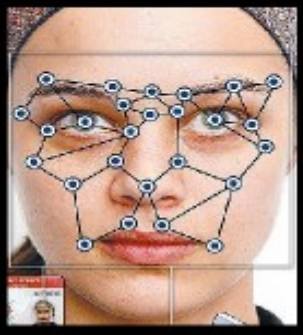
manual

Segurança Digital Eletrônica



terror.noblogs.org

“Era um dia frio e ensolarado de abril, e os relógios batiam treze horas.”

Tudo o que você faz na internet, nas redes sociais, nas suas pesquisas, nos seus e-mails, telefonemas e sms esta sendo vigiado. Suas preferências, gostos, interesses e saberes estão alimentando os servidores inimígos nesta era onde informação é poder. Cada informação que você produzir será usada contra você, experimente abrir o histórico do seu navegador (geralmente é Ctrl+h) e veja toda informação contida lá, todos os sites por onde você navegou, todas suas pesquisas, ou pior, vá em http://google.com/history e veja que todas as pesquisas que você fez estão salvas nos servidores da empresa google. Toda essa informação sobre você é vendida a grandes empresas, e claro, entregue aos estados e polícias... Piores são as redes sociais como facebook, que estão mais próximas do Grande Irmão*. Nós as alimentamos por várias horas diariamente, não só com nossos gostos e interesses, mas também deixando evidente as nossas redes de contatos e afinidades, tornado mais facil, a quem interessa, o nosso mapeamento social, a ponto de sermos induzidos, cooptados, investigados, controlados. O que dizer então dos celulares, que estão com nosco 24 horas por dia, criando um mapeamento de todas as nossas rotas de locomoção, desde nossas casas, até as escolas, trabalhos, manifestações, ações diretas e encontros secretos, gravando conversa por conversa com suas escutas não autorizadas. Estamos em tempos de guerra, num campo de batalha digital onde o estado e o capital estão melhores equipados e armados, toda informação é extremamente importante, então é necessário que se aprenda a jogar este maldito jogo, é hora do contra ataque, as informações do inimigo também estão lá. Devemos abandonar o conforto em nome do sigílio e segurança de nossas futuras ações. A propagação de conhecimento não deve ser interrompida, todos devemos aprender a analisar as táticas inimigas de repressão, e passar a diante nossos conhecimentos de guerrilhas e insurreições sem deixar rastro algum aos investigadores.
A luta se faz nas ruas, campos e trabalho de base, mas boa parte do conhecimento está na rede, e é a rede o meio mais acessivel de todo o conhecimento!
Preparem as armas, as mascaras de gás, tenha sua kalishnikov nas mãos, ascenda seu molotov e atire no escudo do batalhão do choque, conversa fiada não adianta mais, informação é poder, ”parabéns homem pela sua tecnologia, satélite, computador e reconstrução de vítima em cirurgia plástica, por sua inteligência pra desenvolver paredes, vidro a prova de bala e terminar confinado no abrigo anti-nuclear urbano”.

*1984, George Orwell
“Em cada patamar, diante da porta do elevador, o cartaz da cara enorme o fitava da parede. Era uma dessas figuras cujos olhos seguem a gente por toda parte. O GRANDE IRMÃO ZELA POR TI, dizia a legenda.”

TUDO O QUE VOCÊ PRODUZ SERÁ USADO CONTRA VOCÊ

Quem é você? O que você pensa? Por onde você anda? Quais são suas ideologias? Qual foi o seu grau de envolvimento nas ultimas manifestações que ocorreram em junho/lulho de 2013? Você participou de algum distúrbio civil? Invadiu a ALERJ? Destruiu a vidraça de algum banco? Você faz parte de alguma célula Black Bloc?
Você me daria todas estas informações de graça? Responderia questão por questão, descrevendo os mínimos detalhes sem saber quem sou eu e para o que eu quero estas informações?
Imagino que sua resposta seja negativa, mas provavelmente, na prática, você está fornecendo todas estas informações pra alguém muito, mas muito pior do que eu.
No dia 04/09/2013 fomos surpreendidos com a segunite noticia:


G1 RIO DE JANEIRO

04/09/2013 09h08 - Atualizado em 04/09/2013 20h37

Operação contra vandalismo em protestos prende Black Blocs no Rio

Três administradores da página Black Bloc foram presos nesta quarta. Dois menores também foram apreendidos; um procurado segue foragido.

Ao saber desta notícia ficamos angustiados pelos presos, que a partir daquele momento estavam em mãos inimigas, sejeitos a todos os tipos de penas, interrogações e torturas...
Mas isso não é o que mais nos chocou, o que mais nos chocou é que qualquer um que estiver por detraz das barricadas pode ser o próximo capturado. Chocados, pois as pessoas estão há muito tempo alimentando os servidores inimigos com informações pessoais e que deveriam ser confidênciais.
Isso só aconteceu porque as informações que ajudariam as pessoas a se defenderem no campo digital não estão reunidas, não estão bem divulgadas.
No caso do rio, provavelmente, as pessoas que foram presas através da investigação digital, sendo otimista, utilizavam perfis falsos no Facebook para administrarem as páginas de divulgação das táticas Black Bloc. Mas há muito mais detalhes a serem considerados:
-Os perfis eram falsos?
-Utilizavam que sistema operacional(windows?)?
-Utilizavam que navegador?
-Redirecionavam seu IP?
-Assosiavam alguma informação pessoal aos perfis?

-Tinham amigos em comum com algum perfil pessoal verdadeiro?
-Utilizavam os perfis em celulares/tablets/smartphones?
-Saiam por aí falando que eram administradores das páginas?

Dias antes das prisões, foi publicado em vários sítes o numero de informações que foram entregues pela empresa Facebook ao estado brasileiro:


TECNOLOGIA E GAMES

27/08/2013 14h33 - Atualizado em 27/08/2013 16h54

Brasil solicitou informações de 857 usuários do Facebook, diz relatório

Rede social divulgou números sobre requisições de autoridades em 2013. Segundo o Facebook, dados são usados em investigações oficiais.

O metodo que a polícia provavelmente utilizou é bem simples:
=>Os administradores das página deram alguma brecha de segurança ao acessarem seus perfis falsos (ou utilizaram perfis pessoais) => A empresa Facebook obteve seus respectivos IPs => a policia queria prender os responsáveis pelas páginas => Instarou-se uma investigação criminal => A polícia pediu auxilío ao Governo Federal do brasil => Por meio de algum acordo internacional com os EUA, NSA e Facebook se obteve os IPs relacionados aos administradores => Os IPs foram repassados aos responsáveis pela investigação => os investigadores pediram a localização físicas dos IPs aos provedores de internet (Vivo, net, claro) => se obteve os endereços físicos dos administradores => Prisões foram efetuadas.

É preciso se dissiminar os metodos de se obter mais segurança online, para assim, continuar-mos a propagar informações, livres de eventuais investigações e prisões.

“Uma falha da Agência Brasileira de Inteligência, a Abin, deu origem a uma operação para monitoramento dos protestos marcados via rede social. A partir de hoje (20 de Junho de 2013), a organização anunciou que estará monitorando o Twitter, Facebook, Instagram e WhatsApp para avaliar o alcance e comportamento das manifestações que estão tomando conta do Brasil.

De acordo com informações do Estadão, a iniciativa surgiu após o Gabinete de

Segurança Institucional não ter alertado os assessores da presidente Dilma Rousseff sobre os protestos que resultaram, inclusive, na invasão do Congresso Nacional. Assim, foi criado um sistema de monitoramento chamado Mosaico, que filtra as postagens das redes a partir de 700 temas definidos pela Abin.

Assim, espera a agência, será possível prever a rota das passeatas, a infiltração de grupos políticos entre os protestos e até mesmo um possível financiamento deles. Hoje mesmo, por exemplo, descobriram-se planos de manifestações em frente ao Palácio do Planalto, onde já foram instaladas grades para proteger as instalações.

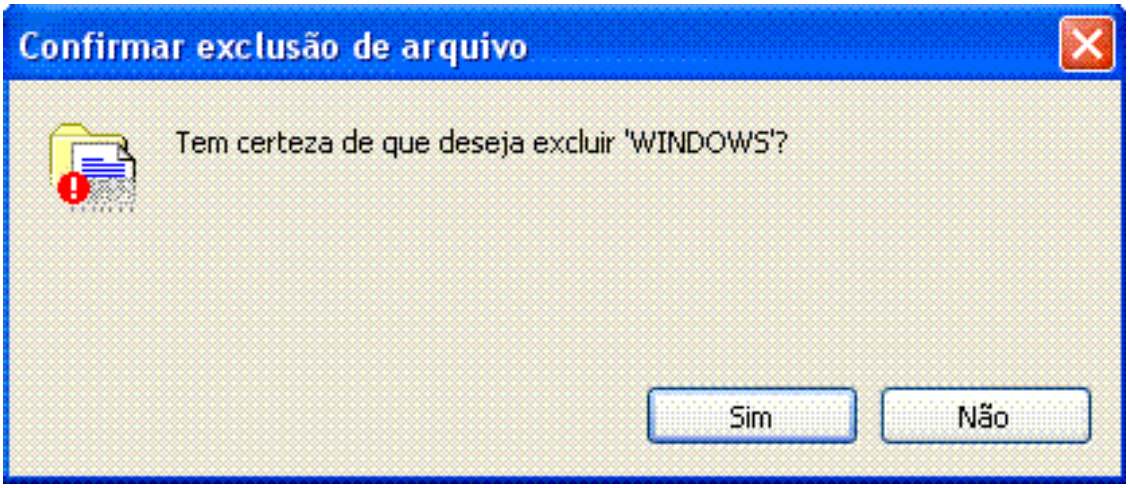
O governo não se pronunciou sobre acusações de invasão de privacidade que estão eclodindo aqui e ali na imprensa nacional, principalmente devido à inclusão do WhatsApp na lista de monitoramento. Enquanto redes como o Twiter ou Facebook têm boa parte de seu conteúdo aberto, o mesmo não pode ser dito do aplicativo de mensagens, cujos envios são compartilhados apenas entre os envolvidos na conversa.”

SISTEMAS OPERACIONAIS

Tudo deve começar a partir do sistema operacional que você utiliza em seu computador. Utilizar Windows ou Mac é totalmente inseguro, pois são plataformas proprietárias controladas por interesses privados de empresas que utilizaram suas informações pessoais em nome do capital, irão juntar todas as suas informações como a procedencia do software, seu IP, navegação, arquivos, programas instalados.
Windows é totalmente inseguro, não é atoa que a maioria dos virus da rede são desenhados para este sistema operacional, a probabilidade de ser atacado digitalmente é muito grande, é não muito dificil de se fazer isso. Nele, seus arquivos mais pessoais não estarão salvos, porque qualquer um os pode acessar diretamente através de um LIVE CD. A maioria de seus programas também são proprietários, e podem juntar mais informações sobre você, a partir dos textos que você lê, os videos que você assiste, a pirataria que você baixa e outros. O Windows é o sistema operacional mais usado no mundo, e sua pirataria também é enorme, mas para a Microsoft, interessa muito que as pessoas só utilizem o windos mesmo que seja pirata, pois mesmo assim as pessoas estarão aprisionadas as suas normas e coletas de dados.
O sistema operacional Mac (sistema operacional de burgues) não é tão acessivel quanto Windows e nem tão vuneravel, porém para adquiri-lo, mesmo que seja pirata, na hora da instalação é preciso fornecer todos seus dados pessoais para a Aple, como documentos, telefone, endereço residêncial e outros. Informações que podem ser repassadas a empresas e governos. Tudo o que você faz no Mac é vigiado, e se você possuir alguma conta de rede social ativa nele, ele ficará postando a sua atual posição física, criando seu mapeamento.

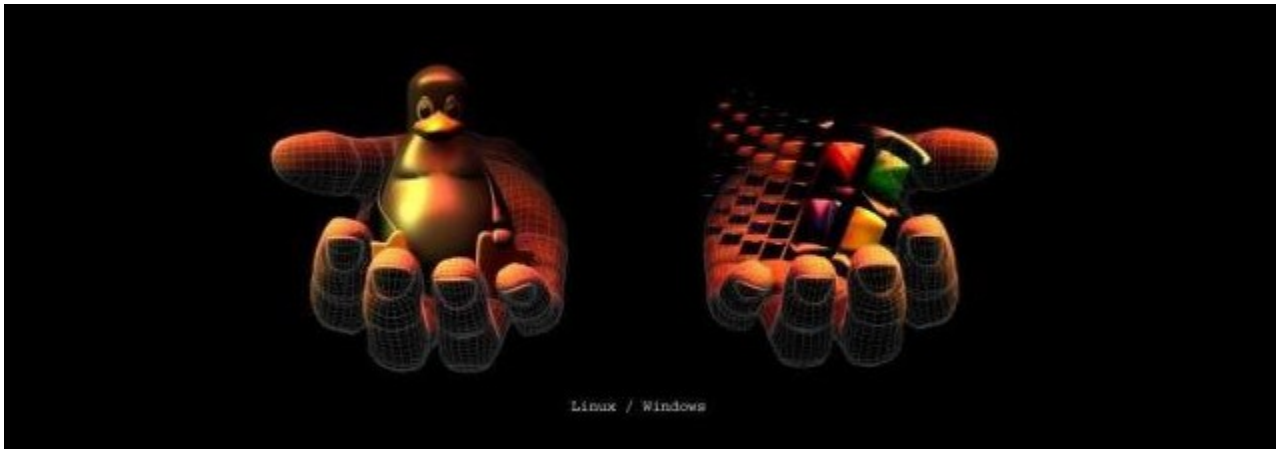
A única saída é utilizar uma distribuição GNU/LINUX. Existem milhares de distribuiçõos disponíveis para cada necessidade de usuário, mas as mais seguras são as baseadas na distribuição DEBIAN. Uma distribuição GNU/LINUX é totalmente livre e grátis, não pertence a nehuma empresa ou estado, é feita e mantida pelos próprios usuários na rede, onde qualquer pessoa pode ajudar a desenvover e modificar novas disribuições e atualizações. Também é seguro pois não é alvo de hackers e crackers, a maioria deles utilizam GNU/LINUX por julgarem ser realmente seguras. Possuem atualizações e correções frequentes, tornando-se quase impossível haver qualquer erro ou falha.

As distribuições GNU/Linux têm seu código aberto. Em termos práticos, podem-se ressaltar duas consequências diretas disso. Primeiramente, toda a comunidade ganha acesso ao código do programa. Isso significa que qualquer pessoa pode lê-lo e interpretá-lo. Assim, as chances de haver qualquer mecanismo de espionagem ou coleta de dados governamental ou corporativo é muito pequeno. Em segundo lugar, a disponibilidade do código garante a todas as pessoas que sabem interpretar a linguagem e programar a liberdade de fazer os seus próprios softwares, introduzindo melhorias e ajudando a comunidade. Funciona como um "faça você mesmo" computacional, sem precisar depender de Microsoft e outras empresas para fazer os programas que você usa. Nesse sentido, a maior parte dos projetos de software livre são colaborativos e encorajam as pessoas a passarem de usuárias a desenvolvedoras.



ESCOLHENDO SUA DISTRIBUIÇÃO GNU/LINUX

Se quisermos uma comunicação segura para difundir práticas libertárias e formar uma rede que busca a autonomia e combate a dinâmica de produção capitalista, devemos começar, nessa difusão, por optar pelo software livre em detrimento do proprietário. Além do benefício de custo (pois além de "livre", é gratuito), tendo o código aberto já podemos nos precaver melhor de espionagem de corporações e governos. Existem diversas versões do sistema operacional GNU/Linux, e não se pode dizer qual é "a melhor" – isso depende da máquina e de quem a utiliza. Você pode pesquisar por uma distro que melhor se encaixe em teu perfil pelo distrowatch.com. Para usuários com menos familiarizados com instalação de sistemas operacionais, há no youtube diversos vídeos ensinando como proceder para migrar para GNU/Linux ou para instalar este sistema ao lado do sistema existente no computador.



Dentre todas as distribuições GNU/LINUX conhecidas, eis aqui as mais indicadas para diferentes tipos de computadores, níveis de segurança altos e facilidade de adaptação:

-Debian

Debian é simultaneamente o nome de uma distribuição não comercial livre (gratuita e de código fonte aberto) de GNU/Linux (amplamente utilizada) e de um grupo de voluntários que o mantêm à volta do mundo. Uma vez que o Debian se baseia fortemente no projecto GNU, é usualmente chamado **Debian GNU/Linux**. O Debian é especialmente conhecido pelo seu sistema de gestão de pacotes, chamado APT, que permite: atualizações relativamente fáceis a partir de versões realmente antigas; instalações quase sem esforço de novos pacotes e remoções limpas dos pacotes antigos. Atualmente o Debian Stable se encontra na versão 7.0, codinome "Wheezy".

O Debian Stable procura sempre manter os pacotes mais estáveis, assim, ele mantém o Gnome 3 e o KDE 4.8 por padrão. O fato dele conter pacotes mais antigos, garantindo a estabilidade, é o grande foco para servidores.

O projecto Debian é mantido por doações através da organização sem fins lucrativos Software in the Public Interest.

O nome Debian vem dos nomes dos seus fundadores, Ian Murdock e de sua ex-mulher, Debra. A palavra "Debian" é pronunciada em Português como Débian.

Várias distribuições comerciais baseiam-se (ou basearam-se) no Debian, incluindo: Linspire (antigo Lindows),Xandros,Knoppix. Kurumin, BrDesktop e Ubuntu.

O contrato social Debian
http://www.debian.org/
http://www.debian.org/index.pt.html/
http://www.forumdebian.com.br/

-Mint

Linux Mint é uma distribuição Linux irlandesa. Possui duas versões: uma baseada em Ubuntu (com o qual é totalmente compatível e partilha os mesmos repositórios) e outra versão baseada em Debian.

Diferencia-se de ambos os sistemas por incluir drivers e codecs proprietários por padrão e por alguns recursos que permitem fazer em modo gráfico configurações que em ambos os sistemas são feitas através do modo texto. Utiliza por padrão o desktop Gnome modificado, com um menu no painel inferior junto à barra de tarefas (o MintMenu), similar ao menu "Iniciar" do Windows. O propósito da distribuição é providenciar um sistema Linux que esteja pronto para uso assim que terminar a instalação. Dessa maneira, o único trabalho do usuário será o de personalizar a aparência, se desejar, e instalar programas extra, caso necessite.

http://www.linuxmint.com/

http://www.linuxmint.com.br/
http://www.linuxmint.com.br/forum/

-Ubuntu

Ubuntu é um sistema operacional de código aberto, construído a partir do núcleo Linux, baseado no Debian. É patrocinado pela Canonical Ltd (dirigida por Jane Silber).

O Ubuntu diferencia-se do Debian por ter versões lançadas semestralmente, por disponibilizar suporte técnico nos 9 meses seguintes ao lançamento de cada versão (as versões LTS – ***L**ong **T**erm **S**upport* – para *desktop* recebem 5 anos de suporte, e para servidor recebem 5 anos de suporte), e pela filosofia em torno de sua concepção. A proposta do Ubuntu é oferecer um sistema que qualquer pessoa possa utilizar sem

dificuldades, independentemente de nacionalidade, nível de conhecimento ou limitações físicas. O sistema deve ser constituído principalmente por software livre. Deve também ser isento de qualquer taxa.

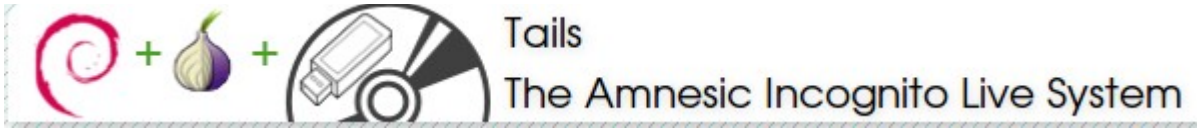
O Ubuntu contou durante o primeiro semestre de 2007 com situações de migração ou adopção por parte de organizações e entidades de renome. O fabricante internacional de equipamento informático Dell que adotou, em maio, o Ubuntu como o sistema operativo de código aberto seleccionado para equipar os seus computadores *desktop* e *notebook* destinados aos usuários finais; e o anterior anúncio, em Março, por parte do Parlamento francês de que em Junho de 2007 daria início à migração de toda a sua rede informática (máquinas clientes e servidores, num total de cerca de 1.154 máquinas) para o Ubuntu, com ênfase no uso da *suite* OpenOffice e do browser Firefox por parte dos utilizadores do Parlamento (577 Deputados).

Segundo estimativas o Ubuntu, em abril de 2009, já possuiria mais de 100 milhões de usuários.

http://www.ubuntu.com/

http://www.ubuntu-br.org/
http://www.ubuntubrsc.com/

-Tails



Tails, *The Amnesic Incognito Live System*, é uma distribuição Linux focada em privacidade. Ela o faz forçando todas as conexões entre o computador e a Internet a passarem pela rede Tor (será explicada na página xx). Tails se diz uma cola entre o sistema operacional Debian, do qual foi originado, e a dita rede Tor. Além de oferecer privacidade através de técnicas de ocultação do IP, Tails vem com várias ferramentas de criptografia de informação, de forma que, mesmo interceptada, informação partindo do computador seja muitíssimo difícil de ser entendida a não ser pelo servidor à qual se destina. Tails termina seu método de proteção da identidade do usuário com uma característica não tão usual: ele não pode ser instalado no disco rígido, tendo que ser executado à partir de mídias removíveis, de forma que os dados do usuário não fiquem na máquina que ele usou, ao mesmo tempo que ele pode, mediante própria configuração da BIOS, usá-lo em qualquer computador. Isso torna o Tails um Live DVD. Tails vem com navegador e cliente de mensagens instantâneas, além de ferramentas para manipulação de imagem, gerenciamento de senhas e controle de tráfego com a rede Tor.

Sem dúvida, Tails é a distribuição linux mais segura de que se tem notícia!

https://tails.boum.org/
https://tails.boum.org/index.pt.html

-Precauções essenciais:

-Só baixe as distribuições GNU/linux através de seus sites oficiais.

-Antes da instalação faça um teste em todas as funções do computador, teclado, microfone, webcam, wireless, etc para saber se a distribuição GNU/Linux que você desejá utilizar é totalmente compativel com seu computador. Esse teste começa automaticamente quando você insere o cd de instalação no seu computador.

-Na hora da instalação de sua distribuição GNU/Linux opte por criptografar todo o seu computador.

-Se você ainda precisar utilizar do windows para rodar algum progama em particular, pode-se utilizar das seguintes opções:
*Tentar usar o WINE para rodar o tal programa;
*Usar uma máquina virtual dentro do linux com o programa VIRTUAL MACHINE para rodar o windows;
*Particione o disco rígido de seu computador, para poder usar os dois sistemas operaconais, oscolhendo qual irá utilizar na hora em que o aparelho for ligado(deixa o computador inseguro).

Sites com mais informações e suporte:
http://www.vivaolinux.com.br/
http://www.linuxbrasil.org.br/
www.linuxdescomplicado.com.br/

NAVEGADORES

É através do navegador do seu computador que é acessada a internet. Por ele, todas suas informaçãoes são passadas, transmitidas e muitas vezes vazadas, gravadas e vendidas. Quem utiliza o Internet Explorer está correndo grande risco, pois ele possuiu várias brechas na segurança, além de pertencer a Microsoft, o Google Chrome também não é nada seguro, pois pertence a empresa Google, que colherá informações de tudo o que você fizer nele.
Para se ter mais segurança, os navegadores recomendados, além do TOR que será explicado a seguir, são o Firefox e o Iceweasel, porém devem estar acompanhados de plugins essênciais.

Firefox

Mozilla Firefox é um navegador livre e multi-plataforma desenvolvido pela Mozilla Foundation com ajuda de centenas de colaboradores. A intenção da fundação é desenvolver um navegador leve, seguro, intuitivo e altamente extensível. Firefox tornou-se o objetivo principal da Mozilla Foundation. Anteriormente o navegador juntamente com o Mozilla Thunderbird, outro produto da Mozilla Foundation eram os destaques da mesma. Cerca de 40% do código do programa foi totalmente escrito por voluntários.

Iceweasel

Iceweasel é um navegador de código aberto exclusivamente destinado às distribuições Linux baseadas no Debian. Ele é idêntico ao Mozilla Firefox, que não pode ser distribuído juntamente com o Debian por ter a marca e o ícone patenteados pela Fundação Mozilla, uma vez que o conteúdo distribuído com o Debian deve ser totalmente livre.

Diferentemente do Firefox, o IceWeasel contém somente softwares livres por definição. Por causa disso:

- Foram trocadas as figuras proprietárias por figuras livres;
- Foi removido o sistema de relato de bugs e falhas;
- Agora é usado o serviço de busca de plugins livres.

Além disso, foram também adicionadas algumas novas funções de privacidade, como por exemplo:

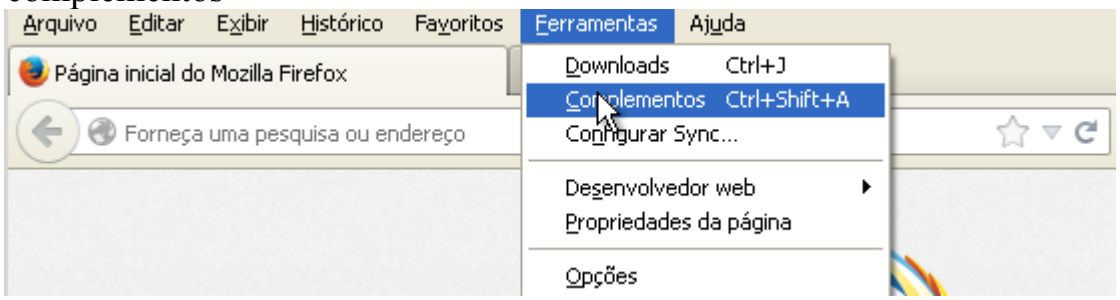
- Proteção contra imagens de dimensão zero que tentam criar novos cookies;
- Advertência contra redirecionamento de URLs.
- Suporta o protocolo ftp para visualização de arquivos e pastas.

PLUGINS

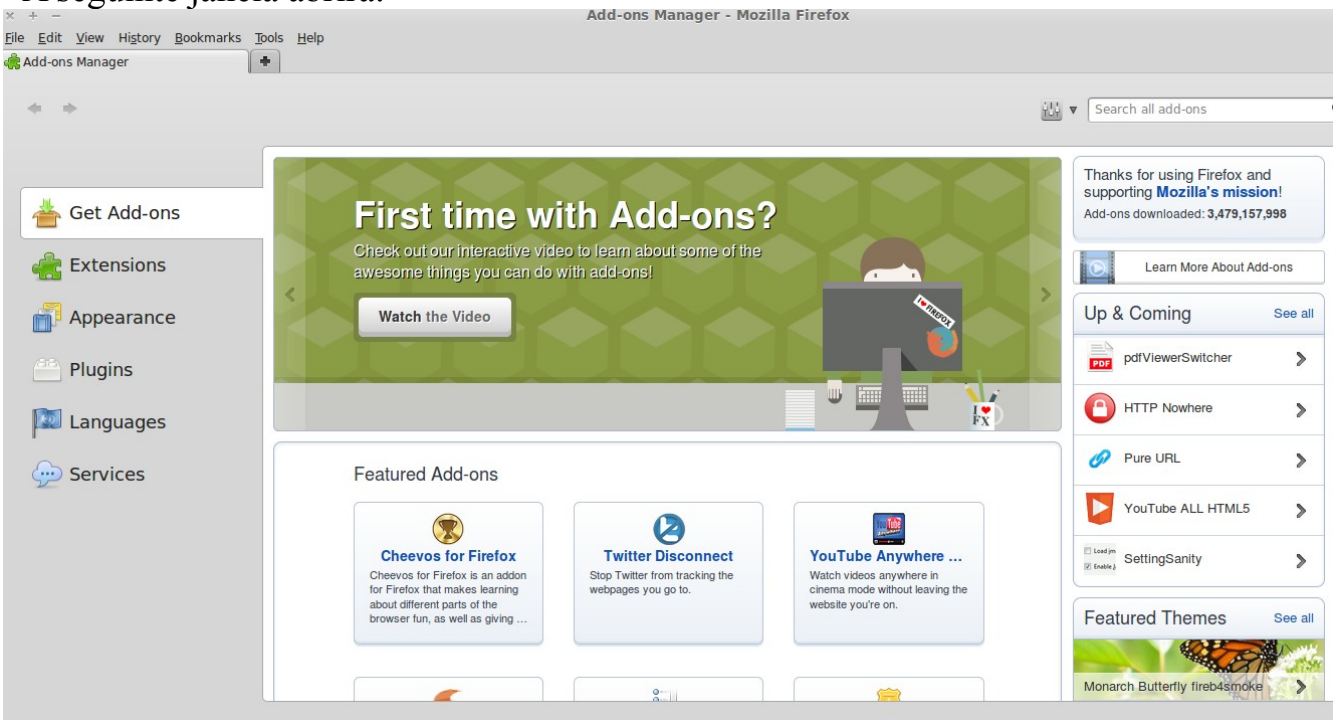
Não basta apenas utilizar os navegadores Firefox ou Iceweasel, para se aumentar a segurança existem alguns plugins essenciais que são muito faceis de serem instaldos e configurados. A seguir você aprenderá a instalar qualquer plugin e como configurar os principais:

<u>Pesquisando e instalando um plugin:</u>

*Abra o navegador e vá a barra de menu, click em Ferramentas e click em complementos



*A seguinte janela abrirá:



é nesta pagina que você pode encontrar a maioria dos plugins que serão descritos a seguir. Alguns plugins você só poderá encontrar no site https://addons.mozilla.org/ ou no site dos desenvolvedores do próprio plugin.

Plugins essenciais e suas configurações:

-AdBlock

Adblock Plus permite que você recupere o controle da internet e visualize a web do jeito que você quiser. O add-on é apoiado por mais de quarenta subscrições de filtro em dezenas de idiomas, que a configuram automaticamente para fins que vão desde a remoção de publicidade on-line de bloquear todos os domínios de malware conhecidos. Adblock Plus também permite que você personalize seus filtros com a ajuda de uma variedade de recursos úteis, incluindo uma opção de contexto para as imagens, um separador para Flash e objetos Java, e uma lista de itens bloqueáveis para remover scripts e folhas de estilo.

https://addons.mozilla.org/pt-br/firefox/addon/adblock-plus/
https://adblockplus.org/en/firefox

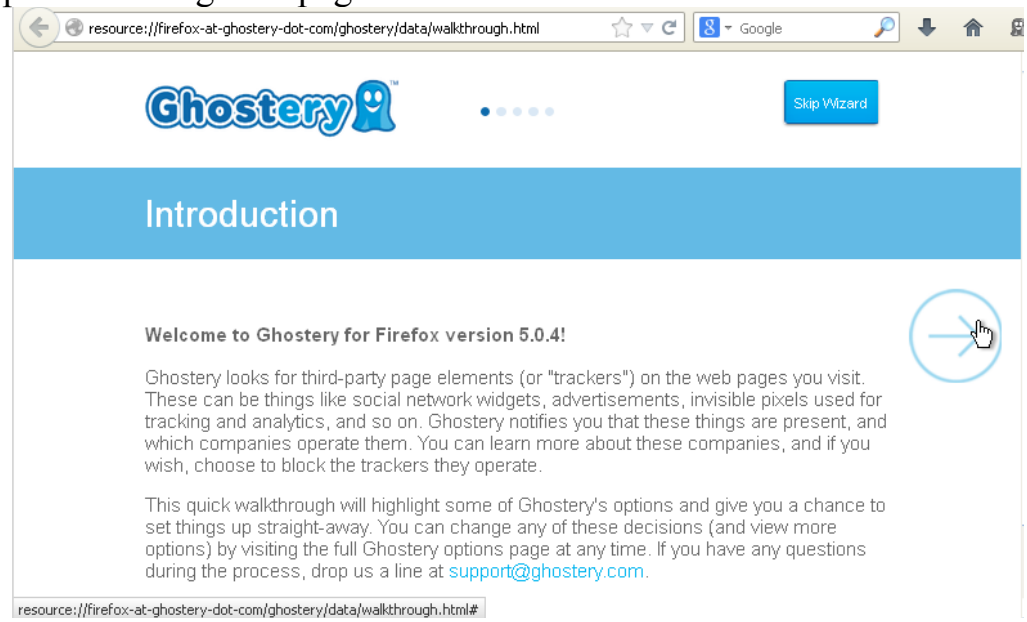
-Ghostery

Veja quem está rastreando sua navegação na web e os bloqueie com Ghostery. Ghostery vê a web "invisível", detectando trackers, web bugs, pixels e balizas colocadas em páginas web, Facebook, Google Analytics, e mais de 1.000 outras redes de publicidade, provedores de dados comportamentais, os editores da web - todas as empresas interessadas em sua atividade. Ghostery é construído e mantido para os usuários que se preocupam com sua privacidade on-line, e é projetado com a privacidade como um objetivo primário. Uso Ghostery é anônimo. Não há registros ou cadastros obrigatórios.

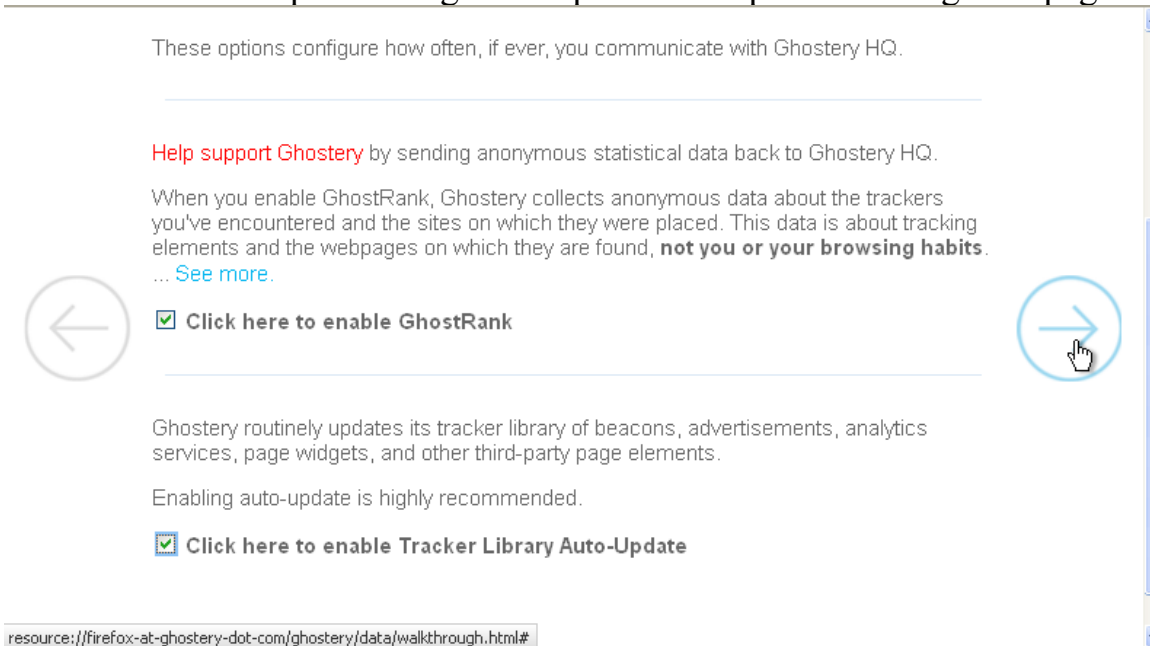
https://addons.mozilla.org/pt-br/firefox/addon/ghostery/
https://www.ghostery.com/

O maior erro das pessoas é não configurar este aplicativo, pulando sua configuração. Para funcionamento correto, siga os seguintes passos:

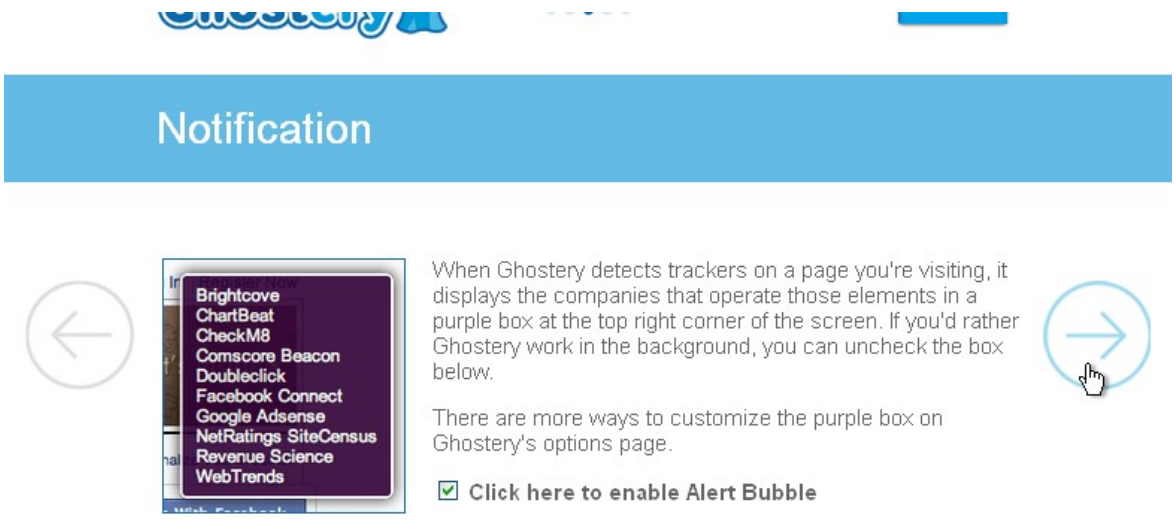
Depois de instalado o plugin, o navegador vai pedir permição para ser reiniciado. Ao reiniciar aparecerá a seguinte página:



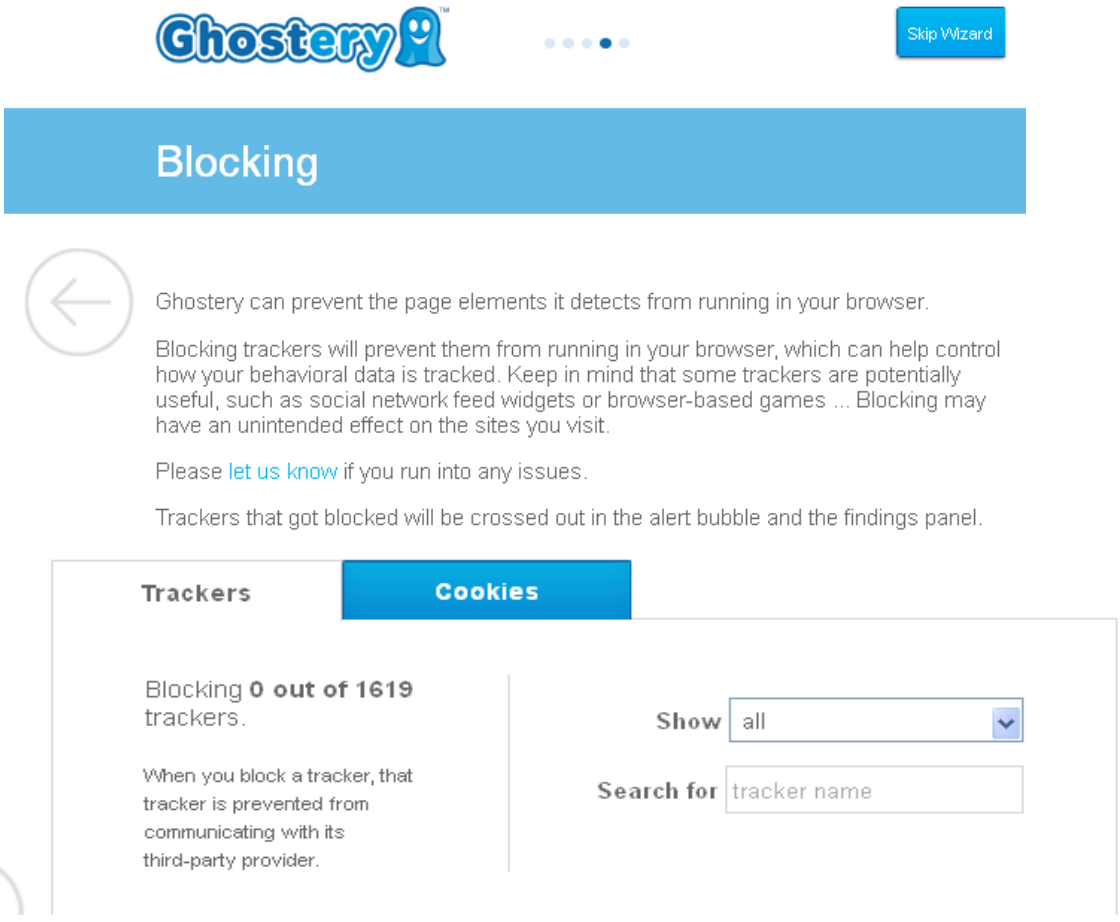
Click na seta azul direita para configurar o aplicativo. Aparecerá a seguinte pagina:

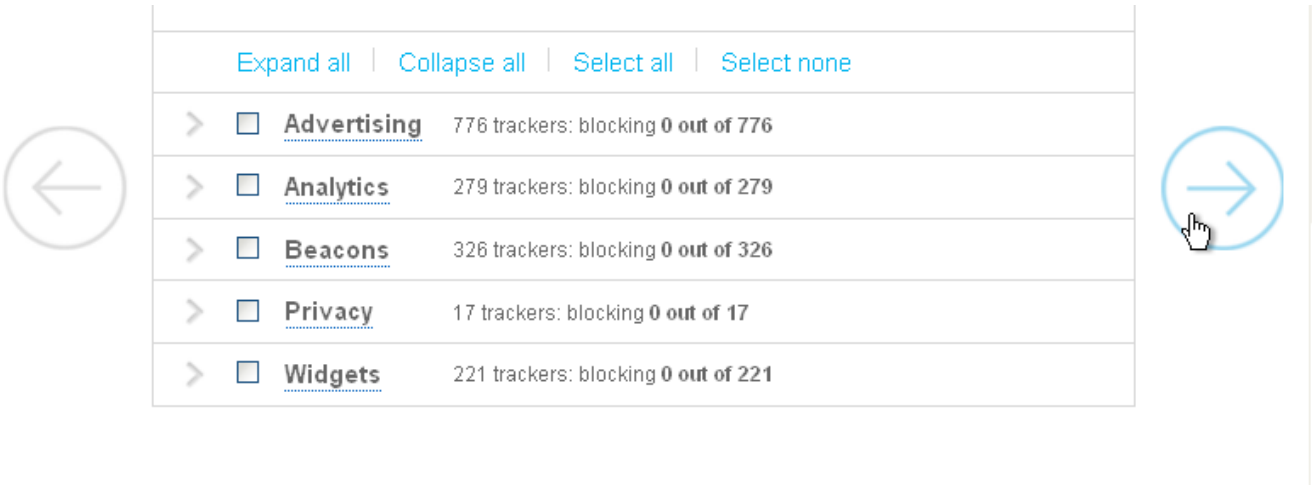


Marque em “Click here to enable GhostRank” e em “Click here to enable Tracker Library Auto-Update”. Click novamente na seta azul do lado direito da tela para passar para o próximo passo:



Marque a opção “Click here to enable Alert Bubble” para ativar a janela de notificações, essa janela é boa para você poder acompanhar o funcionamento do plugin. Vá para o préximo passo:

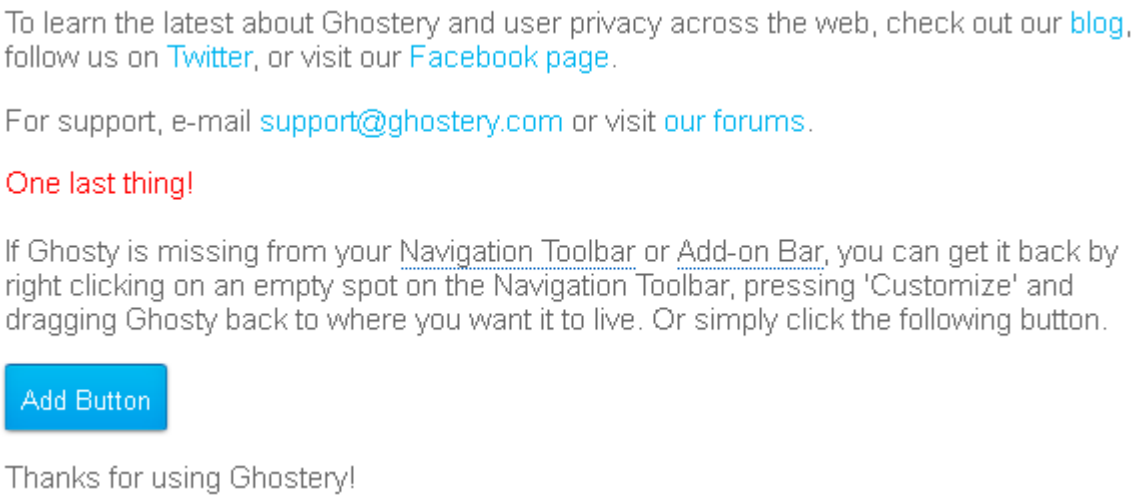




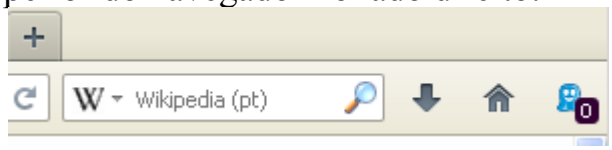
Nesta parte é preciso ter atenção, aqui você irá abilitar o bloqueio de colhedores de informação. Marque as opções “Adversting”, “Analytics”, “Beacons”, “Privacy” e “Widgets”. Em seguida, click na Aba escrita COOKIES:

Aparecerá:

Marque as opções “Adverstising”, “Analitics”, “Beacons” e “widgets”, e click no proximo passo.



PRONTO! Ghostery esta pronto para o uso! Caso o logo do plugin não esteja aparecendo no seu navegador, click no botão “Add Button”. Ele deve estar na aba superior do navegador no lado direito:



-Google sharing

GoogleSharing é um complemento para Firefox que anonimiza suas pesquisas no Google. É fácil de usar, gratuito e com código aberto (livre!).

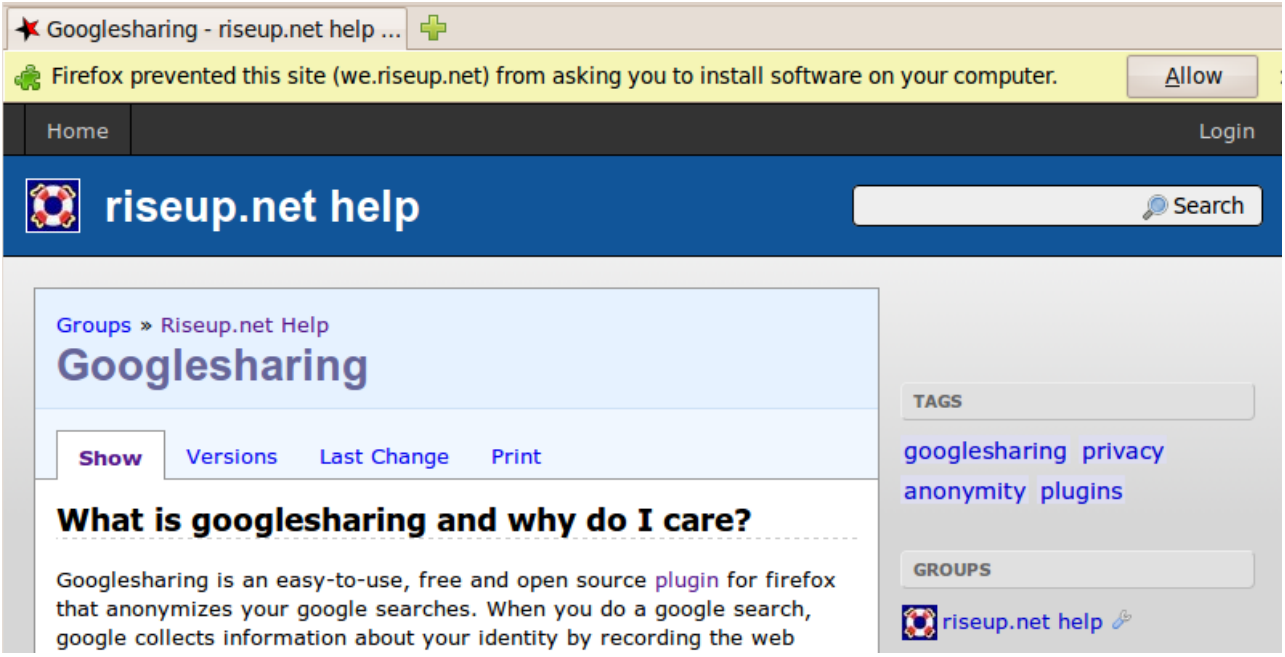
Quando você faz uma pesquisa no Google, eles coletam informação sobre sua identidade gravando os endereços da internet de onde você acessa e o conteúdo de suas pesquisas. Google provavelmente sabe mais sobre suas pesquisas na internet do que você!

GoogleSharing funciona enviando todo seu tráfego relatado pela Google que não não precise de login (como o Gmail) através de um servidor separado, completamente transparente (você não tem que fazer nada). Como um resultado, sua atividade online é misturada com a de todas as demais pessoas que usam o plugin.

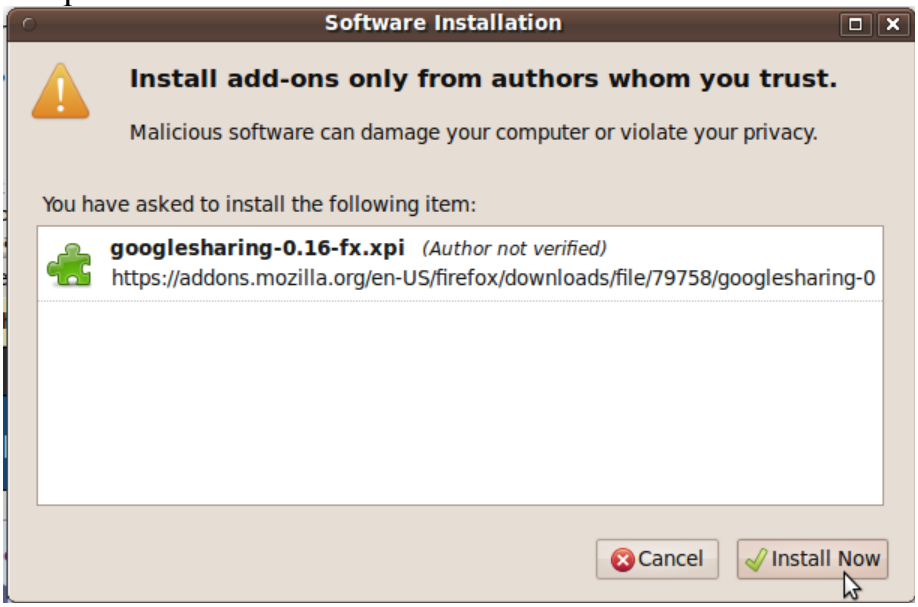
Para informação detalhada sobre como funciona e por que é importante, confira o site do projeto.

Como configuro?

1. Clique aqui para instalar o complemento.
2. Você deverá ver uma barra amarela aparecer no topo de seu navegador que diz algo como “O Firefox impediu este site (addons.mozilla.org) de oferecer a instalação de extenções e temas no seu computador.” Clique e em “Permitir” para instalar.

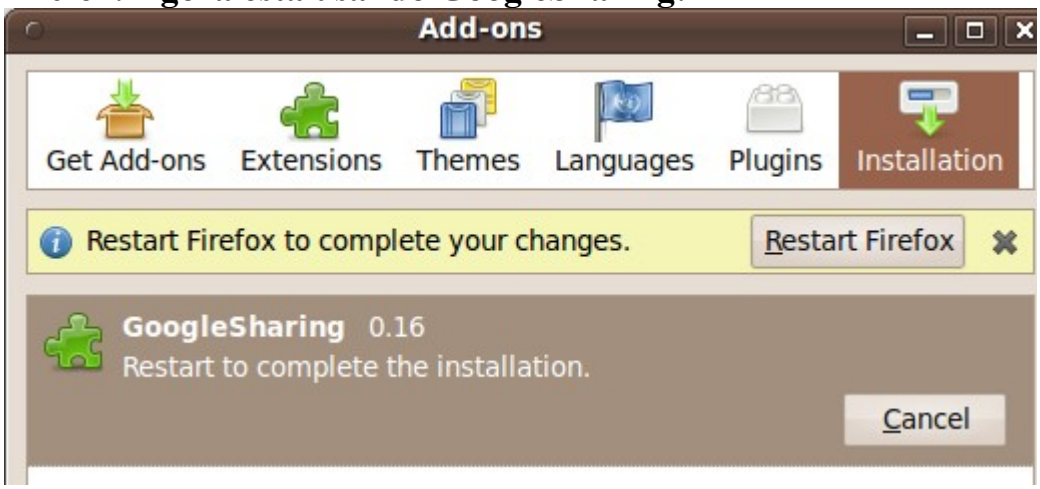


3. Agora você verá esta janela. Espere até que o botão Instalar possa ser clicado, então… clique nele!



4. Reinicie o

Firefox. **Agora está usando GoogleSharing!**



3. Paranóia Opcional

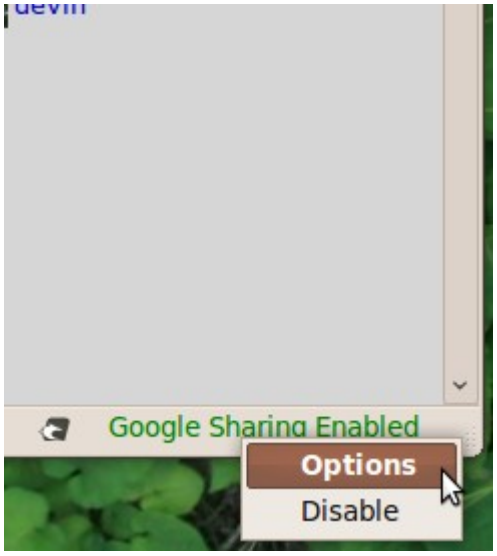
Para maior anonimato, o seguinte é opcional.

Google não é capaz de correlacionar sua atividade com você, como indivíduo, porque está sendo enviada através dos proxy do Googlesharing, e então eles reenviam para o Google. Isto significa que seus pedidos aparecem para o Google como se originassem dos proxy do Googlesharing, não do seu computador. Fantástico!

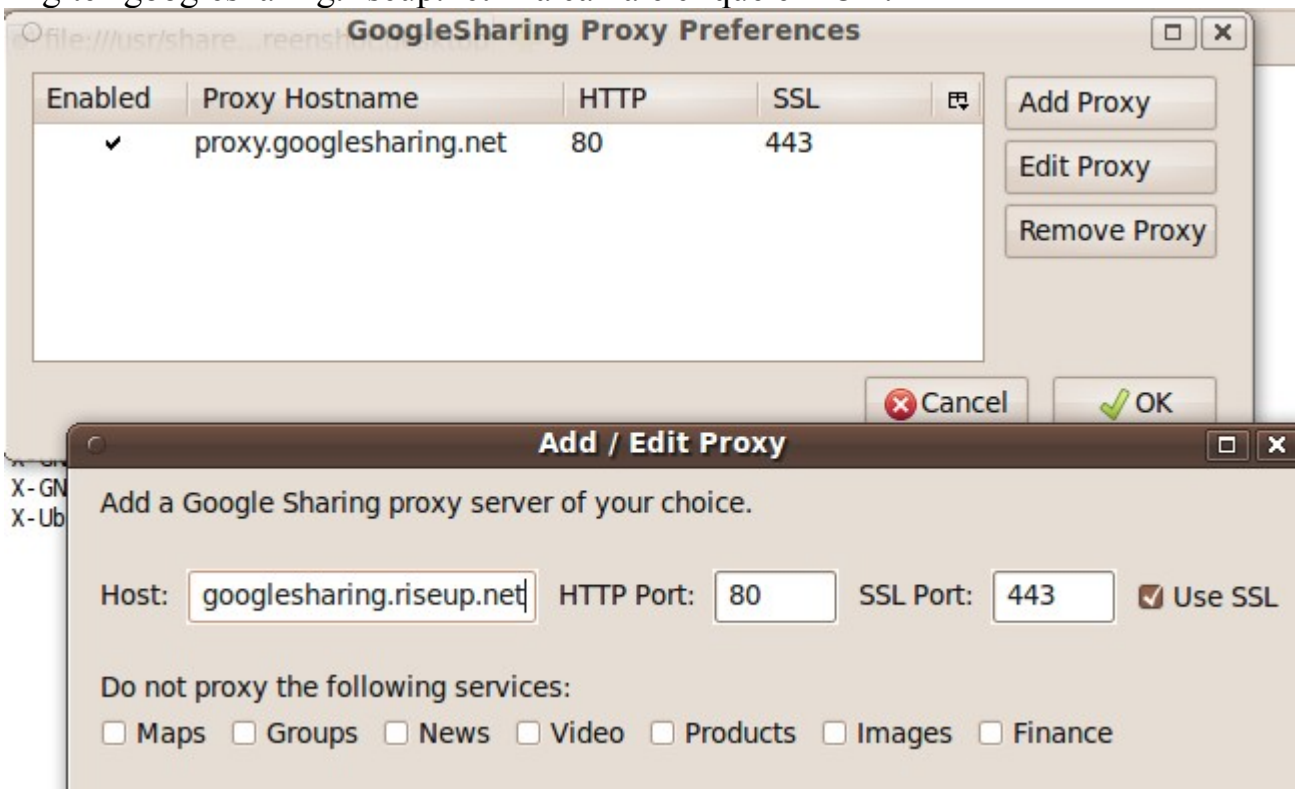
É claro que, isto também significa que os proxy do Googlesharing agora podem teoricamente fazer o que o Google faria, relacionar suas atividades com você e seu computador. Você deveria perguntar: que informação o Googlesharing mantém de mim? Eles dizem que não mantêm registros, então a resposta é **nada**. Mas como ter certeza de que é assim? Não tem como. Você tem que confiar na reputação que têm (e que acreditamos que é muito forte neste área). De fato, **Riseup está rodando dois dos proxy que fazem parte dos recursos do Googlesharing**, assim, podemos assegurar que nenhum registro está sendo mantido *nos servidores que estamos rodando.*

Se quiser, você pode usar apenas os proxys do Googlesharing mantidos pelo Riseup. Ou seja, seu tráfego da internet relacionado ao Google será roteado somente através de nossos servidores. Se você deseja fazer isto, siga os passos seguintes:

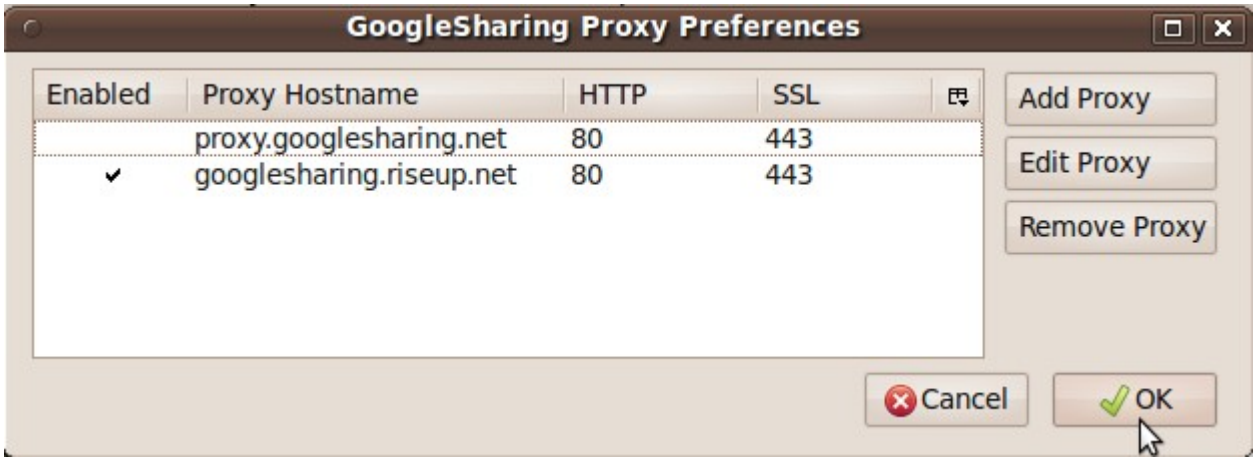
1. Clique com o botão direito sobre o texto “Google Sharing Enabled” no canto direito abaixo de seu navegador e selecione “Opções”.



2. Clique em “Add Proxy” (Adicionar Proxy)
3. Digite “googlesharing.riseup.net” na caixa e clique em OK.



4. Agora clique na coluna à esquerda abaixo de “enabled” (habilitado) para ativar o uso do proxy do Riseup. Se por acaso você quiser voltar a usar o proxy padrão, você pode mudar aqui.



5. Clique em ‘Ok’

https://we.riseup.net/riseuphelp+pt/pt-googlesharing

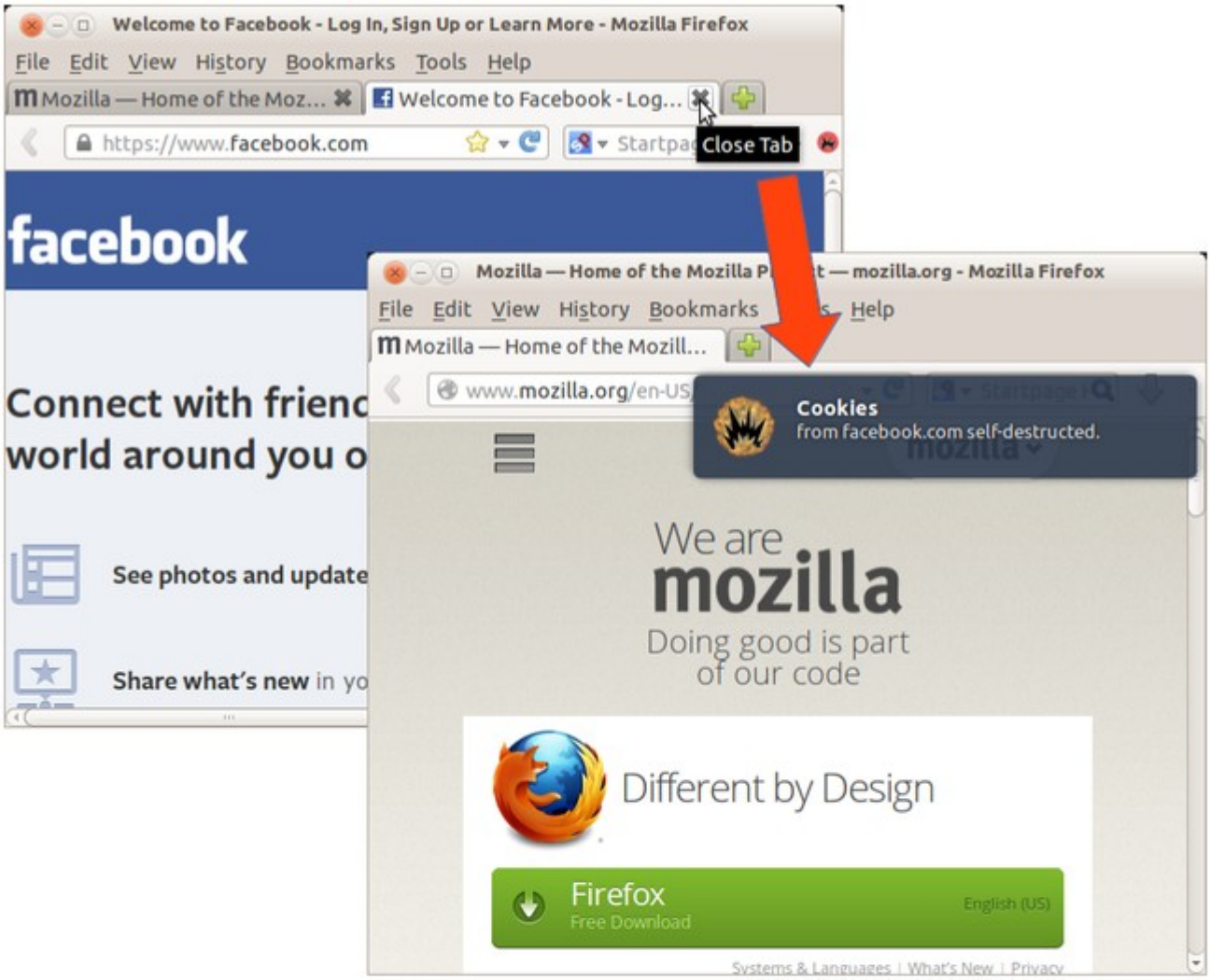
https://addons.mozilla.org/pt-br/firefox/addon/googlesharing/

http://www.googlesharing.net/

-Self-Destructing Cookies

Self-Destructing Cookies remove automaticamente os cookies do seu navegador quando eles não são mais usados por abas abertas. Com este aplicativo as sessões deixam de ficar demoradas e destrói os cookies que são usados por sites para te espiar. Este add-on complementa as soluções baseadas em lista negra, como Adblock e Ghostery.

Este aplicativo exclui automaticamente os cookies de todos sos sites em que voce navega logo que você fecha a aba ou a janela do navegador:



Para configurar clck com o botão direito do mouse no ícone do aplicativo que se localiza na parte inferior direita do navegador, abrirá a seguinte aba:

Nela você pode escolher o tipo de operação que ele exucutará entre, Destruir os Cookies depois de fechar qualquer aba, depois de fechar o navegador, nunca excluir, temporáriamente desativar o plugin e parar de vez de excluir os cookies. É aconselhado que se utilize a primeira opção, mas sempre desative temporariamente se você for acessar alguma pagina de confiança que necessite cookies ativados.

https://addons.mozilla.org/pt-br/firefox/addon/self-destructing-cookies/

Better privacy

Remove e gerencia um novo e raro tipo de cookies, mais conhecido como LSO. A salvaguarda BetterPrivacy oferece várias maneiras de lidar em Flash cookies criados por Google, YouTube, eBay e outros. BetterPrivacy serve para proteger contra cookies especiais de longo prazo , uma nova geração de “Super -Cookies”, que silenciosamente conquistou a Internet. Esta nova geração de cookies oferece rastreamento de usuários ilimitados para a indústria e pesquisa de mercado. Relativas à privacidade em Flash cookies são mais críticos. Este add-on foi feito para sensibilizar os utilizadores oferecer uma maneira mais fácil de visualizar e de gerenciar este tipo de cookie, já que os navegadores são incapazes de fazer isso por você. Flash cookies (Local Shared Objects , LSO) são informações colocadas em seu computador através de um plug-in Flash. Esses Super-Cookies são colocados em pastas do sistema central. Eles são frequentemente usados como cookies do navegador padrão. Apesar de seu potencial ser maior do que os de cookies convencionais, apenas alguns usuários começaram a tomar conhecimento deles.

https://addons.mozilla.org/pt-br/firefox/addon/betterprivacy/

NoScript

A melhor segurança que você pode obter em um navegador web!
Permitir que o conteúdo ativo seja executado apenas a partir de sites que você confia, e proteger-se contra ataques XSS e Clickjacking.

Vencedor do "Prêmio PC World Class World", esta ferramenta lhe dá a melhor proteção disponível na web. Ele faz com que JavaScript, Java e outros conteúdos executáveis só sejam executados apenas a partir de domínios confiáveis de sua escolha, por exemplo, seu site de home-banking, guardando os seus "limites" de confiança contra ataques de cross-site scripting (XSS), DNS religação / CSRF ataques cross-zona (router hacking), e tentativas Clickjacking, graças à sua tecnologia ClearClick único. Ele também implementa o DoNotTrack por padrão. Essa abordagem preventiva evita a exploração de vulnerabilidades de segurança (conhecidas e ainda desconhecidas!) Sem perda de funcionalidade … Especialistas concordam: Firefox é realmente mais seguro com NoScript.

Quando você entra em um síte, todo o java script estará bloqueado, mas se o site for de sua confiança e necessite do complemento, pode configurá-lo clicando em seu ícone que se encontra no lado direito inferior do navegador:

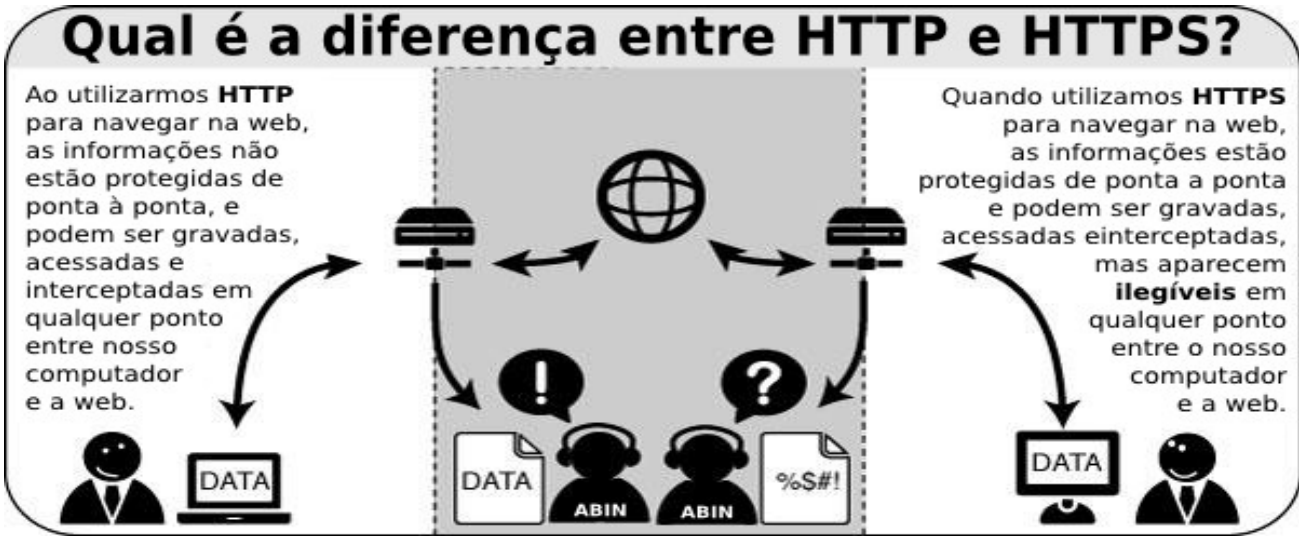
Nele você terá as opões de ativar permanentemente ou temporariamente o javascrpt de qualquer site, ou clicando em opções, pode-se criar uma lista branca dos sites de sua confiança que necessitem de javascript.

https://addons.mozilla.org/pt-br/firefox/addon/noscript/
http://noscript.net/

-HTTPS Everywhere

HTTPS Everywhere é uma extensão do Firefox e Chrome que criptografa suas comunicações com muitos sites grandes, tornando a sua navegação mais segura. HTTPS Everywhere é produzido com uma colaboração entre o Projeto Tor e a Electronic Frontier Foundation. Muitos sites na web oferecem algum suporte limitado para criptografia HTTPS, mas o torná difícil de usar. Por exemplo, eles podem não estar criptografados padrão para, ou encher as páginas com links que levam para o site criptografado. O HTTPS Everywhere corrige esses problemas usando a tecnologia inteligente para reescrever as solicitações destes sites para HTTPS.

https://www.eff.org/https-everywhere



TOR

Seus passos na internet podem estar sendo seguidos. Através da analise de tráfego, empresas criam relatórios, traçando perfis de usuários que são utilizados para monitorar empresas concorrentes, fazer publicidade direcionada, entre outras coisas.

O Projeto TOR é um software aberto que permite que o usuário navegue de forma anônima na internet. O programa modifica o caminho direto remetente-receptor que os pacotes de dados seguiriam, criando caminhos aleatórios através dos servidores voluntários que foram introduzidos na rota. Cada um desses servidores armazenam somente o servidor imediatamente anterior que enviou o pacote e posterior que receberá o pacote, assim, se algum pacote for interceptado, só terão acesso a um enlace do caminho. Logo, não há uma conexão direta entre a origem e o destino final das informações enviadas, garantindo que os usuários se tornem anônimos.

Histórico

O Projeto Tor surgiu da união entre dois centros de pesquisa militares, o Laboratório Central da Marinha para Segurança de Computadores e a Agência de Projetos de Pesquisa Avançada da Defesa, a DARPA (na época sem o 'd', a ARPA ficou conhecida pela criação da precursora da Internet, a ARPANet). A ideia original era proteger as comunicações do governo e dos militares.

A Rede Onion evoluiu e seus objetivos ficaram mais abrangentes, surgindo o Projeto TOR, The Onion Router, que visava a criação da internet invisível, uma área onde qualquer pessoa ou empresa possa navegar em segurança e total anonimato. O projeto acabou caindo no esquecimento, até que a fundação EFF, Electronic Frontier Foundation, um grupo famoso por defender os direitos civis, decidiu abraçar o projeto fornecendo apoio político e financeiro à causa.

Neste trabalho, analisaremos o programa TOR, suas vantagens e desvantagens, além de saber mais sobre as ferramentas que são baseadas neste projeto e como elas interagem.

Por que usar

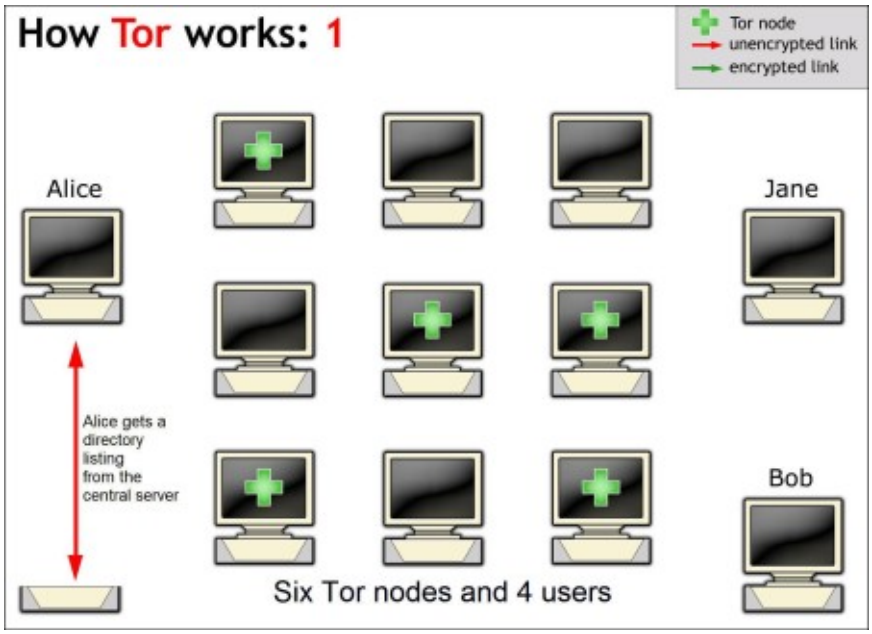
Mesmo antes da Internet, privacidade e liberdade sempre foram motivos de briga, e normalmente figuram entre os primeiros artigos das constituições dos países democráticos. As pessoas desejam poder se expressar sem sofrer opressão, mas desejam também o direito a uma vida privada, isso acontece com a Internet também. Por isso a EFF apoia o Projeto TOR, uma ferramenta que permite que o direito dos internautas de se expressar livremente seja preservado.

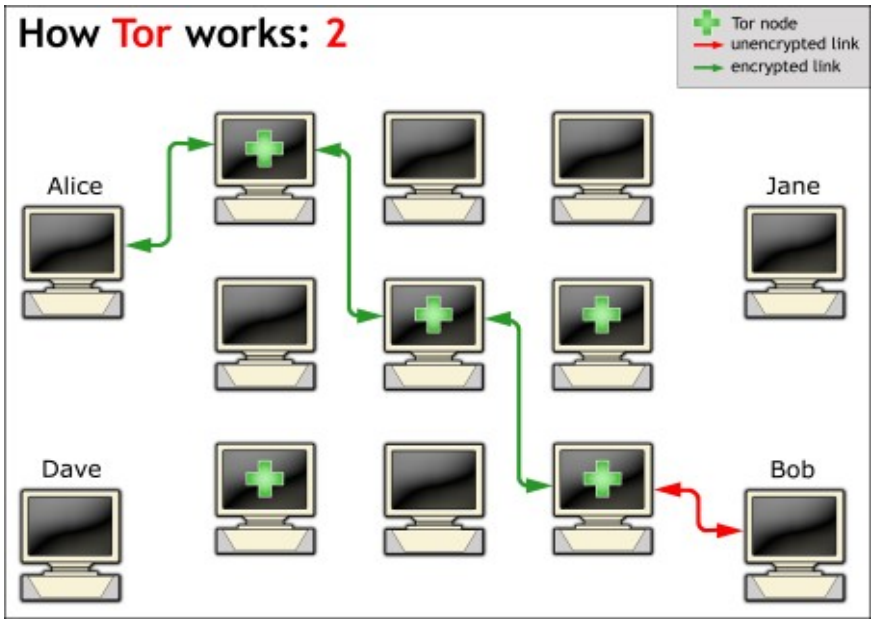
Há muita polêmica em torno do anonimato na internet. Nesta briga há duas frentes muito distintas e bem definidas. Uma que acredita que a liberdade de expressão e a privacidade são direitos que devem ser preservados a qualquer custo (inclusive e principalmente na internet). A outra acredita que essa liberdade ocasionará numa alta de crimes ciberneticos. Na primeira frente, temos grupos de peso, como a fundação EFF, o grupo ativista Human Rights Watch, que defendem o anonimato usado para o bem, como a preservação dos usuários da internet, protegendo suas informações pessoais e a segurança de jornalistas, militares, policiais, ativistas políticos, além da população de países que ainda possuem governos repressores. Já os que são contra, defendem que o anonimato seria utilizado, principalmente, por pedófilos, terroristas entre outros, e que serviria apenas para dificultar o trabalho do governo.

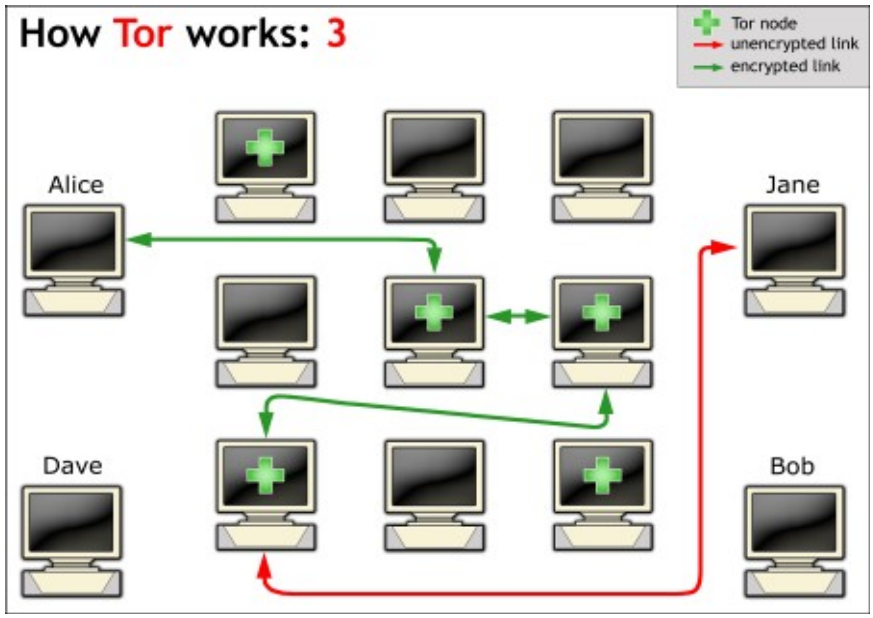
Nesta discussão não há vencedores, há apenas dois lados de uma mesma moeda, que pode ser usada para o bem ou para o mal(sejam lá quais forem), dependendo das intenções de quem a utiliza, já que esta tecnologia é aberta para qualquer pessoa que queira utilizá-la.

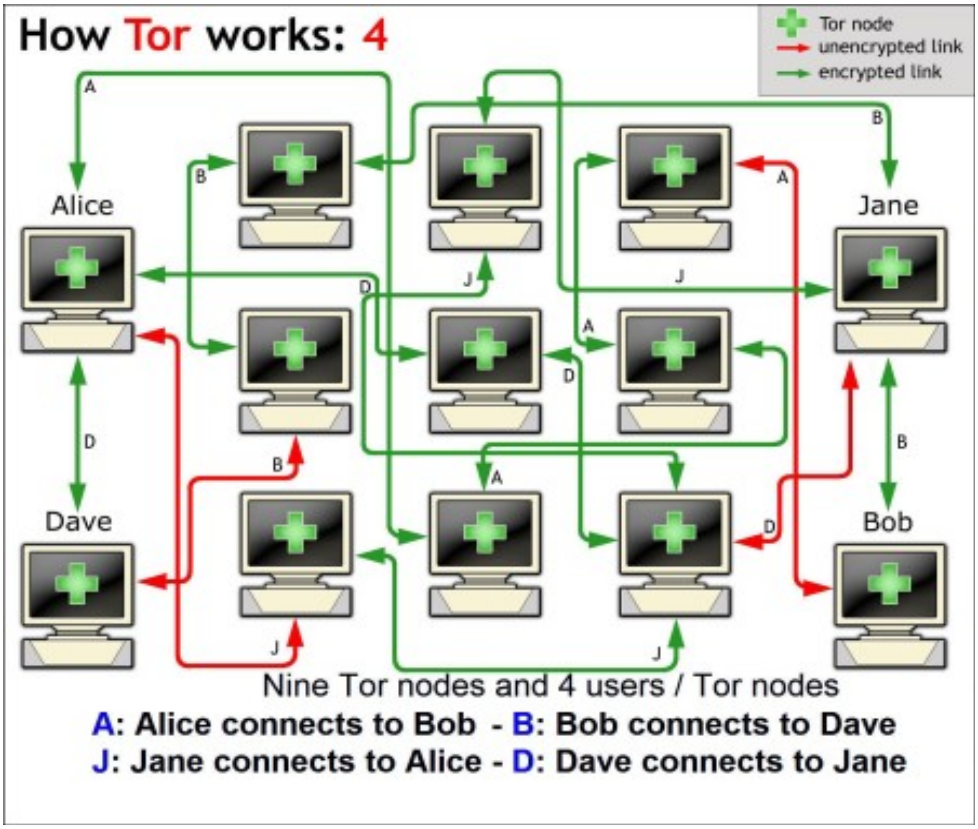
Entenda

Tor remove informações dos pacotes de dados e cria uma rota alternativa e aleatória para o envio das informações, impedindo o rastreamento e interceptação das informações. Essa rota se altera permanentemente, através de diversos servidores voluntários (relays) que cobrem a rota. Estes servidores intermediários não conhecem toda a rota que o pacote percorrerá, apenas o enlace ao qual está diretamente ligado. Com isso, é possível proteger o conteúdo de e-mails, textos de softwares de mensagens instantâneas, IRC e outros aplicativos que usam o protocolo TCP, além de permitir que acesse sites que foram bloqueados pelos administradores da sua rede.


How Tor works: 1
Tor node
unencrypted link
encrypted link
Alice
Jane
Bob
Alice gets a directory listing from the central server
Six Tor nodes and 4 users


How Tor works: 2
Tor node
unencrypted link
encrypted link
Alice
Jane
Dave
Bob


How Tor works: 3
Tor node
unencrypted link
encrypted link
Alice
Jane
Dave
Bob



Instale/Use

No site, temos quatro diferentes pacotes:

- TOR Browser Bundle – é um pacote completo que não requer instalação, é só extrair e executar
- Vidalia Bundle - contém o Tor, Vidalia, Privoxy e Torbutton para instalação. Requer o Firefox e algumas configurações
- Bridge-by-Default Vidalia Bundle - é um pacote Vidalia Bundle com ferramentas adicionais que permitem que pessoas censuradas usem a rede TOR
- Expert Package – contém apenas o TOR, exige que configure o TOR e todos os seus aplicativos manualmente.

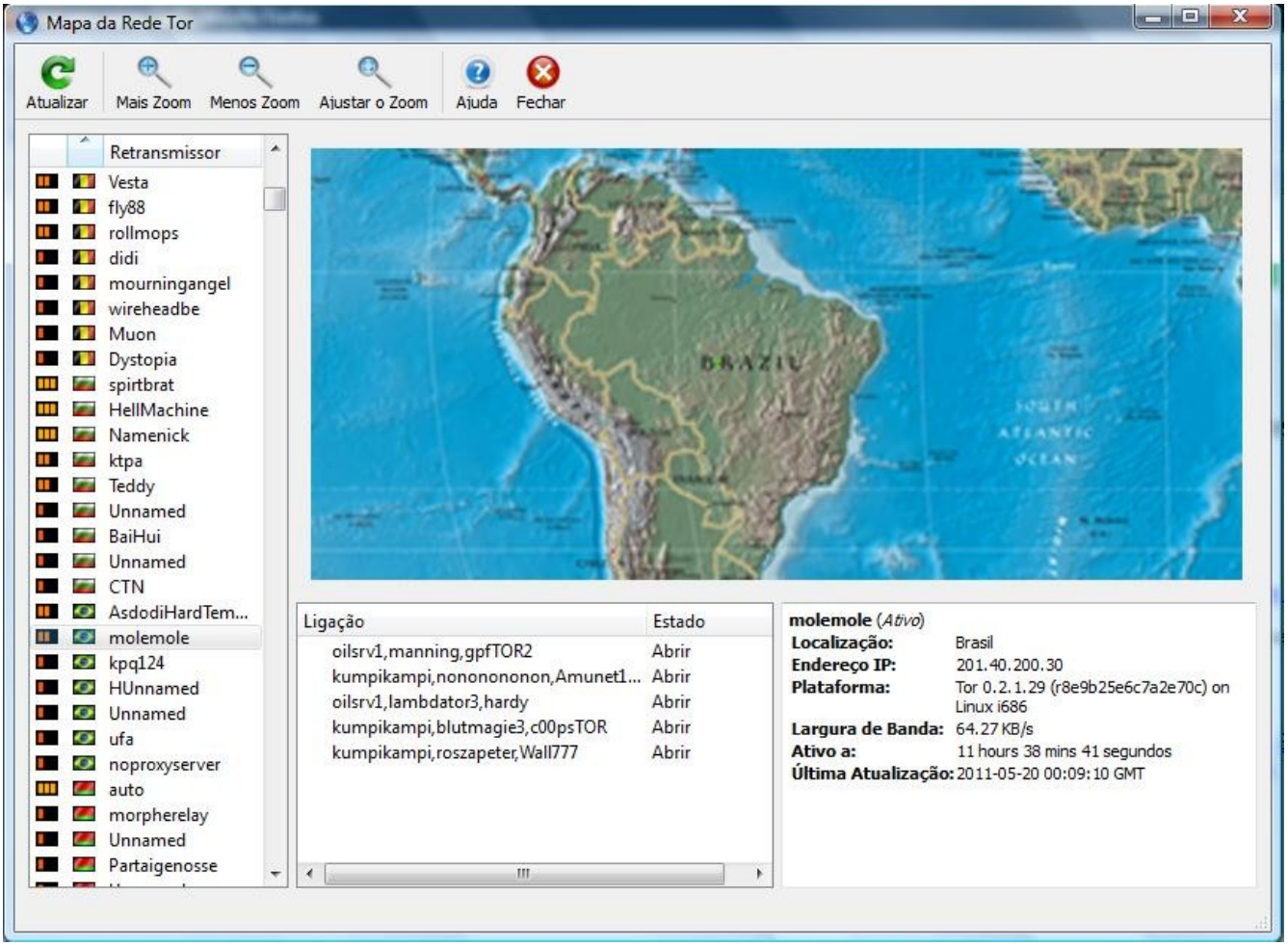
NUNCA UTILIZE O TOR NO WINDOWS!!!

Devido aos caminhos randômicos e as encriptações, a navegação através da rede Tor é bem mais lenta do que usando os navegadores comuns pela rede Internet. Além disso, para aumentar a segurança durante a navegação, o navegador TOR não salva cookies ou histórico da navegação, o que gera um atraso ainda maior.

Através da interface gráfica, Vidalia, podemos ver a rede que está disponível no momento. Na ilustração 2, vemos que no momento que foi feita a imagem havia sete

servidores brasileiros. Podemos, também, acompanhar a banda que está sendo utilizada, além de podermos configurar a rede.

Se decidir utilizar o ‘Expert Package’, que contém apenas o TOR, é necessário configurar os aplicativos para ficar anônimo. Para uso com navegadores, é necessário o uso de um Proxy HTTP que “converse” com o TOR, já que o TOR é Proxy SOCKS, não HTTP. Além disso, é necessário inserir o IP e a porta do Proxy nas configurações do navegador. No Mozilla Firefox, o uso de extensões como o FoxyProxy facilitam o uso do sistema: com ele, o usuário pode criar perfis de configuração, permitindo a mudança dos parâmetros durante a navegação. Ou seja, é possível habilitar ou desabilitar o uso do TOR no navegador com apenas um clique, sem ter que fechar ou abrir o navegador.



Mapa da rede Tor; os relays disponíveis para conexão estão do lado esquerdo

1. Servidor Tor:

   Quanto mais voluntários mantiverem servidores tor, mais rápido sera a conexão através da rede tor. No site do projeto Tor tem tutoriais que dao o passo a passo para configurar um servidor tor, é possível instalar o servidor em vários sistemas

operacionais. Os mais indicados são Linux.

2. TOR Browser Bundle:

   Este pacote pode ser usado em todos os sistemas citados a cima ou rodar direto de um Pendrive, já que ele não precisa ser instalado. O pacote vem com um navegador pré-configurado, e um cliente de mensagens instantâneas e bate-papo que utilizam o TOR.

   Este pacote é muito simples de utilizar, após baixar o executável no próprio site do Projeto TOR, execute o programa como administrador e escolha o local onde ele será armazenado de acordo com a sua preferencia, pode ser em PC ou em um Pendrive.

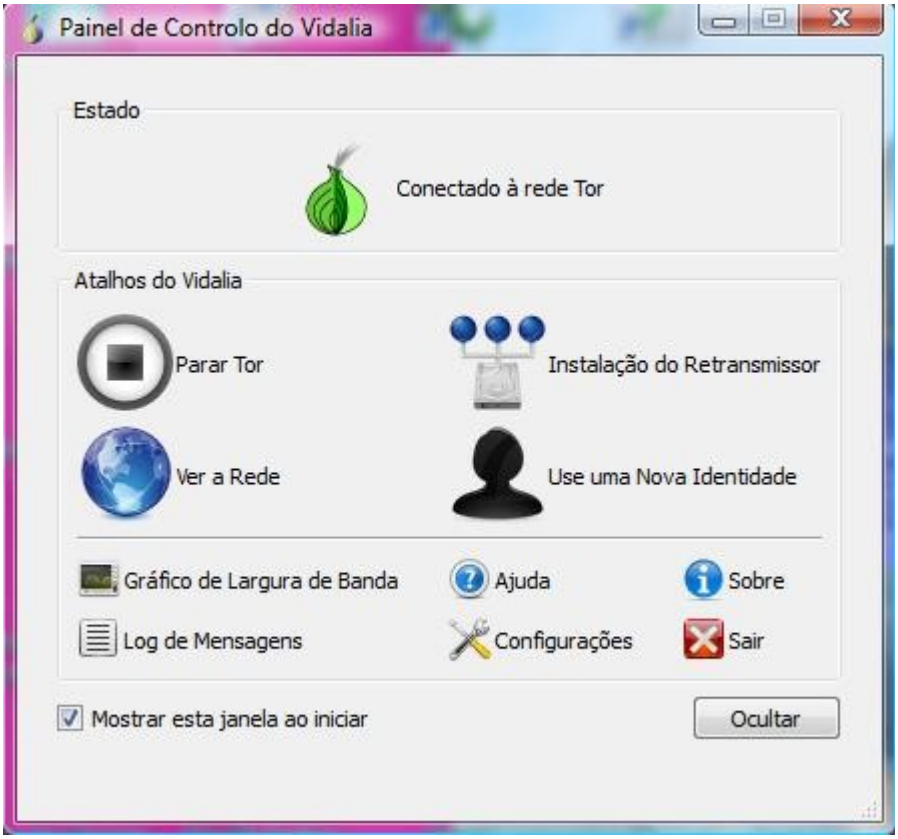
   Assim que a extração dos arquivos estiver completa, clique em 'Start TOR Browser' para iniciar a interface gráfica do TOR, o Vidalia. Através do Vidalia, iniciamos e paramos o TOR, podemos ver a banda consumida, os servidores ativos e suas conexões, além de proporcionar ao usuário uma maneira simples de configurar a rede TOR e um grande sistema de ajuda.

   Assim que estiver conectado a rede TOR, uma janela do Firefox será aberta automaticamente, somente os sites acessados via este navegador estará anônimo, os outros navegadores que você possa abrir não serão afetados. É indicado que todas as janelas de navegação que estavam sendo usadas antes sejam fechadas antes de executar o Vidalia, para evitar confusões. É sugerido também que ao se conectar, verifique no canto direito da pagina se o TOR está habilitado.

   Outra maneira de verificar se o TOR esta realmente sendo usado é acessar o site https://check.torproject.org/, ele informa se o navegador esta usando a rede Tor e qual o seu IP.

   Se desejar utilizar o aplicativo de mensagens instantâneas, basta instalar também o pacote 'TOR IM Browser Bundle' que contém o Pidgin, um cliente de mensagens instantâneas.

   Após utilizar, basta fechar a janela do Firefox e sair do Pidgin.



Vidalia, a interface gráfica do Tor

Curiosidades

Por que cebola?

O Nome *onion*, ou cebola, remete ao modo de transmissão dos pacotes de dados pela rede TOR, chamado de *onion routing* ("roteamento cebola"). O cliente TOR que esta enviando a mensagem seleciona um caminho de roteadores na rede e encripta a mensagem diversas vezes (usando encriptação assimétrica) e, a cada servidor, o pacote recebido (a cebola) é desencriptada, ou seja, uma camada do pacote é retirada, como uma cebola sendo descascada, e um novo caminho randômico pode ser escolhido. Assim apenas o remetente, o ultimo servidor e o receptor veem a mensagem original.

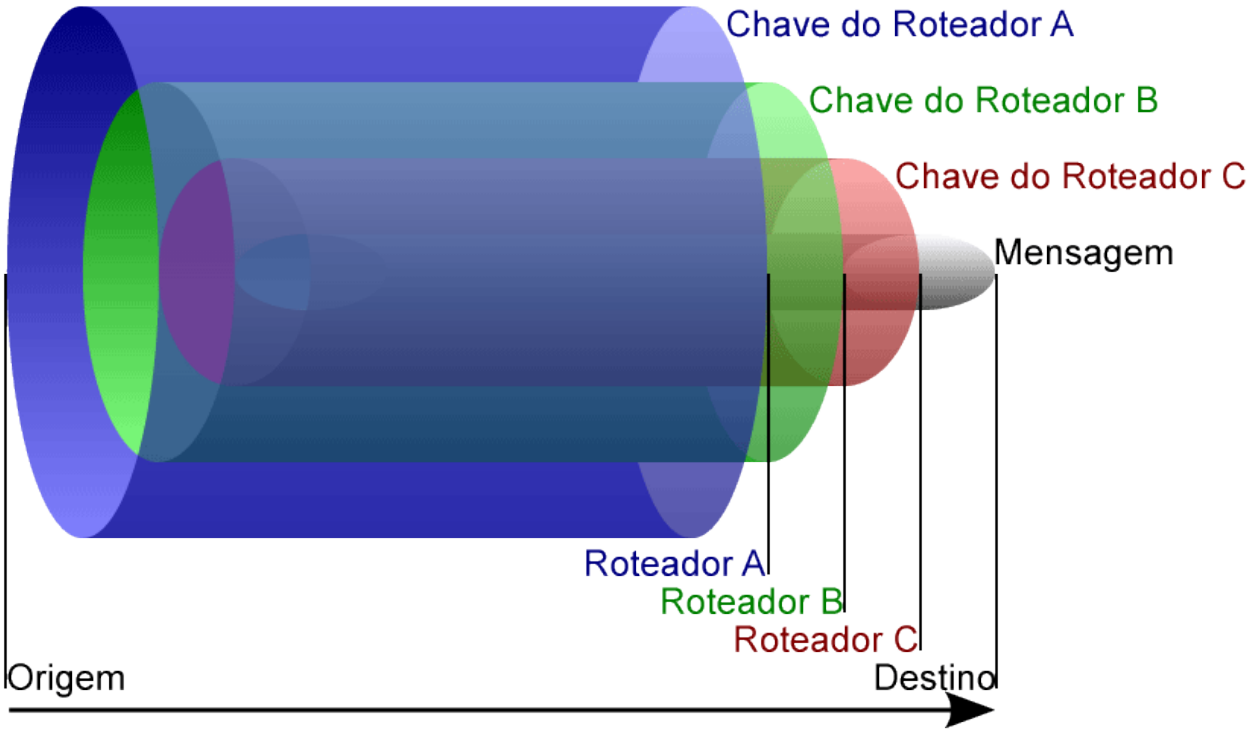


Diagrama do onion routing

Tor e a Política

Jacob Appelbaum, funcionario do Tor e voluntario do Wikileaks, rodava o mundo ensinando a ativistas, politicos e espiões a como usar o Tor e não serem rastreados pelos governos repressores. Em suas palavras: "O importante para mim é que as pessoas tenham comunicação livre de vigilância. O Tor não deveria ser considerado subversivo, mas sim uma necessidade. Qualquer pessoa em qualquer lugar deveria poder falar, ler e formar suas próprias crenças sem ser monitorada. As coisas tinham de chegar a um ponto no qual o Tor não é uma ameaça, e sim utilizado por todos os níveis da sociedade. Quando isso acontecer, venceremos". Uma das facetas do Jacob para 'traficar' o Tor é uma moeda de cinco centavos
que ao ser jogada no chão se abre e revela um cartão de memória Micro SD com uma cópia do Tor. (é ladrão, tem países que usar o TOR é crime!)

Fatos marcantes que ocorreram graças ao Tor:

- Um suspeito membro de alto escalão do exército iraniano utilizou o Tor para vazar informações sobre o aparato de censura de Teerã.
- Um blogueiro tunisiano exilado na Holanda usa o Tor para burlar a censura

estatal.

- Durante as Olimpíadas de Pequim, protestantes chineses usaram o Tor para esconder suas identidades do governo.
- O WikiLeaks roda no Tor, o que ajuda a preservar o anonimato de seus informantes. Nas palavras do fundador Julian Assange da Wikileaks: "Não dá para subestimar a importância do Tor para o WikiLeaks".

Conclusão

Como diria Melvin Kranzberg, historiador norte-americano, *"A tecnologia não é boa, nem má; mas também não é neutra"* (in "A Revolução da Tecnologia da Informação", Manuel Castells): tudo depende do uso que o ser humano dará à tecnologia desenvolvida.

TOR é uma tecnologia aberta, e como tal está disponível para toda e qualquer implementação e alteração e seus desenvolvedores têm ciência dos riscos que esse inovador projeto pode trazer. É inevitável que seu uso logo acabará servindo às conveniências e interesses de cada um, tanto habitantes de países com governos ditatoriais, quanto pedófilos e cibercriminosos, porém isso não reduz a importância desse sistema que protege o direito à privacidade e à liberdade de expressão de seus usuários.

Dicas

- não utilize o tor para acessar suas contas pessoais de e-mail ou facebook

- não utilize o tor para acessar sua conta do banco

- sempre verifique se ele está atualizado

- sempre verefique o blog do desenvolvedor e acompanhe as noticias
https://blog.torproject.org/

BUSCADORES

Você consegue se lembrar dos assuntos que você pesquisou a dois anos atraz? Quais são as suas maiores curosidades, interesses e gostos? Lembra-se de quantas vezes você já pesquisou no google formas de se fazer bombas, como se defender de armas menos letais ou táticas de Black Bloc. Todos estes tipos de informações mais a pirataria que você já pesquisou no google, está sendo contabilizada em um enorme histórico relacionado ao seu ip, contas de e-mails e redes sociais nos servidores da empresa google, e claro, se o estado/policia quiser tais informações, elas serão repassadas, sem burocracia nenhuma, tendo como garantia acordos internacionais. Nos é ensinado desde de criança, quando começamos a aprender a navegar na internet, de que o google sempre nos ajudará a encontrar sites sobre assuntos de nossos interesses e necessidades. Desde crianças (graças a maldita incerção digital precoce) alimentamos os servidores desta empresa. O google te conhece melhor do que a sua mãe, e até melhor do que você mesmo.

A única saída é parar de alimentar este monstro, da mesma forma o yahoo, bing e companhia. Existem outras ferramentas de pesquisa que tem como maior compromisso criptografar suas pesquisas e NÃO gravar nenhum historico sobre você, suas pesquisas e seu IP. E por não gravar nenhum histórico sobre ti, nem mesmo em uma invasão do

estado/policia aos servidores físicos de tais buscadores, nada será encontrado sobre você. As ferramentas são:
-Duck Duck Go

https://duckduckgo.com/
Antes do vazamento do escândalo da vigilância do PRISM, era apenas um bebê. Mas quando o mundo ficou sabendo do PRISM e o "acesso direto" do governo dos EUA a servidores de empresas como o Google, o tráfego de usuários subiu. O DuckDuckGo, afinal, é um mecanismo de busca que promete não rastrear os usuários e ainda oferece anonimidade total. E seus resultados são muito bons!
Ah sim, e o Google compartilha seus dados com o governo dos Estados Unidos sem o seu conhecimento nem consenso.

Se isso parece algo que você gostaria de fazer parte, então comece a fazer buscas no DuckDuckGo. Como ele usa cerca de 50 fontes, você vai conseguir resultados similares aos oferecidos pelo Google. O DuckDuckGo é ainda melhor que mecanismos tradicionais de busca em alguns pontos; ele combina resultados, remove links irrelevantes e spam para que sua busca mostre conteúdo relevante. Além disso, uma opção de busca anônima usa o Tor para rotear sua pesquisa por uma série de camadas criptografadas.

Existem algumas ausências notáveis, como a falta de recurso de autocompletar. E como mecanismo geral de busca, o DuckDuckGo não vai oferecer resultados precisos como se você usar um recurso vertical como Amazon, Facebook ou YouTube. Mas não se preocupe: o DuckDuckGo sabe disso e tem uma solução chamada Bang. Você pode

redirecionar sua busca para sites específicos ao adicionar códigos como “!amazon” “! facebook” “!yt” e mais. Você pode até fazer isso no Google: adicione “!g” e o DuckDuckGo fará uma busca criptografada (leia: anônima) no Google para você.

Então este é o DuckDuckGo. Se você já ouviu falar nele, mas não testou ainda, dê uma chance. Se nunca ouviu, seja bem-vindo. Eis a sua chance de manter seus dados longe de espionagem e publicidade ao mesmo tempo que consegue fazer boas buscas.

-Startpage

Outra ferramenta de pesquisas é a Startpage https://startpage.com/
StartPage não armazena seu endereço de IP, não utiliza cookies de rastreamento, ou faz um registro de suas pesquisas. Não guarda qualquer informação sobre as pessoas que fazem buscas através StartPage ou o que procuram. StartPage protege você de vigilância da NSA e espionagem. Sua sessão de pesquisa com StartPage é protegido por criptografia SSL poderosa para que ninguém - nem hackers e nem mesmo do governo federal - podem espionar suas pesquisas. StartPage lhe dá 100% real os resultados do Google em total privacidade. Quando você busca com Startpage, são removidas todas as informações de identificação de sua consulta e o submete anonimamente para o Google por você. Recebem os resultados e os devolvem para você em total privacidade. StartPage é uma empresa holandesa, por isso não está sob a jurisdição dos EUA. Estando sediada na Holanda, os programas de coleta de dados dos EUA, como PRISM, o Patriot Act, tribunais FISA, etc não se aplicam diretamente. StartPage oferece um proxy livre com todas as pesquisas. Com este proxy, não só você pode procurar em particular, mas você pode ver as páginas que você encontrar através StartPage anonimamente e em completa segurança.

CRIPTOGRAFIA

A criptografia é o método de codificar mensagens de modo a garantir que só a pessoa que tenha em mãos o código correto possa lê-la. Em resumo, ela serve para proteger informações, preservar a privacidade das pessoas e permitir a autenticidade de informações (assinatura digital).

Proteger informações significa que você pode escolher quem acessa suas informações. Preservar a privacidade das pessoas quer dizer que quem não estiver autorizado a acessar suas informações não conseguirá decifrá-las. Permitir a autenticidade de informações evita que falem em seu nome coisas que você não disse.

Criptografia (Do Grego kryptós, "escondido", e gráphein, "escrita") é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta"), o que a torna difícil de ser lida por alguém não autorizado. Assim sendo, só o receptor da mensagem pode ler a informação com facilidade. É um ramo da Matemática, parte da Criptologia. Cifragem é o processo de conversão de um texto claro para um código cifrado e decifragem é o processo contrário, de recuperar o texto original a partir de um texto cifrado. De fato, o estudo da criptografia cobre bem mais do que apenas cifragem e decifragem. É um ramo especializado da teoria da informação com muitas contribuições de outros campos da matemática e do conhecimento, incluindo autores como Maquiavel, Sun Tzu e Karl von Clausewitz. A criptografia moderna é basicamente formada pelo estudo dos algoritmos criptográficos que podem ser implementados em computadores.

Instalando programas de criptografia

Neste tutorial ensinamos apenas como utilizar o programa GNU Privacy Guard, que é uma ferramenta de criptografia inteiramente baseada em software livre. Aqui trataremos o uso do GPG no modo texto e no modo gráfico.

Instalando o GPG

Existem duas opções para usar o GPG: modo texto, onde você digita os comandos manualmente, e o modo gráfico, mais intuitivo e recomendado para quem ainda não tem familiaridade com criptografia.

Todos os programas para o Modo Gráfico são na verdade extensões do GPG em modo texto, o que significa que todos os programas de criptografia aqui listados sempre vão utilizar o mesmo chaveiro, ou seja, tanto seu(s) gerenciador(es) de chaveiro como seu(s)

programa(s) de email utilizarão sempre as mesmas informações de chave pública e privada.

Modo Texto no GNU/Linux

Se você usa GNU/Linux ou outro *NIX (BSD like, etc), provavelmente sua distribuição deve ter um pacote do GPG. A instalação do mesmo depende de qual distribuição de linux você usa. Aqui ensinaremos como instalar nas distribuições mais populares.

Se você usa o Indymix, todos os programas de criptografia que você necessita já estão instalados e você pode pular para a próxima seção!

Se o seu Linux é o Debian ou compatível (como Kurumin, Knoppix ou Gnoppix), entre na internet, abra um terminal e digite o comando para instalar o GPG:

```
su -c "apt-get update ; apt-get install gnupg"
```

Se você usa outra distribuição de Linux, procure na documentação específica do seu sistema como fazer isso, ou baixe os fontes do programa e compile.

Modo Gráfico no GNU/Linux

No Linux, nós recomendamos que você use o GPA: GNU Privacy Assistant. Sua instalação depende de qual distribuição de linux você usa. Aqui ensinaremos como instalar nas distribuições mais populares. Se você usa Indymix, todos os programas de criptografia que você necessita já vem instalados e você pode pular para a próxima seção!

Se você usa Debian ou compatível (como Kurumin, Knoppix ou Gnoppix), basta se conectar à internet, abrir um terminal e dar o comando para sua instalação:

```
su -c "apt-get update ; apt-get install gpa"
```

Em seguida, digite a senha de administrador do sistema, caso esta seja pedida.

Para outras distribuições, consulte a documentação correspondente. Ou, se você preferir, baixe o código fonte do GPA e compile-o você mesmo.

Como criar uma chave de criptografia

-Abra seu terminal e digite gpg --gen-key. Aparecerá:

```
linux linux # gpg --gen-key
gpg (GnuPG) 1.4.12; Copyright (C) 2012 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
Your selection? 1
```

Nas primeiras linhas é exibida informações sobre o programa gpg, a versão e a liberdade de redistribuição.

Na parte inferior, escolha a primeira opção (1) RSA and RSA (default) que é a mais comum. Digite o numero da opção (1) e aperte enter.

-Na seguinte opção selecione o tamanho que sua chave terá:

```
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048)
Requested keysize is 4096 bits
```

Escolha entre 1024 e 4096 bits. Quanto menor os bits, menor será o tempo para encriptar uma mensagem, e quanto maior forem os bits, maior será o tempo de emcriptação. 4096 bits é o recomendado, pois os numeros inferiores já podem ser descriptografados.

-Agora escolha por quanto tempo sua chave irá funcionar:

```
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 0
Key does not expire at all
Is this correct? (y/N) y
```

0 = não expira, vai funcionar para sempre.

<n> = a chave expira em n dias

<n>w =a chave expira em n semanas

<n>m =a chave expira em n meses

<n>y =a chave expira em n anos

Se você escolhar alguma opção em que a chave deverá expirar, por explo em algumas semanas, escolha a opção <n>m, mas no lugar da letra n, cocloque o numero de semanas desejadas, como 6m, ou 20m. Depois q a chave expirar, não funcionará mais a encriptação e descriptação, assim você deverá fazer outra chave. Criar chaves que expiram em n tempo pode se tornar uma dor de cabeça se você não estiver bem organizado, pois mensagens podem ser perdidas e quando você fazer uma nova chave, terá que avisar a todos os contatos que possuiam a sua chave antiga que ela expirou e que você repassará outra.

A melhor escolha é a escolha 0 pois não expirará. Mas escolha qual responder melhor seus critérios e necessidades.

Depois de escrever o a opção desejada, aparte enter e confirme com a letra y (sim) ou corrija com n (no) e aparte enter.

-Segue-se então:

```
You need a user ID to identify your key; the software constructs the user ID
from the Real Name, Comment and Email Address in this form:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: terror
Email address: contatoterror@riseup.net
Comment:
```

Agora você vai precisar disponibilizar seu nome, seu e-mail e algum comentário, pois a chave que estas prestes a criar precisas se basear nestas informações.

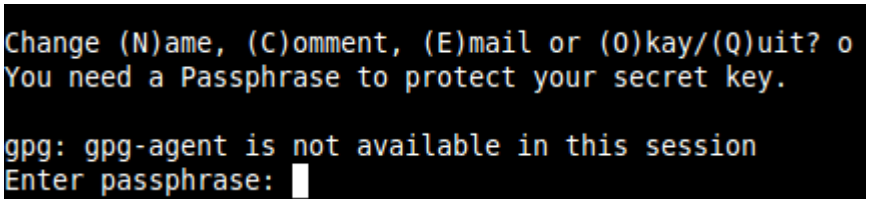
Em Real name coloque seu nome, pode ser seu nome de verdade, ou apelido, nome de guerra... o que for, lembre-se de qual será a funcionalidade desta chave, se é uma chave pessoal ou pra ativismo, não crie provas contra si mesmo.

Em Email segue-se a mesma dica.

Em Comment você pode colocar um comentário, ou simplesmente deixar em branco.

No exemplo à cima, colocamos o nome e o e-mail do site.

-Agora confirme e crie uma senha:

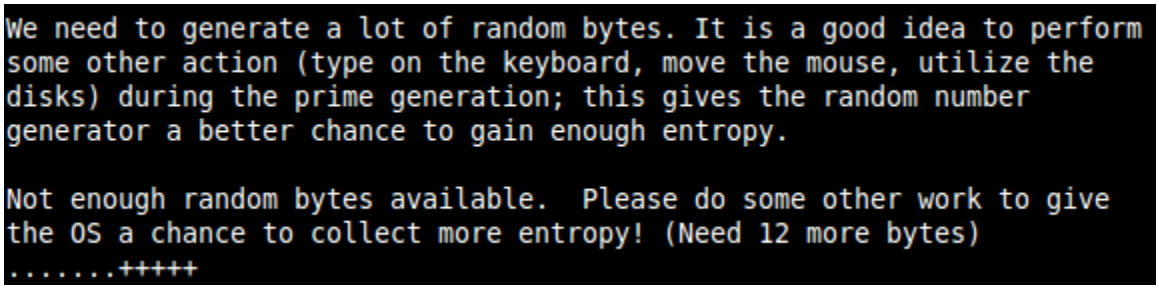


Se precisar mudar algo, (N) para nome, (C) para comentário, (E) para mudar o e-mail ou (O) para confirmar seus dados. Ah, e (Q) pra cancelar tudo-não faça isso!

Em seguida você deverá criar uma senha para ter acesso a suas chaves, pois somente com essa senha será possível encriptar e descriptar suas mensagens, se você perder a senha, já era, não terá acesso as informações secretas, a chave não servirá de nada. Crie uma boa senha, e não seja burro de escreve-la na sua agenda!

Em seguida será solicitado que você repita a senha para confirmar!

-Agora o gpg estará criando sua chave:



Enquanto o programa esta criando sua chave, você tem que ajuda-lo a gerar muitas informações que o ajude a criar um código único. Isso deve ser feito clicando teclas aleatórias no teclado, abrindo outros programas, mechendo no mouse, etc. Caso você não faça isso, vai demorar ainda mais e será exibida uma mensagem com a inferior do a da imagem a cima, pedindo que você ajude executando as tarefas já mensionadas.

-Firmeza, chave pronta:

No caso deste exemplo,

*pub 4096R/87D6666B 2013-10-23

é a nossa chave pública, a chave que será distribuida para as pessoas poderem mandar mensagens criptografadas para nós. Pub de público, os primeiros números 2048R é o tamanho e o tipo de nossa chave, 87D6666B é o numero de nossa chave pública, que será passada para as pessoas que irão nos mandar mensagens criptografadas, e os ultimos numeros 2013-10-23 é o data em que a chave foi criada.

*Key fingerprint = 6666 32CD 37C8 8BB2 28C5 4C7A FC18 D4D3 87DD E96B

é a impressão digital de nossa chave.

*uid terror <contatoterror@riseup.net>

é o nome da pessoa e seu e-mail a qual a chave está vinculada.

*sub 4096R/A866661F9 2013-10-23

Sub é a subchaves. Ela é uma outra chave que vai junto com a principal. É utilizada para assinatura de criptografia.

Como compartilhar sua chave pública

Existem basicamente dois métodos para que você transmita sua chave pública:

-Você enviar sua chave para uma pessoa (por email, disquete, cd, etc.).

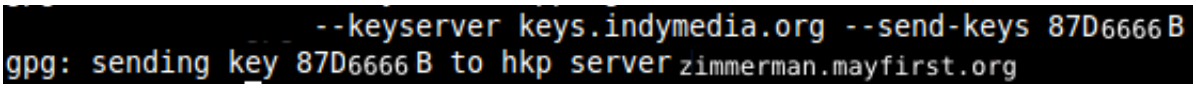
-Você enviar sua chave pública para um servidor e cada pessoa que quiser usá-la baixa a chave do servidor.

Enviar sua chave para um servidor é o meio mais cômodo de compartilhar sua chave com as pessoas que vão enviar mensagens criptografadas para você. Dessa forma você não precisa ficar mandando suas chave pública pra todo mundo. O servidor de chaves públicas é um site onde as pessoas que queiram te enviar um e-mail criptografado, poderão pesquisar seu e-mail ou nome para descobrir qual é o código de sua chave

publica. Utilizaremos no exemplo o servidor http://zimmerman.mayfirst.org/.

Para mandar sua chave para um servidor de chaves, use o comando

gpg --keyserver keys.indymedia.org --send-keys sua chave publica



no nosso caso colocamos nossa chave no final do comando. Pronto, sua chave está lá no servidor do indymedia.

Se você não souber sob quais nomes suas chaves públicas estão registradas, liste-as com o comando

gpg --list-keys

É importante observar que você pode exportar qualquer chave pública do seu chaveiro, que não precisa ser necessariamente sua.

Como adicionar uma chave pública de alguém na sua lista

Para importar uma chave pública de um servidor, você precisa saber qual é o servidor e qual é o ID da chave. Com isso em mãos, basta digitar

gpg --keyserver servidor.de.chaves --recv-keys id-da-chave

que a chave pública será importada. Por exemplo, se o servidor que você estiver usando for o keys.indymedia.org, e o ID da chave for B9A88F6F, seu comando será

gpg --keyserver keys.indymedia.org --recv-keys B9A88F6F

Se você não tiver o ID da chave que você quer adicionar, primeiro faça uma busca no servidor de chaves. Por exemplo, se eu quiser saber qual é o ID da chave do do blog terror, basta que eu dê o comando

gpg --keyserver keys.indymedia.org --search-keys contatoterror@riseup.net

A saída provável será

```
             gpg --keyserver zimmerman.mayfirst.org --search-keys contatoterror@riseup.net
gpg: searching for "contatoterror@riseup.net" from hkp server zimmerman.mayfirst.org
(1)     terror <contatoterror@riseup.net>
          4096 bit RSA key 87D6666B, created: 2013-10-23
Keys 1-1 of 1 for "contatoterror@riseup.net".  Enter number(s), N)ext, or Q)uit > 1
```

será listada as chaves registradas com o e-mail procurado que estiverem no servidor utilizado. Digite o numero do resultado que você procura e aperte enter, nesse caso, o e-mail procurado foi o resultado (1):

```
gpg: requesting key 87D6666B from hkp server zimmerman.mayfirst.org
gpg: key 87D6666B: "terror <contatoterror@riseup.net>" not changed
gpg: Total number processed: 1
gpg:              unchanged: 1
```

assim você obtém a chave publica de terror, que aparece na segunda linha.

Aí é só adicionar a chave, usando o comando

gpg --zimmerman.mayfirst.org --recv-keys Numero da chave

Você poderia, ao invés de procurar pelo email do terror, procurar apenas pelo nome , usando o comando

gpg -- zimmerman.mayfirst.org --search-keys terror

É importante ressaltar que você só encontrará a chave desejada desde que a pessoa que você procura deixou a chave naquele servidor.

Listando seu chaveiro

Você pode ver todas as chaves do seu chaveiro - incluindo seu par de chaves pública e privada - digitando

gpg --list-keys

A saída é algo do tipo

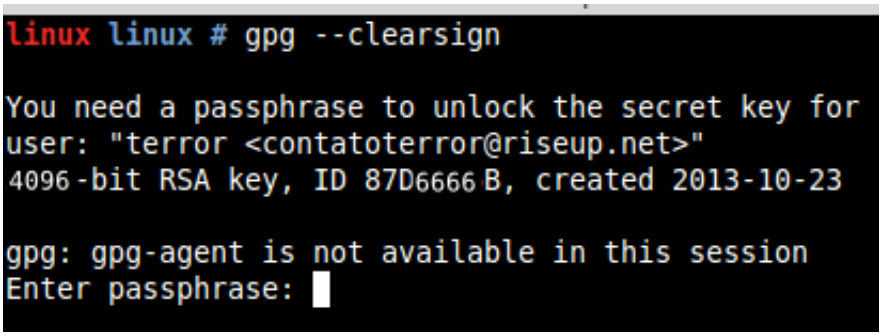
/users/alice/.gnupg/pubring.gpg
---
pub 1024D/BB7576AC 1999-06-04 Alice (Judge) <alice@cyb.org>
sub 1024g/78E9A8FA 1999-06-04

Como criptografar mensagens e arquivos

Existem muitas maneiras de criptografar mensagens ou arquivos. A primeira delas

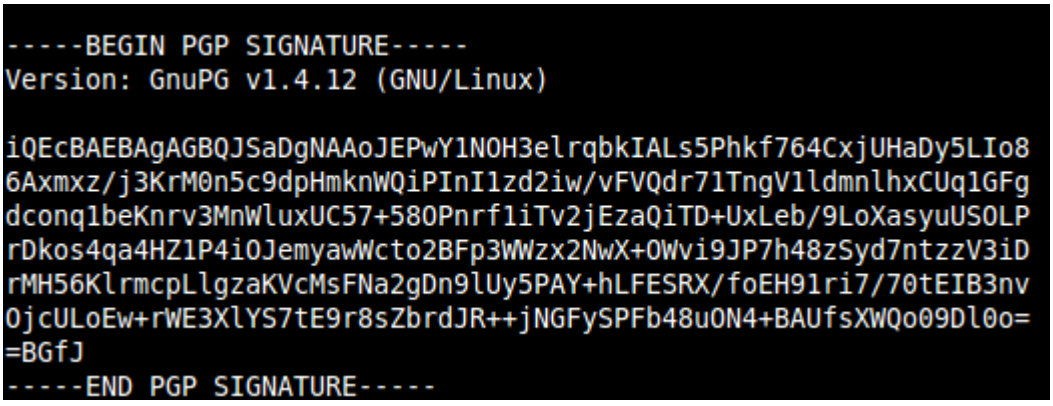
consiste em entrar no GPG para escrever sua mensagem. No seu terminal, digite:

gpg –clearsign



E entre com sua senha. A opção clerasign pede ao GPG para que ele crie uma criptografia utilizando texto comum, isto é, codificado em caracteres ASCII (legíveis ao usuário). Não sabe o que é ASCII ou texto comum? Então veja uma nota aqui.

Depois de entrar com sua senha, o GPG estará esperando para que você escreva sua mensagem. Escreva sua mensagem - "Testando essa parada", por exemplo - e após escrevê-la, pule uma linha e digite simultaneamente as teclas Ctrl e D do seu teclado. Isso fará com que o GPG crie uma assinatura da sua mensagem. O resultado deve ser algo do tipo:



Certo. Assinei minha mensagem. E agora, o que faço com isso? Bom, se você quiser mandá-la pra alguém, copie e cole todo esse texto, desde o `-----BEGIN PGP SIGNED MESSAGE-----` até o `-----END PGP SIGNATURE-----` e cole no corpo da sua mensagem de email. Se o destinatário tiver sua chave pública, ele poderá facilmente verificar se a assinatura confere. Mas caso você queira guardar essa mensagem assinada, basta copiar

tudo e colar num arquivo.

'"ATENÇÃO:"' se porventura você alterar essa mensagem, sua respectiva assinatura perderá seu valor. Se você quiser alterar a mensagem, faça e depois assine novamente.

Vejamos agora uma segunda maneira de assinar mensagens. Escreva seu texto num arquivo, por exemplo no texto.txt. Em seguida, digite no seu terminal:

```
gpg --clearsign texto.txt
```

Depois de entrar com sua senha, o GPG escreverá a mensagem assinada no arquivo texto.txt.asc. Com esse procedimento é possível assinar qualquer tipo de arquivo, e o formato da mensagem assinada será em texto simples (ASCII). Para criar uma assinatura separada da mensagem - a mensagem no arquivo texto.txt e apenas a assinatura no arquivo arquivo.txt.asc - é só digitar:

```
gpg -a --detach-sig texto.txt
```

As mensagens e assinaturas armazenadas em texto simples ocupam mais espaço do que se estivessem no formato "binário". Se você quiser guardar a assinatura num formato binário, que é pouco amigável para ser visualizada num editor de textos mas que ocupa pouco espaço - basta digitar

```
gpg --sign texto.txt
```

E a mensagem assinada estará no arquivo texto.txt.gpg. Além de assinar, a opção sign compacta a mensagem, ocupando menos espaço ainda. Essa forma de assinar não é boa para trocar mensagens com outras pessoas, já que não está num formato legível. Prefira sempre a opção clearsign.

Como verificar mensagens assinadas

Uma vez que você tenha recebido uma mensagem ou arquivo assinado, você terá de verificar se a assinatura está correta. Existem várias maneiras de fazer isso.

A maneira mais simples é a que se segue: você recebeu uma mensagem como essa:

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Alow!
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.2.3 (GNU/Linux)

iD8DBQFAMU1TvSy1nGtWZ3cRAtz2AJ41a1dGqGwb0wT+kz4WoFq9/4+RoQCfZH29
0gPrLalgr5OrC4gC9LahbOw=
=d2qf
-----END PGP SIGNATURE-----
```

Para verificar essa assinatura, copie todo esse texto, desde o "'-----BEGIN PGP SIGNED MESSAGE-----'" até o "'-----END PGP SIGNATURE-----'", digite, no seu terminal

```
gpg
```

depois, cole todo o texto e em seguida digite simultaneamente as teclas Ctrl e D do seu teclado. Se tudo der certo, o GPG detectará que trata-se de uma mensagem assinada e verificará sua validade. No caso da mensagem acima, termos:

```
gpg: Assinatura feita em Seg 16 Fev 2004 20:08:03 BRT usando DSA, ID da chave 123666XXX
gpg: Assinatura correta de jhon123
```

Se você recebeu uma mensagem assinada num arquivo, por exemplo o mensagem.txt.asc, basta digitar

```
gpg --verify mensagem.txt.asc
```

Que a assinatura será verificada. Se você recebeu uma mensagem com a assinatura num arquivo separado - mensagem.txt e mensagem.txt.asc, por exemplo - digite

```
gpg --verify mensagem.txt.asc mensagem.txt
```

Como codificar uma mensagem para alguém

Assim como para assinar mensagens, existem várias maneiras de se criptografar uma mensagem. A primeira delas consiste em digital sua mensagem no próprio gpg. Vamos lá. No terminal, digite:

```
gpg -e -a -r email@da.pessoa
```

E em seguida escreva sua mensagem. Quando terminal, pule uma linha e em seguida digite simultaneamente as teclas Ctrl e D do seu teclado. O GPG então fornecerá a mensagem codificada para o usuário cujo email é email@daSTOPSPAM.pessoa. Agora é só copiar todo o texto, desde `-----BEGIN PGP MESSAGE-----` até `-----END PGP MESSAGE-----` e colar no seu email ou arquivo!

Para uma encriptar e compactar um arquivo, digite:

```
gpg -r nome-do-usuário -e mensagem.txt
```

O arquivo de saída será `mensagem.txt.gpg`

Se você quiser apenas encriptar e que o arquivo de saída possa ser enviado por email - texto comum, isto é, codificado em caracteres ASCII (legíveis ao usuário), digite

```
gpg -r nome-do-usuário -e -a mensagem.txt
```

E o arquivo de saída será mensagem.txt.asc

Não sabe o que é ASCII ou texto comum? Então veja uma nota aqui.

Como decodificar uma mensagem que enviaram para você

A maneira mais simples de desencriptar uma mensagem é colá-la diretamente no GPG. Suponha que você tenha recebido a mensagem

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.2.3 (GNU/Linux)

hQEOA3v8xQeh8DSxEAP8DGLGac9OdZzX7KxRqpkaYuJ/8NVN5AyhtQKZwRogZwwZ
19g/teTPQLYwgcCLQoDKxsnX3lBGEzjAGxXme6aqcJetD0sXcULtap99AfpJqIO/
lCDjxFqNRP45Uwnnbafiudhjsdhksdhksdhfudshcf+F/JJL65Q9ROHW08kOB1IM1sD
/RsQu1pqZl/X8PRZyVdLSwpzGpR5uaxA837f+Zl0+1Fh2DhoiE2AxnLXdwlMlRtK
SrpqBdWifULoX46E1+DOd128e24K74d+utMux4uk8t9Lb0D5C8RDfShKHoLJIwul
fhEmtN8bo2Kmg/z8sWnDjW3Ik3opVtsTPNPQQh1J9GV40lUBViB6IzhkXhhNZ4ae
qexbLilOVwJczLa3y3UmwkiXcs92k6thpUCIJjyeRTtpey2LKdVLHLd1o5ti8/or
nqYoq1eXHcVOckmfxH3Uq8ZAEX6bzSKc
=g5JE
-----END PGP MESSAGE-----
```

Tudo que você precisa fazer é digitar

```
gpg
```

no seu terminal e em seguida colar a mensagem. O GPG detectará que trata-se de uma mensagem privada e pedirá pela sua senha, mais ou menos assim:

```
gpg: Vá em frente e digite sua mensagem ...
```

Digite a frase secreta:

Digite sua senha e em seguida pressione simultaneamente as teclas Ctrl e D do seu teclado que a mensagem secreta irá aparecer!

Se alguém lhe enviou uma mensagem.txt.asc, basta dar este comando para desencriptá-la e guardar o texto em mensagem.txt:

```
gpg -d mensagem.txt.asc > mensagem.txt
```


```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.2.3 (GNU/Linux)

hQEOA3v8xQeh8DSxEAP8DGLGac9OdZzX7KxRqpkaYuJ/8NVN5AyhtQKZwRogZwwZ
19g/teTPQLYwgcCLQoDKxsnX3lBGEzjAGxXme6aqcJetD0sXcULtap99AfpJqIO/
lCDjxFqNRP45Uwnnbafiudhjsdhksdhksdhfudshcf+F/JJL65Q9ROHW08kOB1IM1sD
/RsQu1pqZl/X8PRZyVdLSwpzGpR5uaxA837f+Zl0+1Fh2DhoiE2AxnLXdwlMlRtK
SrpqBdWifULoX46E1+DOd128e24K74d+utMux4uk8t9Lb0D5C8RDfShKHoLJIwul
fhEmtN8bo2Kmg/z8sWnDjW3Ik3opVtsTPNPQQh1J9GV40lUBViB6IzhkXhhNZ4ae
qexbLilOVwJczLa3y3UmwkiXcs92k6thpUCIJjyeRTtpey2LKdVLHLd1o5ti8/or
nqYoq1eXHcVOckmfxH3Uq8ZAEX6bzSKc
=g5JE
-----END PGP MESSAGE-----
```

Esse comando funciona tanto para arquivos criptografados em texto simples quanto em formato "binário".

Verificando Impressões Digitais e Assinando Chaves

Conforme você viu na seção O limite da confiabilidade, é possível verificar pela impressão digital da chave pública se ela pertence realmente a quem afirma pertencer.

Suponha que alguém envia uma chave pública e você a adiciona em seu chaveiro. Posteriormente você tem a oportunidade de encontrar ao vivo o suposto dono da chave e ele lhe fornece a impressão digital da chave num papel.

Chegando em casa, você decide verificar se a impressão digital bate com a chave pública. No seu terminal, digite

```
gpg --fingerprint email@da.pessoa
```

onde email@da.pessoa é o email da pessoa que você encontrou. A impressão digital da chave será impressa. Confira se ela é idêntica àquela que você tem anotada. Se elas forem iguais, você pode começar a pensar em assinar essa chave pública. Aqui mostrarei o procedimento de assinar uma chave pública e em seguida reproduzirei um trecho do Guia Foca Linux, que por sua vez foi retirado da lista debian-user-portuguese EM lists.debian.org, que trata de modo muito sério a assinatura de chaves.

Digite no seu terminal:

```
gpg --edit-key email@da.pessoa
```

Aparecerão informações sobre essa chave. Digite

```
sign
```

E digite sua senha. Pronto, a chave estará assinada.

Certo, assinei a chave pública daquela pessoa. E agora, o que faço com isso? Você pode exportar a chave pública dessa pessoa - que será automaticamente exportada com sua assinatura. Você tanto pode exportá-la num arquivo e enviá-la para essa pessoa quanto mandar essa chave assinada para um servidor de chaves.

Suponha que Arrelia assinou a chave de Pasqualin, exportou-a no arquivo pasqualin.asc e enviou-a para Pasqualin. Quando Pasqualin adicionar a chave contida em pasqualin.asc no seu chaveiro, a assinatura feita por Arrelia da chave pública de Pasqualin será automaticamente adicionada ao chaveiro de Pasqualin. Agora, sempre que Pasqualin enviar sua chave pública para alguém, a assinatura de Arrelia sempre estará presente.

Um outro método para o intercâmbio de assinaturas utiliza os servidores de chaves. Por

exemplo, se a chave pública de Pasqualin estiver armazenada no servidor chaves.privacidade.net, basta que Arrelia assine a chave pública de Pasqualin e exporte-a para esse servidor para que o servidor adicione a assinatura de Arrelia na sua cópia da chave pública de Pasqualin. Em seguida, basta que Pasqualin atualize seu chaveiro, de forma que sua própria chave pública seja baixada do servidor chaves.privacidade.net para que a assinatura de Arrelia entre no seu chaveiro.

Aqui segue o texto retirado do Guia Foca Linux:

Trocando assinaturas de chaves digitais
Assinaturas digitais

Chaves digitais e a teia tipo de problema: Ao usuário é dado o poder de "assinar" uma chave digital, dizendo "sim, eu tenho certeza que essa chave é de fulano, e que o e-mail de fulano é esse que está na chave".

Note bem as palavras "certeza", e "e-mail". Ao assinar uma chave digital, você está empenhando sua palavra de honra que o nome do dono de verdade daquela chave é o nome que está na chave, e que o endereço de e-mail daquela chave é da pessoa (o "nome") que também está na chave.

Se todo mundo fizer isso direitinho (ou seja, não sair assinando a chave de qualquer um, só porque a outra pessoa pediu por e-mail, ou numa sala de chat), cria-se a chamada teia de confiança. Numa teia de confiança, você confia na palavra de honra dos outros para tentar verificar se uma chave digital é legítima, ou se é uma "pega-bobo".

Suponha que Marcelo tenha assinado a chave de Cláudia, e que Roberto, que conhece Marcelo pessoalmente e assinou a chave de Marcelo, queira falar com Cláudia. Roberto sabe que Marcelo leu o manual do programa de criptografia, e que ele não é irresponsável. Assim, ele pode confiar na palavra de honra de Marcelo que aquela chave digital da Cláudia é da Cláudia mesmo, e usar a chave pra combinar um encontro com Cláudia. Por outro lado, Roberto não conhece Cláudia (ainda), e não sabe que tipo de pessoa ela é. Assim, rapaz prevenido, ele não confia que Cláudia seja uma pessoa responsável que verifica direitinho antes de assinar chaves. Note que Roberto só confiou na assinatura de Marcelo porque, como ele já tinha assinado a chave de Marcelo, ele sabe que foi Marcelo mesmo quem assinou a chave de Cláudia.

Enrolado? Sim, é um pouco complicado, mas desenhe num papel as flechinhas de quem confia em quem, que você entende rapidinho como funciona. O uso da assinatura

feita por alguém cuja chave você assinou, para validar a chave digital de um terceiro, é um exemplo de uma pequena teia de confiança.

Trocando assinaturas de chaves digitais com um grupo de pessoas

Lembre-se: ao assinar uma chave digital, você está empenhando sua palavra de honra que toda a informação que você assinou naquela chave é verdadeira até onde você pode verificar, e que você tentou verificar direitinho. Pense nisso como um juramento: "Eu juro, em nome da minha reputação profissional e pessoal, que o nome e endereços de e-mail nessa chave são realmente verdadeiros até onde posso verificar, e que fiz uma tentativa real e razoável de verificar essa informação." Sim, é sério desse jeito mesmo. Você pode ficar muito "queimado" em certos círculos se você assinar uma chave falsa, pensando que é verdadeira: a sua assinatura mal-verificada pode vir a prejudicar outros que confiaram em você.

- de preferencia a troca e assinatura de chaves ao vivo.
- só assine chaves de pessoas que você conhece e que são de sua confiança.
- de niveis de confiança a diferentes chaves, confança alta as chaves de quem você confia, confiança media as chves de quem você só conhece, etc.

```
   gpg --fingerprint <seu nome ou 0xSuaKEYID>
   gpg --receive-key <0xKEYID> (procura a chave especificada nos
keyservers)
   gpg --sign-key <0xKEYID> (assina uma chave)
```

Assuma se você sabe cifrar e decifrar mensagens. Caso não saiba, ainda não é hora de querer sair assinando chaves.

Recebendo sua chave assinada

Se alguém assinou sua chave, é conveniente você atualizar sua cópia da sua chave pública para que ela contenha essa nova assinatura. Você pode fazer isso de duas maneiras: importando a chave que a pessoa te enviou pela forma usual, ou seja, utilizando o comando gpg --import ou, caso ela a tenha enviado para um servidor de chaves, atualizando seu chaveiro de acordo com as últimas modificaçõs de chaves do servidor.

Para essa segunda opção, basta digitar:

`gpg --refresh-keys --keyserver` zimmerman.mayfirst.org

onde keys.indymedia.org é o servidor de chaves para o qual a pessoa mandou a chave assinada. Esse comando fará com que todas as chaves públicas do seu chaveiro - inclusive a sua - sejam atualizadas a partir das chaves públicas existentes no servidor de chaves. Assim, se alguém assinou uma chave e a exportou para o servidor de chaves, esse comando atualizará seu chaveiro substituindo a chave pública antiga pela nova.

É muito interessante dar esse comando periodicamente para atualizar seu chaveiro, independentemente de alguém ter assinado uma chave. As atualizações de chaves podem acontecer sem ninguém te avisar.

Confiando em chaves

Assinar chaves mostra a outras pessoas que você confia na procedência de determinadas chaves públicas. Mas pode acontecer de você assinar a chave de um amigo seu mas não confiar nas chaves que ele assina. Existe uma maneira de lembrar a você em quais colegas seus você confia quando eles assinam chaves de outras pessoas, que é o chamado nível de confiabilidade daquela chave.

Essa informação não é passada a outros usuários. Quando exportada, não existirá diferença nenhuma se a chave pública foi definida por você com alto ou baixo nível ente, uma chave pública é considerada válida apenas se ela for assinada por você. Mas usando o conceito de Teia de Confiabilidade, o GPG é bem flexível em considerar uma chave válida, por exemplo, se:

- Ela foi assinada por você '"ou"'
- Ela foi assinada por alguém que você confia totalmente '"ou"'
- Ela foi assinada por três chaves que você confia moderadamente '"ou"'
- Se existe um caminho entre você e a chave pelo qual todas as chaves estão assinadas. João assinou a chave de Raimundo, que assinou a chave de Maria, cuja chave você assinou; esse caminho permite que o GPG considere válida a chave de João, sem que você precise assiná-la. Normalmente o número de pessoas nessa corrente, para que a chave torne-se válida, não pode ser maior que cinco.

Voce não precisa decorar esse esquema! Uma vez que você seleciona o nível de confiabilidade de uma chave, o GPG automaticamente recalcula a validade de todas as chaves do seu chaveiro, usando um método um pouco mais sofisticado do que o exemplificado acima.

Removendo chaves

Se você quiser remover a chave pública de alguém, use o comando

```
gpg --delete-key email@da.pessoa
```

onde email@da.pessoa é o email da pessoa cuja chave você quer apagar. Agora, se você quiser remover um par de chaves (pública e privada), use o comando:

```
gpg --delete-secret-and-public-key seu@email
```

onde seu@email é o seu email. Exemplo:

```
gpg --delete-secret-and-public-key truta@uzma.net
gpg (GnuPG) 1.2.3; Copyright (C) 2003 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.

sec  1024D/90716386 2004-02-18   Truta <truta@uzma.net>

  Deletar esta chave do chaveiro? s
  Esta é uma chave secreta! - realmente deletar? s
  pub  1024D/90716386 2004-02-18   Truta <truta@uzma.net>

  Deletar esta chave do chaveiro? s
```

Mas tome cuidado: uma vez que você apagou seu par de chaves, não há mais como recuperá-las, ler mensagens criptografas para você ou assinar mensagens. Lembre-se de revogar sua chave pública antes de cancelá-la (veja como na próxima seção).

Cancelando um par de chaves

Se você quiser cancelar um par de chaves, por qualquer motivo - alguém roubou sua chave secreta e sua senha, por exemplo - você usará o comando para revogar sua chave.

O comando

```
gpg --output revoke.asc --gen-revoke ID
```

revogará minha chave cuja identificação é ID (que pode ser tanto o nome do par de chaves, como o seu número ou o email correspondente) e gerará um certificado de revogamento no arquivo `revoke.asc`. Esse certificado serve para ser enviado a quem tiver minha chave pública para que saibam que cancelei meu par de chaves. É uma espécie de assinatura de cancelamento.

Outros comandos

Para maiores informações sobre como usar o gpg em modo texto, consulte as Referências ou então digite no seu terminal

```
man gpg
```

Resumão: tabela de consulta rápida

O GPG no modo texto apresenta muitos comandos e frequentemente nos esquecemos dos parâmetros e da ordem pela qual eles precisam ser passados ao programa.

- Criar par de chaves: "gpg --gen-key"
- Compartilhar chave pública: "gpg --export --armor -o chave.asc email@do.usuario"
- Enviar chaves a um servidor: "gpg --keyserver servidor.de.chaves --send-keys nome-da-chave"
- Listar chaves do seu chaveiro: "gpg --list-keys"
- Importar chaves: "gpg --import nome-do-arquivo"
- Procurar chave num servidor: "gpg -- zimmerman.mayfirst.org --search-keys email-ou-nome"
- Receber chaves de um servidor: "gpg --keyserver servidor.de.chaves --recv-keys id-da-chave"
- Assinar em texto simples: "gpg --clearsign nome-de-arquivo (opcional)"
- Verificar assinatura: "gpg --verify nome-do-arquivo"
- Criptografar mensagem: "gpg -e -a -r nome-ou-mail"
- Criptografar em arquivo: "gpg -r nome-ou-email -e -a nome-do-arquivo"
- Descriptografar: gpg -d nome-do-arquivo
- Ver impressão digital: gpg --fingerprint nome-ou-email
- Atualizar chaves públicas de um servidor: gpg --refresh-keys --keyserver servidor-de-chaves

Criptografia do disco rígido

Quando falamos de segurança da informação, podemos usar várias técnicas e ferramentas para evitar intrusões remotas e locais através do terminal. Mas nós devemos pensar em outras possibilidades além do acesso ao terminal propriamente dito.
Como podemos garantir a segurança do nosso computador se ele for roubado? E se alguém conseguir clonar o HD? E se apreenderem nosso computador?
Nessas situações não teremos o que fazer, o ladrão (invasor) vai ter acesso a todas as nossas informações.
O que podemos fazer para evitar esse tipo de situação?
A solução é criptografar o disco, isso é feito na instalação do seu sistema operacional GNU/Linux de escolha. Geralmente esta etapa da instalação é logo após você escolher o hd onde será instalado o seu linux, mas isso varia entre todas as distribuições, então pesquise como criptografar a distribuição que você escolheu. Lembre-se, se você perder a senha, já era! E cuidado, não coloque seu computador para hibernar, pois neste estado

ele se encontra vunerável a um ataque: https://under-linux.org/content.php?r=5804

Cuidados a serem tomados

-utilize criptografia sempre que, ao enviar uma mensagem, quiser assegurar-se que somente o destinatário possa lê-la;
-utilize assinaturas digitais sempre que, ao enviar uma mensagem, quiser assegurar ao destinatário que foi você quem a enviou e que o conteúdo não foi alterado;
-só envie dados sensíveis após certificar-se de que está usando uma conexão segura;
-utilize criptografia para conexão entre seu leitor de *e-mails* e os servidores de *e-mail* do seu provedor;
-cifre o disco do seu computador e dispositivos removíveis, como disco externo e *pen-drive*. Desta forma, em caso de perda ou furto do equipamento, seus dados não poderão ser indevidamente acessados;
-verifique o *hash*, quando possível, dos arquivos obtidos pela Internet (isto permite que você detecte arquivos corrompidos ou que foram indevidamente alterados durante a transmissão).

-utilize chaves de tamanho adequado. Quanto maior a chave, mais resistente ela será a ataques de força bruta;
-não utilize chaves secretas óbvias;
-certifique-se de não estar sendo observado ao digitar suas chaves e senhas de proteção;
-utilize canais de comunicação seguros quando compartilhar chaves secretas;
-armazene suas chaves privadas com algum mecanismo de proteção, como por exemplo senha, para evitar que outra pessoa faça uso indevido delas;
-preserve suas chaves. Procure fazer *backups* e mantenha-os em local seguro (se você perder uma chave secreta ou privada, não poderá decifrar as mensagens que dependiam de tais chaves);
-tenha muito cuidado ao armazenar e utilizar suas chaves em computadores potencialmente infectados ou comprometidos, como em *LAN houses*, *cybercafes*, *stands* de eventos, etc;
-se suspeitar que outra pessoa teve acesso à sua chave privada (por exemplo, porque perdeu o dispositivo em que ela estava armazenada ou porque alguém acessou indevidamente o computador onde ela estava guardada), solicite imediatamente a revogação do certificado junto à AC emissora.

-mantenha seu sistema operacional e navegadores *Web* atualizados (além disto contribuir para a segurança geral do seu computador, também serve para manter as cadeias de certificados sempre atualizadas);
-mantenha seu computador com a data correta. Além de outros benefícios, isto impede que certificados válidos sejam considerados não confiáveis e, de forma contrária, que certificados não confiáveis sejam considerados válidos;

E-MAIL

O uso mais frequente da criptografia é no envio e recebimento de emails. Uma vez que os pacotes de informação são transmitidas de servidor em servidor pela internet até chegar no computador de destino, qualquer pessoa pode monitorar esses pacotes e obter seu conteúdo. Utilizando a criptografia assegura que apenas o destinatário comprenderá o conteúdo da mensagem. Como vimos em criptografia, é bem simples criptografar um e-mail. Porém não basta criptografar suas mensagens e continuar a merce do hotmail, yahoo, gmail e compania, pois, por mais que as mensagens estejam criptografadas, você pode ser boicotabo por estas impresas, como por exemplo, tendo suas contas bloqueadas, canceladas e suas mensagens não enviadas. Existem saídas antigovernamentais para isso, como os servidores do RiseUp.

Mail.riseup

https://mail.riseup.net/

https://help.riseup.net/pt/pt-email

O serviço de e-mail Riseup é uma exelente ferramenta de comunicação, com servidor físico escondido em algum lugar do mundo, sua infra estrutura é mantida por quem o utiliza, através de doações. É um serviço autonomo, anarquista e anticapitalista. Não grava nenhuma informação sobre seus usuários, nem seobre seus Ips e nem irá entregar-las a polícia. O sistema de obtenção de uma conta é feita através de dois modos:

-modo de rede de confiança, onde duas pessoas que já possuem contas de e-mail riseup enviam um código de convite para uma terceira pessoa que esteja interessada em obter uma conta.

-modo de análise de seu pedido, onde o servidor irá analisar seu pedido, onde você deverá preencher um formulário explicando por que você necessita uma conta de e-mail riseup e para que! Não se assuste, é garantida toda a integridade e sigilo da sua mensagem, que irá criptografada até o servidor e depois do seu pedido ser aprovado, ou rejeitado, sua mensagem será excluída e não existirá nenhum rastro sobre você! O único jeito é confiar na imagem e estatus de segurança do servidor, que é respeitado em vários países e por vários coletivos anarquistas. Você pode confirmar isso mandando um e-mail para vários coletivos anarquistas do brasil perguntando sobre a reputação do servidor. Certamente a resposta será positiva e de que você pode confiar no riseup!

Primeiros passos

Visite user.riseup.net. Ali você pode alterar sua senha, adicionar pseudônimos (atalhos), configurar filtros de email, aumentar sua cota e pedir ajuda.

Nós destruimos automaticamente a informação que você nos dá como parte de seu pedido de conta. Considere remover de suas configurações da conta qualquer informação que possa lhe indentificar, como seu nome, data de nascimento, pergunta secreta e email alternativo. Porém, se você esquecer sua senha e não tiver gravado seu email alternativo (ou esquecer o que escreveu, ou o email alternativo não for mais acessível) então perderá o acesso à sua conta.

Proteja sua senha

A Internet está cheia de pessoas tentando roubar sua conta de email. Em algum momento, é provável que você receberá um email falso de alguém fingindo ser de riseup.net. Esses emails costumam dizer que você deve fazer alguma coisa para manter sua conta.

- Nunca dê sua senha a ninguém, especialmente se dizer ser de riseup.net.
- Nunca confie que o endereço “De:” de um email é de quem diz ser, porque isso pode ser forjado facilmente.
- Links em mensagens de email costumam ser uma fraude. Para ter segurança, redigite o link na barra de endereços do navegador ao invés de clicar nele. E, também, tome cuidado com erros de digitação, como riseupp.net (percebeu a letra repetida?) ao invés de riseup.net

Mensagens são apagadas automaticamente em algumas pastas

Em algumas pastas especiais, as mensagens são apagadas automaticamente depois de um certo número de dias:

- Lixo: apagadas depois de 21 dias.
- Spam: apagadas depois de 7 dias.
- Enviados: apagadas depois de 120 dias.

Cota

Por muitas razões, nós não fornecemos muito espaço de armazenamento para email. Se você precisa de mais espaço, considere baixar seu email usando clientes de email ou aumente sua cota visitando user.riseup.net. Leia mais sobre cota.

O que há de especial no email riseup.net

Sua conta de email riseup.net é uma maravilha. Apesar de não ter tanto espaço de armazenamento como provedores de email corporativas que vigiam e colaboram com governos, o email riseup.net tem muitas características que não se encontra com facilidade:

Nós encriptamos o tráfego sempre que possível.

> Quando você envia um email via riseup.net para outro provedor de email, o email é encriptado para sua viajem inteira.

Nós não revelamos sua localização para destinatárias dos emails.

> Quando você envia um email via riseup.net, seu endereço IP não é embutido no email. Com provedores de email corporativos, qualquer pessoa que recebe seu email pode descobrir sua localização física aproximada a partir do endereço de IP que fica junto da mensagem.

Nós não calculamos teu endereço IP.

> Nosso comprometimento é manter a menor quantidade de dados possível sobre você. Diferente de provedores corporativos, nós não calculamos endereço IP de ninguém que esteja usando os serviços riseup.net, incluindo email.

Apoio mútuo

Não existe email gratuito. Serviços como gmail, hotmail, e yahoo fazem dinheiro a partir da vigilância: eles constroem um perfil sobre seu comportamento e bombardeiam anúncios direcionados a você.

Riseup.net é diferente. Esse serviço é um trabalho de amor por ativistas como você, comprometidas com a construção de ações e infraestruturas de segurança alternativas.

O serviço de email riseup.net toma muito tempo e dinheiro para continuar funcionando, e é sustentado inteiramente por pequenas doações de quem usa.

Use um cliente de email

É verdade que a interface web do riseup.net não é muito elegante. Você pode usar conta de email riseup.net com clientes de email IMAP ou POP, que são programas cheios de funcionalidades para lidar especificamente com emails.

Riseup recomenda Thunderbird, que é um cliente de email livre e código-aberto. Thunderbird se configura automaticamente, você precisa usar seu endereço de email e

senha.

O que é um cliente de email?

Atualmente, a maioria das pessoas está familiarizada com webmail, em que você acessa seu email usando um navegador de internet como Firefox ou Chrome.

Um **cliente de email**, por outro lado, é um programa feito para acessar e escrever email. Existem muito clientes de email gratuitos e/ou Software Livre disponíveis para a maioria das plataformas.

Recomenda-se Thunderbird, Evolution, Kmail, Balsa, Mutt, Pine

Escolha IMAP ou POP

Clientes de email podem acessar sua conta de email usando POP ou IMAP.

	POP	IMAP
Armazenamento	**Seu computador**. Normalmente, quando você usa POP, todo o seu email é baixado para seu computador e removido dos servidores riseup.net.	**Servidor Riseup**. IMAP deixa todas as suas mensagens no servidor. Outra maneira de entender isto é que um cliente IMAP permite que você veja os dados armazenados no servidor.
Mobilidade	**Baixa**. POP só funciona bem quando você costuma mais acessar sua conta de email de um mesmo computador.	**Alta**. IMAP permite que você acesse sua conta muitos clientes (inclusive webmail) mantendo sincronia.
Velocidade	**Rápido**, já que tudo é baixado para seu computador de uma só vez.	**Lento**, já que o cliente de email tem que comunicar com o servidor várias vezes.
Cota de armazenamento	Você nunca precisa se preocupar com sua cota se seu cliente for configurado para apagar as mensagens do servidor depois de baixá-las para seu computador.	Você terá uma cota limitada.

Configuração Básica do Cliente

Apesar de alguns clientes de email se configurarem automaticamente, a maioria precisa de algumas informações básicas para se conectar a sua conta de email Riseup.

Suponha que seu endereço de email seja `collective@riseup.net`:

- servidor de recebimento de mensagens: `mail.riseup.net`
- servidor de envio de mensagens: `mail.riseup.net`
- login ou nome de usuária `collective`
- usar conexão segura: `sim` (Isto é necessário. A conexão segura deve ser do tipo SSL, TLS or StartTLS).

Nota: Não ative **senhas seguras** ou **autenticação segura**. These are somewhat of a misnomer. Estes métodos de especificar senhas requer que o servidor de email mantenha uma cópia de sua senha. Nós consideramos isto um risco de segurança, por isto não ativamos "senhas seguras". A conexão com riseup.net é criptografada, por isto não é necessário.

Use Thunderbird!

Thunderbird é o cliente de email recomendado para usar com riseup.net. Ele tem muitas funcionalidades é um Sofware Livre e de Código Aberto da Fundação Mozilla, a mesma que faz o Firefox.

Thunderbird se configura automaticamente para usar sua conta de email riseup.net.

Porque eu deveria usar um cliente de email?

- Ao usar um cliente de email, você não precisa ter acesso à internet sempre. Você pode acessar, baixar todos os seus email, desconectar e ler os emails quando quiser. Isto é muito conveniente se sua conectividade não é RELIABLE, é devagar ou talvez tenha acesso limitado. Você pode também escrever emails a qualquer momento, salvar, e os enviar mais tarde quando tiver acesso à internet.
- O webmail Riseup é um pouco limitado. Clientes de email têm muito mais funcionalidades.
- Clientes de email em geral são mais rápidos que o webmail.
- A maioria dos clientes de email permite que você gerencie múltiplas contas todas em um lugar. Isto pode ser muito útil se você tem contas de email diferentes para diferentes partes de sua vida.

Existem também algumas desvantagens:

- Para usar um cliente de email, você deve instalar o programa em seu computador e configura-lo especialmente para sua conta (ou contas).

- Os clientes de email armazenam mensagens em seu computador, por isto outras pessoas podem ler seu email se tiverem acesso a seu computador.

Posso usar o webmail e o cliente de email juntos?

Sim, você pode alternar quando quiser. É comum as pessoas usarem um cliente de email em casa ou no trabalho, e o webmail quando estão viajando. Se você usa ambas opções, deve se familiarizar com as diferenças entre IMAP e POP.

THUNDER BIRD

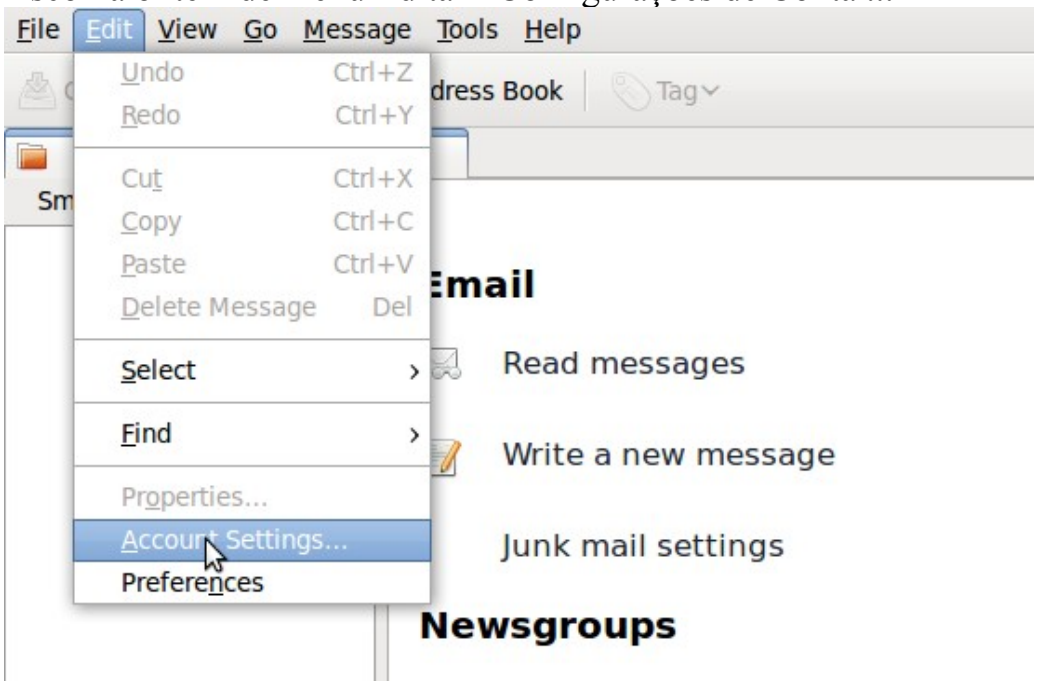
Thunderbird é o cliente de correio recomendado pelo riseup.net. Ele é software livre e está disponível para Linux. Você pode baixar o Thunderbird no site do thunderbird. Como Software Livre, Thunderbird faz parte do commons digital, uma espécie de tesouro comum para todos. Outlook, por outro lado, é a ferramenta da Microsoft para dominar o mundo.

Thunderbird tem muitos recursos, incluindo: suporte IMAP e POP, várias contas, busca rápida, soletrar enquanto você digita, controles avançados de spam, RSS, vistas de pastas virtuais, filtragem de mensagens, livro de endereços, e suporte para criptografia OpenPGP.

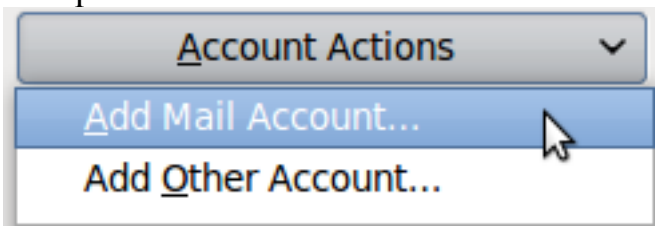
Configuração

A primeira vez que executar o Thunderbird, o assistente de conta irá orientá-lo através da criação de uma conta. Se o assistente não abrir, você pode fazer isso:

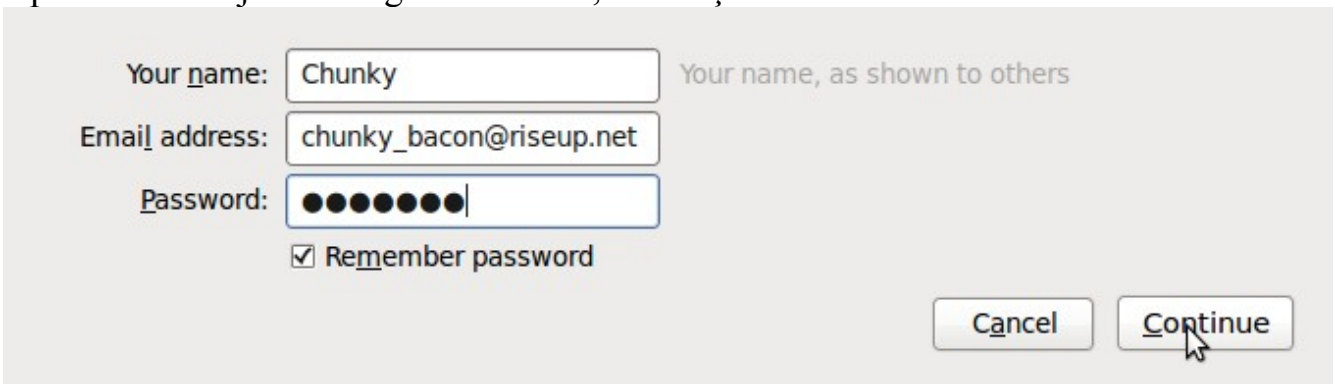
1. Escolha o item de menu Editar> Configurações de Conta ...



2. Clique em Adicionar Conta ... .

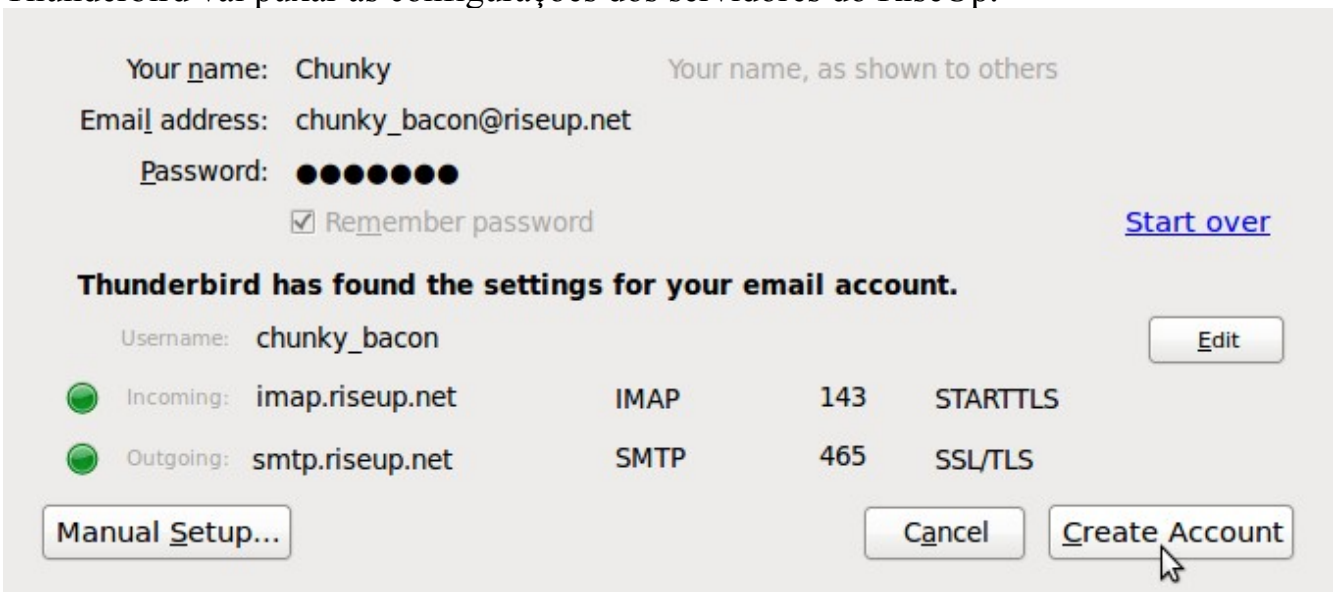


Aparecerá uma janela. Digite seu nome, endereço de e-mail e senha.



Clique em Continuar

Thunderbird vai puxar as configurações dos servidores do RiseUp.



Você precisa decidir se você quer usar IMAP ou POP. Ele vai por padrão escolha IMAP, então se você quiser IMAP, você pode simplesmente clique em Continuar. Para mudar para POP, clique em editar. Em seguida, clique no menu suspenso que diz IMAP e

alterá-lo para pop. Agora clique em Configuração do Re-Test. Deve mostrar-lhe usando POP. Se assim for, clique em Continuar.

Se isso não funcionar, você pode ter digitado seu nome de usuário ou senha errada. Clique em Iniciar e tente novamente . Caso contrário ...
Está pronto!

Deve verificar automaticamente seu e-mail agora e cada poucos minutos depois . Divirta-se com o Thunderbird !

Opções escondidas que melhoram radicalmente a velocidade thunderbird

Por padrão , o Thunderbird fala com o servidor de e-mail cada vez que você abrir um e-mail ou alterar o seu estado. Isso pode sentir realmente lento em uma conexão de rede lenta ou se o servidor Riseup estiver ocupado.

Felizmente, há algo que você possa fazer sobre isso ! Thunderbird tem algumas configurações ocultas para tornar-se totalmente sincronizado com o servidor de correio quando ele se conecta . Isso geralmente torna a sua experiência mais agradável e ágil .

Para definir essas opções , acesse no menu Editar > Preferências item> guia Avançado > botão Config Editor .

-use_status_for_biff : este conjunto de falsas
-mail.server.default.autosync_offline_stores : Defina como true

Melhore a sua segurança de email

-Idealmente, você não deve usar StartTLS . Pelo contrário, é muito melhor usar TLS regulares. Para maior segurança, vá para as configurações da conta e mudar o tipo de conexão a partir de StartTLS para TLS.
-Há muitas vulnerabilidades nas conexões. Se você precisar de alta segurança, você deve sempre se conectar a serviços Riseup usando o Riseup VPN. Isso vai evitar uma longa lista de possíveis ataques contra a sua comunicação .
-Para maior segurança de mensagem, configure o Enigmail (será explicado a seguir) com Thunderbird para obter a configuração OpenPGP .

Enigmail

No Thunderbird instale enigmail e execute o Assistente de Configuração OpenPGP

-Se você não tiver feito isso, gere um par de chaves OpenPGP como foi ensinado anteriormente .
-Baixe instale o Enigmail. Pode ser diretamento dos complementos do thunderbird ou atrvés do site: https://addons.mozilla.org/pt-BR/thunderbird/addon/enigmail/?src=search

Escolha se você quer configurar OpenPGP para todas as suas identidades ou apenas para algumas selecionadas, caso você use mais de uma identidade no Thunderbird. Se você tem múltiplas identidades, escolhendo a configuração OpenPGP para todas as identidades vão usar uma chave para todas elas.
Escolha se você quer assinar todos os seus e-mails enviados. A Assinatura não criptografa e-mails, ela coloca a sua assinatura digital em todos os seus e-mails enviados para permitir que outros verefiquem se você enviou o e-mail. Recomenda-se não assinar todos os seus e-mails enviados, uma vez que vincula fortemente que você envia via e-mail criptografado diretamente para si mesmo. É melhor apenas criptografar seus e-mails para destinatarios que suportam criptografia.
Escolha se você quiser criptografar todos os seus e-mails enviados por padrão. Isso não é recomendado, pois é complicado se o seu destinatário não suporta criptografia. Você pode ajustar as regras de criptografia, mais tarde, que permitirá escolher quais e-mail você irá criptografar.
Criar uma chave, se você não tiver feito isso, ou selecione uma chave existente para usar. Se você tem várias chaves e / ou múltiplas identidades, você pode ter que fazer algumas alterações manuais depois de associar a tecla direita com a identidade correta.
Reveja as alterações propostas e clique em Next
Se não houver erros, OpenPGP está pronto para usar. Clic em Concluir.

Configurando Regras OpenPGP

No Thunderbird, a extensão Enigmail fornece a capacidade para você configurar regras que Thunderbird vai usar para automatizar quem vai ou não receber e-mails criptografados de você.

O sistema de regras é muito poderoso e pode criar uma ampla gama de opções possíveis. Este guia irá criar uma regra para sempre enviar e-mails criptografados para um endereço de e-mail específico (ou vários endereços de e-mail) e opera sob a suposição de que seus e-mails não são criptografadas por padrão. No entanto, o sistema de regras parece ser poderoso o suficiente para que se a maioria dos seus contatos usam criptografia OpenPGP, você pode criptografar por padrão e criar uma regra que envia e-mails não criptografados para contatos que você tem que não suporta criptografia.

-Navegue para **OpenPGP → Edit Per-Recipient Rules**

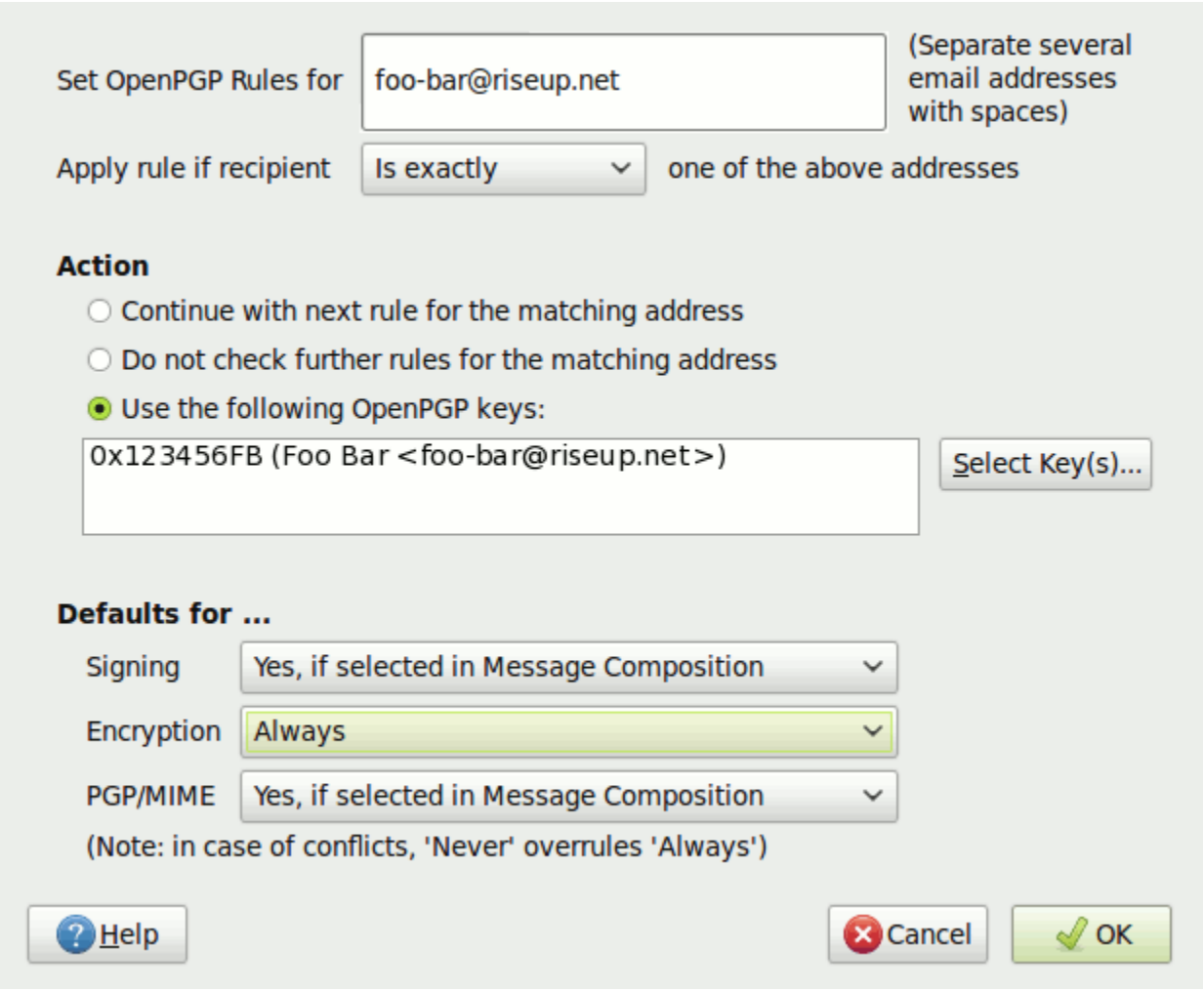
-Clique no botão **Add** no canto superior direito.

Digite o(s) endereço(s) de e-mail no topo, separados por espaços para combinar vários endereços de e-mail, selecione **is exactly.**

Escolha a **ação** a ser aplicada sobre correspondente à regra. Para este exemplo, escolher **Use as seguintes chaves OpenPGP**: e pressione a tecla Selecionar. Na caixa que aparece a partir desse botão, selecione a chave OpenPGP para a pessoa a quem você está enviando e-mail. Se você não tem a sua chave pública, clique em **faltando download**, que irá procurar os servidores de chaves para o e-mail(s) que você digitou na caixa de correspondência.

Alterar **criptografar** nos **padrões de ...** seção para **sempre** e deixe assinatura e PGP / MIME como **Sim, se selecionado na composição da mensagem**.

Pressione o botão OK quando tiver concluído a configuração da regra....



Agora você está pronto para enviar OpenPGP (GPG) e-mails para qualquer destinatário via Thunderbird e permitir criptografia automaticamente para o destinatário escolhido na regra que você acabou de criar.

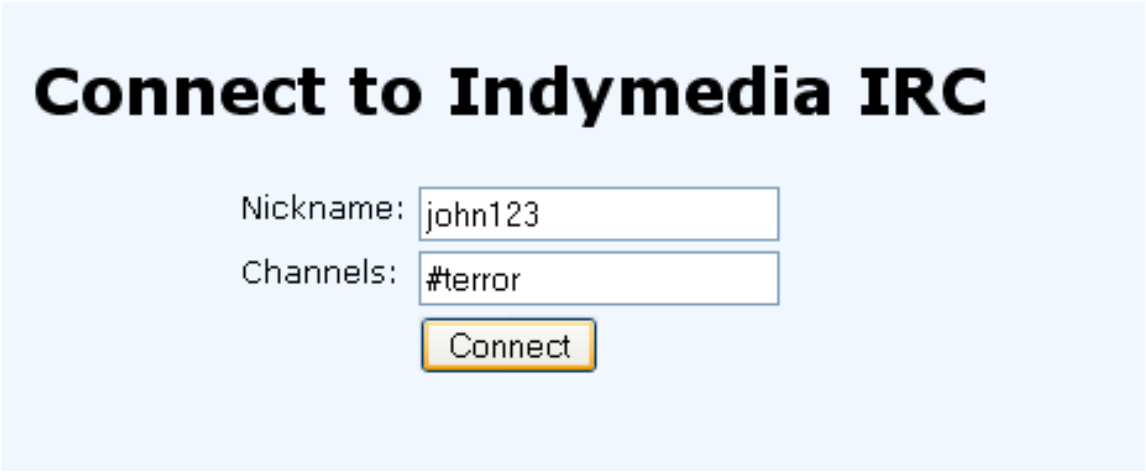
BATE-PAPO

Esqueça o mensenger, o bate papo do facebook ou do uol. Todos eles pertencem a empresas que guardarão todas as informações que puderem sobre você. Para se comunicar de forma instantanea na internet existe a ferramenta IRC.
IRC é um dos sistemas de bate-papo mais antigos, com um protocolo simples mas muito funcional. Se hoje estamos na era dos Messengers, na idade da pedra as pessoas se

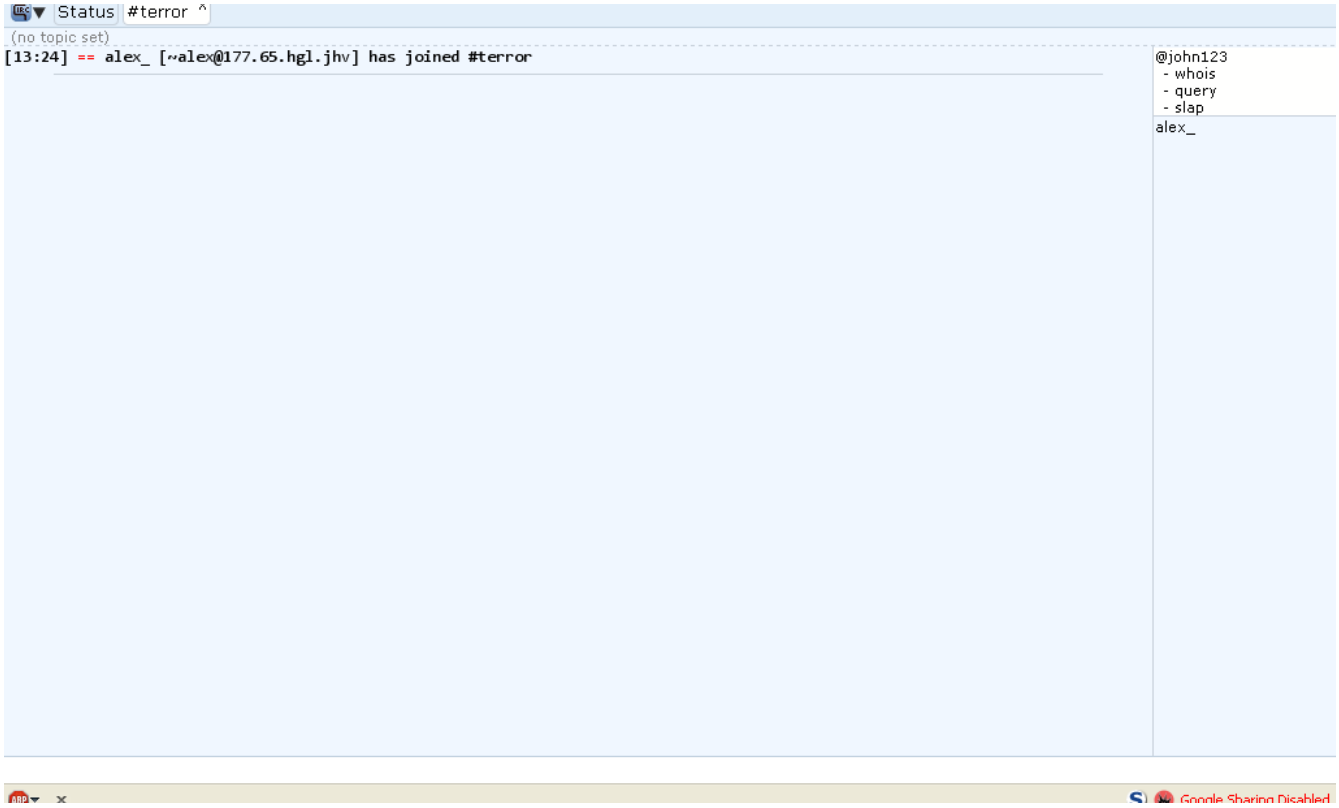
comunicavam em tempo real através do IRC. Assim como em outros tipos de bate-papo, no IRC é possível participar de uma ou mais salas e ainda manter conversações privadas.
A rede Indymedia e o CMI Brasil utilizam sua própria rede de bate-papo, e o IRC foi escolhido como protocolo por ser um sistema simples e que não consome muita conexão ou performance dos computadores, além de ser muito rápido mesmo para pessoas que usam internet através de linha discada.

<u>Acessando uma sala de bate papo irc através do navegador:</u>

1) Abra seu navegador e digite o link do servidor de irc que você irá utilizar:
exemplo: https://chat.indymedia.org



2) Em Nickname coloque o seu nome, apelido, codinome... Em Channels coloque o nome do canal que você utilizará para conversar com outras pessoas. O nome do canal é a senha, pode ser qualquer nome ou código, e pode ser inventado por qualquer um na hora do acesso.

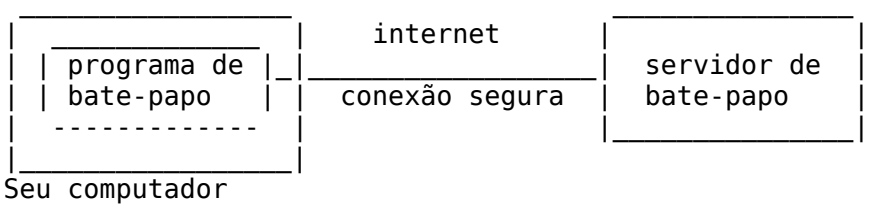


Quando você entrar na sala, terá na parte inferior uma caixa para digitar suas mensagens, elas apareceram na parte central da tela. No lado direito superior da tele estará a lista de pessoas online no canal que você conectar, se você clicar no nome de alguém, aparecerá 3 opções, whois que serve para vereficar se a pessoa realmente por traz do nickname é ela mesma, query para começar uma conversa particular com alguém, e slap para chamar atenção de alguém.

Mas também é necessário a criptografia no batepapo do IRC:
Conforme diz a seção Criptografia e Internet, a internet é uma rede na qual as informações podem ser facilmente interceptadas. Isso quer dizer que usando um sistema de bate-papo comum é possível que mesmo em conversas privadas alguém escute o seu diálogo.

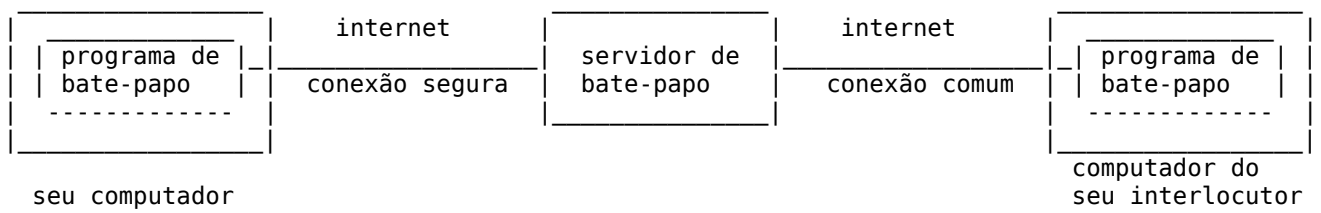
Para evitar esse tipo de coisa e preservar sua identidade, é possível utilizar a tecnologia SSL (Secure Sockets Layer), também conhecida como conexão segura.

A conexão segura utiliza criptografia para conectar você ao servidor. Tudo o que é enviado ao servidor e dele até você só poderá ser interpretado por ambas as partes. Seria algo como esse desenho:



As mensagens, antes de chegar ao servidor ou do servidor até você, passam por vários computadores e nesse caminho ainda poderá ser interceptada, mas só poderá ser interpretada se possuir uma das chaves privadas -- a do seu computador, no caso das mensagens enviadas pelo servidor, ou a do servidor, no caso das mensagens enviadas pelo seu computador.

Se você usa conexão segura e está conversando no bate-papo com alguém que não usa conexão segura, então em as mensagens entre vocês só estarão criptografadas na metade do caminho entre você e seu interlocutor:



Para que a conversa seja realmente segura é indispensável que todas as partes envolvidas numa conversa utilizem a conexão segura.

Uma outra vantagem desse tipo de conexão é o mascaramento do IP dos usuários, que é número que identifica cada computador que está na internet. Se alguém sabe o seu número IP, é bem possível que ela saiba identificar qual em qual país está o seu computador e qual é o provedor de acesso.

Por isso, é interessante que o seu IP não esteja disponível para aqueles que frequentam o mesmo bate-papo que você, e é isso que a conexão segura faz: todos os usuários com conexão segura aparentam estar utilizando o próprio servidor de bate-papo como seu computador pessoal.

Configurando uma conexão segura no bate-papo do CMI

Método simples

A forma mais simples de se conectar por conexão segura no bate-papo do CMI é através do endereço https://irc.indymedia.org/, mas esta forma não é totalmente segura, ainda sim sendo melhor que uma conexão comum. A seguir damos instruções para as formas mais seguras de conexão.

Usuários de GNU/Linux

Há várias formas de fazer uma conexão segura. A mais simples é usar um cliente de IRC com SSL habilitado. A seguir alguns exemplos de clientes com tal suporte:

- BitchX-SSL
- Epic-SSL
- Irssi
- Xchat

Para todos eles, o seguinte comando deve funcionar:

```
/server -SSL irc.indymedia.org 994
```

Para o Xchat digite:

```
/sslserver irc.indymedia.org 994
```

No presente momento, o suporte ao Xchat está em avançado estágio, conseguindo habilitação em diferentes distribuições de GNU/Linux e outros Sistemas Operacionais. O método ideal é selecionar as caixinhas 'Usar SSL' e 'Aceitar certificado inválido' na tela 'Lista de Servidores'. Além disso na caixa Servidores adicionar 'irc.indymedia.org/994'. Quando está conectando você poderá ver informações sobre o certificado SSL seguido da habitual informação de conexão do IRC. Verifique que você aparece como irc@127.0.0STOPSPAM.1, para ter certeza que está conectado atravéz de conexão segura.

Administração de apelidos

O sistema IRC permite que apelidos e canais (salas de bate-papo) sejam registrados e protegidos com senha. Isso possibilita, dentre outras funcionalidades:

- Usuários e usuárias registrados/as com senha possam desconectar da rede um/uma usuário/a que esteja usando seu apelido.
- Usuários e usuárias registrados/as enviam mensagens para outros usuários/as registrados.
- Canais registrados tem suas configurações preservadas

Toda atividade administrativa básica no sistema IRC é baseada em apelidos, da mesma

forma como sua caixa postal é protegida através de um par usuário/senha. Para você possuir uma sala de bate-papo ou desfrute dos privilégios de operador de uma sala, por exemplo, é necessário utilizar um apelido registrado.

Registrando um apelido

Para que um/uma usuário/a tenha exclusividade sobre um apelido, é preciso que ele/ela o registre perante um *servidor de apelidos* presente no servidor de bate-papo. Esse servidor é conhecido como *nickserv*. Para registrar um/uma usuário/a, é necessário enviar uma mensagem específica ao nickserv, contendo

- O comando *register*, que indica o registro de apelidos.
- Uma senha para a proteção do apelido.

Isso pode ser feito simplesmente digitando, em qualquer janela do bate-papo, o comando

```
/msg nickserv register SENHA
```

Identificando um apelido

O/A usuário/a detentor de um apelido deve se identificar ao servidor de apelidos (*nickserv*) toda a vez que desejar utilizá-lo. Caso contrário, o/a usuário/a não poderá desfrutar dos privilégios de operador/a das salas em que está registrado/a -- através do servidor de canais (*chanserv*) -- e nem mesmo ter acesso em sua caixa postal do servidor de mensagens (*memoserv*).

A identificação de um apelido é feita com o comando

```
/msg nickserv identify SENHA
```

Caso a senha esteja correta e o/a usuário/a que você estiver usando estiver registrado/a, a identificação estará estabelecida.

Em muitos servidores de IRC é indispensável que um/uma usuário/a usando um apelido já registrado se identifique, caso contrário ele/ela será desconectado/a do servidor após determinado intervalo de tempo. No caso da rede Indymedia isso não ocorre: um/uma usuário/a pode utilizar um apelido registrado sem se identificar e nesse caso não terá acesso aos privilégios que esse apelido possui.

Em geral, e isso vale também para os servidor da rede Indymedia, um apelido que não é identificado por mais de um mês é automaticamente desregistrado e todos os seus privilégios são revogados. Por isso, antes de sair de férias, tome cuidado para não ficar mais de um mês sem se conectar ao IRC, utilize uma conexão persistente ou então confie seu/sua usuário/a para um amigo ou amiga manter seu registro em ordem.

Desconectando um apelido

No sistema IRC, dois/duas usuários/as não podem usar um mesmo apelido ao mesmo tempo. O que é muito frequente de acontecer é, ao se conectar ao servidor, o/a usuário/a receber a notificação de que o apelido que ele/ela tentou utilizar já está em uso.

No caso de um apelido registrado, é possível recuperar um apelido da seguinte maneira:

Recuperando de outro/outra usuário/usuária

Caso seu apelido registrado esteja sendo usado por outra pessoa que não o tenha identificado, você pode recuperá-lo com o comando *recover*:

```
/msg nickserv recover APELIDO SENHA
```

Em seguida, o/a usuário/a pode assumir novamente aquele apelido e se identificar perante o servidor de nomes:

```
/nick APELIDO
/msg nickserv identify SENHA
```

Recuperando de uma conexão fantasma

Quando a conexão com a internet do servidor ou do usuário sofre alguma falha, o/a usuário/a pode se desconectar do bate-papo sem que o servidor tome conhecimento e o apelido continua a figurar como estando em uso. Quando o/a usuário/a se conectar novamente, ele/ela deverá, à semelhança do comando *recover* visto no ítem anterior, utilizar o comando *ghost* para matar a conexão fantasma e liberar o uso do apelido. O comando é o seguinte:

```
/msg nickserv ghost APELIDO SENHA
```

Em seguida, o/a usuário/a pode assumir novamente aquele apelido e se identificar perante o servidor de nomes:

```
/nick APELIDO
/msg nickserv identify SENHA
```

Mudando a senha de um apelido

Usuários/usuárias que já tenham identificado seu apelido podem alterar a senha do mesmo com o comando

```
/msg nickserv set password NOVA-SENHA
```

Registro de canais

O sistema IRC prevê o registro de salas de bate-papo (também conhecidas como *canais*) para que usuários/as possam criar espaços mais restritos de conversação. O esquema de registro de canais é semelhante ao de apelidos, e o/a usuário/a que registra um canal precisa necessariamente utilizar um apelido já registrado.

O/A usuário/a que entra num canal vazio que não está registrado é considerado o/a fundador/a daquele canal e ganha o status de operador/a. Esse canal pode então ser registrado com o comando:

```
/msg chanserv register NOME-DO-CANAL SENHA
```

Os nomes de canal por convenção começam com os caracteres # ou &, e por isso o procedimento de registro do hipotético canal *#quitanda* seria feito da seguinte maneira:

```
/join #quitanda
/msg chanserv register #quitanda abacaxi
```

O primeiro comando faz com que o/a usuário/a entre no canal *#quitanda*. Caso o canal não seja registrado e nenhum/a outro/outra usuário/a esteja nele, o canal é criado e o segundo comando pode ser utilizado, que por sua vez registra perante o servidor de canais o *#quitanda* com a senha *minha-senha*. O/A usuário/a que efetuou esse procedimento passa então a ser o/a *fundador*/a do canal e pode:

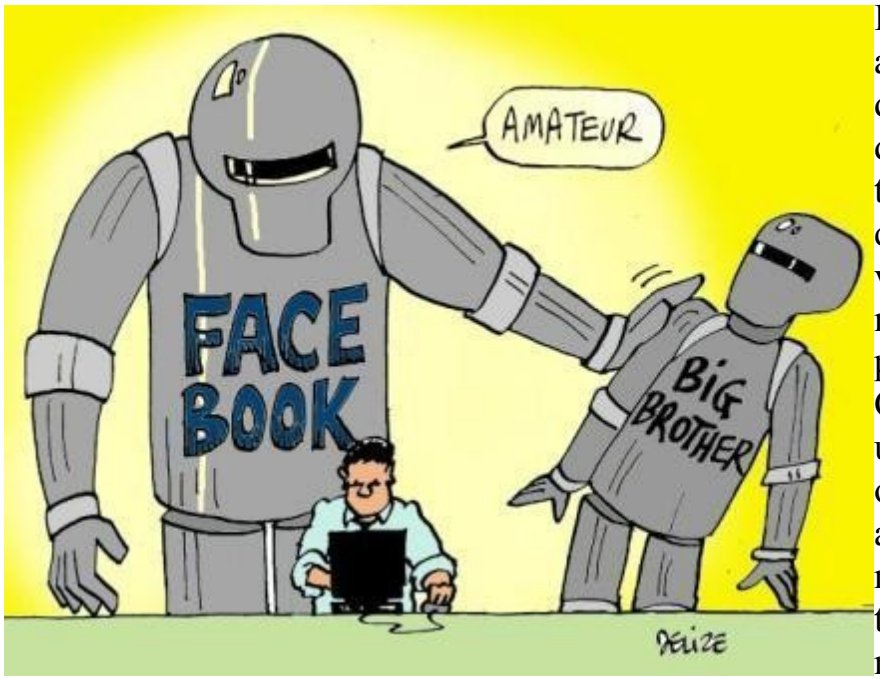
- Fornecer a outros apelidos privilégios nesse canal, como por exemplo o status de operador/a
- Controlar as opções de um canal

http://docs.indymedia.org/view/Sysadmin/SecureIRCpt

REDES SOCIAIS

Finalmente o ponto que dói pra muita gente. Apesar de ser um pouco tarde, mas APAGUEM SUAS CONTAS pessoais de TODAS AS REDES SOCIAIS!!! Cometam esse suicídio virtual o mais rápido possível. Quem já leu o contrato e a política de privacidade do Facebook, Twiter, Instagran e outros? Só para ter uma ideia, lá está escrito que TUDO o que você subir nas redes já não é mais seu! Simples. Qualquer frase, foto, comentário, like, cutucada, twit, tudo se torna propriedade de empresas. E não só isso, como já foi dito, todos os seus acessos, requisições, cliques, espiadas, pesquisas, tudo fica registrado e pode ser entregue a qualquer governo ou empresa. Estamos falando de mercado. Eles vendem para quem quiserem ou, se o Estado ameaçar direito, pra qualquer Governo.

FACEBOOK



É assustador que o mito de um arquivo mundial contendo detalhes íntimos de cada um dos terráqueos tenha se tornado realidade. Já se foi qualquer pretensão de uma vida privada, os nossos maiores segredos agora são propriedades de uma empresa. Como disse um alguém em um fórum qualquer: "o objetivo do Facebook é analisar e mercantilizar os nossos dados; tudo sobre todos os íntimos detalhes da nossa vida, dos nossos amigos, do nosso padrão de consumo, dos nossos amores, das nossas crenças políticas e religiosas, e por aí vai. O problema não está só nas pequenas coisas que postamos, toda a catalogação que eles podem construir é potencialmente incendiária. É o sonho erótico de um Estado policial."

O Facebook aparece como um espaço que toma a troca constante de informações como experiência cotidiana, o que reduz a interação entre as pessoas à emissão e recepção de opiniões.

Cada vez mais vigiado, cada vez mais lucrativo. Quem diria que a gente ia ser dominado voluntariamente? Que a gente ia entregar toda a nossa informação de mão beijada? O mundo está cada dia mais parecido com o Admirável Mundo Novo de Aldous Huxley. Como na saga do escritor inglês, parece tudo bem e nós sorrimos. O Big brother de George Orwell veio em forma de entretenimento. As duas obras literárias de um futurismo pessimista se apresentam de forma misturada no presente. Controle de cada movimento, sem precisar de nenhuma ameaça declarada.

Um tempo atrás as ações do Facebook na bolsa caíram porque um relatório revelou uma presença muito grande de perfis "fakes" na rede. Isso é, cadastros que não correspondem a existência de uma pessoa real. Esse dado revela o interesse direto em relação ao mapeamento das pessoas. Interesse esse que está a serviço dos mercados e do governo. Para cada pessoa no planeta, um perfil correspondente. Quem não tem uma conta no

Facebook sabe muito bem o quanto está ficando difícil se informar sobre atos e mobilizações políticas sem estar conectado nessa rede social. Mesmo as comunicações pessoais, os convites para eventos e festas, acabam ficando restritos ao ambiente privado da empresa Facebook.

Quando digo isso, a resposta dos compas é sempre a mesma: “ora, mas se a gente não divulga lá, deixamos de atingir uma quantidade de pessoas imensa e a nossa divulgação fica fragilizada!”. Ok, concordo. Mas o problema é justo esse.. De certa forma o Facebook está conseguindo monopolizar os canais de comunicação – para cada pessoa no mundo, um perfil que lhe corresponda. Outras ferramentas estão sendo deixadas de lado para privilegiar as redes sociais corporativas. Aos poucos as coisas vão deixando de serem divulgadas "também no Facebook " para serem divulgadas "só no Facebook ". Parece até que esquecemos como as coisas eram divulgadas antes…

Cruzando as informações dos usuários com informações fornecidas pelos dispositivos móveis, a coisa fica ainda mais tensa. Não bastasse fornecer dados sobre a nossa rede de contato, é só acessar a conta a partir de um Smart Phone que fornecemos também os dados sobre os lugares que estamos e por onde circulamos.

Um tempo atrás, o perfil do movimento pelo fim da violência Mães de Maio foi retirado temporariamente do ar pela empresa. Da mesma forma, o pessoal da Marcha das Vadias reclamava que suas fotos estavam sendo censuradas pelo Facebook. Nada disso deveria causar tanta indignação ou surpresa. É preciso lembrar sempre que o Facebook é um espaço tao público quanto um shopping center. O movimento que você participa cogitaria privilegiar um shopping como espaço de atuação???

Pra evitar a história dos perfis fakes, o Facebook anda fechando essas contas. Para aqueles que usam nomes e fotos falsas, com frequência aparecem casos onde é solicitado o envio do número de celular do usuário e até mesmo o seu documento de identidade escaneado.

A partir da rede criada por Mark Zuckerberg – que conta hoje com mais de 700 milhões de usuários – o governo do EUA declarou que nunca antes teve tanta informação de um número tao grande da população. Tudo isso, sem precisar torturar ninguém em troca de dados, nem violar diretamente sua privacidade.

Na Espanha está se debatendo uma reforma no Código Penal. Entre os pontos de discussão existe uma medida que inclui como novo delito a difusão em redes sociais de mensagens que incitem a "alteração da ordem pública". A pena será de três meses a um ano de prisão, ou uma multa, dependendo do caso. Tal medida corresponde a um movimento geral de criminalização das revoltas populares, mas que agora é facilitado pelas redes sociais. Existe alguma dúvida de que o Facebook ou outras empresas de comunicação virtual cederiam as informações de seus usuários com um gentil pedido da polícia? Acho que não..contanto que isso não seja divulgado.

O fato é que pra muita gente, até mesmo conseguir um emprego ou um serviço acaba dependendo da obtenção de uma conta na empresa. Frente a isso, o mínimo que se pode fazer é adotar uma política de redução de danos: consuma a droga, mas use seringas descartáveis. Preste atenção no tipo de informação que você divulga, alguns assuntos simplesmente não devem ser tratados de jeito nenhum via Facebook. Cuidado também com as fotos que você posta! Desapegue do seu ego de ativista: não precisa colocar fotos suas no meio da manifestação com o povão pra provar que você luta contra o capitalismo!

Só para dar um breve resumo do problema; ao usar o Facebook, ativistas não apenas fazem sua própria comunicação, sua opinião, seus "curtir", etc. transparentes e disponíveis para processamento. Ao invés disso — e consideramos ainda mais importante — eles/as expõem estruturas e indivíduos que tem pouco ou nada a ver com o Facebook. A capacidade do Facebook de investigar a rede atrás de relações, semelhanças, etc. é difícil de ser entendida por pessoas leigas. O falatório no Facebook reproduz estruturas políticas para autoridades e empresas. Este falatório pode ser pesquisado, organizado e agregado não apenas para obter declarações precisas sobre relações sociais, pessoas-chave, etc, mas também para realizar previsões, das quais se pode deduzir regularidades. Depois dos celulares, o Facebook é a mais sutil, barata e melhor tecnologia de vigilância disponível.

Usuários do Facebook como informantes não-intencionais?

Sempre pensamos que a esquerda queria outra coisa: continuar nossas lutas na internet e usá-la para nossas lutas políticas. É disso que se trata para nós — mesmo hoje. É por

isso que vemos usuários/as de Facebook como um perigo real para nossas lutas. Em particular, ativistas que publicam informações importantes no Facebook (muitas vezes não sabendo o que estão fazendo), que são cada vez mais utilizadas por órgãos de segurança pública. Poderíamos quase ir tão longe ao ponto de acusar esses/as ativistas de colaboracionismo, mas ainda não chegamos a este ponto. Ainda temos esperança que as pessoas percebam que o Facebook é um inimigo político e que aqueles/as que o usam fazem-no mais e mais poderoso. Usuários/as ativistas do Facebook alimentam a máquina, e assim revelam nossas estruturas — sem qualquer necessidade, sem qualquer mandado judicial, sem qualquer pressão.

Instamos a todos/as: Não tagueie os coleguinhas na foto: quer se foder, se fode sozinho.. Mas acima de tudo: Fortaleça e previlegie outros espaços de comunicação que sejam mais democráticos e seguros. Apague todas as suas fotos! Fechem suas contas no Facebook! Você está colocando outras pessoas em perigo! Aja contra esse monstro de dados!

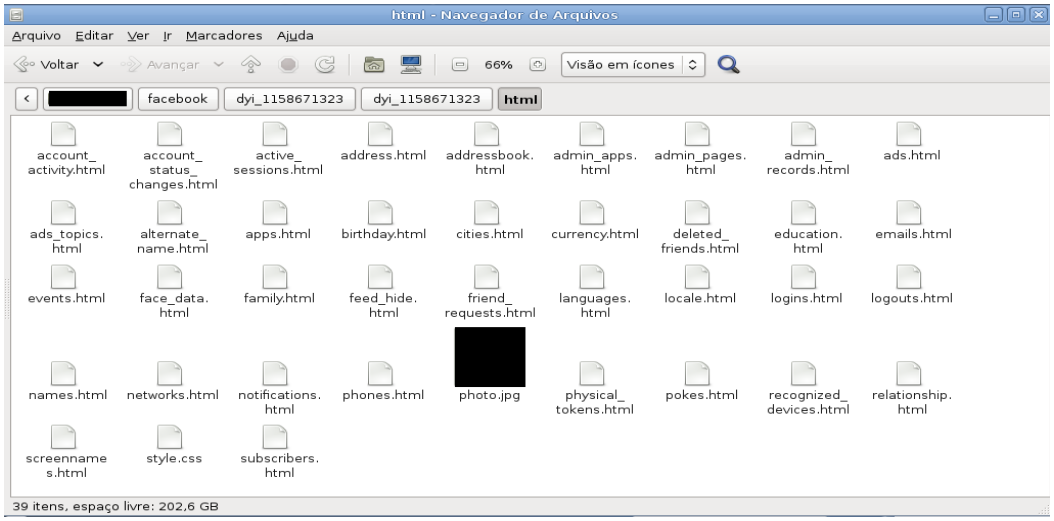
“Aquele que marcar o amiguinho na foto do Black Bloc quebrando a vidraça do Itau merece justiçamento, merece o micro-ondas do morro”

-Passo zero: Solicitar arquivo expandindo de seus dados:

Todxs sabem que o Facebook é um dos maiores bancos de armazenamento de dados pessoais que existe na internet. Bem, problemáticas a parte, o mínimo que esta empresa poderia nos oferecer nosso arquivo completo.

Então acesse *Configurações da Conta;* e logo na primeira página já tem uma opção de *“baixe uma cópia dos seus dados”;*

Solicite o arquivo expandido, e você receberá algo assim:



Nele existe, além do assustador arquivo intitulado **“ads_topics”,** um arquivo incrível chamado **“address book”.**

Estando ou não você no Facebook aconselho baixar uma cópia de seus dados. No Address Book você recebe absolutamente todos os e-mails de todos os seus contatos desta rede social.

Agora você já está preparadx para escrever para seus amigxs e chamá-lxs para sair, ao invés de ficar esperando um simpático e bem íntimo convite para um evento no facebook.

-1º passo: cancelar a conta no facebook

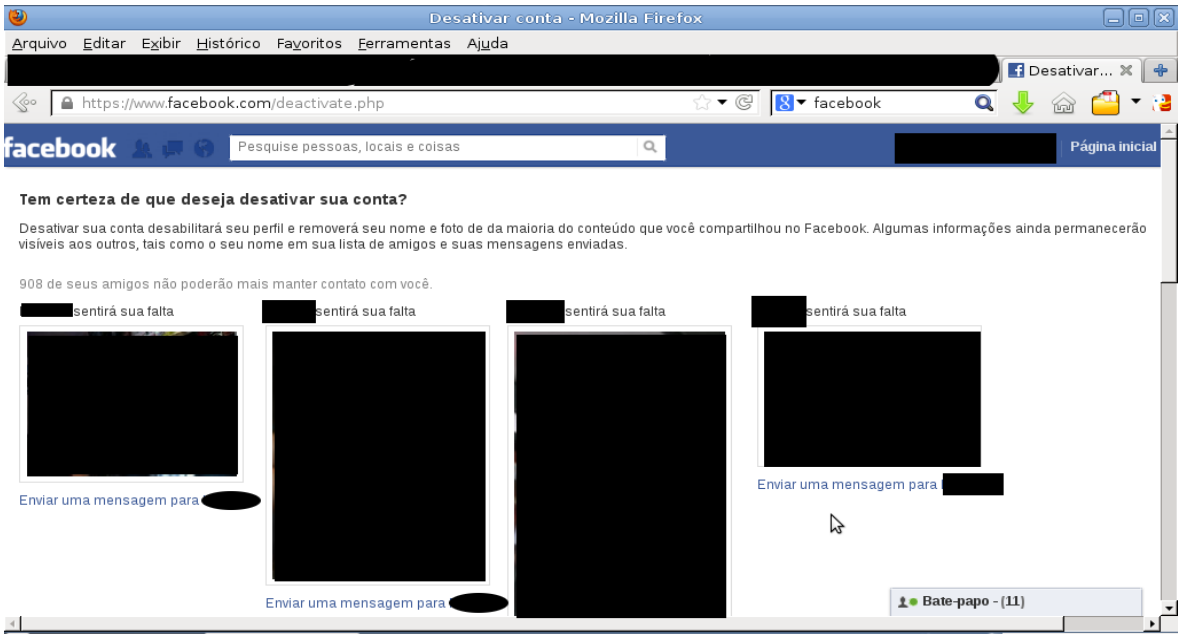
O Facebook nunca deleta as informações que um dia você forneceu a Ele.

Então o processo de sair do Facebook é mais no seu imaginário do que realidade, mas é um 1º passo.

PASSO A PASSO:

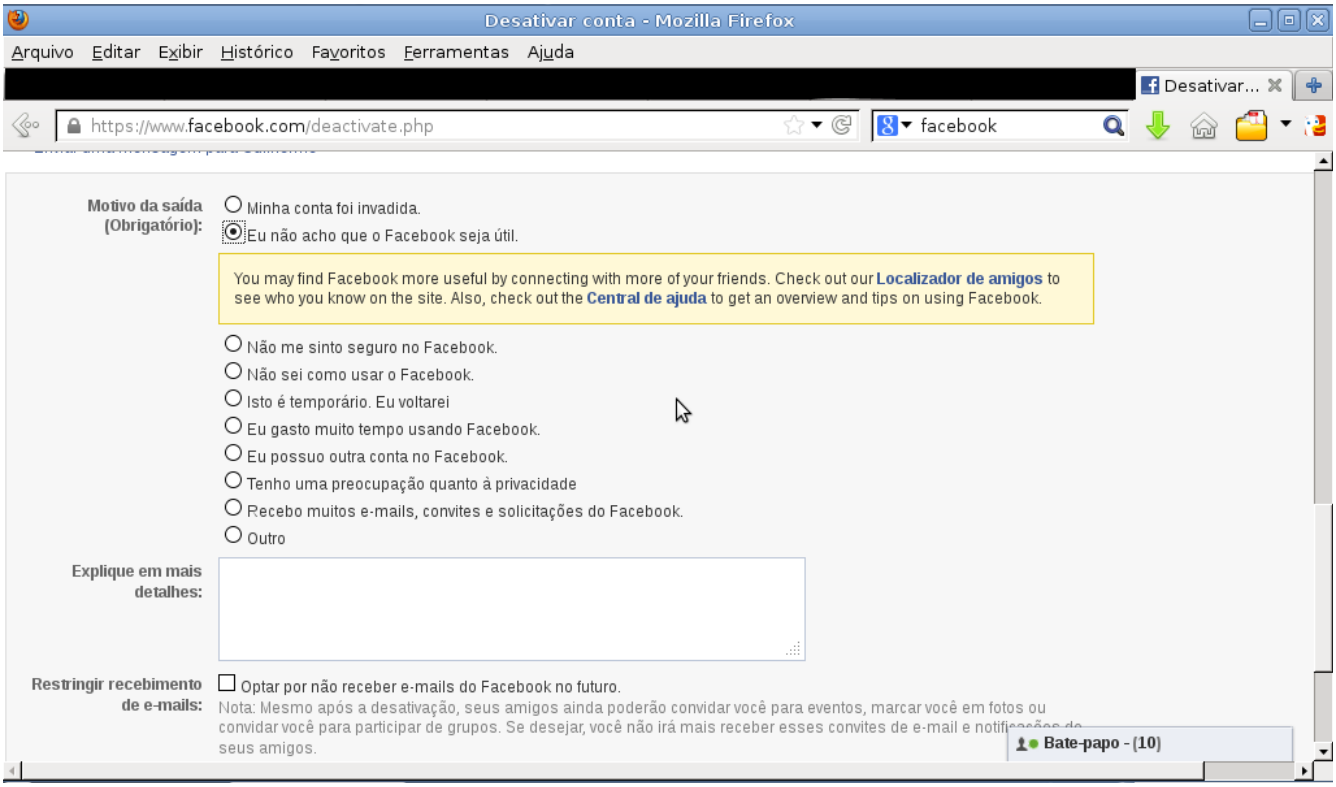
Acesse sua conta;

Vá em configurações da conta > Segurança > Cancelar minha conta;



Depois, não importa qual seja a razão para a sua saída, o Facebook vai insistir e insistir que dá para você contornar esta situação.

Me lembro que a primeira vez que eu saí do facebook foi bem mais difícil! Eram mais e mais janelas e para conseguir achar o botão de *desativar conta* era um verdadeiro martírio. Enfim, parece que isso mudou.



Pronto, agora você já "saiu" do Facebook, mas pode ficar tranquilx - ou não - que assim que você quiser voltar sua conta estará lá intacta. É só você reativar que todas suas mensagens, fotos e amigxs estarão extamente como você deixou. Talvez você que não esteja mais igual, mas isso fica pra outra postagem.

Redução de danos

Sendo o facebook uma enorme rede de concentração de dados, por onde as ondas de revolta de junho e julho de 2013 foram divulgadas, e não havendo outras ferramentas libertarias que não o substitua (até então), é possível utilizar contas falsas para monitorar a própria rede:
- Crie contas falsas
- Não coloque fotos suas
- Não marque os amiguinhos nas fotos de faixadas de bancos destruidas

- Não converse coisas importantes e sigilosas atraves dele
- Não fique marcando os eventos em que você estará presente
- lembre-se que podem te rastrear, então cuidado com o que fala e divulga.

BLOGS

Uma ótima maneira de se espalhar conhecimento na internet é criando um blog. Mas até mesmo para se fazer um blog que contenha mensagens e ensinamentos insurgentes, que podem ser enquadrados como apologia ao crime, é preciso ter algum cuidado. A primeira coisa a se fazer é escolher um servidor. Esqueça o Blogspot, Flogão, Instagran, wordpress.com e outros servidores corporativos como estes. É muito óbvio a insegurança de utilizar estas ferramentas captalistas de entreterimento, pois se a policia e o estado solicitarem informações sobre o administrador e seu ip de qualquer blog destes servidores, facilmente consiguirão todas elas. Além de poderem tirar tais blogs do ar a qualquer instante.

Também existem servidores de blogs deste lado da barricada, servidores que não colhem informações pessoais de seus utilizadores e que não irão ceder nenhuma informação para a polícia.

-MILHARAL

https://milharal.org/

O Milharal é um sistema para blogs sociais!

Ele é gerenciado coletivamente por um grupo de voluntári@s, que recebe doações dos coletivos e sítios hospedados para manter sua infraestrutura funcionando.

O **Coletivo Milharal** surgiu com o intuito de suprir a demanda por blogs em WordPress numa plataforma com requisitos mínimos de segurança, privacidade, acesso e controle da informação.

Esperamos de você e do seu projeto que usem o recurso oferecido com sabedoria e respeitem a seguinte **Política de Hospedagem:**

O Coletivo Milharal é uma plataforma independente e autônoma de comunicação para movimentos sociais, coletivos, grupos, militantes e ativistas que desejam mudanças sociais. Esperamos que essa iniciativa possa garantir na prática a liberdade de expressão para os setores não dominantes dessa sociedade. Desta forma, não hospedaremos sites com vínculos partidários, comerciais ou ainda que expressem visões contrárias aos nossos princípios de autogestão, anti-capitalismo, solidariedade e apoio mútuo.

Entendemos a hospedagem do seu site como uma cooperação entre as partes e não como uma prestação de serviços. Por essa razão, caso pretenda hospedar materiais de conteúdo político sensível o **Coletivo Milharal** deve ser informado das ações que cada projeto toma. É necessário ressaltar que o conteúdo publicado é de responsabilidade única dos/as autores/as do site, não cabendo ao **Coletivo Milharal** a responsabilidade jurídica por conteúdo impróprio ou ilegal publicado. Lutaremos pela manutenção de conteúdos postados que estejam em sintonia com nossos princípios ético-políticos, buscando alternativas às solicitações abusivas – de remoção de conteúdo – que ameacem a liberdade de expressão.

A moderação de comentários, a construção do site e demais mudanças no visual do site serão de responsabilidade da parte hospedada. Hospedar o seu site não significa que iremos fazer o seu site.

Em nenhum momento cobraremos pelo uso do serviço ou pelo suporte. Da mesma forma, não buscaremos nos financiar através do mesmo sistema contra o qual lutamos, isto é, através da publicidade, patrocínio estatal ou privado, subsídios governamentais ou através da exploração do trabalho. Quando for necessário, o **Coletivo Milharal** fará uma campanha de doações para manter ou ampliar os recursos técnicos – como a compra de hardware novo – e esperamos que você nos apoie!

O **Coletivo Milharal** reserva-se ao cancelamento e término da hospedagem no caso em que a cooperação e a política de hospedagem não seja respeitada. Nestes casos, nós nos comprometemos a avisar os/as administradores/as do site com antecedência e disponibilizar todos os arquivos hospedados.

Por defender e realizar a democracia direta, os casos não descritos ou contemplados nessa política de hospedagem serão analisados e decididos nas instâncias internas do **Coletivo Milharal**.

A solicitação de um novo site deverá ser feita através da seção **"Criar blog"**. Em caso de dúvida, o contato deverá ser feito através do email **contato ARROBA milharal.org**

Por conta das diversas tentativas de censura na Internet e contra o monitoramento em massa, o nosso serviço terá como preocupação primária a salvaguarda dos seus dados (backups), assim como a manutenção da privacidade dos/as usuários/as.

Por padrão os sites hospedados possuem conexão criptografada (SSL). Não registramos IPs e apenas mantemos o email que você nos deu como contato. Por esse motivo recomendamos a utilização de emails seguros que se preocupem com a sua privacidade.

Não compartilhamos os seus dados com ninguém! Não compartilhamos informações de usuários/as com nenhum outro grupo ou indivíduo. Não monitoraremos suas comunicações e não utilizaremos os seus dados para minerar informações, estudos ou pesquisas.

Para criar um novo blog/site é necessário enviar uma descrição do seu projeto para:

admin@milharal.org

-NOBLOGS

https://noblogs.org/

Conectando pessoas radicais. Não comercial, antifascista, antisexista, plataforma de blog com privacidade orientada.
Noblogs.org é uma plataforma de blogging, um lugar virtual onde você pode abrir o seu blog ou o seu site e conhecer outras pessoas que já experimentaram o mesmo desejo.

Noblogs.org é um projeto do Coletivo A /I e pelo menos dez anos continua a prestar serviços de comunicações e conspiração para militantes e ativistas, e em geral a todos aqueles que reconhecer as prerrogativas da nossa luta manifesto e luta por uma sociedade mais justa, mais livre, para escapar do controle generalizado de empresas muito interessadas em saber quem você é e o que você pensa, ama e odeia.
Noblogs.org é um mundo de pessoas, coletivos, grupos, bandas, grupos pequenos de coordenação informal.

Noblogs.org é o servidor onde este blog está ospedado: https://terror.noblogs.org/

-NETWORK23

https://network23.org/

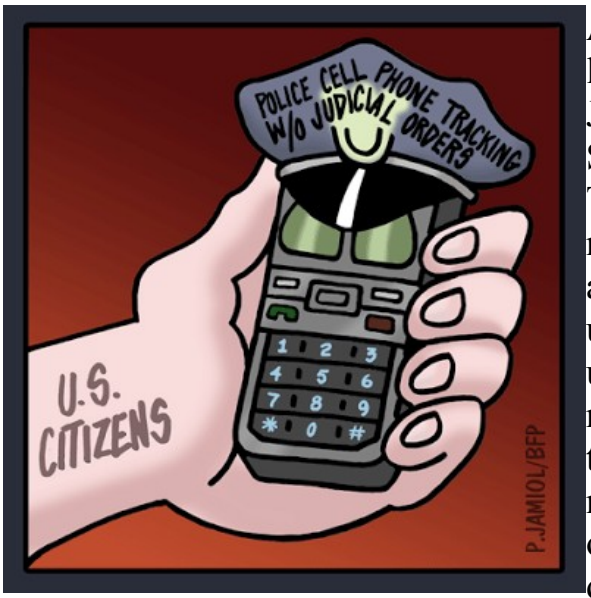
Servidor de blogs de ativistas anticapitalistas, como o movimento anti-G8, localizado no exterior, onde dificilmente os coxinhas brasileiros poderão por os pés para fechalo. Também utiliza a plataforma livre wordpress, sendo facil a migração de/para outros servidores.

PROGRAMAS ESSÊNCIAIS

Tipo de software	**Software não-livre**	**Software livre**
Compactação/descompactação de arquivos	WinRar, WinZip	7-Zip
Compartilhamento de arquivos via torrent	µTorrent, BitTorrent	Deluge, Transmission, qBittorrent
Comunicação por voz	Skype	GNU Telephony (artigo no PCWorld)
Desenho gráfico	Ilustrator, Corel Draw	Inkscape
Desenho assistido	AutoCAD	FreeCAD, OpenSCAD
Diagramação	InDesign	Scribus
Edição de áudio	FL Studio (FruityLoops)	LMMS, Audacity
Edição de imagens	Adobe Photoshop	GIMP
Edição de texto	Bloco de notas	Beaver, Notepad++, Gedit
Edição de vídeo	Adobe Premiere, Sony Vegas	Cinelerra, Openshot
Edição HTML WYSIWYG	Adobe Dreamweaver	SeaMonkey Composer
Escritório	Microsoft Office	LibreOffice
Gerência de emails	Outlook	Evolution ou Thunderbird
Gravação de CD/DVD	Nero, gravador do Windows	Brasero
Leitura de PDF	Adobe Reader, Foxit Reader	Evince, Sumatra PDF
Mapas	Google Maps, Bing Maps	OpenStreetMap
Máquina de busca	Google, Yahoo!, Bing	YaCy (em espanhol), DuckDuckGo[2]
Mensagens instantâneas	AIM, MSN, etc.	Pidgin[3], aMSN
Modelagem e animação	Autodesk 3ds Max	Blender
Navegação na internet	Internet Explorer, Opera, Chrome, Safari	Firefox
Rede social	Facebook, Orkut, Google+	Diaspora
Sistema operacional	Microsoft Windows ou Apple OS X	Distribuições de GNU/Linux

TELEFONE CELULAR

“Qualquer barulho que Winston fizesse, mais alto que um cochicho, seria captado pelo aparelho; além do mais, enquanto permanecesse no campo de visão da placa metálica, poderia ser visto também. Naturalmente, não havia jeito de determinar se, num dado momento, o cidadão estava sendo vigiado ou não. Impossível saber com que freqüência, ou que periodicidade, a Polícia do Pensamento ligava para a casa deste ou daquele individuo. Era concebível, mesmo, que observasse todo mundo ao mesmo tempo.
A realidade é que podia ligar determinada linha, no momento que desejasse. Tinha-se que viver - e vivia-se por hábito transformado em instinto na suposição de que cada som era ouvido e cada movimento examinado, salvo quando feito no escuro.”



A primeira rede de telefonia celular do Brasil foi lançada pela TELERJ, na cidade do Rio de Janeiro em 1990, seguida da cidade de Salvador. Segundo a União Internacional das Telecomunicações, o Brasil é sexto maior mercado do mundo em telefonia celular e atualmente, são 202,94 milhões de aparelhos em uso no Brasil,sendo assim o quarto país que mais utiliza telefones celulares no mundo. Atualmente no Brasil existem 247 milhões de linhas de telefones celulares ativas. Em 1989, existiam 4 milhões de assinantes do serviço móvel em todo o mundo. Em 2009 eram 4,6 bilhões, a caminho de 6 bilhões antecipados para 2013.A União Internacional de Telecomunicações considera que "O telemóvel foi a tecnologia mais rapidamente adotada de toda história".

Imagina se desse pra monitorar todas estes aparelhos...

Eu tenho certeza que você tem um celular no bolso. Em 25 anos, o celular se espalhou pelo mundo como nenhuma outra tecnologia. Chegamos a situação absurda de que no brasil existam mais celulares do que habitantes. Com os aparelhos celulares chegamos à combinação ideal entre a sociedade e o Big Brother de Orwell por meio de uma comunicação capitalista nos levando a uma submissão voluntária. Nesta situação, os indivíduos e grupos que necessitam de privacidade e liberdade estão ameaçados por vigilâncias policiais.

Se no início o telefone foi associado com o empresário, gradualmente tornou-se uma ferramenta essencial do ser humano liberal. Assim, se assemelha a muitas de suas "qualidades" emblemáticas políticas: individualista, consumidor, moderno, flexível, eficiente, móvel, em constante comunicação, etc. A utilização em massa causou a disseminiação desses valores, causando uma mudança gigantestca nas relações sociais. Por outro lado, não se nega que o celular pode ser muito útil em alguns casos. Em situações de emergência (detenções, acidentes, assaltos, etc.) não há outro meio de comunicação para alertar e reagir de forma rápida e eficiênte.

Controle Policial

O seu celular pode ser usado para ouvir sem a sua permissão. Enquanto você está falando com alguém pelo telefone celular é muito fácil para as autoridades ouvirem e gravarem a conversa em colaboração com a empresa de telefonia. No Brasil há dados oficiais sobre o número de 20 mil escutas legais. Escutas feitas com uma ordem judicial, os estados têm, em geral, mecanismos que permitem que a polícia possaa agir por iniciativa contra possíveis atos de terrorismo, pela segurança nacional, inteligência, contra "grupos subversivos", crime em geral e questões econômicas. Não há necessidade de colocar um dispositivo na linha física ou entrar na sua casa, com o perigo e custos que isso implica. Com a digitalização das comunicações, só é necessário um programa de computador e alguns cliques para monitorar a população.

Se o telefone está desligado, mas com sua bateria instalada, tecnicamente pode-se usá-lo como um microfone ambiente para ouvi-lo. A utilização desta técnica revelou, pela

primeira vez em 2003, em uma investigação do FBI no caso de alguns membros da máfia italiana. Duas solicitação judiciais do FBI falam sobre um "sistema de escuta localizado em telefone Celular". Os detalhes técnicos da transação não foram divulgados, mas especialistas dizem que é provável que eles tenham instalado sem acesso físico ao telefone, e funcionou igualmente com o telefone ligado ou desligado, mas sempre com a bateria instalada.

Com a nova geração de telefones celulares ou smartphones tipo iPhone, BlackBerry, Android, etc. ficamos mais vulneráveis. Esses dispositivos funcionam como pequenos computadores com os sistemas operacionais muito mais complexos, desenvolvidos por Apple, Microsoft, Google,etc. Estas empresas de software proprietário são conhecidas por darem prioridade aos seus interesses financeiros antes da a segurança de seus produtos, e estão totalmente dispostas a trabalhar em estreita colaboração com a polícia. Assim, como um computador que executa o Windows está cheio de vírus a cada poucos minutos, um telefone celular com qualquer sistema operacional proprietário pode ser atacado por um vírus ou um programa espião fomentado tanto por policiais como por particulares.

Na internet existem até mesmo "empresas" que oferecem seus serviços para maridos possesivos para espiar suas esposas... Em 2007, o especialista em segurança Rik Farrow publicou um exemplo de falha de segurança no iPhone, que permite a hacker tomar o controle total do aparelho, e entre outras coisas, utilar-lo como um microfone, até mesmo desligado. Lembremos que nos iPhones, até então, não é possivel remover a bateria. Outra porta de entrada vulnerável a ataques é sistema de Bluetoth, onde qualquer laptop com programas específicos pode ter acesso aos arquivos de um celular.

Localização

Ele sempre sabe onde você está. Uma máquina movel que acompanha seu posicionamento ao vivo. Para enviar uma chamada ou uma mensagem, o operador de telefonia precisa saber onde encontrar o seu celular, ou mais precisamente qual das suas antenas serão usadas para passar a comunicação. Assim, você pode aproximar a sua localização para as antenas mais próximas. A precisão desta técnica, denominada Cell-ID, dependente da densidade de antenas na rede telefónica. As cidades têm antenas de 100 ou 200 metros de distancia entre si. Mas nos campos, as antenas podem ser separadas por até 35 km. Outras informações, tais como os movimentos celulares na rede telefónica ou a sua proximidade com outras antenas podem ser utilizadas para refinar a sua localização a poucos metros no campo, por exemplo.

Operadoras de telefonia começaram nos últimos anos a usar essas informações para

propor e vender serviços (chamado dois serviços LSB): Para informar usuários de celulares quais restaurantes existem perto de sua localizaçãoo, para chamar automaticamente o táxi livre mais próximo, para lhe enviar publicidade segmentada, etc. Além colocar-lhe serviços personalizados de acordo com sua localização, as operadoras começaram a vender essa informação para outras pessoas. Várias operadoras e empresas ao redor do mundo oferecem serviços para que os pais possam localizar suas crianças. Todo seu argumento baseia-se no uso do medo dos pais, e como de costume, a suposta segurança das crianças justifica novas ameaças à nossa privacidade e incentiva controle social.

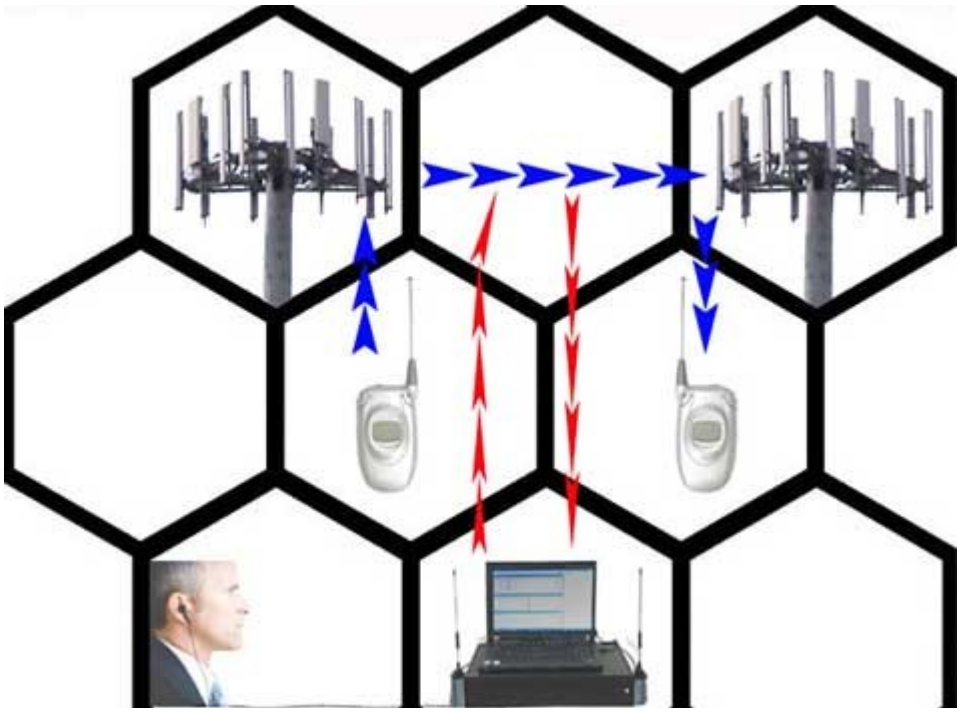
Este novo controle social pode oferecer o serviço de poder rastrear seus colegas e poder ver-los em tempo real onde estão em um mapa. A difusão dessas tecnologias e serviços de localização é acelerada pela criação de leis que impõem números centralizados de emergência, 112 na Europa, o 911 nos EUA. Estes dois números de emergência específicos que melhoram qualidade de serviço, localizam o local do chamador e são transmitido automaticamente as equipes de resgate. Então os governos e as operadoras de telefonia móvel sóobrigados por lei a trabalhar juntos para melhorar a precisão da localização de todos os telefones no mercado. As recomendações dos especialistas em serviços deste tipo recomendam uma precisão de 10 a 150 metros em áreas urbanas, 10 a 500 metros de suburbanas e rurais e 10 a 500 metros ou estradas.

A Retenção de Dados

O governo sabe onde você esteve e com quem você falou no último ano. O brasil possui leis relativas à conservação de dados que exige que as operadoras de telefonia e provedores de serviço de Internet armazenem por 12 meses as informação que identifique a origem e o destino de toda comunicação eletrônica.
- Devem manter uma lista com todas as chamadas realizadas. Assim como os números IMSI (que identificam os cartões SIM) e IMEI (número que identifica os telefones).
- Deve ser capaz de identificar as pessoas por trás desses números. Isso é feito através da ativação do numero do cartão SIM onde é necessário ceder o seu CPF.
- Devem registrar o horario de início e término da chamada e qual foi o tipo de comunicação (chamadas, voice mail, mensagens,etc).
- Devem manter toda essa informação, mesmo de chamadas não atendidas, mas não no caso de chamadas que falharam.
-Devem manter uma lista das antenas e suas localidades físicas das quais os celualares se

conectaram.
-Não pode reter quaisquer dados que revelem o o conteúdo da comunicação (exeto em investigações).
- As operadoras tem que dar essas informações aos agentes autorizados quando solicitadas.
- O período de retenção pode ser prorrogado até dois anos.

Com estas informações podem saber sem problema algum onde você esteve nos últimos 12 meses, que estavam com estavam com você, com quem você está em contato, quem são seus colegas, onde você mora e com quem, etc. Além destas informações estarem a disposição da polícia para qualquer investigação, também podem ser vendidas por empresas e funcionários corruptos a detetives e investigadores particulares.



Melhores Práticas

Tendo em vista as possibilidades de vigilância que telefones celulares permitem, temos que tomar providencias:
- Não tenha celular!
- Deixe-o em casa! Em vez de tê-lo sempre com você estaja com ele somente quando for reqalmente preciso.
- Quando estiver ligando para alguém, não fale sobre as atividades políticas ou criminosas: ações, reuniões, campanhas, etc. Pense duas vezes antes de fazer uma chamada: "Existem outras maneiras de comunicar isso? ". Dizer coisas

comprometedoras no celular pode até mesmo envolver quem não tem nada a ver com o assunto.
-Não o leve param ações diretas e manifestações em que se é possível algum embate com a polícia ou invasão ou destruição de lojas e bancos.
-Quando for para alguma reunião, de preferencia deixe o celular em casa, ou o desligue e retire a bateria a 3 kilometros de distancia do ponto de encontro. Não o ligue em nenhuma pausa da reunião, pois isso vai revelar sua localização, e caso você o desligue de novo, após a pausa, só vai provar que está escondendo algo. Só o religue depois que a reunião acabar, a no minimo 3 kilometros de distancia, mas combine com as outras pessoas que estavam na reunião, horários diferentes para cada um poder religar o celular, pois se você ligar o seu celular, que ficou horas desligado, e de companhia forem ligados mais todos os outros, o grupo estará provando que possuem alguma ligação entre si. Nunca ligue e desligue todos os celulares do grupo na mesma hora e nem no mesmo local. Tenha um relógio de pulso para poder ver as horas, para não ter que ligar o celular.
-Se você tem algum motivo importante para manter o celular ligado nesses tipos de encontros, lembre-se que está pondo todos em risco, então não deixe que sua necessidade pessoal passe por cima da necessidade de outros. Caso realmente precise estar com ocelular ligado na reunião, faça um favor a si mesmo e aous outros, NÃO VÁ NA REUNIÃO.
-Nunca passe informações por telefonema e nem por sms sobre o horario e local de encontros para ações e reuniões. Isso facilmente cria uma rede.
-Nunca acesse seu e-mail e contas de redes sociais através de seu celular. Tome cuidado com o que você pesquisa na internet através dele, lembre-se que a operadora de telefonia móvel grava tudo o que você faz nele.
-Opte por modelos menos modernos como smartphones, e que possam ter sua bateria retirada.
-Se você atua em algum coletivo, lembre-se que o descuido de qualquer um pode colocar todos em perigo.
-Só ligue seu Bluetooth quando for necessário.
-Só ligue o roteador do seu celular quando for necessário.
-Não utilize iPhone ou semelhantes que não permitem a remoção da bateria. Mas em ultimo caso, você pode enrolar o iPhone em 4 camadas papel alumínio para interromper a conexão com as antenas da operadora, mas o seu iPhone ainda poderá ser utilizado como um microfone, então o melhor caminho é tomar vergonha na cara e não comprar esse simbolo do capital, as crianças indonésias agradecem por isso!
-Não tenha imagens, videos e mensagens gravadas no celular, pois caso ele seja roubado pela polícia, não haverá prova de nada nele.
-Sempre que enviar e receber as mensagens de sua base, ou de companheiros, com informações sobre o ato ou a policia, leia e apague em seguida, não acumule provas contra si!

-Evite colocar o nome de verdade dos seus contatos de seu grupo de ação na lista telefonica do celular.
-Em dias de manifestações, onde o conflito é eminente, utilize chips e frios. Compre algum chip novo, e só o ligue no local da manifestação. Utilize-o somente para um numero pequeno de manifestações e nunca o use fora destas ocasiões. Não o coleque créditos telefonicos neste chip com seu cartão de credito ou em lojas que possuam cameras ou que você frequente. Diz-se chip frio porque ele não deve estar no seu CPF, cadastre-o somente na hora da manifestação com um número de CPF que não tenha nenhuma ligação com você. Você pode encontrar um gerador de CPF http://www.geradordecpf.org/, geralmente o CPF gerado nesses sites faz com que o chip dure um dia, aí ele é bloqueado e você tem que comprar outro. Ou então utilize o CPF de alguém famoso, um coxinha, um representante politico...
Nas mesmas situações, também utilize um celular frio, um celular onde você ou alguém próximo nunca tenha utilizado um chip pessoal nele. Você pode conseguir um celular frio comprando em bazares e brechós, ou até mesmo na biqueira.
-Estes procedimentos também valem e são necessárias a TABLETS.
-Lembre-se que nem sempre existiu aparelhos celulares e que as pessoas utilizavam outros meios de se organizar. Marighella não sequestrou o embaixador dos EUA em meio a ditadura militar utilizando um smartphone.

CAMERAS

Sorria, você está sendo filmado! Em cada esquina da cidade, encima de cada vitrine de banco que por nós foi apedrejada, na porta de cada butique luxuosa pixada, nos caixas das lojas saqueadas, no peito do gambé, no *dhrone* sobre nossas cabeças em meio as fugas, encima dos prédios corporativos, encima do furgão da policia militar (ah, o TV coxa!), nos celulares grampiados e provavelmente nesse computador que você está usando para ler isso agora. Cada canto da cidade está vigiado por uma câmera de algum sistema de vigilancia particular ou estatal. Graças ao maldito evento corporativo da Copa do Mundo a situação vem piorando, porcausa da integração de monitoramneto de cameras em tempo real e ações coletivas das policias militares, guardas civis, companias de engenharia de trafego de transito e mega empresas, todos nós estamos sendo vigiados na grande prisão de concreto. Cada um de nós está sujeito de produzir provas contra si mesmos, e tudo isso pela segurança de todos. As câmeras estão presentes em cada esquina para única e exclusivamente proteger a propriedade privada e interesses da burguesia (meio óbvio isso, não existem cameras de segurança na favela, apenas nos centros das cidades e nas casas e lojas luxuosas).

Hoje é praticamente impossível se esquivar desse tipo de monitoramento em locais abertos, é preciso sempre lembrar que você esta sendo filmado, que cada gesto seu esta sendo medido e analisado. E que muito diferente dos supermercados que tem seus produtos magaicamente desaparecendo nas mangas e debaixodas blusasde mágicos famintos em pontos cegos dos corredores de departamento, em manifestações de ruas sempre haverá uma camera apontada pra você. Em ações diretas sempre é preciso ter a cautela de estar com o rosto mais coberto quanto for possível, e de ter outra roupa para poder se trocar na hora da fuga..

Cuidados devem ser tomados:

- Nunca faça uma reunião em local aberto onde tenha, ou possa ter, cameras de vigilância.

- Caso esteja em algum lugar que possua cameras e precise falar algo comprometedor a alguém, tampe a boca com um livro, um pano ou com as mãos para que que os movimentos de seus lábios não sejam gravados, evitando assim o artificio de leitura de lábios por parte de possíveis investigações.
- Sempre que for fazer ulguma ação direta, em manifestações ou não, lembre-se que você poderá estar sendo filmado. Analise os riscos, cubra o rosto.
- De preferencia use roupas pretas, é mais dificil pra policia poder rastrear alguém vestido assim em meio a multidão através de cameras, seria mais interessante se todas as pessoas que vão para manifestações e protestos se vestissem de preto, assim tudo se misturaria nas tvs da policia, principalmente a noite, e quando ocorrer alguma ação, dificilmete consiguirá identificar e seguir alguém através das cameras.
- Caso você esteja com algum grupo de afinidade, ou em um Black Bloc e vá fazer alguma ação direta como por exemplo, pixar a faixada de alguma loja, ou quebrar a vidraça de algum banco, combine com o seu grupo de portar lanternas e lasers potentes, sendo que estas podem ser apontadas para as cameras dos reporteres carniceiros, evitando assim o registro de imagens comprometedoras. Isso também funciona muito bem pra impedir a visão policial vinda dos elicópteros que monitoram as marchas de revolta.
- Lembre-se: apontar um laser pra um policial ou seu helicóptero é crime. Mas quem é o criminoso aqui?
- Por mais que sejam utilizadas para vigiar a todos, as cameras ainda servem para nos proteger das agressões policiais e de prisões arbitrárias. A maioria dos malditos celulares possuem cameras, então sempre pronto para apertar o botão de gravar se isso provar o abuso de autoridade dos porcos fardados, sempre grave prisões e abordagens. Se o gambé vier falar que você não pode gravar ele, saiba que isso é mentira, você esta na rua e ele é uma pessoa pública, ninguém precisa ser reporter pra gravar algo, e além de tudo, se ele vier falar com você, tu tem todo o direito de gravar sua conversa com ele, além de suas ameaças.

ESCUTAS E CAMERAS ESCONDIDAS

É bem possível que grupos de atuações polítcas mais radicais estajam sendo monitorados no ultimo lugar em que qualquer um poderia imaginar. No seu QG, no seu ponto de encontro, no seu local de reuniões sigilosas pode haver alguma camera ou escuta escondida. No local que você e seu grupo de ações pensam estar seguros pode estar minado de olhos e ouvidos digitais do inimigo. Sempre é necessário fazer varreduras nestes locais. Ter certeza que o acesso a estes locais é restrito e só você e seu grupo de apoio tem acesso a ele, garantir que ninguém mais abaixo do conhecimento de segurança basica em comum tenha acesso a ele.
De tempos e tempos, fazer uma verificação detalhada de cada metro quadrado do espaço e de cada objeto que se encontre nele.
Verificar:
-dentro de tomadas;
-dentro de armários;
-nos forros do teto e paredes;
-embaixo de mesas e cadeiras;
-atraz de armários;
-dentro de computadores;
-dentro de sofás;
-atraz de quadros;
-dentro de rádios;
-dentro de abajours;
-dentro de tvs....

Verefique tudo que possa ser aberto. Não se esqueça de procurar por fundos falsos e partes ocas das paredes.
Caso alguém encontre uma escuta ou camera escondida, só restara a destruição do mesmo, mas deverá ser feita uma conversa com todos os utilizadores do espaço para tentarem descobrir quais foram os pontos fracos na segurança coletiva que permitiram a instalação de tais aparelhos. Deverão também abortar todas as ações e operações ilegais planejadas e destruirem tudo que possa lhes incriminar. Além da nova paranóia de que sempre haverá alguém na rua vigiando quem entra e sai do tal espaço, que deverá ter como preucaução básica a saida e a chegada das pessoas em grupos para evitarem possíveis sequestros.

O QUÃO FORTE É A SUA SENHA?

Ter a senha roubada é um enorme medo para muitos usuários de serviços da internet. Desde o login de E-mails à Contas de banco, todos nós temos senhas que acessam diferentes partes de nossas vidas. Infelizmente, muitos de nós utilizam senhas fracas ou comuns para vários tipos de sites. Hackers podem roubar suas senhas de formas mais simples do que você pode imaginar. Muitas pessoas utilizam como senha seus nomes, data de nascimento, palavras comuns que hackers podem facilmente descobrir para ter acesso a informações pessoais.
Informações pessoais que podem ser muito comprometedoras, como arquivos, contatos, conversas secretas sobre assuntos ilegais ou planos de ação direta.
Ter sua senha roubada pode significar muita dor de cabeça, se te roubam a senha de seu e-mail de ativismo você pode correr risco de que quem o invadiu consiga alguma informação comprometedora, ou que forje provas contra você. O mesmo acontece com suas contas de redes sociais.
Para se livrar de possíveis dores de cabeça, ridicularizações públicas e até mesmo de uma possível prisão é preciso ter alguns critérios na hora da confecção e administração de suas senhas.

<u>O que NÃO fazer:</u>
-Nunca utilize a mesma senha para diversas coisas;
-Não utilize uma senha que seja igual ao seu login, por exemplo john123@riseup.net com a senha john123;
-Não utilize a data de seu nascimento como senha;
-Evite senhas ridículas como 12345678, qwerty, asdfghjkl, 87654321, senhariseupjohn, senha, senha123, numero do RG etc.
- Na criação de alguma conta em algum site, não de respostas verdadeiras às perguntas de segurança, como “qual é a cidade natal de seus pais”, “Qual foi a sua professora da primeira série”, etc. Caso alguém saiba estas respostas, poderá conseguir acesso as respectivas contas;
-Não guarde as suas senhas em documento no computador ou em uma agenda ou caderno;
-Quando fazer login em algum site, rejeite a opção de guardar a sua senha;
-Não crie sua senha em geradores de senha oferecidos online.

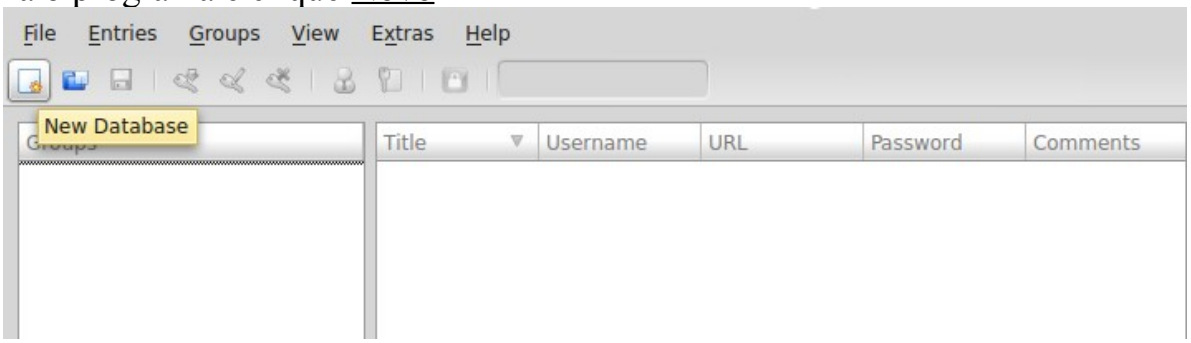
O que fazer:
-Tenha senhas diferentes para diferentes logins, contas e sites;
-Senhas maiores são mais dificeis de serem quebradas;
-Capriche na sua senha de criptografia do seu computador;
-Utilizie caracteres diferentes e combinados, como letras maiuscas com letras minúsculas, símbolos e números. Exemplo de senha: qkdES-&d86mknFG+sod@%~=;
-Troque suas senhas em um período contínuo de 3 em 3 meses.
-Utilize o KeePassX para guardar suas senhas:

KeePassX

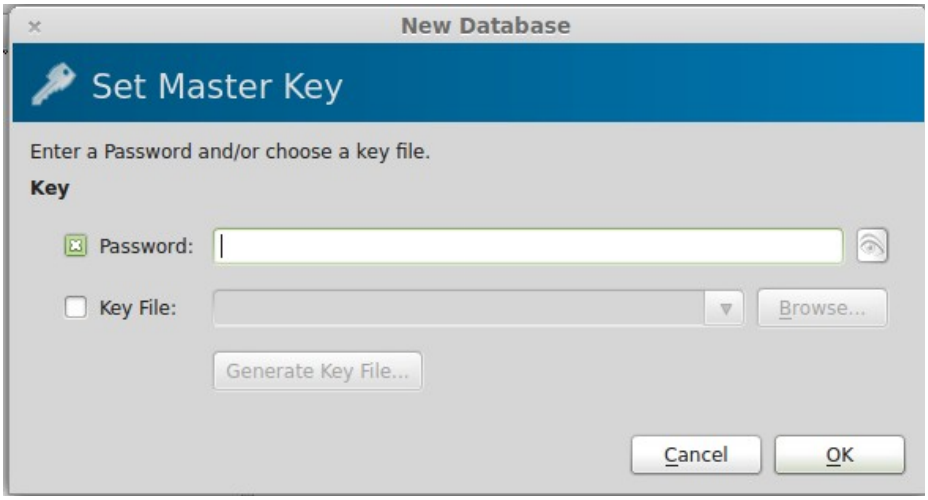
KeePassX é uma ferramenta de administração de senhas. Nele você pode salvar todas as suas senhas criando um arquivo criptografado com uma senha mestra. O Programa é livre e roda muito bem em linux e possui um gerador de senhas próprio.

Para salvar e gerenciar suas senhas utilize os seguintes passos:

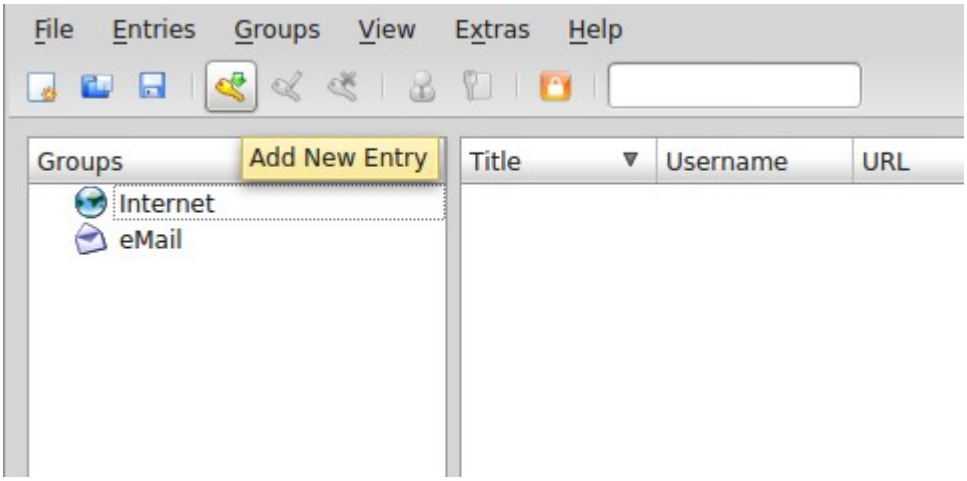
1) abra o programa e clique Novo



2) Crie uma senha. Essa senha será a senha mestra, portanto faça uma senha grande e bem difícil! (mas que você lembre). Repita a senha.

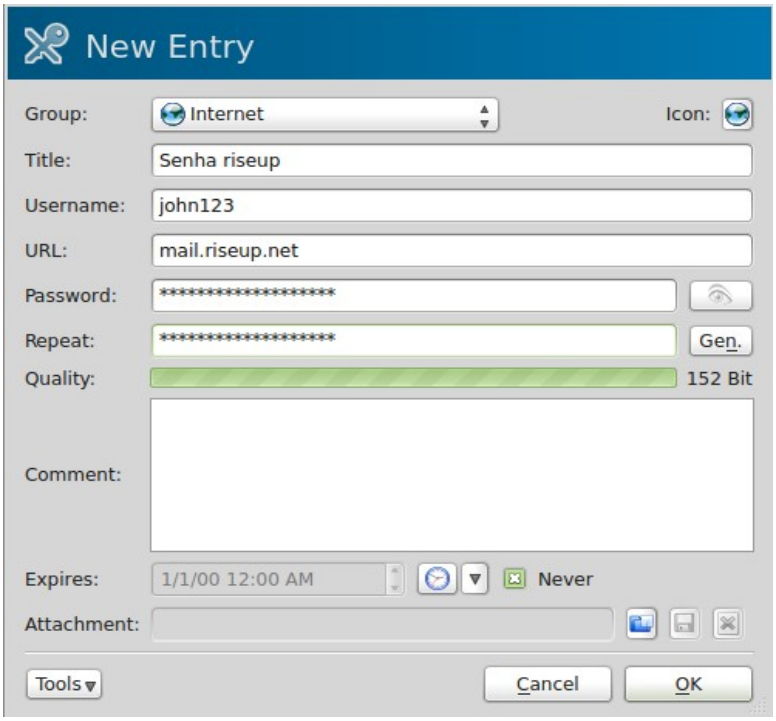


3)Abrirá a seguinte janela:

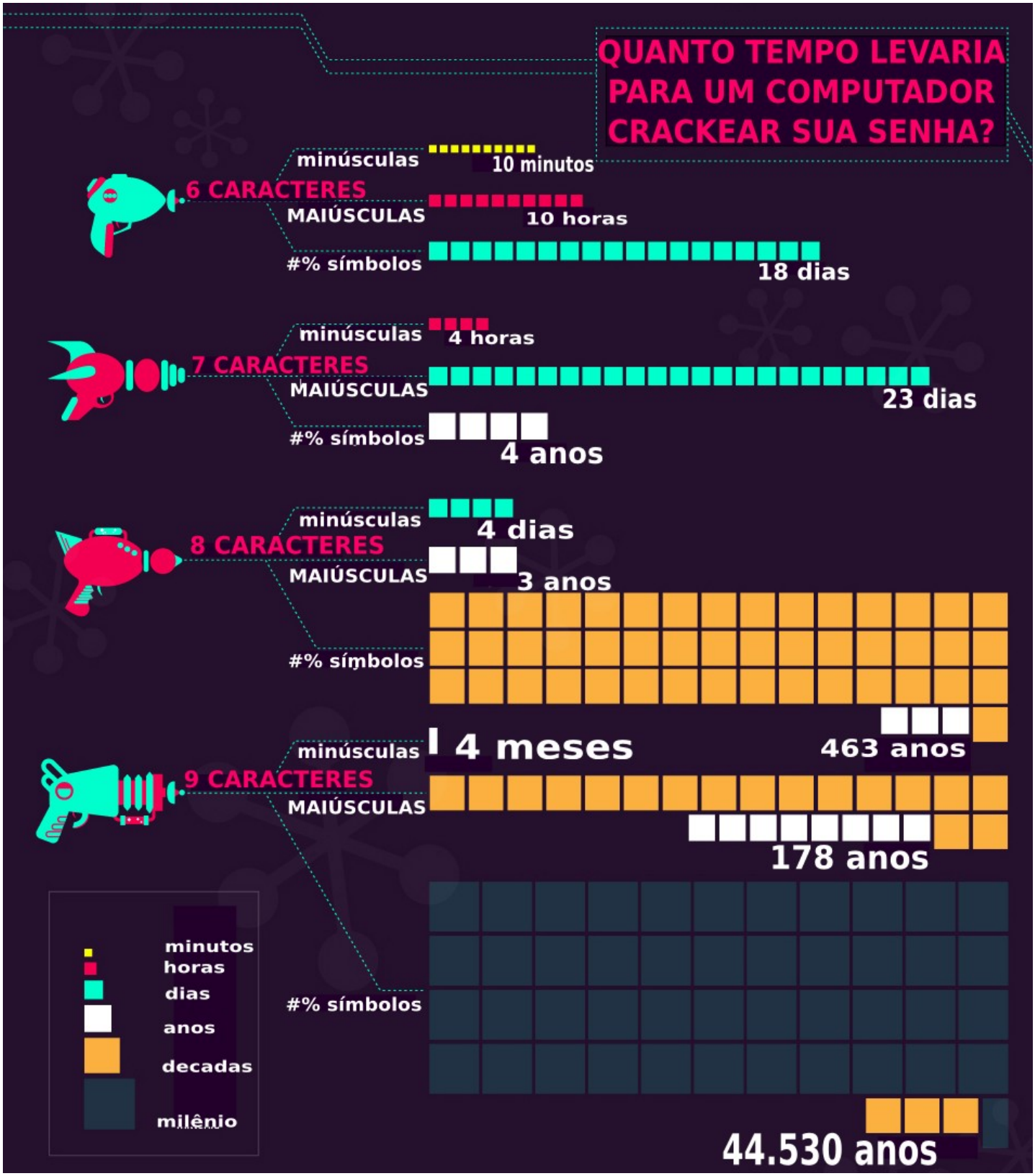


Click em Adicionar nova entrada:

4) Na seguinte janela adicione um titulo, o seu login, sua senha, url e comentários. Você também pode marcar uma data nele pra saber quando será preciso trocar essa senha.



5) Salve o arquivo. Agora sempre que você precisar abrir este documento, terá que utilizar a sua senha mestre para ter acesso ao conteúdo. Somente com esta senha mestra você terá acesso a informação, pois o conteúdo estara criptografado.


QUANTO TEMPO LEVARIA PARA UM COMPUTADOR CRACKEAR SUA SENHA?
6 CARACTERES
minúsculas
10 minutos
MAIÚSCULAS
10 horas
#% símbolos
18 dias
7 CARACTERES
minúsculas
4 horas
MAIÚSCULAS
23 dias
#% símbolos
4 anos
8 CARACTERES
minúsculas
4 dias
MAIÚSCULAS
3 anos
#% símbolos
463 anos
9 CARACTERES
minúsculas
4 meses
MAIÚSCULAS
178 anos
#% símbolos
44.530 anos
minutos
horas
dias
anos
decadas
milênio


Lembre-se, meu filho,
Black Bloc não tem líder!

CRIMES DIGITAIS

Crime informático, **e-crime**, **cybercrime**, **crimes eletrônicos** ou **crime digital** são termos utilizados para se referir a toda a atividade onde um computador ou uma rede de computadores é utilizada como uma ferramenta, uma base de ataque ou como meio de crime.

Adicionalmente embora os termos crimes eletrônicos ou cybercrimes sejam mais apropriadamente utilizados para descrever atividades criminais que façam o uso de computadores ou de uma rede de computadores, estes termos também são utilizados para descrever crimes tradicionais, tais como fraudes, roubo, chantagem, falsificação e apropriação indébita, na qual computadores ou rede de computadores são usados para facilitar as atividades ilícitas.

Essa categoria de crime apresenta algumas características, dentre elas: transnacionalidade – pois não está restrita apenas a uma região do globo - universalidade – trata-se de um fenômeno de massa e não de elite - e ubiqüidade – ou seja, está presente nos setores privados e públicos.
O crime por computador pode acarretar danos tanto pessoais como empresariais. Os danos pessoais são obtidos no envio de mensagens com conteúdo pejorativo, falso ou pessoal em nome da pessoa, utilizando somente os dados dos e-mails, na movimentação de contas bancárias com o intuito de fazer transações, saques ou até mesmo pagamento de contas, na utilização de dados de cartão de crédito para fazer compras e na divulgação de fotos ou imagens com intenção de causar danos morais.

As empresas também sofrem com estas invasões nos seus dados e informações confidenciais. Os crimes ocasionam não somente danos financeiros, mas também danos empresariais, visto que as organizações têm que fazer novamente a manutenção das máquinas danificadas.

O aparecimento dos primeiros casos de crimes informáticos data da década de 1960, que nada mais eram que delitos onde o infrator manipulava, sabotava, espionava ou exercia uso abusivo de computadores e sistemas. A partir de 1980, houve um aumento das ações criminosas, que passaram a refletir em, por exemplo, manipulações de caixas bancários,

abusos de telecomunicação, pirataria de programa e pornografia infantil.

Classificação:

Crime virtual puro - compreende em qualquer conduta ilícita, a qual atenta o hardware e/ou software de um computador, ou seja, tanto a parte física quanto a parte virtual do microcomputador.

Crime virtual misto - seria o que utiliza a Internet para realizar a conduta ilícita, e o objetivo é diferente do citado anteriormente. Por exemplo, as transações ilegais de valores de contas correntes.

Crime virtual comum - é utilizar a Internet apenas como forma de instrumento para realizar um delito que enquadra no Código Penal, como, por exemplo, distribuição de conteúdo pornográfico infantil por diversos meios, como messengers, e-mail, torrent ou qualquer outra forma de compartilhamento de dados.

O criminoso informático é denominado - vulgarmente - hacker, e este pode ser classificado em dois tipos: interno e externo. Interno são aqueles indivíduos que acessam indevidamente informações sigilosas de um nível superior. Normalmente são funcionários da empresa ou servidores públicos. O externo é aquele que não tem acesso e utiliza um computador ou redes externas, ressaltando que não tem ligação à organização que ataca.

Segurança:

O problema da segurança informática pode ser decomposto em vários aspectos distintos, sendo mais relevantes os seguintes:

Autenticação - é um dos aspectos fundamentais da segurança. Em muitos casos, antes de fazer sentido qualquer tipo de comunicação ou qualquer tipo de mecanismo para a

garantia de outros aspectos de segurança, há que previamente garantir que as entidades intervenientes são quem afirmam ser. A autenticação é o processo através da qual é validada a entidade de um utilizador.

Confidencialidade - reúne as vertentes de segurança que limitam o acesso à informação apenas às entidades autorizadas (previamente autenticadas), sejam elas utilizadores humanos, máquinas ou processos.

Integridade - permite garantir que a informação a ser armazenada ou processada é autêntica, isto é, que não é corrompida.

Ainda tem o principio da disponibilidade que os computador a rede tem que esta disponível a todos momentos não podendo cair em nível global.

Crimes Comuns:
Os crimes mais comuns praticados contra organizações são:

Espionagem - ocorre quando obtém informações sem autorização;

Violação de autorização - quando utiliza a autorização de outra pessoa para finalidades desconhecidas;

Falsificação por computador - acontece quando ocorre uma modificação dos dados;

Vazamento - revelação indevida de informação;

Sabotagem computacional - ocorre quando os dados são removidos ou modificados com o intuito de alterar o funcionamento da máquina;

Recusa de serviço - não atende à solicitação das requisições legítimas dos usuários;

Moral - ocorre quando o servidor on-line (público ou prívado)(prestador de serviços, como comunicações, entretenimento, informativo, etc...) expressa diretamente ou indiretamente, atos tais como, racismo, xenofobia, homofobia, humilhação, repreensão, ou outros atos que agridem moralmente o usuário;

Repúdio - negação imprópria de uma ação ou transação efetivamente realizada.

E todos esses **crimes** acarretam em penalizações perante a **lei**.

Existem ainda outros tipos de crimes praticados, tanto contra organizações quanto contra indivíduos. São estes:

Spamming - conduta de mensagens publicitárias por correio eletrônico para uma pequena parcela de usuários. Esta conduta não é ilícita, mas sim antiética.

Cookies - são arquivos de texto que são gravados no computador de forma a identificá-lo. Assim, o site obtém algumas informações tais quais: quem está acessando ao site, com que periodicidade o usuário retorna à página da web e outras informações almejadas pelo portal. Alguns sites obrigam o usuário a aceitar cookies para exibir seu conteúdo. O problema maior é descobrir se o cookie é legítimo ou não e se, além disso, para o que serão utilizadas as informações contidas no cookie;

Spywares - são programas espiões que enviam informações do computador do usuário para desconhecidos na rede.

Hoaxes - são e-mails, na maioria das vezes, com remetente de empresas importantes ou órgãos governamentais, contendo mensagens falsas, induzindo o leitor a tomar atitudes prejudiciais a ele próprio;

Sniffers - são programas espiões semelhantes ao spywares que são introduzidos no disco rígido e tem capacidade de interceptar e registrar o tráfego de pacotes na rede;

Trojan horse ou cavalos de Tróia - quando instalado no computador o trojan libera uma porta de acesso ao computador para uma possível invasão. O hacker pode obter informações de arquivos, descobrir senhas, introduzir novos programas, formatar o disco rígido, ver a tela e até ouvir a voz, caso o computador tenha um microfone instalado. Como a boa parte dos micros é dotada de microfones ou câmeras de áudio e vídeo, o trojan permite fazer escuta clandestina, o que é bastante utilizado entre os criminosos que visam à captura de segredos industriais;

Cyberbullying - definido como quando a Internet, telefones celulares ou outros dispositivos são utilizados para enviar textos ou imagens com a intenção de ferir ou constranger outra pessoa.

Pirataria - baixar músicas, filmes e softwares pagos na Internet para depois copiar em CD ou DVD e distribuí-los gratuitamente ou mediante pagamento (sendo que o dinheiro não é repassado ao detentor dos direitos legais).

No Brasil:

A atuação da polícia em crimes de computador requer investigação especializada e ação efetiva. Empresas em diversos pontos do País têm sido vítimas dos crimes de

computadores, e o fato só não é mais grave, porque existe a "síndrome da má reputação", que leva as empresas a assumirem os prejuízos, encobrindo os delitos, ao invés de ter uma propaganda negativa, e também porque o grupo de criminosos digitais ainda é pequeno.

Em uma pesquisa divulgada pela consultoria Mi2g Intelligence Unit, em dezembro de 2004, foi constatado que o Brasil é o sétimo de dez países que mais possuem hackers responsáveis pelas invasões de sites no mês de outubro de 2004. Além disso, o Brasil é considerado um dos países que tem mais hackers ativos no mundo, com 75% dos ataques às redes mundiais partindo do Brasil.

Os criminosos digitais brasileiros agem em campos diversos, como roubo de identidade, fraudes de cartão de crédito, violação de propriedade intelectual e protestos políticos (isso é crime?).

De acordo com a empresa britânica de segurança da informação, a cópia de software e dados protegidos por direitos autorais e pirataria, bem como o vandalismo on-line, são alguns dos métodos ilícitos cada vez mais adotados por hackers brasileiros.

Outro recorde alcançado pelos piratas do Brasil foi o número de grupos de hackers na lista TOP 10, dos "dez mais ativos". O Brasil ocupa todas as posições.

Com isso, eles conseguiram que o português se tornasse a língua oficial do movimento hacker na internet.

A proliferação de ferramentas gratuitas para ataques, as poucas leis para a prevenção dos crimes digitais e o crescente índice de grupos organizados para explorar oportunidades para o "cybercrime" são as principais causas apontadas pelo estudo para o aumento dessas ações na internet.

Poucos hackers brasileiros têm a mesma especialização em computadores como têm os europeus que vêm atacando desde os anos 90, que até mesmo chegaram a escrever seus próprios programas para garantir ataques bem sucedidos.

Desde 1995, a Polícia Civil de São Paulo orgulha-se de ter dado o primeiro passo em harmonia com a vanguarda internacional da investigação digital, ao ser a primeira instituição da América Latina a possuir página na Rede Internacional de Dados - Internet, com diversas informações sobre a atividade policial desenvolvida, orientações de auxílio ao cidadão, bem como campo para receber sugestões e denúncias, além de um arquivo com fotos digitalizadas dos criminosos mais procurados pela polícia, e fotos de crianças desaparecidas.

A Polícia Civil de São Paulo, através do DCS - Departamento de Comunicação Social, vem, há algum tempo, efetuando investigações de crimes por computadores com muito sucesso - apesar de não existir atribuição administrativa para tanto, existe apenas o embasamento jurídico do próprio Código de Processo Penal (art. 6º e incisos) - e

decisões em inquéritos policiais, bem recebidos pelo Ministério Público e Juiz Corregedor da Capital.

As denúncias de crimes praticados pela Internet tem aumentado. Dados do Ministério Público Federal (MPF) apontam que entre 2007 e 2008 o número de procedimentos abertos na Procuradoria para investigar crimes cibernéticos subiu 318%. Em 2007, foram abertas 620 investigações, menos de um terço dos 1.975 procedimentos abertos somente no ano passado. De acordo com a assessoria de comunicação da entidade, três denúncias feitas em 2007 são investigadas pelo MPF de Bauru.

Em 11 de Fevereiro de 2009, Dia Mundial da Internet Segura, a SaferNet – entidade voltada ao combate aos crimes e violações aos Direitos Humanos na Internet – em parceria com o Departamento da Polícia Federal (DPF) e o MPV, divulgaram os indicadores anuais sobre as denúncias de delitos relacionados à rede mundial.

Os dados da Central Nacional de Denúncias de Crimes Cibernéticos mostram que em 2008 foram denunciadas 91.038 páginas da Internet, das quais 57.574 (63,2%) referentes ao crime de pornografia infantil. A variação em comparação com o período anterior é três vezes superior. O endereço eletrônico da SaferNet disponibiliza uma ferramenta que possibilita acompanhar e comparar a quantidade de denúncias sobre páginas consideradas criminosas.

Hackers, Phreakers e Pirates

Existe uma camada de "cybercriminosos" que, pela sua longa e ativa permanência no meio, merecem um destaque especial. Estes "cybercriminosos" existiam mesmo antes de a Internet se popularizar da forma como fez nos últimos anos.

Assim, independentemente de partilharem o meio com muitos outros utilizadores "normais" (milhões e milhões, no caso da Internet), os h/p&p formam uma micro-sociedade que difere de todas as outras por ser mais invisível e resguardada. É esta invisibilidade que leva com que surjam definições para estes indivíduos.

Apesar do termo hacker ter sido usado desde os anos 50 para descrever programadores "free-lancer" e de tecnologia de ponta, essa conotação tem caído em desuso, dando lugar a uma outra que tem sido popularizada pelos media: hacker é aquele que obtém acesso não autorizado a um sistema de computadores.

No entanto, é frequente o uso da palavra hacker em qualquer tipo de crime relacionado com computadores.

O uso indiscriminado dos termos para referir as muitas e variadas formas não ortodoxas de uso de computadores tem sido contra a compreensão da extensão destas atividades. Podemos então dar as seguintes definições mais acuradas:

Hacker - Indivíduo associado especializado em obter acesso não autorizado em sistemas e redes de computadores;

Phreaker - Indivíduo associado especializado em obter informação não autorizada sobre o sistema telefónico;

Pirate - Indivíduo especializado em reunir e distribuir software protegido por copyright.

As leis no Brasil

O Brasil é um país onde não se tem uma legislação definida e que abrange, de forma objetiva e geral, os diversos tipos de crimes cibernéticos que ocorrem no dia-a-dia e que aparecem nos jornais, televisão, rádio e revistas(mentira). A mídia é a principal ferramenta de propagação desses acontecimentos e como conseqüência disso, o crescimento do comércio e mercado virtual fica prejudicado por não se existir uma grande segurança para os usuários contra esses crimes informáticos.

Na ausência de uma legislação específica, aquele que praticou algum crime informático deverá ser julgado dentro do próprio Código Penal, mantendo-se as devidas diferenças. Se, por exemplo, um determinado indivíduo danificou ou foi pego em flagrante danificando dados, dados estes que estavam salvos em CDs de sua empresa, o indivíduo deverá responder por ter infligido a Lei 163 do Código Penal, que é "destruir, inutilizar ou deteriorar coisa alheia: pena – detenção, de um a seis meses, ou multa". Os crimes informáticos, mesmo sem uma lei específica, podem ser julgados pela Lei brasileira. Seguem abaixo os principais crimes, ressaltando de que são crimes contra o computador, portanto um bem, e que são previstos no Código Penal Brasileiro.

Pirataria - Copiar em CDs, DVDs ou qualquer base de dados sem prévia autorização do autor é entendido como pirataria de acordo com a Lei 9.610/98. De acordo com o Art. 87 da mesma lei, "o titular do direito patrimonial sobre uma base de dados terá o direito exclusivo, a respeito da forma de expressão da estrutura da referida base". A mesma lei também não protege os criminosos que copiam sem prévia autorização programas de softwares. As penas podem variar de 2 meses a 4 anos, com aplicação ou não de multa, a depender se houve reprodução parcial ou total, venda e se foi oferecida ao público via cabo, fibra óptica.

Dano ao patrimônio - Previsto no art.163 do Código Penal. O dano pode ser simples ou qualificado, sendo considerado qualificado quando "o dano for contra o patrimônio da

União, Estado, Município, empresa concessionária de serviços públicos ou sociedade de economia mista". Observe que para qualificado o objeto do dano deverá ser União, Estado, Município, empresa concessionária de serviços públicos ou sociedade de economia mista, podendo ser aplicado, por exemplo, aqueles crimes de sabotagem dentro de repartições públicas. A mesma lógica é utilizada quando se trata de vírus, por ser considerada como tentativa (perante comprovação) de dano. A punição para dano simples é de detenção, de um a seis meses, ou multa. Já para dano qualificado, a pena prevista é detenção de seis meses a três anos e multa.

Sabotagem informática - A sabotagem, em termos econômicos e comerciais, será a invasão de determinado estabelecimento, visando prejudicar e/ou roubar dados. Segundo Milton Jordão, "consiste a sabotagem informática no acesso a sistemas informáticos visando a destruir, total ou parcialmente, o material lógico ali contido, podendo ser feita através de programas destrutivos ou vírus". A Lei apenas prevê punição de 1 a 3 anos de prisão e multa, porém não inclui a sabotagem informática em seu texto.

Apropriação indébita - O Código Penal faz menção apenas à apropriação indébita de bens materiais, tais como CPU, mouse e monitor, ficando excluídos desses a apropriação de informações. Contudo, se a apropriação se deu através de cópia de software ou de informações que legalmente pertencem a uma instituição, podem-se aplicar punições por pirataria. A pena para apropriação indébita está prevista no artigo 168 sendo de reclusão de 3 a 6 anos e multa para quem praticar ato fraudulento em benefício próprio.

Estelionato - Neste tipo de crime, o Código Penal pode ser aplicado de acordo com o seu artigo 171, desde que o mesmo tenha sido consumado. Segundo Da Costa (1997), "consuma-se pelo alcance da vantagem ilícita, em prejuízo alheio. É também admissível, na forma tentada, na sua amplitude conceitual, porém é de ser buscado o meio utilizado pelo agente, vez que impunível o meio inidôneo". A pena é de reclusão de 1 a 5 anos e multa.

Divulgação de segredo - O Código Penal nada cita caso o segredo seja revelado via computador, sendo tratado da mesma forma que divulgado por documento, por se tratar de uma forma de correspondência.

Lei Carolina Dieckmann

A **Lei Carolina Dieckmann** é o apelido que recebeu a Lei Brasileira 12.737/2012, sancionada em 3 de dezembro de 2012 pela Presidente Dilma Rousseff (publicada no DOU 03/12/12 PÁG 01 COL 03.), que promoveu alterações no Código Penal Brasileiro (Decreto-Lei 2.848 de 7 de dezembro de 1940), tipificando os chamados delitos ou crimes informáticos.

A legislação é oriunda do Projeto de Lei 2793/2011, apresentado em 29 de novembro de 2011, pelo Deputado Paulo Teixeira (PT-SP), que tramitou em regime de urgência e em tempo "record" no Congresso Nacional, em comparação com outros projetos sobre delitos informáticos que as casas de leis apreciavam (como, por exemplo, o PL 84/1999, a "Lei Azeredo", também transformado em lei ordinária 12.735/2012 em 3 de dezembro de 2012).

O Projeto de Lei que resultou na "Lei Carolina Dieckmann" foi proposto em referência e diante de situação específica experimentada por uma burguesa, em maio de 2011, que supostamente teve copiadas de seu computador pessoal 36 (trinta e seis) fotos em situação íntima, que acabaram divulgadas na Internet.

O Lei vem merecendo críticas de juristas, peritos, especialistas e profissionais de segurança da informação, pois seus dispositivos são amplos, confusos e podem gerar dupla interpretação, ou mesmo interpretação subjetiva, o que pode ser utilizado para enquadramento criminal de condutas triviais ou mesmo para a defesa e respaldo de infratores cibernéticos, o que tornaria a lei injusta e ineficaz. Para outra corrente, ainda, as penas são pouco inibidoras, sendo muitas situações enquadráveis nos procedimentos dos Juizados Especiais, o que poderia contribuir para a não eficiência no combate ao crime cibernético no Brasil.

A PRESIDENTA DA REPÚBLICA

Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Art. 1º Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.

Art. 2º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:

> "**Invasão de dispositivo informático**
>
> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
>
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de

permitir a prática da conduta definida no **caput**.

§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:

I - Presidente da República, governadores e prefeitos;

II - Presidente do Supremo Tribunal Federal;

III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou

IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal."

"**Ação penal**

Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos."

Art. 3º Os arts. 266 e 298 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, passam a vigorar com a seguinte redação:

"**Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública**

Art. 266. .....

§ 1º Incorre na mesma pena quem interrompe serviço telemático ou

de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

§ 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.” (NR)

“**Falsificação de documento particular**

Art. 298. .....

Falsificação de cartão

Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.” (NR)

Art. 4º Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial.

Brasília, 30 de novembro de 2012; 191º da Independência e 124º da República.

DILMAROUSSEFF
José Eduardo Cardozo

Claro que estas leis só se aplicam a pobres e negros. Playboys, Grandes empresas e Governantes são IMUNES a essas leis e represárias.

LEI 12.850 A LEI ANTI BLACK BLOC

Como já não bastava a maldita Lei de Segurança Nacional, as grandes elites, deparadas as atuais revoltas populares, decretaram no dia 2 de agosto de 2013 a Lei 12.850. É a lei que define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal. Com o aval desta lei, qualquer um pode ser preso pela suposta "organização criminosa" em que se possa ter alguma relação, relação esta que será provada, ou induzida, atarvés de métodos digitais de investigação, sem mandato nenhum, sem você nem sequer saber que é um suspeito... Diante de tal lei, Células Black Blocs podem ser consideradas como terroristas se tiverem alguma ligação internacional, o que não é muito dificil, pois as táticas Black Bloc são táticas internacionais, e as diferentes ramificações do anarquismo então, estão todas condenadas, pois todas são internacionalistas.

CAPÍTULO I

DA ORGANIZAÇÃO CRIMINOSA

Art. 1º Esta Lei define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal a ser aplicado.

§ 1º Considera-se organização criminosa a associação de 4 (quatro) ou mais pessoas estruturalmente ordenada e caracterizada pela divisão de tarefas, ainda que informalmente, com objetivo de obter, direta ou indiretamente, vantagem de qualquer natureza, mediante a prática de infrações penais cujas penas máximas sejam superiores a 4 (quatro) anos, ou que sejam de caráter transnacional.

§ 2º Esta Lei se aplica também:

I - às infrações penais previstas em tratado ou convenção internacional quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente;

II - às organizações terroristas internacionais, reconhecidas segundo as normas de direito internacional, por foro do qual o Brasil faça parte, cujos atos de suporte ao terrorismo, bem como os atos preparatórios ou de execução de atos terroristas, ocorram ou possam ocorrer em território nacional.

Art. 2º Promover, constituir, financiar ou integrar, pessoalmente ou por interposta pessoa, organização criminosa:

Pena - reclusão, de 3 (três) a 8 (oito) anos, e multa, sem prejuízo das penas correspondentes às demais infrações penais praticadas.

§ 1º Nas mesmas penas incorre quem impede ou, de qualquer forma, embaraça a investigação de infração penal que envolva organização criminosa.

§ 2º As penas aumentam-se até a metade se na atuação da organização criminosa houver emprego de arma de fogo.

§ 3º A pena é agravada para quem exerce o comando, individual ou coletivo, da organização criminosa, ainda que não pratique pessoalmente atos de execução.

§ 4º A pena é aumentada de 1/6 (um sexto) a 2/3 (dois terços):

I - se há participação de criança ou adolescente;

II - se há concurso de funcionário público, valendo-se a organização criminosa dessa condição para a prática de infração penal;

III - se o produto ou proveito da infração penal destinar-se, no todo ou em parte, ao exterior;

IV - se a organização criminosa mantém conexão com outras organizações criminosas independentes;

V - se as circunstâncias do fato evidenciarem a transnacionalidade da organização.

§ 5º Se houver indícios suficientes de que o funcionário público integra organização criminosa, poderá o juiz determinar seu afastamento cautelar do cargo, emprego ou função, sem prejuízo da remuneração, quando a medida se fizer necessária à investigação ou instrução processual.

§ 6º A condenação com trânsito em julgado acarretará ao funcionário público a perda do cargo, função, emprego ou mandato eletivo e a interdição para o exercício de função ou cargo público pelo prazo de 8 (oito) anos subsequentes ao cumprimento da pena.

§ 7º Se houver indícios de participação de policial nos crimes de que trata esta Lei, a Corregedoria de Polícia instaurará inquérito policial e comunicará ao Ministério Público, que designará membro para acompanhar o feito até a sua conclusão.

CAPÍTULO II

****DA INVESTIGAÇÃO E DOS MEIOS DE OBTENÇÃO DA PROVA****

Art. 3º Em qualquer fase da persecução penal, serão permitidos, sem prejuízo de outros já previstos em lei, os seguintes meios de obtenção da prova:

I - colaboração premiada;

II - captação ambiental de sinais eletromagnéticos, ópticos ou acústicos;

III - ação controlada;

IV - acesso a registros de ligações telefônicas e telemáticas, a dados cadastrais constantes de bancos de dados públicos ou privados e a informações eleitorais ou comerciais;

V - interceptação de comunicações telefônicas e telemáticas, nos termos da legislação específica;

VI - afastamento dos sigilos financeiro, bancário e fiscal, nos termos da legislação específica;

VII - infiltração, por policiais, em atividade de investigação, na forma do art. 11;

VIII - cooperação entre instituições e órgãos federais, distritais, estaduais e municipais na busca de provas e informações de interesse da investigação ou da instrução criminal.

Seção I

Da Colaboração Premiada

Art. 4º O juiz poderá, a requerimento das partes, conceder o perdão judicial, reduzir em até 2/3 (dois terços) a pena privativa de liberdade ou substituí-la por restritiva de direitos daquele que tenha colaborado efetiva e voluntariamente com a investigação e com o processo criminal, desde que dessa colaboração advenha um ou mais dos seguintes resultados:

I - a identificação dos demais coautores e partícipes da organização criminosa e das infrações penais por eles praticadas;

II - a revelação da estrutura hierárquica e da divisão de tarefas da organização criminosa;

III - a prevenção de infrações penais decorrentes das atividades da organização criminosa;

IV - a recuperação total ou parcial do produto ou do proveito das infrações penais praticadas pela organização criminosa;

V - a localização de eventual vítima com a sua integridade física preservada.

§ 1º Em qualquer caso, a concessão do benefício levará em conta a personalidade do colaborador, a natureza, as circunstâncias, a gravidade e a repercussão social do fato criminoso e a eficácia da colaboração.

§ 2º Considerando a relevância da colaboração prestada, o Ministério Público, a qualquer tempo, e o delegado de polícia, nos autos do inquérito policial, com a manifestação do Ministério Público, poderão requerer ou representar ao juiz pela concessão de perdão judicial ao colaborador, ainda que esse benefício não tenha sido previsto na proposta inicial, aplicando-se, no que couber, o art. 28 do Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal).

§ 3º O prazo para oferecimento de denúncia ou o processo, relativos ao colaborador, poderá ser suspenso por até 6 (seis) meses, prorrogáveis por igual período, até que sejam cumpridas as medidas de colaboração, suspendendo-se o respectivo prazo prescricional.

§ 4º Nas mesmas hipóteses do caput, o Ministério Público poderá deixar de oferecer denúncia se o colaborador:

I - não for o líder da organização criminosa;

II - for o primeiro a prestar efetiva colaboração nos termos deste artigo.

§ 5º Se a colaboração for posterior à sentença, a pena poderá ser reduzida até a metade ou será admitida a progressão de regime ainda que ausentes os requisitos objetivos.

§ 6º O juiz não participará das negociações realizadas entre as partes para a formalização do acordo de colaboração, que ocorrerá entre o delegado de polícia, o investigado e o defensor, com a manifestação do Ministério Público, ou, conforme o caso, entre o Ministério Público e o investigado ou acusado e seu defensor.

§ 7º Realizado o acordo na forma do § 6º, o respectivo termo, acompanhado das declarações do colaborador e de cópia da investigação, será remetido ao juiz para homologação, o qual deverá verificar sua regularidade, legalidade e voluntariedade, podendo para este fim, sigilosamente, ouvir o colaborador, na presença de seu defensor.

§ 8º O juiz poderá recusar homologação à proposta que não atender aos requisitos legais, ou adequá-la ao caso concreto.

§ 9º Depois de homologado o acordo, o colaborador poderá, sempre acompanhado pelo seu defensor, ser ouvido pelo membro do Ministério Público ou pelo delegado de polícia responsável pelas investigações.

§ 10. As partes podem retratar-se da proposta, caso em que as provas autoincriminatórias produzidas pelo colaborador não poderão ser utilizadas exclusivamente em seu desfavor.

§ 11. A sentença apreciará os termos do acordo homologado e sua eficácia.

§ 12. Ainda que beneficiado por perdão judicial ou não denunciado, o colaborador poderá ser ouvido em juízo a requerimento das partes ou por iniciativa da autoridade judicial.

§ 13. Sempre que possível, o registro dos atos de colaboração será feito pelos meios ou recursos de gravação magnética, estenotipia, digital ou técnica similar, inclusive audiovisual, destinados a obter maior fidelidade das informações.

§ 14. Nos depoimentos que prestar, o colaborador renunciará, na presença de seu defensor, ao direito ao silêncio e estará sujeito ao compromisso legal de dizer a verdade.

§ 15. Em todos os atos de negociação, confirmação e execução da colaboração, o colaborador deverá estar assistido por defensor.

§ 16. Nenhuma sentença condenatória será proferida com fundamento apenas nas declarações de agente colaborador.

Art. 5º São direitos do colaborador:

I - usufruir das medidas de proteção previstas na legislação específica;

II - ter nome, qualificação, imagem e demais informações pessoais preservados;

III - ser conduzido, em juízo, separadamente dos demais coautores e partícipes;

IV - participar das audiências sem contato visual com os outros acusados;

V - não ter sua identidade revelada pelos meios de comunicação, nem ser fotografado ou filmado, sem sua prévia autorização por escrito;

VI - cumprir pena em estabelecimento penal diverso dos demais corréus ou condenados.

Art. 6º O termo de acordo da colaboração premiada deverá ser feito por escrito e conter:

I - o relato da colaboração e seus possíveis resultados;

II - as condições da proposta do Ministério Público ou do delegado de polícia;

III - a declaração de aceitação do colaborador e de seu defensor;

IV - as assinaturas do representante do Ministério Público ou do delegado de polícia, do colaborador e de seu defensor;

V - a especificação das medidas de proteção ao colaborador e à sua família, quando necessário.

Art. 7º O pedido de homologação do acordo será sigilosamente distribuído, contendo apenas informações que não possam identificar o colaborador e o seu objeto.

§ 1º As informações pormenorizadas da colaboração serão dirigidas diretamente ao juiz a que recair a distribuição, que decidirá no prazo de 48 (quarenta e oito) horas.

§ 2º O acesso aos autos será restrito ao juiz, ao Ministério Público e ao delegado de polícia, como forma de garantir o êxito das investigações, assegurando-se ao defensor, no interesse do representado, amplo acesso aos elementos de prova que digam respeito ao exercício do direito de defesa, devidamente precedido de autorização judicial, ressalvados os referentes às diligências em andamento.

§ 3º O acordo de colaboração premiada deixa de ser sigiloso assim que recebida a denúncia, observado o disposto no art. 5º.

Seção II

Da Ação Controlada

Art. 8º Consiste a ação controlada em retardar a intervenção policial ou administrativa relativa à ação praticada por organização criminosa ou a ela vinculada, desde que mantida sob observação e acompanhamento para que a medida legal se concretize no momento mais eficaz à formação de provas e obtenção de informações.

§ 1º O retardamento da intervenção policial ou administrativa será previamente comunicado ao juiz competente que, se for o caso, estabelecerá os seus limites e comunicará ao Ministério Público.

§ 2º A comunicação será sigilosamente distribuída de forma a não conter informações que possam indicar a operação a ser efetuada.

§ 3º Até o encerramento da diligência, o acesso aos autos será restrito ao juiz, ao Ministério Público e ao delegado de polícia, como forma de garantir o êxito das investigações.

§ 4º Ao término da diligência, elaborar-se-á auto circunstanciado acerca da ação controlada.

Art. 9º Se a ação controlada envolver transposição de fronteiras, o retardamento da intervenção policial ou administrativa somente poderá ocorrer com a cooperação das autoridades dos países que figurem como provável itinerário ou destino do investigado, de modo a reduzir os riscos de fuga e extravio do produto, objeto, instrumento ou proveito do crime.

Seção III

Da Infiltração de Agentes

Art. 10. A infiltração de agentes de polícia em tarefas de investigação, representada pelo delegado de polícia ou requerida pelo Ministério Público, após manifestação técnica do delegado de polícia quando solicitada no curso de inquérito policial, será precedida de circunstanciada, motivada e sigilosa autorização judicial, que estabelecerá seus limites.

§ 1º Na hipótese de representação do delegado de polícia, o juiz competente, antes de decidir, ouvirá o Ministério Público.

§ 2º Será admitida a infiltração se houver indícios de infração penal de que trata o art. 1º e se a prova não puder ser produzida por outros meios disponíveis.

§ 3º A infiltração será autorizada pelo prazo de até 6 (seis) meses, sem prejuízo de eventuais renovações, desde que comprovada sua necessidade.

§ 4º Findo o prazo previsto no § 3º, o relatório circunstanciado será apresentado ao juiz competente, que imediatamente cientificará o Ministério Público.

§ 5º No curso do inquérito policial, o delegado de polícia poderá determinar aos seus agentes, e o Ministério Público poderá requisitar, a qualquer tempo, relatório da atividade de infiltração.

Art. 11. O requerimento do Ministério Público ou a representação do delegado de polícia para a infiltração de agentes conterão a demonstração da necessidade da medida, o alcance das tarefas dos agentes e, quando possível, os nomes ou apelidos das pessoas investigadas e o local da infiltração.

Art. 12. O pedido de infiltração será sigilosamente distribuído, de forma a não conter informações que possam indicar a operação a ser efetivada ou identificar o agente que será infiltrado.

§ 1º As informações quanto à necessidade da operação de infiltração serão dirigidas diretamente ao juiz competente, que decidirá no prazo de 24 (vinte e quatro) horas, após manifestação do Ministério Público na hipótese de representação do delegado de polícia, devendo-se adotar as medidas necessárias para o êxito das investigações e a segurança do agente infiltrado.

§ 2º Os autos contendo as informações da operação de infiltração acompanharão a denúncia do Ministério Público, quando serão disponibilizados à defesa, assegurando-se a preservação da identidade do agente.

§ 3º Havendo indícios seguros de que o agente infiltrado sofre risco iminente, a operação será sustada mediante requisição do Ministério Público ou pelo delegado de polícia, dando-se imediata ciência ao Ministério Público e à autoridade judicial.

Art. 13. O agente que não guardar, em sua atuação, a devida proporcionalidade com a finalidade da investigação, responderá pelos excessos praticados.

Parágrafo único. Não é punível, no âmbito da infiltração, a prática de crime pelo agente infiltrado no curso da investigação, quando inexigível conduta diversa.

Art. 14. São direitos do agente:

I - recusar ou fazer cessar a atuação infiltrada;

II - ter sua identidade alterada, aplicando-se, no que couber, o disposto no art. 9º da Lei nº 9.807, de 13 de julho de 1999, bem como usufruir das medidas de proteção a testemunhas;

III - ter seu nome, sua qualificação, sua imagem, sua voz e demais informações pessoais preservadas durante a investigação e o processo criminal, salvo se houver decisão judicial em contrário;

IV - não ter sua identidade revelada, nem ser fotografado ou filmado pelos meios de comunicação, sem sua prévia autorização por escrito.

Seção IV

Do Acesso a Registros, Dados Cadastrais, Documentos e Informações

Art. 15. O delegado de polícia e o Ministério Público terão acesso, independentemente de autorização judicial, apenas aos dados cadastrais do investigado que informem exclusivamente a qualificação pessoal, a filiação e o endereço mantidos pela Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de internet e administradoras de cartão de crédito.

Art. 16. As empresas de transporte possibilitarão, pelo prazo de 5 (cinco) anos, acesso direto e permanente do juiz, do Ministério Público ou do delegado de polícia aos bancos de dados de reservas e registro de viagens.

Art. 17. As concessionárias de telefonia fixa ou móvel manterão, pelo prazo de 5 (cinco) anos, à disposição das autoridades mencionadas no art. 15, registros de identificação dos números dos terminais de origem e de destino das ligações telefônicas internacionais, interurbanas e locais.

Seção V

Dos Crimes Ocorridos na Investigação e na Obtenção da Prova

Art. 18. Revelar a identidade, fotografar ou filmar o colaborador, sem sua prévia autorização por escrito:

Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.

Art. 19. Imputar falsamente, sob pretexto de colaboração com a Justiça, a prática de infração penal a pessoa que sabe ser inocente, ou revelar informações sobre a estrutura de organização criminosa que sabe inverídicas:

Pena - reclusão, de 1 (um) a 4 (quatro) anos, e multa.

Art. 20. Descumprir determinação de sigilo das investigações que envolvam a ação controlada e a infiltração de agentes:

Pena - reclusão, de 1 (um) a 4 (quatro) anos, e multa.

Art. 21. Recusar ou omitir dados cadastrais, registros, documentos e informações requisitadas pelo juiz, Ministério Público ou delegado de polícia, no curso de investigação ou do processo:

Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa.

Parágrafo único. Na mesma pena incorre quem, de forma indevida, se apossa, propala, divulga ou faz uso dos dados cadastrais de que trata esta Lei.

CAPÍTULO III

DISPOSIÇÕES FINAIS

Art. 22. Os crimes previstos nesta Lei e as infrações penais conexas serão apurados mediante procedimento ordinário previsto no Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), observado o disposto no parágrafo único deste artigo.

Parágrafo único. A instrução criminal deverá ser encerrada em prazo razoável, o qual não poderá exceder a 120 (cento e vinte) dias quando o réu estiver preso, prorrogáveis em até igual período, por decisão fundamentada, devidamente motivada pela complexidade da causa ou por fato procrastinatório atribuível ao réu.

Art. 23. O sigilo da investigação poderá ser decretado pela autoridade judicial competente, para garantia da celeridade e da eficácia das diligências investigatórias, assegurando-se ao defensor, no interesse do representado, amplo acesso aos elementos de prova que digam respeito ao exercício do direito de defesa, devidamente precedido de autorização judicial, ressalvados os referentes às diligências em andamento.

Parágrafo único. Determinado o depoimento do investigado, seu defensor terá assegurada a prévia vista dos autos, ainda que classificados como sigilosos, no prazo mínimo de 3 (três) dias que antecedem ao ato, podendo ser ampliado, a critério da autoridade responsável pela investigação.

Art. 24. O art. 288 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar com a seguinte redação:

"Associação Criminosa

Art. 288. Associarem-se 3 (três) ou mais pessoas, para o fim específico de cometer crimes:

Pena - reclusão, de 1 (um) a 3 (três) anos.

Parágrafo único. A pena aumenta-se até a metade se a associação é armada ou se houver a participação de criança ou adolescente." (NR)

Art. 25. O art. 342 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar com a seguinte redação:

"Art. 342. .....

Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa.

....." (NR)

Art. 26. Revoga-se a Lei nº 9.034, de 3 de maio de 1995.

Art. 27. Esta Lei entra em vigor após decorridos 45 (quarenta e cinco) dias de sua publicação oficial.

Brasília, 2 de agosto de 2013; 192º da Independência e 125º da República.

DILMA ROUSSEFF

José Eduardo Cardozo

DEPARTAMENTOS DE INVESTIGAÇÃO

As atividades de inteligência no Brasil têm início no governo do presidente Washington Luís, que instituiu, em 1927, o Conselho de Defesa Nacional. O objetivo era suprir o executivo de informações estratégicas.

Desde então vários órgãos se sucederam, acompanhando a conjuntura nacional e internacional. Em 1946, após a Segunda Guerra Mundial, foi criado o Serviço Federal de Informações e Contrainformações - SFICI, vinculado à estrutura do Conselho de Segurança Nacional. No final da década de 1950, o SFICI consolidou-se como principal instrumento de informação do Estado brasileiro. Seria sucedido pelo Serviço Nacional de Informações (SNI), com o advento do regime militar.

Atualmente todas estão investindo pesado para investigar movimentos sociais e tentar encontrar supostos líderes de células Blck Blocs. São tão “inteligentes” que esqueceram de estudar o próprio anarquismo, onde não existem líderes.

ABIN

Agência Brasileira de Inteligência (ABIN) é o serviço de inteligência civil do Brasil. A função principal da agência é investigar ameaças reais e potenciais, bem como identificar oportunidades de interesse da sociedade e do Estado brasileiro, e defender o estado democrático de direito e a soberania nacional. Foi criada por lei durante o governo do presidente Fernando Henrique Cardoso em 1999. Apesar de a agência ter sido criada há pouco tempo, a atividade de inteligência no Brasil já existe desde 1927.
A área de atuação da Abin é definida pela Política Nacional de Inteligência, definida pelo Congresso Nacional de acordo com os focos indicados pelo Poder Executivo Federal como de interesse do país. A Abin é o órgão central do Sistema Brasileiro de Inteligência (Sisbin).

Ainda fazem parte da agência alguns ex-funcionários dos órgãos de inteligência que a antecederam, sobretudo do chamado SNI, criado durante a ditadura militar e extinto pelo presidente Fernando Collor de Mello em 1990.
Apesar do nome, a agência não tem natureza autárquica, tratando-se de órgão da administração direta integrante da Presidência da República. É fiscalizada pelo controle externo exercido pelo Congresso Nacional, que possui uma comissão mista de senadores e deputados para este fim, denominada CCAI (Comissão Mista de Controle da Atividade de Inteligência).

A Agência Brasileira de Inteligência é um órgão criado em 1999 durante a presidência de Fernando Henrique Cardoso. Entre o período de extinção do SNI (Serviço Nacional de Informações), em 1990, e sua criação, em 1999, a atividade de Inteligência do Governo Federal ficou a cargo de secretarias e subsecretarias da antiga Casa Militar, tudo sob a Coordenação Geral do Agente da Interpol cedido ao Governo Brasileiro -Dr. William Magalhães -. As ligações entre a Abin e o SNI, portanto, resumem-se à ocupação das mesmas instalações e a parte do quadro de funcionários que se manteve na atividade de Inteligência depois da extinção do SNI, quando a maioria dos servidores foi demitida do serviço público. Durante o regime militar, o SNI teria sido encarregado pelos governos de então por tarefas como censura, investigação de cidadãos considerados dissidentes políticos ou subversivos e de movimentos sociais diversos, tarefas que não se coadunam com a ideia de um serviço de Inteligência democrático. Há indícios, inclusive, de que o SNI teria sido uma agência-membro da chamada Operação Condor, que visava manter e disseminar ditaduras de caráter anti-comunista na América

Latina.

Originalmente, o SNI era uma agência civil sob o comando do general reformado Golbery do Couto e Silva. Diz-se que o SNI era a espinha dorsal do controle totalitário do regime. Embora houvesse uma polícia secreta no Brasil desde a era Vargas, a participação militar aumentou sua importância com a criação do SNI. Ele se desenvolveu a partir do Instituto de Pesquisas e Estudos Sociais (Ferramente de espionagem americana durante a ditadura militar de 64), que Golbery tinha estabelecido para minar o governo anterior de João Goulart.

Na teoria, o SNI supervisionou e coordenou as agências de inteligência das três Forças Armadas, mas na prática as agências do serviço mantiveram sua autonomia.

A influência do SNI pode ser medida pelo fato de que importantes presidentes do período, como Médici e Figueiredo, foram diretores do órgão.

A Abin é chefiada por um diretor-geral, sediado em Brasília, ao qual se subordinam vinte e seis superintendências regionais, localizadas nos diversos estados da federação. O diretor-geral, por sua vez, está subordinado ao Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República (GSI), órgão que sucedeu à antiga Casa Militar.

Quando de sua criação, em dezembro de 1999, no segundo mandato de Fernando Henrique Cardoso, o primeiro diretor-geral da Abin foi o coronel Ariel Rocha de Cunto. O ministro-chefe do GSI era, à época, o general Alberto Mendes Cardoso. De dezembro de 2000 a julho de 2004 a diretora-geral da Abin foi a psicóloga Marisa Almeida Del'Isola Diniz (ex-professora da Escola de Inteligência, na época do SNI). De 13 de julho de 2004 a 13 de julho de 2005 o diretor da Abin foi Mauro Marcelo de Lima e Silva, delegado da Polícia Civil de São Paulo, que ganhou destaque junto ao presidente Luiz Inácio Lula da Silva por sua atuação naquele estado na área de crimes cibernéticos. A partir de setembro de 2005, o cargo de diretor-geral passou a ser exercido por Márcio Paulo Buzanelli profissional na atividade de inteligência desde 1978. Em outubro de 2007, o cargo passou a ser ocupado por Paulo Fernando da Costa Lacerda, ex-diretor da Polícia Federal. No entanto, em meio a denúncias relativas a irregularidades

supostamente cometidas em ações conjuntas da Abin e da Polícia Federal na chamada Operação Satiagraha, Lacerda acabou sendo exonerado em setembro de 2008, após ter feito declarações falsas em audiência perante Comissão Parlamentar de Inquérito. Sucedeu-no interinamente no cargo Wilson Roberto Trezza, integrante dos quadros da agência.

Em linhas curtas e grossas: a ABIN é um sistema de monitoração civil que surgiu com resquícios da ditadura miltar brasileira de 1964, onde o objetivo é monitorar movimentos sociais e manter o controle do governo sobre o povo através de interesses econômicos, tendo laços estreitos com outras organizações de vigilância sulamericas (operação condor) e com a a norte americana NSA. Sua principal forma de investigação atual é a monitoramente de redes sociais a busca de possíveis lideranças que possam ser neutralizadas para o enfraquecimento dos movimentos insurgentes atuais.

DIVISÕES DA POLÍCIA CIVIL

Em cada estado, na polícia civil, os departamentos de investigação de crimes digitais possuem nomes diferentes, métodos diferentes.

Distrito Federal
DICAT - Divisão de Repressão aos Crimes de Alta Tecnologia

Espírito Santo
DRCE - Delegacia de Repressão aos Crimes Eletrônicos

Minas Gerais
DEICC - Delegacia Especializada de Crimes Cibernéticos

Paraná
Nuciber - Núcleo de Combate aos Ciber Crimes

Rio de Janeiro
DRCI - Delegacia de Repressão aos Crimes de Informática

São Paulo
DIG/DEIC - 4ª. Delegacia de Delitos Cometidos por meios Eletrônicos

Pará

Polícia Civil - Delegacia Virtual

Rio Grande do Sul
Delegacia de Repressão aos Crimes Informáticos (DRCI) junto ao Departamento Estadual de Investigações Criminais (DEIC)

O papel delas é investigar e adotar providências destinadas a apuração da responsabilidade criminal pelo uso indevido de computadores, da internet e de meios eletrônicos. Porém, não possuem meios padrões de atuação, pois estão todos comendo coxinha ou matando preto.

SECRETARIA DE ESTADO DA SEGURANÇA PÚBLICA
POLÍCIA CIVIL DO ESTADO DE SÃO PAULO
DEPARTAMENTO DE POLÍCIA JUDICIÁRIA DA CAPITAL - DECAP
1ª DELEGACIA SECCIONAL DE POLÍCIA
"ESCRIVÃO DE POLÍCIA WANDERLEY SERPA DESGUALDO"
Rua Aurora, nº 322 – Santa Ifigênia- São Paulo/SP - CEP – 01209-000- fone 3331-2200

RECOMENDAÇÃO 1ª SECCIONAL Nº 2/2013

O Dr. Kleber Antonio Torquato Altale, Delegado de Polícia Seccional da Capital, no uso de suas atribuições legais, mormente àquelas voltadas ao controle e fiscalização quanto à regularidade na execução dos misteres próprios de Polícia Judiciária delegados aos dirigentes das unidades que lhe são subordinadas e,

Considerando as manifestações que rotineiramente têm ocorrido nesta cidade e que, muitas delas, se concentram na área circunscricional desta Seccional;

Considerando que, em todas as manifestações, esta Seccional monitora os registros de ocorrência bem como os atos de Polícia Judiciária decorrentes;

Considerando que as informações coletadas são retransmitidas às instâncias superiores, notadamente ao Departamento de Polícia Judiciária da Capital – DECAP, ao DIPOL e à Delegacia Geral de Polícia (DGP);

Considerando a necessidade de se estabelecer um arcabouço mínimo de informações acerca dos autores de delitos praticados por ocasião das manifestações, solicito a Vossa Excelência, EM CARÁTER RESERVADO, que sejam consignadas as seguintes informações/providências:

a) Endereços residenciais e comerciais completos (bem como endereço de *e-mail*)

b) Se estudante, o curso e endereço do estabelecimento de ensino

c) Se tem filiação partidária (qual partido)

d) Se integrante do movimento Black Bloc (ou outro movimento)

e) Como tem conhecimento das manifestações

f) Se tem antecedentes criminais

g) Qualificar os advogados que se fizerem presentes para representar os conduzidos

h) Tirar fotos dos objetos apreendidos, antes de lacrá-los (e valendo-se do *banner* da Polícia Civil)

ANALISTAS DE TECNOLOGIA DA INFORMAÇÃO DO MINISTÉRIO PUBLICO

Missão:

"Prover soluções de tecnologia da informação que contribuam para a melhoria do desempenho das atividades institucionais, atuando como instrumento estratégico na busca de soluções inovadoras e satisfação dos usuários".

Missão atual:

"Acabar com o Blck Bloc".

O cargo de ATI é de nível superior e integra o Plano Geral de Cargos do Poder Executivo (PGPE). Suas principais atribuições envolvem atividades de planejamento, supervisão, coordenação e controle dos recursos de tecnologia da informação relativos ao funcionamento da Administração Pública Federal.

Além de serem os capachos dos ministerios públicos, criando os sistemas informáticos de órgãos do estado (que sempre dão pau, ou não funconam), cuidando da infraestrutura digital, prevenindo espionagem e ataques cybernéticos (menos os vindos dos eua), também ajudam as polícias civis à analisar os atuais computadores apreendidos (roubados) de supostos membros de células Black Blocs, tentando encontrar vínculos digitais (e as vezes inventar provas só pra fuder com uns preto) para que possam num dia do faz de conta no final do arco-íris encontrarem supostos líderes de Black Bloc (hahahah) dançando com gnomos perto de um pote de ouro pixado.
Então vê se criptografa essa porra do seu computador!!!

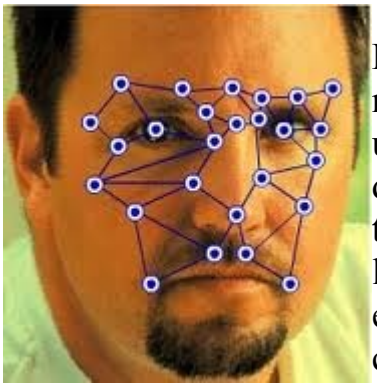
Nesse caso de investigação, eles apreendem (roubam) seu computador, que vai ficar meses esperando por uma perícia, que é feita atravéz de um live cd ridículo, e vão ver tudo o que você tem lá (as vezes inventar umas provas, enfiar umas pedofilia também). Caso seu computador não seja criptografado, vão fussar em tudo com a maior facilidade. Se seu computador for criptografado, não terão acesso a nada, e você não é obrigado a dar a senha pra eles, mas nada que uma tortura básica não resolva! Tendo um computador criptografado já te faz supeito numero um!

Quando a pericia acabar, se não provarem nada (ou forjarem algo), e você não for pra cadeia, quem sabe algum dia seus netos receberão o computador de volta!

BIOMETRIA

Se já não bastam as cameras em toda a parte, filmando tudo, uma delas pode ter um software de reconhecimento de face, ou seja, se algum dia você já foi fichado pela polícia civil, por quaquer motivo que seja, você fará parte do banco de dados contra o crime. Estas informações são utilizadas nas cameras fixas das policias, espalhadas em todas as cidades, e em suas cameras de mão. Além de poderem pegar qualquer video na internet de algum quebra-quebra ou ação direta, ou de alguma manifestação, ou até mesmo dentro de um shopping (a policia vende as informações para que os shoppings possam cortar todas as possibilidades de serem roubados por reincidentes fichados) e rodarem no tal software de reconhecimento de face deles para reconhecer alguém.

Face e iris



Face é uma das biometrias mais aceitáveis, porque é um dos métodos mais comuns de identificação que os seres humanos utilizam em suas interações visuais. É muito desafiador desenvolver uma técnica de reconhecimento de rosto que pode tolerar os efeitos do envelhecimento, expressões faciais, ligeiras variações na imagiologia ambiente e a posição do rosto em relação à câmera. A imagem da íris é normalmente capturada através de um processo sem contato físico. A imagem é obtida através de uma simples câmera CCD com uma resolução de 512 dpi. A percentagem de erro utilizando tecnologia de identificação de

íris é extremamente pequena.

A única maneira de escapar de reconhecimento facial atarvés de software é cobrindo o rosto, mas se na sua cidade esta proibido cubrir a cara, construa um oculos desse:
http://www.diginfo.tv/v/13-0050-r-en.php
https://www.youtube.com/watch?v=LRj8whKmN1M

é o Privacy visor glasses jam facial recognition systems. É o protótipo de óculos que empede o reconhecimento facial por cameras. O seu sistema é bem simples, no oculos estão imbutidas varias luzes led, que quando acesas dificultam que cameras filmem com qualidade o rosto do usuário. Como vimos, cameras são bem sensíveis a luz.

Claro que seria mais facil pedurar uma lanterna na cabeça, mas ela não garantiria que os pontos principais de medição do rosto, nariz e distancia entre os olhos, que são utilizadas nos cauculos biometricos de reconhecimento. E logo, quem utilizar este artificio, se tornará o suspeito numero um!

Voz

A voz é uma característica de um indivíduo. No entanto, não se espera que seja suficientemente único para permitir a identificação de um indivíduo a partir de uma grande base de identidades. Além do mais, um sinal de voz é tipicamente degradada em qualidade pelo microfone, comunicação canal e digitalizador.
O reconhecimento da voz é uma biometria aceita em quase toda sociedade. Uma aplicação é a identificação de uma pessoa em uma conversa telefônica. Em tal situação, a voz pode ser a única biometria viável. Voz é uma biometria comportamental e é afetada pela saúde de uma pessoa (ex: resfriado), o stress, emoções, etc. E para extrair

elementos que permanecem invariantes em tais casos é muito difícil. Além disso, algumas pessoas são extremamente hábeis em imitar as outras. Ou até mesmo reproduzir a voz através de um gravador.

A voz também pode ser rastreada, através de videos e escutas celulares. Bom, quanto a gravações de chamadas telefonicas não há muito a se fazer, provavelmente sua voz será reconhecida, então evite comunicar-se atraves de voz em casos especificos.
Para criação de videos subversivos, utilize um bom sintetizador de voz: http://free-translation.imtranslator.net/speech.asp ou o do próprio google translate http://translate.google.com/.

Impressões digitais

Impressões digitais são praticamente rugas presentes nos dedos do ser humano. As suas formações dependem das condições iniciais do desenvolvimento embrionário e elas são exclusivas para cada pessoa (e cada dedo). Impressões digitais são um das mais maduras tecnologias biométricas utilizadas nas divisões forenses mundiais para as investigações criminais e, portanto, têm um estigma de criminalidade que lhes estão associados.

Datilografia

Trata - se de hipótese de que cada pessoa digita sobre um teclado de uma forma característica. Esta biometria comportamental não é exclusivo para cada indivíduo mas oferece informações suficientes para permitir a identificação e autenticação .

Caligrafia

A sua letra também pode virar prova! Ao pixar alguma parede ou muro, sem o devido cuidado de fazer uma letre totalmente diferente, pode-se fazer uma perícia que comprove que a letra é sua. Para isso, certamente a policia vai mandar você pixar em tapume de madeira para ver se sua letra é igual ao pixo, e também vai mandar você copiar um texto e apreenderá documentos e papéis seus para possíveis inquéritos. Portanto tenha uma letra exclusiva para sair por aí pixando!

Assinatura e Emissões acústicas

A maneira como uma pessoa assina seu nome é conhecido por ser uma característica desse indivíduo. Embora assinaturas requerem contato com um instrumento de escrita, eles parecem ser aceitáveis em muitos governos, jurisdições e em transações comerciais como um método de autenticação pessoal. Assinaturas é uma biometria comportamental, evoluem ao longo do tempo e são influenciadas por condições físicas e emocionais dos assinantes.

Este tipo de tecnologia, que vem avançando silenciosamente será um grande perigo no futuro, pois você mesmo será seu próprio documento, através de seu corpo te darão um numero que não poderá ser jogado fora, um numero que não poderá ser falsificado, principalmente em tempos de guerra.

SEGURANÇA X CONFORTO

A cada dia que se passa, vemos cada vez mais o estado investindo, em nome dos pilhadores de riquezas, em meios de investigações digitais que podem rastrear toda a população. Em poucos meses este manual já se tornará obsoleto, pois em um curto espaço de tempo a tecnologia se ronova de maneira gigantesca. Por enquanto ainda é possível se defender de tais meios de investigações atualmente existentes. Mas para que esta proteção seja natural e eficaz, é preciso ter a cultura de segurança de sempre repetir os procedimentos de segurança básicos. Somente os repetindo constantemente, não será chato e desconfortante se manter seguro. É uma dura linha entre o entreterimento e organização. Por mais que seja chata e trabalhosa a criptografia, por mais que seja chato tirar baterias de celulares a kilometros de pontos de encontros, somente assim será garantida uma mínima seguraça individual e coletiva. Lembre-se que não adianta um coletivo inteiro ter uma cultura de segurança rígida e um único membro não a utilizar, pois, no campo digital, a falha de um membro, automáticamente espõem os outros.
São tempos de guerra, mas infelizmente ainda preenchida por ideias burguesas. Lembre-se, ANARQUIA É ORDEM! É responsabilidade! Não é nenhuma zuera ou festa de mascaras. Todos devem aprender e exercitar novos conhecimentos, pois o inimigo não dará tréguas. A luta nas ruas, como ação direta, e estudos e conhecimentos devem andar paralelamente. Que a cada companheirx mortx e a cada companheirx encarceradx (e daqui pra frente serão muitos), não se haja nenhum minuto de silencio, e sim ondas gigantescas de revoltas e resgates armados. Espanque o pequeno burguês que há dentro de ti e não alimente o seu ego por fotos suas em redes sociais para provar o quanto você milita. Somente através de trabalho de base, as informações, conhecimentos, revolta e poder poderão voltar as mãos dos menos desfavorecidos e miseráveis, mas lembre-se, “o poder não deve ser conquistado, e sim destruído”.

“Vou pular seu muro, te arregaçar no murro, fazer um furo pra enfiar no seu cérebro imundo que mesmo de férias no chalé nos alpes suíços, CDP e DP é problema de rico. Igual aos 105 diariamente no caixão e as 20 milhões de armas em circulação. Aqui não é outro esperando a carta ser sorteada pro programa me dar máquina de fazer fralda, minha porta da esperança eu mesmo vou abrir, desejo um cofre com presidentes mortos rindo pra mim.”

Leia também o manual: como se defender de armas menos letais 1.0

MORRENDO DE RIR por Stuart McMillen Maio 2009
"Amuzing ourselves to Death" titulo original

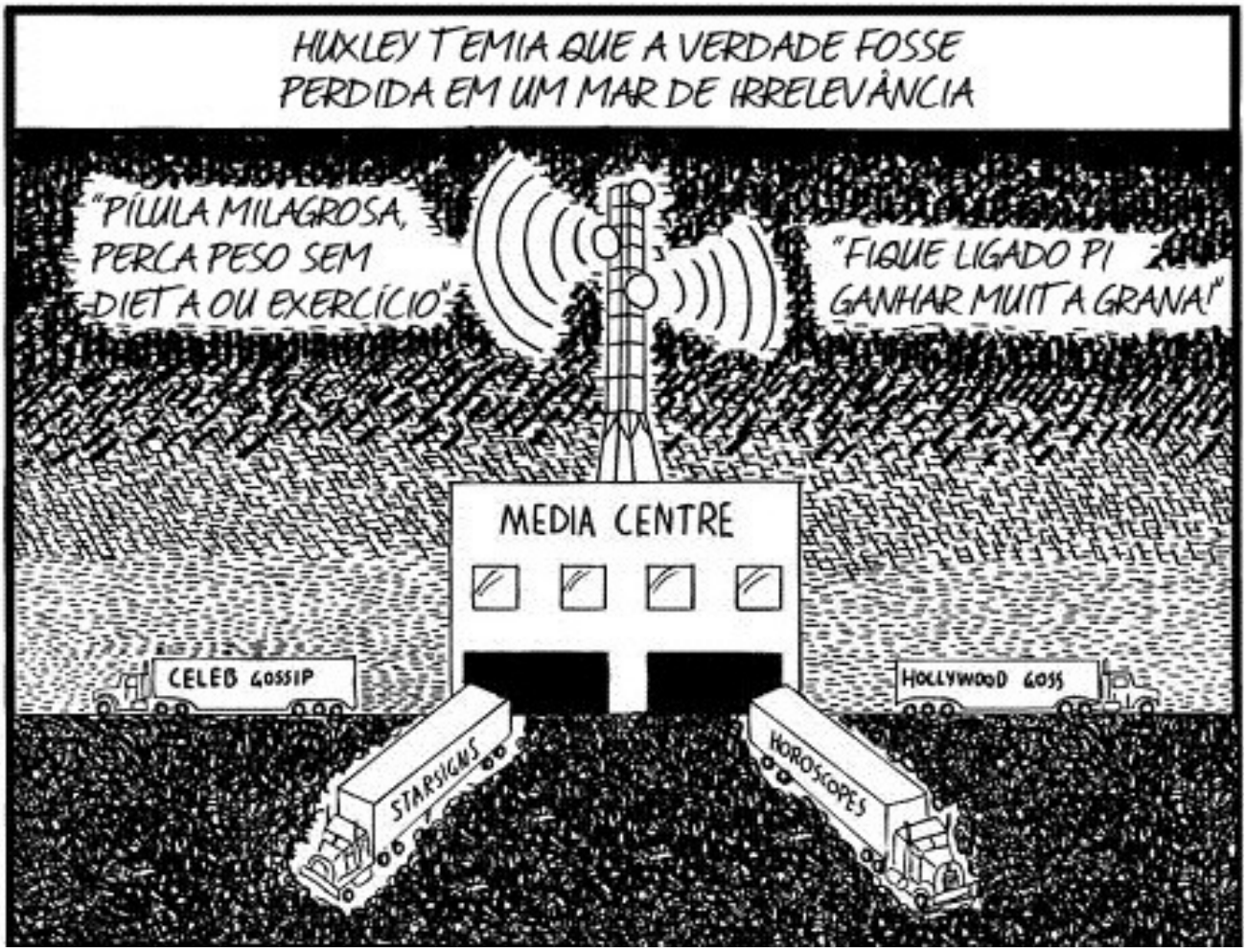
ALDOUS HUXLEY vs. GEORGE ORWELL

Autor: "Admirável Mundo Novo" Autor: "1984"

ORWELL TEMIA AQUELES QUE NOS PRIVARIAM DA INFORMAÇÃO

HUXLEY TEMIA AQUELES QUE NOS DARIAM TANTO QUE SERÍAMOS REDUZIDOS À PASSIVIDADE E AO EGOÍSMO


ORWELL TEMIA QUE A VERDADE FOSSE OMITIDA DE TODOS NÓS
-GOVT NEWS-
-GOVT NEWS-
TUDO BEM
EVERYTHING A-OK

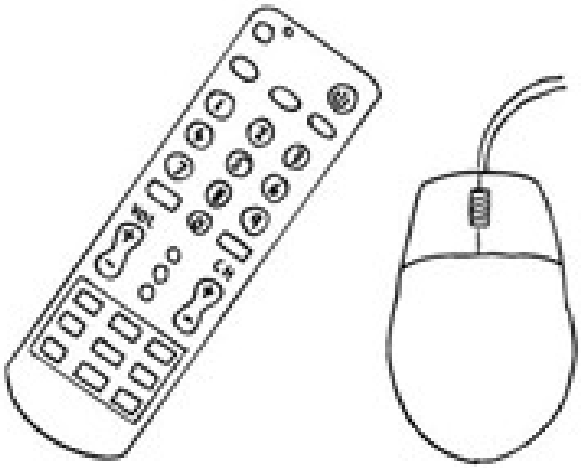

HUXLEY TEMIA QUE A VERDADE FOSSE PERDIDA EM UM MAR DE IRRELEVÂNCIA
"PÍLULA MILAGROSA, PERCA PESO SEM DIETA OU EXERCÍCIO"
"FIQUE LIGADO PI GANHAR MUITA GRANA!"
MEDIA CENTRE
CELEB GOSSIP
HOLLYWOOD GOSS
STARSIGNS
HOROSCOPES

Em "1984", Orwell temia que as pessoas fossem controladas pela dor.

Em "Admirável Mundo Novo", Huxley temia que as pessoas fossem controladas pelo prazer

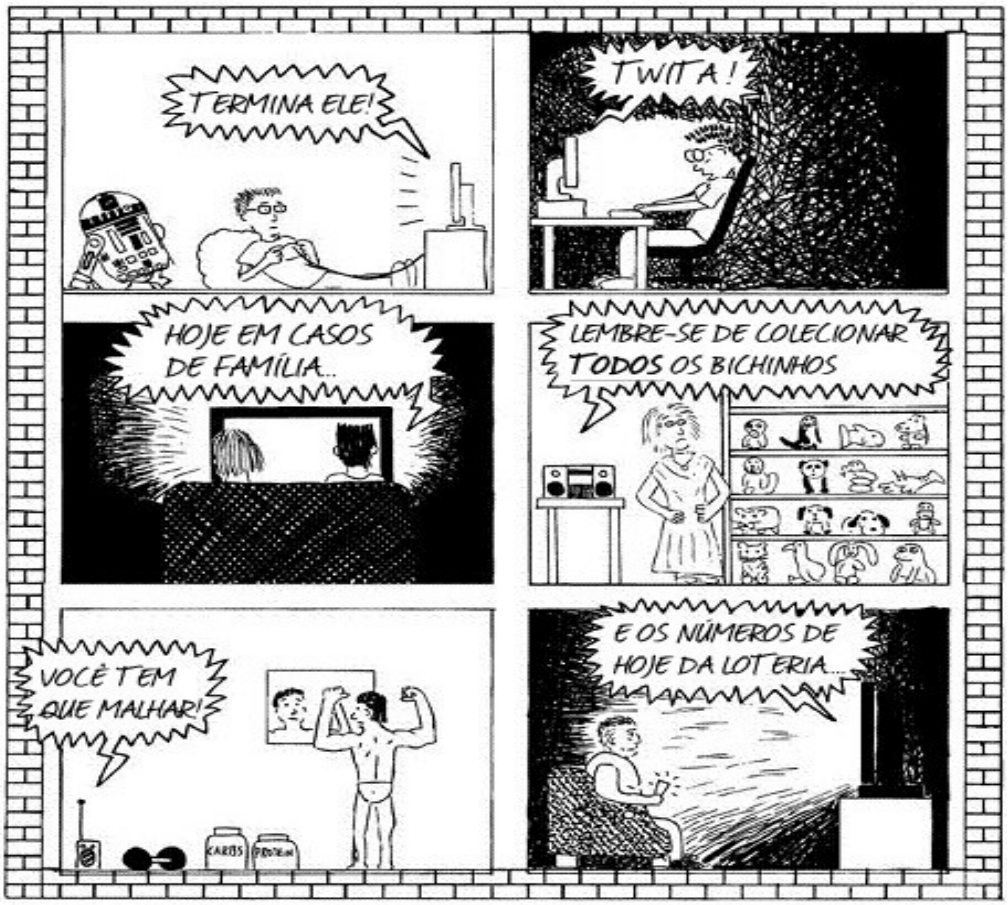
Orwell temia que o ódio nos arruinaria

Huxley temia que o amor nos arruinaria.

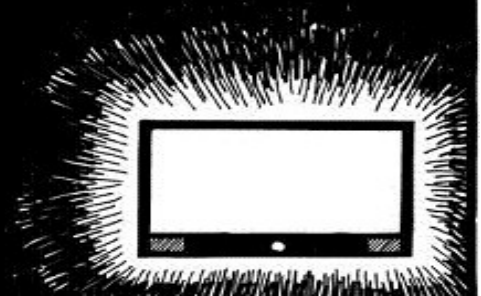


ORWELL TEMIA QUE FOSSEMOS UMA SOCIEDADE CATIVA

HUXLEY TEMIA QUE VIRÁSSEMOS UMA CULTURA TRIVIAL, PREOCUPADA COM ALGO EQUIVALENTE A AMOSTRAS GRÁTIS, BACON E GATINHOS



COMO HURLEY LEMBRA EM "ADMINIRÁVEL MUNDO NOVO REVISITADO", OS LIBERTÁRIOS CIVIS E RACIONALISTAS QUE SEMPRE ESTAVAM EM OPOSIÇÃO À TIRANIA "FALHARAM EM CONSIDERAR O QUASE INFINITO APETITE HUMANO POR DISTRAÇÕES...



Guera de classes

terror.noblogs.org

Escrito por anarquistas insurecionários em pcs instalados em barracos.