⚙ no canto superior direito e selecione **Pessoal** para editar seu perfil.



FRASES SECRETAS

Uma boa frase secreta é essencial para resguardar seus dados. Nós (e muitos especialistas em segurança) recomendamos o método Diceware para criação de senhas. É o **único procedimento** que consideramos seguro para gerar sua frase secreta. Fácil de seguir, resulta em senhas ultrafortes, capazes de resistir aos ataques mais engenhosos.

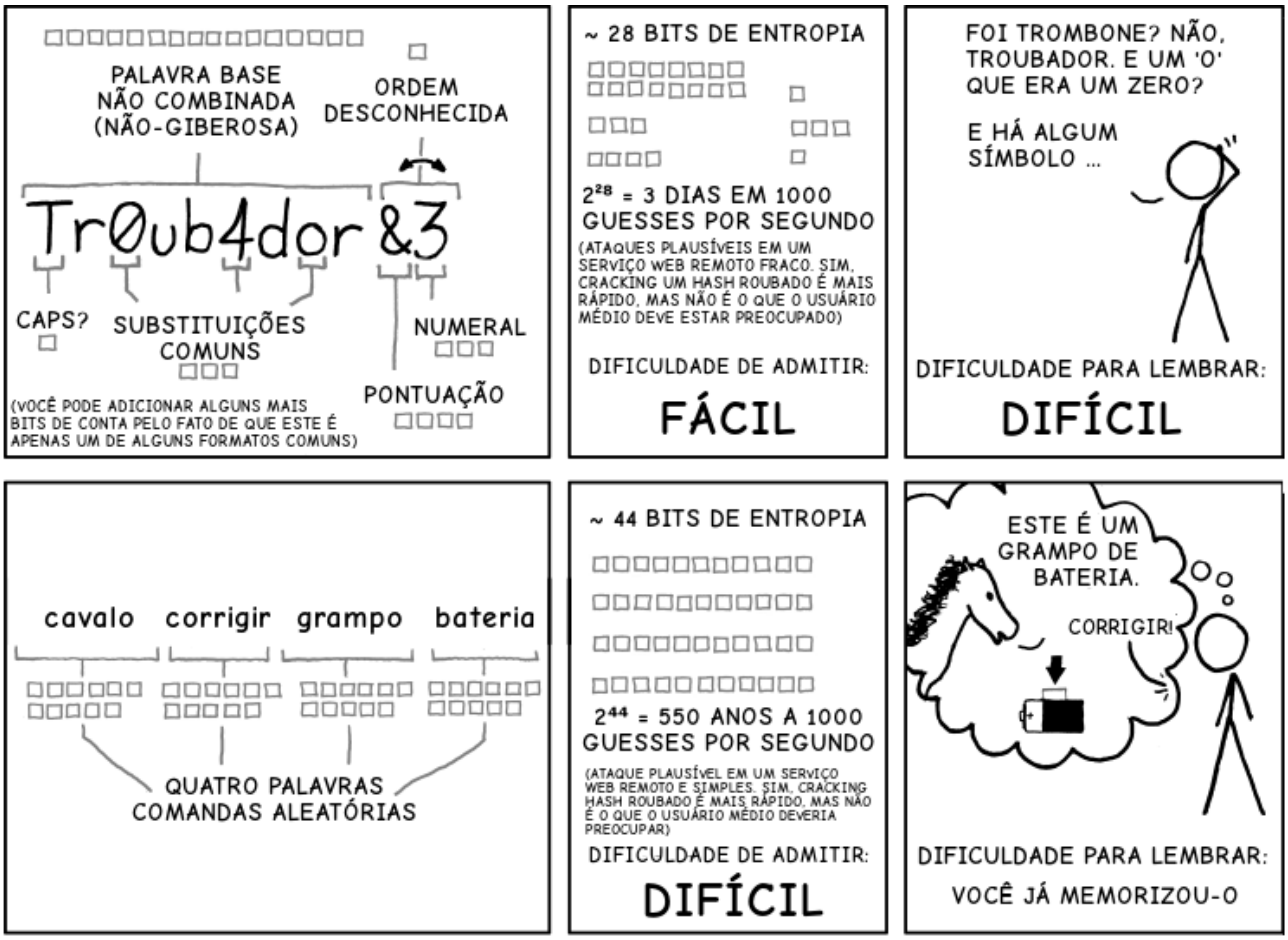


imagem cedida por xkcd.com.

O quadrinho acima explica o conceito do método Diceware segundo o qual uma frase secreta deve ter de fato pelo menos **cinco palavras** para maior segurança.

Nunca registre como sua frase secreta no Gibberfish uma senha que você use em outro lugar.

Crie **sempre** uma senha única para cada serviço conta ou dispositivo que usar.

AUTENTICAÇÃO EM DUAS ETAPAS

Depois de mudar sua frase secreta é extremamente recomendável também habilitar a autenticação em duas etapas 2FA. Para isso será necessário instalar no seu dispositivo móvel um aplicativo que gere um código único de seis dígitos que deverá ser inserido no início de cada sessão. Para invadir sua conta um hacker precisaria conhecer sua frase secreta e ter a posse física do seu dispositivo. Essa combinação aumenta a sua segurança. Como o Gibberfish é parte do ecossistema Nextcloud você pode usar o aplicativo Nextcloud 2FA. Ele oferece FreeOTP disponível para download nas lojas de aplicativos do Android e do iOS.

COFRES DE CHAVES

Se você ainda não tem o hábito é uma boa ideia passar a armazenar suas frases secretas em um cofre de chaves como o KeePass. Esse recurso torna fácil lembrar com segurança de todas as suas frases secretas. O cofre em si terá que ser protegido com uma senha gerada pelo método Diceware. Além disso recomendamos **veementemente** que você habilite criptografia de disco inteiro no dispositivo que armazenará seu cofre.

Esse método garante que você precise lembrar de somente uma frase secreta aquela que abre o seu cofre de chaves.

HIGIENE DIGITAL

Ter boa higiene digital significa usar práticas de segurança robustas consistentemente.

Por robustas queremos dizer procedimentos que tenham sido estabelecidos ou analisados por especialistas em segurança confiáveis. Estes incluem mas não se limitam a a Electronic Frontier Foundation (EFF) o Guardian Project e o projeto Tor.

Falamos de consistente para enfatizar que empregar qualquer prática de segurança intermitentemente é tão ineficaz quanto não usála nunca. Uma vez que tiver desenvolvido um modelo de ameaças e uma estratégia para derrotálas siga a estratégia **sempre** que quiser navegar com privacidade.

AMEAÇAS

Compreender as ameaças que você e seu grupo vão encontrar é um passo importante no estabelecimento de uma estratégia de segurança útil. A ideia é usar apenas as técnicas necessárias para se proteger contra prováveis adversários. Assim, você evita que seu regime de segurança se torne tão cansativo que seja deixado de lado. A administração já deve ter criado um Modelo de Ameaças que descreva os desafios de segurança que você e seu grupo podem esperar. Se tiver alguma dúvida, entre em contato com ela e pergunte.

Cada usuário deve compreender o Modelo de Ameaças do grupo e usar consistentemente mesmas as práticas de segurança.

Para mais informações sobre Modelos de Ameaças, consulte esta excelente cartilha produzida pela EFF.

COMUNICAÇÕES EXISTENTES

É provável que você esteja acrescentando o Gibberfish a uma miríade de serviços e contas associados às suas atividades online. Esses serviços e contas podem já ter sido comprometidos. Por isso recomendamos o uso de contas recémcriadas para toda atividade que envolva seu servidor Gibberfish ou o conteúdo armazenado nele.

Sabemos que isso não é sempre conveniente ou apropriado para todos. Se for o seu caso reforce a segurança de qualquer conta ou serviço que pretenda usar para atividades particulares. Mude suas senhas para barrar o acesso de quem possa têlas conseguido sem o seu conhecimento. Sempre que possível habilite a autenticação em duas etapas. Verifique se há atualizações de software disponíveis para todos os seus dispositivos inclusive seu smartphone e instaleas.

TOR

O Tor é o melhor caminho para proteger sua privacidade on-line, e é por isso que o utilizamos para implantar seu servidor Gibberfish. Embora o nome se refira especificamente ao projeto The Onion Router, o Tor passou a englobar uma série de produtos e serviços gratuitos que as pessoas podem usar para resguardar suas atividades on-line. Nossa recomendação é que todos os internautas usem o Tor Browser para se manter anônimos.

Por favor leia atentamente a documentação e o FAQ a respeito da navegação na rede Tor fornecidos pelo próprio projeto. Eles contêm recomendações importantes sobre privacidade. Vale ressaltar que usar o Tor Browser não garante que todas as suas atividades online são anônimas.

O Tor oferece outras ferramentas gratuitas para ajudar a reforçar sua segurança. Ao avaliar seu Modelo de Ameaças você talvez perceba vantagens em utilizar bridges e o Linux Tails. As bridges ou pontes são servidores que permitem acesso ao Tor em países onde ele é bloqueado. Já o Linux Tails é um sistema operacional completo contando com os programas mais comuns que pode ser posto para funcionar a partir de um pen drive. É extremamente seguro.

Descubra esses e outros serviços Tor em:

https://www.torproject.org/projects/projects.html.en

CHAMADAS DE VÍDEO

Com o Talk da Nextcloud é possível iniciar e participar de chamadas de vídeo usando seu navegador. Para melhor desempenho em dispositivos móveis recomendamos a instalação do aplicativo Nextcloud Talk disponível no iTunes, Google Play e F-Droid.

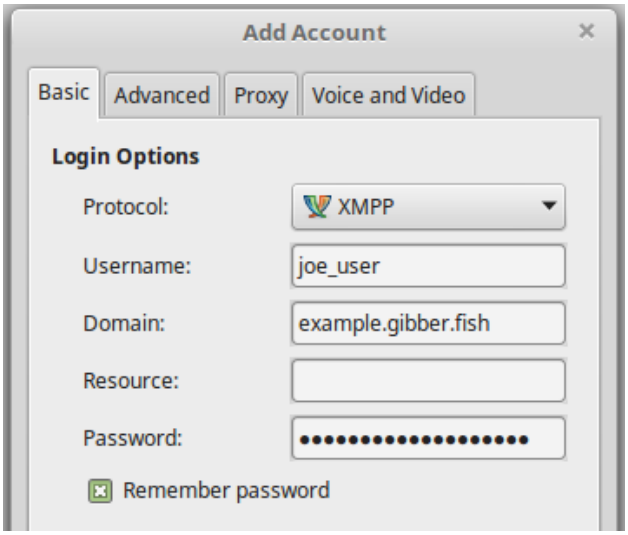
BATE-PAPO

O sistema de batepapo funciona a partir do protocolo XMPP padrão que possibilita a comunicação não apenas com outros usuários do Gibberfish mas com qualquer pessoa que use um servidor XMPP. Seu endereço XMPP é <your username>@<your gibberfish server>. Por exemplo,

joe_user@example.gibber.fish

Quando você se logar pela primeira vez sua lista de batepapo no lado direito da tela estará vazia. Você pode **adicionar contatos** pelo menu na parte inferior. Apenas comece a digitar e uma pesquisa por pessoas cadastradas no servidor será feita automaticamente. Você também pode buscar usuários externos pelos respectivos endereços XMPP.

Para manter sua conexão ao Gibberfish após encerrar a sessão você pode se conectar diretamente ao servidor usando um cliente compatível com XMPP como Adium Pidgin ou um dos muitos aplicativos móveis disponíveis.



O servidor de batepapo é acessível como um serviço onion do Tor pela porta 5222. Peça o endereço Tor do seu servidor à administração.

No entanto não há garantia de privacidade em batepapos com usuários externos ao servidor a não ser que você **e** seus contatos usem um plugin para criptografia de ponta a ponta como o OTR. A maioria dos clientes de batepapo oferece criptografia de ponta a ponta além de fornecer manuais para ajudar você a compreender o recurso e habilitálo.

CLIENTES PARA DESKTOP E DISPOSITIVO MÓVEL

O Gibberfish funciona com os clientes da Nextcloud para desktop e dispositivo móvel permitindo que você sincronize seus arquivos automaticamente com o servidor. Como precaução esse recurso é desabilitado por padrão. Para usar esses clientes peça à Administração para alterar as regras de acesso aos arquivos. Se você quiser sincronizar os arquivos localmente certifiquese de ativar a criptografia de disco inteiro para o seu dispositivo. Assim seus arquivos são protegidos caso seu aparelho seja perdido roubado ou hackeado.

É difícil mas possível que seus dados sejam interceptados por atacantes engenhosos quando em trânsito. Por essa razão **não recomendamos** que você sincronize seus dados sem considerar cuidadosamente seu Modelo de Ameaças e suas práticas de segurança.

LEITURA ADICIONAL

Para informações mais detalhadas acerca dos principais recursos consulte o Manual do Usuário Nextcloud localizado na sua pasta inicial no Gibberfish.

Os administradores devem também se familiarizar com o Manual do Admin.

Por fim, sugerimos que você se inscreva no blog do Gibberfish, no aplicativo de notícias, para ficar por dentro de anúncios importantes e acompanhar nossa garantia do canário.

OBSERVAÇÕES FINAIS

Esperamos que você goste do Gibberfish. Trabalhamos duro para tornálo uma plataforma segura e fácil de usar assim como trabalharam as muitas pessoas que contribuiram independentemente para os vários projetos de código aberto que integramos ao nosso serviço. Agradecemos especialmente ao pessoal da Nextcloud sem a qual nossa plataforma não seria possível.

Dependemos de doações para sobreviver. Se você puder por favor considere contribuir com qualquer quantia em https//gibberfish.org/pt/donate. Seremos imensamente gratos!

Por segurança respondemos apenas a solicitações feitas pela pessoa registrada como administradora. Se você tiver dúvidas relativas ao serviço por favor entre em contato com ela.