PARA IR MAIS LONGE

- Documentação oficial do Tails (em várias línguas): tails.net/doc
- Instalação: tails.net/install
- Ajuda do Tor Browser: support.torproject.org
- Pontes Tor: bridges.torproject.org
- Ver se o Tor está bloqueado na tua rede: explorer.ooni.org

SOBRE ESTA ZINE

Inspirado livremente em guias de segurança digital de outros movimentos. Texto original, escrito para um movimento não-violento pela habitação e verificado na documentação oficial do Tails e do Tor Project. Informação revista a 25 de Outubro de 2026: o software muda depressa, confirma sempre no site oficial.

Série Prevenção Anti-Censura: n.º 1 O Telemóvel é um Bufo, n.º 2 Mensagens Encriptadas, n.º 3 GrapheneOS.

Defender a privacidade é defender o direito a organizar-nos, a falar e a ter casa.

Copia, imprime, partilha. Sem fins lucrativos. Assembleia Popular / Acampada, Lisboa.

ACAMPADA
ASSEMBLEIA POPULAR

LISBOA · OUT. 2026



SÉRIE PREVENÇÃO ANTI-CENSURA
N.º 4 DE 4

TAILS 101

Computador amnésico e anónimo para quem se organiza

LÊ · COPIA · PARTILHA

PREVENÇÃO ANTI-CENSURA

O QUE É O TAILS?

O Tails é um sistema operativo, como o Windows ou o macOS, mas que vive numa pen USB. Ligas a pen, arrancas o computador a partir dela e trabalhas num ambiente limpo, sem tocar no disco do computador.

Três ideias para guardar:

Amnésico. Tudo corre na memória RAM. Quando desligas, apaga-se: histórico, ficheiros abertos, rascunhos. Só fica o que decidires guardar.

Anónimo. Tudo o que vai para a internet passa pela rede Tor. Os sites não vêem o teu endereço IP e a operadora não vê que sites visitas. Se um programa tentar ligar-se directamente, o Tails bloqueia.

Pronto a usar. Traz navegador, editor de texto, gestor de palavras-passe, ferramenta para limpar metadados e mais.

É software livre e gratuito. Desde 2024 é desenvolvido dentro do Tor Project, a mesma organização que faz o Tor Browser.

Não é magia. É uma ferramenta que reduz rastos, se for bem usada.

LIMITES (LÊ ISTO)

O Tails reduz muito o risco, mas não faz milagres.

- **Keyloggers físicos:** um pequeno aparelho entre o teclado e o computador regista o que escreves, mesmo no Tails. Usa o teclado no ecrã quando desconfiares e cola as palavras-passe a partir do KeePassXC.
- **Câmaras e olhares:** quem vê o teu ecrã ou as tuas mãos vê tudo. Escolhe bem o lugar.
- **Firmware comprometido:** nenhum sistema operativo protege contra um computador alterado a esse nível.
- **Erros humanos:** entrar numa conta com o teu nome desfaz o anonimato.
- **Tor visível:** a rede local sabe que usas Tor, a não ser que uses uma ponte. Redes de faculdades, bibliotecas ou empresas podem bloqueá-lo.
- **Correlação:** quem observe ao mesmo tempo a tua ligação e o destino pode cruzar padrões. Para trabalho delicado, evita redes ligadas ao teu nome.
- **Apagar não é apagar:** ficheiros apagados de uma pen comum recuperam-se. Não guardes nada sensível sem cifra.

BONS HÁBITOS

Uma sessão, uma identidade. Não mistures o email pessoal com o trabalho do colectivo na mesma sessão. Para trocar de "papel", desliga e volta a arrancar o Tails. O botão "New Identity" do navegador não chega.

Actualiza sempre. Sai uma versão nova mais ou menos todos os meses, muitas vezes com correcções de segurança urgentes. Quando o Tails avisar, aceita.

Desliga quando sais. Um portátil com sessão aberta numa assembleia é um caderno aberto. Bloqueia o ecrã ou desliga.

Usa a pen só para o Tails. Não a ligues a outros sistemas para passar ficheiros.

Atenção ao que escreves. Estilo de escrita, horários, pormenores do bairro: tudo isto identifica, mesmo pelo Tor.

Combina com outras protecções. O Tails protege o computador; não protege um grupo de Signal mal gerido nem uma conversa ao telefone (ver zines n.º 1 e n.º 2).

Aprende devagar. Começa por coisas simples: ler notícias, escrever um texto. A segurança faz-se com prática, em conjunto.

PARA QUE NOS SERVE?

Organizar pela habitação toca em informação sensível. O Tails faz sentido quando:

- **Redigimos comunicados** da assembleia e não queremos o texto colado ao portátil pessoal de alguém.
- **Pesquisamos fundos, empresas e partes senhorias** em registos públicos, notícias e bases de dados. Pelo Tor, essas pesquisas não ficam ligadas a nós.
- **Recebemos testemunhos** de pessoas inquilinas, de vizinhança em risco de despejo, de quem tem estatuto migratório frágil. Proteger fontes é proteger pessoas.
- **Usamos um computador emprestado** ou partilhado e não queremos deixar lá nada.

E quando não vale a pena? Para o email pessoal, as redes sociais com o teu nome, o homebanking. Aí o anonimato não faz sentido, e misturar isso com trabalho sensível na mesma sessão estraga o resto.

Pergunta-chave antes de começar: **o que estou a proteger, de quem, e o que acontece se falhar?** A resposta decide quanto cuidado é preciso.

O QUE PRECISAS

Uma pen USB de 8 GB ou mais. Vai ser apagada por inteiro. Melhor uma nova, só para o Tails, de preferência USB 3.0 ou mais recente (é bem mais rápida).

UM COMPUTADOR COMPATÍVEL

- processador de 64 bits (Intel ou AMD);
- pelo menos 3 GB de RAM (com menos pode arrancar, mas fica instável);
- capaz de arrancar a partir de USB.

Não funciona em Macs com chip Apple (M1, M2 e seguintes), em computadores com processador ARM, nem em telemóveis ou tablets. Alguns Macs antigos com Intel funcionam.

Um portátil é melhor que um computador fixo: é mais fácil perceber se alguém mexeu no equipamento e mais difícil esconder lá um aparelho espião.

Cerca de uma hora e uma ligação razoável (o download tem perto de 2 GB).

Um telemóvel ou papel impresso com as instruções, porque o computador vai reiniciar a meio.

Antes de comprar, vê no site os problemas conhecidos com certos modelos.

FERRAMENTAS DE BOLSO

KEEPASSXC: GESTOR DE PALAVRAS-PASSE

Guarda todas as palavras-passe num ficheiro cifrado, aberto com uma só frase-passe. Grava a base na Pasta Persistente. Usa o gerador para criar palavras-passe longas e diferentes para cada conta. Uma base por projecto ou colectivo: assim só fica aberto o que estás a usar.

METADATA CLEANER: LIMPAR METADADOS

Fotos, PDFs e documentos levam informação escondida: autoria, data, modelo do telemóvel, por vezes localização. Antes de publicar uma foto ou um comunicado, passa o ficheiro pelo Metadata Cleaner. Atenção: em formatos complexos (um .docx com imagens dentro) não apaga tudo. Limpa as imagens antes de as meter no documento e, sempre que der, publica em texto simples.

ONIONSHARE: PARTILHAR SEM NUVEM

Partilhar ficheiros, receber ficheiros (útil para quem quer enviar um testemunho sem se expor), abrir uma pequena página ou uma sala de conversa, tudo através de um endereço .onion. Quem recebe usa o Tor Browser. Quando fechas o OnionShare, o endereço morre.

ARMAZENAMENTO PERSISTENTE

Por defeito o Tails esquece tudo. Às vezes precisamos de guardar alguma coisa entre sessões: rascunhos, a base de palavras-passe, a palavra do Wi-Fi da sede.

O **Armazenamento Persistente** é uma parte cifrada da própria pen, protegida por uma frase-passe. Cria-se no ecrã de boas-vindas ou em **Apps ▸ Tails ▸ Persistent Storage**. Depois escolhes o que guardar:

- **Pasta Persistente** (documentos);
- ligações de rede, ponte Tor, marcadores do navegador;
- chaves GnuPG e SSH;
- **Software Adicional** (por exemplo o Thunderbird, que já não vem de base).

Cuidados:

- **Frase-passe longa:** 5 a 7 palavras ao acaso. Se a esqueceres, não há recuperação.
- **Não está escondido.** Quem tiver a pen percebe que existe uma parte cifrada.
- **Guarda só o necessário.** Menos lá dentro, menos se perde.
- **Faz cópias de segurança.** As pens avariam. O Tails Cloner copia tudo para uma segunda pen.

INSTALAR (VISÃO GERAL)

Há dois caminhos.

1. A PARTIR DO SITE OFICIAL: TAILS.NET

O site tem um assistente para Windows, macOS e Linux. Os passos gerais:

1. Descarregar a imagem do Tails para o computador (não para a pen).
2. **Verificar o download.** O site explica como. Garante que ninguém trocou o ficheiro pelo caminho. Não saltes este passo.
3. Gravar a imagem na pen com o programa indicado. Nota: o balenaEtcher, sugerido no site, envia alguns dados à empresa que o faz; o site indica alternativas.
4. Reiniciar o computador a partir da pen.

2. CLONAR DE OUTRA PESSOA

Se alguém de confiança já tem Tails, abre **Apps ▸ Tails ▸ Tails Cloner** e copia o sistema para a tua pen em poucos minutos. É prático em oficinas colectivas. O risco: se a pen de origem estiver comprometida, o problema passa para a tua.

Instala sempre a partir de um computador em que confies.

PRIMEIRO ARRANQUE

1. **Com o computador desligado**, liga a pen.
2. Liga o computador e abre o menu de arranque. A tecla muda de marca para marca (F12, Esc, F9...). Num Mac Intel, mantém a tecla Option carregada.
3. Escolhe a pen. Aparece um ecrã com a opção "Tails", que arranca sozinha em poucos segundos.

Surge o **ecrã de boas-vindas**:

- **Língua e teclado:** escolhe Português e o teu teclado. Podes guardar esta escolha na pen.
- **Armazenamento Persistente:** se já o criaste, escreve aqui a frase-passe.
- **Definições adicionais (botão +):**
- *Palavra-passe de administração:* só se precisares de instalar algo. Vale só para essa sessão. Sem ela, o sistema fica mais protegido.
- *Anonimização do endereço MAC:* activa por defeito. Esconde a identidade da placa de rede na rede local. Mantém ligada, salvo se a rede recusar a ligação.
- *Navegador inseguro:* só para redes com página de login (cafés, bibliotecas). Se não precisas, desactiva.

Carrega em **Start Tails**.

LIGAR AO TOR E NAVEGAR

Liga-te ao Wi-Fi. Abre-se o assistente **Tor Connection** com duas opções:

- **Ligar automaticamente:** a escolha certa na maior parte dos casos.
- **Esconder que estou a usar Tor:** útil se a rede bloqueia o Tor ou se não queres que a rede saiba que o usas. Precisas de uma **ponte** (bridge), que podes pedir em bridges.torproject.org a partir de outra rede. Guarda-a com antecedência.

O ícone da cebola no canto superior indica se estás ligade ao Tor.

No **Tor Browser**:

- **Sobe o nível de segurança para "Safest"** (ícone do escudo). Desliga o JavaScript em todos os sites. Algumas páginas ficam partidas, mas a maior parte dos ataques ao navegador deixa de funcionar.
- **Confirma o cadeado (HTTPS)** antes de escrever o que quer que seja.
- **Endereços .onion** só abrem no Tor Browser e nunca saem da rede Tor.
- **Downloads e envios** passam pela pasta "Tor Browser".

Site bloqueia o Tor? Experimenta "New Tor circuit for this site".