TEM BOI NA LINHA?

guia prático de combate à vigilância na internet

DANDO NOME AOS BOIS

Boi na Linha: intrometidx, intrusx;
metáfora popular usada quando há algum/a intrusx no meio de uma comunicação.

Para os movimentos sociais, a comunicação rápida e segura entre membros de um coletivo, entre coletivos, ou entre ativistas independentes é fundamental tanto para o planejamento e a eficácia das ações, como também para o fortalecimento do próprio movimento de resistência.

Na era analógica, espionar as comunicações de um indivíduo ou grupo e apreender documentos sensíveis, eram ações bastante comuns, apesar de serem dirigidas a alvos específicos e um tanto difíceis de serem camufladas. Com a internet, essa prática se tornou mais discreta, silenciosa e ainda mais comum, sendo utilizada em larga escala, para a espionagem em massa, e por motivos que ultrapassam os estritamente políticos.

A cada dia fica mais evidente que grande parte das atividades na internet estão sujeitas à vigilância, e que há, quase sempre, bois na linha: algo ou alguém coletando seus dados privados, espiando suas conversas e e-mails, ou registrando os sites acessados por você. Esses bois não são inofensivos, e podem inviabilizar as ações de um grupo, expor os ativistas, e favorecer a repressão.

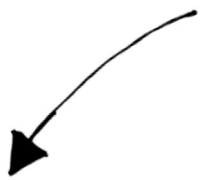
MAS CALMA, É POSSÍVEL COMBATER A VIGILÂNCIA E MANDAR OS BOIS PASTAREM!
Felizmente, certas propriedades físicas do nosso mundo fazem com que cifrar informações seja mais fácil que decifrá-las. A mudança de alguns hábitos e a utilização de criptografia e de softwares livres e de código aberto, podem proporcionar um bom nível de privacidade, ainda que não garanta uma segurança total.

"TEM BOI NA LINHA?" É UM GUIA PRÁTICO DE COMBATE À VIGILÂNCIA NO ÂMBITO DOS MOVIMENTOS SOCIAIS, E É DESTINADO A GRUPOS DE ATIVISTAS, JORNALISTAS, MIDIALIVRISTAS OU A QUALQUER PESSOA QUE PRECISE OU DESEJE SE PROTEGER, E PROTEGER SUAS COMUNICAÇÕES E ARQUIVOS, DA VIGILÂNCIA DO ESTADO E DE INSTITUIÇÕES PRIVADAS.

AMEAÇAS E RISCOS AO NAVEGAR NA INTERNET

Quando você envia um e-mail para alguém, este percorre um caminho cheio de buracos que podem afetar a sua privacidade. Aqui nesse desenho mostramos o percurso e algumas brechas onde o boi (interceptação) aparece.

O **boi** pode estar interceptando os cabos de tráfego ou acessando os registros de acesso no provedor de internet. Ou seja além de ver as informações dos seus dados, ele pode saber que sites você está acessando e quando aconteceram esse acessos.

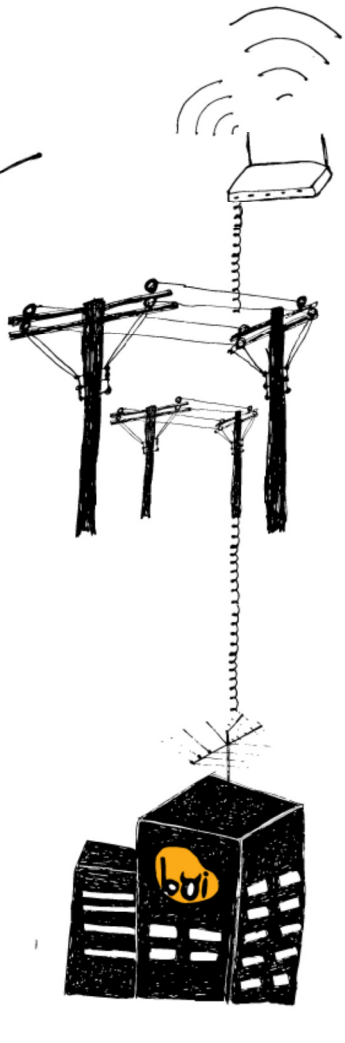


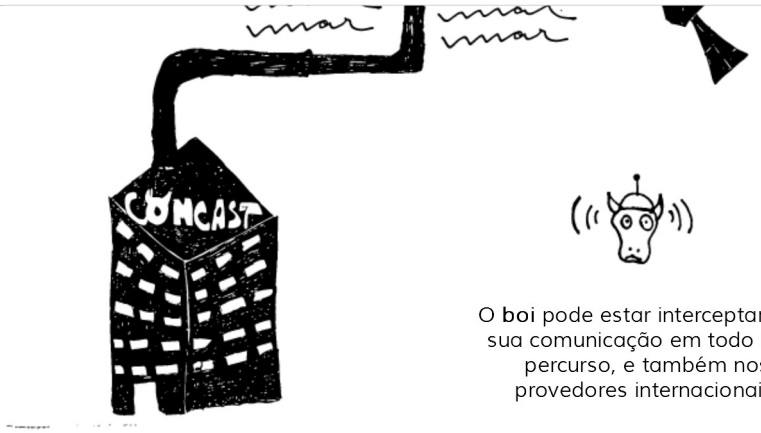
O primeiro passo da informação que sai

que encaminham o email para os servidores.

O **boi** pode estar interceptando a sua comunicação sem fio e capturando os dados que você acabou de enviar, por exemplo a mensagem do seu email. Essa invasão se dá através de uma técnica que se chama sniffing.

O roteador da sua casa manda a informação para os provedores de acesso da internet através de cabos.





O **boi** pode estar interceptando a sua comunicação em todo esse percurso, e também nos provedores internacionais.

MANDE O BOI PASTAR!

SAIBA COMO SE DEFENDER

SENHAS FORTES

Ter uma senha forte é muito importante, afinal ela é a chave para entrar nos seus dados privados. Algumas práticas simples podem ajudar você a escolher, manter e guardar suas senhas com segurança.

1

Use senhas longas.

3

Não use a mesma senha para serviços diferentes.

5

Não marque "guardar a senha" no navegador de computadores

Escolha senhas com maiúsculas, minúsculas, números e símbolos especiais.

Mude suas senhas periodicamente. Uma boa indicação seria de 3 em 3 meses.

Para guardar suas senhas utilize um chaveiro de senhas, como Keepass.

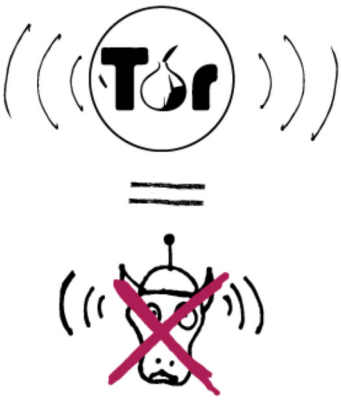
Teste sua senha

NAVEGAÇÃO ANÔNIMA

Se o boi está na linha, ele só vai ouvir ruído, e nem vai saber de onde veio.

Quando navegamos na internet basicamente transferimos pacotes de informação com dados, endereço de rementente e destinatário. Chamamos o endereço de remetente do nosso pacote de IP. Ele localiza geograficamente onde estamos. Ou seja, se olhamos os registros de IP de acesso de um site, podemos identificar de onde vêm esses acessos.

Os provedores de Internet também podem identificar qual cliente usou um IP em determinado horário. Para navegar privativamente é necessário mascarar o IP, que identifica nossa localização. Isto quer dizer que ao mascarar o IP, os pacotes de informações serão enviados com outro endereço de envio, ou seja, outro IP será identificado como seu, com diferente local de acesso. Assim ninguém saberá de onde vem seu acesso.



TOR

O Tor é uma rede global descentralizada. Cada participante, quando vai mandar um pacote pra Internet, repassa primeiro por três outros participantes, e o pacote finalmente sai pra Internet pública pelo último deles. Isso é feito de uma forma que garante matematicamente que quem recebe o pacote não saiba de onde ele se originou, e que seu provedor não saiba o que você está enviando ou acessando.

A forma mais fácil e segura de usar essa rede pra acessar a Web é através do Tor Browser Bundle. Além de ligar o Tor automaticamente, esse navegador toma uma série de outras medidas pra tornar sua navegação segura e anônima.

Download TOR Browser Bundle

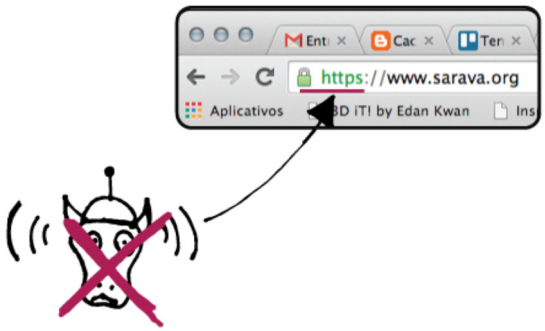
NAVEGAÇÃO CRIPTOGRAFADA

Mesmo quando conseguimos mascarar o IP de procedência (onde estamos), as nossas informações ainda podem ser interceptadas no percurso até o destino final. Se o boi aparece na linha nesses casos ele pode escutar, ler e ver o que você está comunicando.

HTTPS

Para que nossas informações naveguem de forma criptografada, ou seja ilegível para quem não deve ter acesso, é necessário usar endereços de sites que contenham certificados de segurança que garantem que a informação trafegada entre a pessoa que acessa e o destino final estejam seguras.

Esses certificados são reconhecidos pelo protocolo HTTPS que está localizado na barra de endereço do seu navegador (ex: https://meusite.com). Alguns sites oferecem esses serviços, outros tem o certificado mas não usam como obrigatório e outros infelizmente não se preocuparam com isso ainda.



HTTPS EVERYWHERE

Para garantir que seu navegador tente sempre acessar os sites através do protocolo seguro existem alguns adicionais de navegador como o HTTPS Everywhere. (O Tor Browser Bundle já vem com ele instalado)

Instalar HTTPS Everywhere

NÃO DEIXE QUE O BOI LEIA SEUS E-MAILS

Quando nos comunicamos atráves de emails, podemos ter nossa comunicação interceptada em diversos momentos no percurso da mensagem entre o remetente e destinário, ou mesmo no seu destino final. Para garantir nossa privacidade é importante usar da criptografia nas mensagens dos e-mails ou usar serviços de e-mail seguro.

GPG

Recomendamos usar ferramentas como GPG, usadas em conjunto com leitores de e-mail (Thunderbird, Mail, etc).

Para usar a criptografia você deve primeiramente instalar o GPG no seu computador e depois criar um par de chaves (pública e privada) e trocar chaves públicas com o destinatário (que também deve ter feito o mesmo processo).

Para saber mais detalhes sobre como usar as ferramentas consulte o site Security in a Box (em breve em português).

Download GPG Tools (Mac OS X)
Download GPG4USB (Windows)
Download GnuPG (Linux)

SERVIÇOS DE E-MAIL SEGURO

Recomendamos alguns serviços de e-mail que possuem uma política transparente e de respeito a privacidade dxs usuárixs. Usando esses serviços o boi vai ter mais trabalho para conseguir ler as suas mensagens.

Riseup
Aktivix
Autistici

CHAT SEM BOIADA

As nossas conversas de chat também podem ser interceptadas através de uma invasão nos nossos canais de comunicação. Além disso nosso histórico de conversas é registrado deixando de ser privado caso haja requerimento para acessá-lo.

chat, recomendamos o uso de ferramentas como Jitsi. Através desse software você pode conectar suas contas de Gmail e Facebook usando da criptografia para conversar com seus contatos.
É necessário que seus contatos também utilizem a mesma ferramenta para que vocês consigam fechar "seus cadeados".

Download Jitsi

PLATAFORMAS SEGURAS PARA CRIAÇÃO DE BLOGS E SITES

O uso de plataformas seguras garante que suas ações não serão monitoradas, seus dados não serão disponibilizados para grupos com interesses escusos, além de permitir, em alguns casos, que tudo seja feito de forma anônima.

BLOGS

Os serviços abaixo oferecem hospedagem para blogs baseados na plataforma WordPress.

- Milharal
- Network 23 (em inglês)
- Noblogs

HOSPEDAGEM DE SITES

O Autistici é um coletivo italiano formado por ativistas. Além de hospedagem de sites, elxs também oferecem e-mails, listas, newsletters, fóruns e serviços de mensagens instantâneas. Também são responsáveis pelo Noblogs.

- Autistici

APAGAR VESTÍGIOS

IMAGENS

O armazenamento de imagens, tais como fotografia, vídeo, gif e dentre outros, contém informações adicionais que mostram, por exemplo, data de criação, modificações, tipo de câmera utilizada, ISO, lente, programa de edição e várias outras informações que podem ser utilizadas para identificar pessoas.
Entenda como funciona aqui.

Para apagar os vestígios contidos nesses arquivos específicos, recomendamos os programas listados abaixo:

Download Steel bytes (Windows)
Download Image MetaData Stripper (MAC OS)
Download MAT (Linux)

ARQUIVOS

Alguns arquivos podem continuar gravados no seu computador mesmo quando você os deleta.
Através de programas especializados, eles podem ser restaurados, parcial ou totalmente.
Para apagar esses traços sensíveis existem algumas ferramentas como o Eraser.

Download Eraser

ou de investigação. Para aumentar sua privacidade e segurança nesses sites, além das ferramentas já mencionadas para fugir do boi, você pode tomar algumas precauções para diminuir os riscos de coleta de informações que você considere importantes e privadas.

DICAS

➔ Não utilizar o perfil pessoal para articular ações, criar eventos, publicar informações sensíveis, trocar ideias e documentos ou fazer qualquer movimento (mesmo via mensagens privadas) que possa ser usado contra você.

➔ Não utilizar o perfil pessoal para administrar páginas ativistas no Facebook.

➔ Usar o Tor sempre que acessar redes sociais para ações ativistas.

VOCÊ SABIA?

Em 2013, o STJ (Superior Tribunal de Justiça) do Brasil determinou que o Google Brasil quebrasse o sigilo de comunicações por e-mail de usuários investigados em até dez dias. Caso descumprisse a ordem, a empresa teria de pagar multa diária de R$ 50 mil. Esta é uma ação legal, garantida pelo MLAT – Tratado de Assistência Legal Mútua. Por meio de um MLAT, um governo estrangeiro pode pedir ajuda ao governo dos EUA para obter evidências de entidades nos EUA, incluindo empresas, como o Google e o Facebook. Se o governo dos EUA aprovar a solicitação, o Google ou Facebook deve responder a ele".

Saiba mais sobre o MLAT

COMO SE PROTEGER AO USAR O CELULAR

Para criptografar informações transmitidas por dispositivos móveis como celular, há aplicativos que facilitam sua privacidade e segurança na troca de mensagens.

MENSAGENS DE TEXTO SEM BOIADA

Recomendamos o Textsecure para Android, que usa os contatos SMS do telefone para mandar mensagens sem custos com a operadora e permite conversas em grupo.
Para iPhone, existe o aplicativo Chat Secure, que usa seus contatos do Facebook, Gmail ou Jabber para conversas criptografadas.

Download Textsecure (Android)
Download Chat Secure (iPhone)

CONVERSAS POR VOZ SEM GRAMPO

A Legislação Brasileira proíbe a instalação de grampos em linhas telefônicas de terceiros sem ordem Judicial, masss... Sabemos que o boi pode aparecer na linha quando menos se espera, pois não é difícil adquirir aparelhos de interceptação ou mesmo grampear o seu telefone a distância. Para mandar o boi dormir, indicamos os aplicativos Ostel e Redphone. Eles funcionam por VOIP, ou seja, ligações telefônicas feitas via internet.

Download Ostel (Android, iPhone, Blackberry)
Download RedPhone (Android)

GLOSSÁRIO

Certificado de segurança: um arquivo que um site te dá, e que seu navegador (ou outro software) pode usar pra conferir que o site é legítimo frente a uma Autoridade Certificadora. A infraestrutura da internet permite que alguém no meio da conexão finja ser um site (do banco ou de e-mail, por exemplo) e capture suas senhas e informações. A presença de um certificado tira essa insegurança.

Chave: uma grande sequência de bits aleatórios usado pra criptografar (embaralhar) uma mensagem ou arquivo de forma que só quem tenha a mesma chave (ou a chave secreta, dependendo do esquema de criptografia) possa ver a mensagem original.

Chaveiro de senhas: um programa pra guardar todas as suas senhas, protegidas com uma única senha (bem forte!). Feito pra você não ter que lembrar várias senhas diferentes. Vem com um gerador de senhas grandes e aleatórias.

Criptografia: uma técnica matemática pra "embaralhar" uma mensagem ou arquivo e torná-lo ilegível, podendo ser lida somente por quem tem a chave certa.

Dados: qualquer tipo de informação que um computador pode guardar — texto, endereços IP, horários, destinatários e remetentes, música, imagens, vídeos...

IP: um código numérico que identifica um dispositivo em uma rede de computadores. No caso da Internet, um endereço IP identifica a localização de uma pessoa — a lan house, telecentro, residência, aeroporto, etc, de onde está partindo uma conexão.

Metadados ou metainformação: são dados que não são exatamente o conteúdo de uma mensagem ou obra, e sim informações sobre esse conteúdo. Pra um e-mail, por exemplo, os metadados são os endereços IP e de e-mail do destinatário e remetente, o assunto e o horário de envio da mensagem. Um arquivo de imagem pode conter em seus metadados a câmera utilizada, a abertura da lente, as coordenadas geográficas da foto (via GPS). Um arquivo do Microsoft Word pode guardar informações sobre o computador e o usuário usados pra escrevê-lo.

Protocolo HTTPS: camada adicional de segurança que permite que os dados sejam transmitidos por meio de uma conexão criptografada até o site de destino. Além disso, o site pode emitir um certificado de segurança pra provar que ele é quem diz ser.

Roteador: é um aparelho que encaminha mensagens e informações através da Internet. Quando se acessa ou site ou envia uma mensagem atraŭes da Internet, ela é encaminhada de roteador em roteador até chegar ao destino. Fazendo uma analogia com o funcionamento dos Correios, um roteador é uma das agências pelas quais uma carta ou encomenda passa até chegar ao destinatário.

Registro de acesso: são os registros guardados por um site sobre quem se conectou a ele e quais páginas foram acessadas. Ao se analisar um registro de acesso, é possível determinar que um determinado endereço IP ou usuário acessou uma página ou fez uma determinada ação dentro de um aplicativo. O endereço de IP ou nome de usuário pode então ser usado pra identificar um indivíduo.

Sniffing: é um grampo digital. Um sniffer "fareja" os impulsos elétricos do cabo de rede ou as ondas de rádio wifi, e consegue ver e gravar todos os dados que passam pela rede, que normalmente seriam destinados a outras pessoas. Se o alvo não usa algum tipo de criptografia pra se comunicar e acessar a web, é muito fácil usar uma ferramenta desse tipo pra gravar as páginas acessadas, conversas e senhas usadas.

OUTROS MATERIAIS

Este é apenas um guia básico de combate à vigilância na internet.
Não confie sua vida a ele, continue pesquisando.

OUTROS GUIAS E MANUAIS

Manual de Segurança do Saravá
Security in a Box (em inglês)
Cultura de Segurança – um manual para ativistas
Tech tools for activism (em inglês)
Como combater a vigilância online

SITES E BLOGS

Artigo 19
Escola de Ativismo
Gus
Oficina Antivigilância
Saravá
Tactical Technology Collective
The Occupied Times
Surveillance Self-Defense

• Política de Privacidade ^ Top

Este projeto foi selecionado no Contralab - Laboratório tático contra repressão, da NUVEM - Estação Rural de Arte e Tecnologia.
Realizado por CMI-Rio - Centro de Mídia Independente Rio de Janeiro e gaivotas.