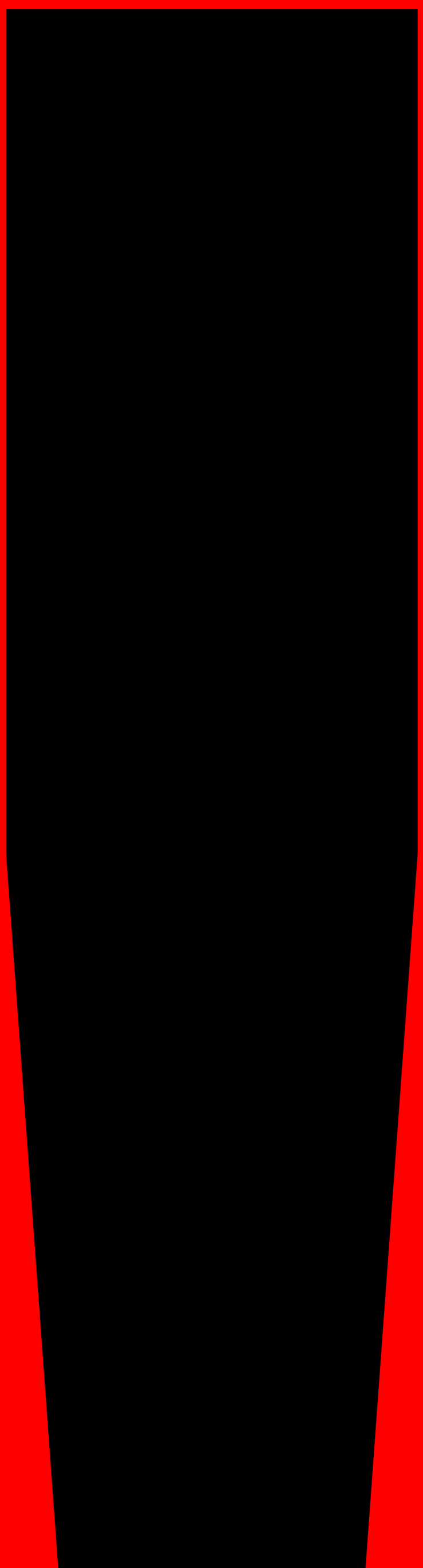
MANUAL DE SEGURANÇA DIGITAL PARA ATIVISTAS



UM MANUAL DE SEGURANÇA DIGITAL PARA ATIVISTAS

São tempos sombrios pelo mundo inteiro; no Brasil, a ameaça do fascismo lança sombras desde o Estado até os indivíduos. Se, por um lado, Jair Bolsonaro representa a possibilidade de um Estado ditatorial – principalmente pelas suas conexões com o Exército -, seus seguidores também representam o “fascismo transversal”, esse fascismo da vida cotidiana dos “homens de bem”. De maneira importante os fascistas também estão se tornando muito mais sofisticados tecnicamente; é só ver os ataques que são feitos a partir dos chans.
Por isso, é extremamente importante que nós ativistas nos apropriemos das ferramentas de segurança digital.

Esse manual foi construído com base em diversos outros materiais que existem na Internet. Por exemplo, o DIY Feminist Cybersecurity Guide; o Kit de Primeiros Socorros de Segurança Digital para Defensores dos Direitos Humanos; o Guia de Cultura de Segurança; o Manual para Ativistas, produzido pelo Organizing for Autonomous Telecomms e traduzido pela Editora Monstro dos Mares; o Pequeno manual de segurança digital e o manual Cultura de segurança: Autodefesa na era digital, da Frente Antifa; e o Guia Paranóico de Segurança em Tempos Digitais.
É preciso dar crédito a todas essas pessoas, das quais roubamos descaradamente.

! *PONTO IMPORTANTE:*
ESSAS INFORMAÇÕES SÃO VÁLIDAS PROVISORIAMENTE.
PROCURE AS INFORMAÇÕES MAIS ATUALIZADAS!

UMA CULTURA DE SEGURANÇA DIGITAL

1. UMA CULTURA DE SEGURANÇA DIGITAL

!

Não fazer: Falar sobre ativismo fora de espaços seguros; Falar sobre planos específicos fora do seu grupo de afinidade.

Fazer: Estudar bastante sobre cultura de segurança; criar camadas de segurança; usar pseudônimos

Em primeiro lugar, uma CULTURA DE SEGURANÇA é condição sine qua non para que assumir quaisquer outras das medidas desse manual. Existem vários materiais na Internet sobre cultura de segurança, e uma boa fonte é o Guia de Cultura de Segurança publicado pelo pessoal da crimethinc extremo sul. A cultura de segurança transcende a segurança digital, e inclui todos os aspectos da vida política do ativista; é uma atitude em relação à segurança e a privacidade que busca diminuir a paranóia minimizando os riscos com antecedência. O Guia define “cultura de segurança” da seguinte forma:

Uma cultura de segurança é um conjunto de hábitos compartilhados por uma comunidade cujos membros possam realizar atividades ilegais, cuja prática minimiza os riscos de tais atividades. Ter uma cultura de segurança poupa a todos o trabalho de ter que decidir medidas de segurança inúmeras vezes, desde o princípio, e pode ajudar a diminuir a paranoia e o pânico em situações de estresse — diabos, ela pode salvar você da prisão também. A diferença entre protocolo e cultura é que a cultura se torna inconsciente, instintiva e portanto espontânea; depois que o comportamento mais seguro possível se tornou um hábito a todos no círculos pelos quais você circula, você pode gastar menos tempo e energia enfatizando a necessidade dele, ou sofrendo as consequências de não o ter, ou se preocupando sobre os riscos que você está correndo, já que você já sabe que já está fazendo tudo o que pode para ser cuidadoso. Se você tem o hábito de não dar nenhuma informação importante sobre si, você pode trabalhar com estranhos sem ficar se agoniando se eles são informantes ou não; se todos sabem o que não se pode falar no telefone, os seus inimigos podem grampear todas as linhas que quiserem que não irão conseguir nada.
O princípio central de toda cultura de segurança, o ponto que nunca é enfatizado o suficiente, é que as pessoas nunca devem ser inteiradas de qualquer informação importante que elas não precisam saber. Quanto maior for o número de pessoas que

sabem de algo que pode colocar indivíduos ou projetos em risco — quer este algo seja a identidade de uma pessoa que cometeu um ato ilegal, a localização de um encontro particular, ou os planos de alguma atividade futura — maiores são as chances de que o conhecimento caia nas mãos erradas. Compartilhar essas informações com pessoas que não precisam sabê-las lhes faz um desserviço, bem como àqueles que elas põem em risco: isso as coloca numa situação desconfortável de serem capazes de arruinar a vida das outras pessoas se elas cometerem um simples erro. Se elas forem interrogadas, por exemplo, elas terão algo a esconder, ao invés de serem capaz de honestamente alegar ignorância

O material original é bem útil para entender um pouquinho dessa cultura de segurança. Um ponto importante para a segurança digital é que é importante compartimentalizar sua atividade política online das suas atividades cotidianas. Não tem problema (por enquanto!) postar críticas ao governo no Facebook, mas você não vai querer falar sobre suas atividades de ação direta e contrapoder por lá! Podemos compreender a cultura de segurança digital como uma atitude “em camadas” em relação ao tipo de informação que estamos dispostos a compartilhar em contextos diferentes:

- A primeira camada é a faceta pública, aquilo que falamos abertamente (inclusive criticamente) em relação ao Estado e ao Capital. Nesses espaços, nunca fale sobre seu envolvimento (ou de outra pessoa) em grupos de ação direta ou outras formas de ativismo; sobre o desejo de outra(s) pessoa(s) em se envolver nesses grupos (incluindo o famoso “quem se interessar, me dá um ‘oi’ pra gente conversar”); sobre se outra(s) pessoa(s) são parte de um grupo; sobre sua participação (ou de outra pessoa) em ações ilegais; sobre seus planos (ou de outra pessoa) para futuras ações; e em defesa de ações realizadas por outrém. Esse é o famoso “Não pergunte, não diga:” você não precisa saber do que não vai participar.
Nem dizer nada a quem não vai fazer algo com você.

- A segunda camada é composta daqueles grupos de ativistas a que nos aliamos, ainda que indiretamente; por exemplo, grupos de Whatsapp e Telegram, ou mesmo grupos de Facebook, congregam muitas pessoas frustradas com o estado atual das coisas, e também juntam ativistas. Aqui a gente pode ser mais

franco na crítica, mas as limitações da primeira camada ainda se aplicam! Esses grupos podem ser úteis para nos aproximarmos de aliados em potencial, e para energizar o movimento, mas nunca para organizar ações.

-A terceira camada é composta pelo nosso grupo de afinidades. Aqui só estão os ativistas em quem confiamos e que nos apóiam nas nossas lutas. É com esse grupo que podemos planejar ações. E é nas comunicações com esse grupo que precisamos ter mais cuidado, já que elas podem ser monitoradas. Essa camada deve ser compartimentalizada das outras; aqui você deve usar pseudônimos, e nunca fazer referência à sua vida cotidiana para seus companheiros (e vice-versa, como já vimos!)

Algumas dicas de segurança na primeira e segunda camadas, extraídas do manual “Cultura de segurança: Autodefesa na era digital“:

Tudo em redes sociais pode e é filtrado pela polícia em tempo real. Essas informações ficam armazenadas nos servidores e podem ser buscadas no futuro e usadas como prova contra você.

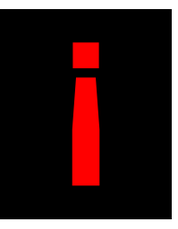
Não coloque NENHUMA informação pessoal nas redes: data de aniversário, cidade natal, etc.

Não confirme presença em eventos e evite mapas sociais, linkando-se a outras pessoas.

Não conecte diferentes partes da sua vida em um mesmo perfil (principalmente, mantenha as três camadas da sua vida separadas).

Existem redes sociais alternativas onde você tem mais controle sobre suas informações. Diaspora ou GnuSocial, por exemplo, são redes feitas pela comunidade de software livre, e têm como objetivo a comunicação e não a venda de informações. A rede riseup.net foi estruturada pensando em trabalho colaborativo de grupos e indivíduos em rede. Existem opções de comunidades virtuais e você deve fazer essa escolha conscientemente

Como fazer para nos comunicarmos com mais segurança com nosso grupo? E-mail, chat, e aplicativos de mensagens instantâneas que costumávamos usar devem ser abandonados ou trocados por alternativas seguras. Vamos começar aqui pela administração de senhas, porque isso será fundamental para todos os outros passos.



MAIS INFORMAÇÕES:

https://crimepensar.noblogs.org/post/2017/05/09/cultura-de-seguranca/

SENHAS

2. SENHAS

Não fazer: *Usar senhas inseguras; usar a mesma senha em vários sites/serviços diferentes; gravar a senha no navegador.*

Fazer: *Usar gerenciadores de senha seguros.*

Todo analista de segurança fala sobre a importância de utilizar senhas seguras, e de não usar a mesma senha para todos os sites, ou armazenar as senhas no navegador (em alguns casos como no Chrome/Chromium elas são sincronizadas pela internet e é muito fácil de ter acesso indevido à essas senhas, mesmo usando outros navegadores). Use gerenciadores de senhas, como o bitwarden ou o KeePassXC, em todos os seus dispositivos, se quiser senhas seguras. Esses gerenciadores podem gerar senhas automáticas, com criptografia forte, que podem ser sincronizadas por diferentes dispositivos. Com esses programas, você só precisa memorizar uma única senha, e as outras ficam gravadas; assim, se uma das suas contas for comprometida, as outras estarão seguras. O KeePassXC e derivados usam arquivos locais, dando mais controle mas necessitando de um pouco mais de trabalho (é preciso sincronizar o arquivo semi-manualmente, usando a nuvem para sincronizar automaticamente, ou pendrive e similares).

MAIS INFORMAÇÕES:

https://www.apc.org/en/irhr/digital-security-first-aid-kit-3

E-MAIL

3. E-MAIL

Não fazer: *Falar sobre atividade política em e-mails não-seguros*

Fazer: *Usar serviços seguros, como Protonmail, Tutanota, riseup.net, e autistici*

Nunca se comunique com ativistas, ou fale sobre ação direta, por e-mail corporativo, institucional, ou comercial. Jamais utilize contas do GMail, Yahoo, ou Outlook para essas comunicações. Você quer evitar que o conteúdo dessas mensagens esteja visível para a empresa que fornece o serviço, ou para seu chefe!

A única opção é utilizar clientes de forneçam criptografia ponto-a-ponto. Existem diversas opções de clientes: o Tutanota ou o Protonmail são bastante úteis, e bastante utilizados por agentes preocupados com privacidade. O riseup.net, muito utilizado por ativistas, tem algumas vantagens também: os servidores físicos são criptografados, as mensagens criptografadas individualmente, a ID de usuário sempre está oculta, e os serviços correm em Tor; além disso, para criar uma conta, você precisa de um convite, que normalmente só pode ser obtido com outro ativista que confia em você. O autistici também tem características semelhantes, mas, para conseguir uma conta, você precisa fazer uma solicitação com justificativa, que é avaliada por outros ativistas anonimamente.

Idealmente, crie uma conta em pelo menos dois desses serviços. Isso porque eles usam modos diferentes de se comunicar, de modo que às vezes a complementaridade é essencial para utilizá-los de maneira adequada.

Não preciso nem falar que não é pra usar seu nome real, ou qualquer nome que possa ser usado para te identificar, nessas contas, né? Não use também pseudônimos que podem ser utilizados para te encontrar em outros espaços (p. ex., não use seu @ do Twitter ou coisa do tipo!).

Essas contas poderão ser utilizadas depois para criar outros serviços, como apps de mensagem instantânea.

MAIS INFORMAÇÕES:

https://www.apc.org/en/irhr/digital-security-first-aid-kit-10

NAVEGAÇÃO

4. NAVEGAÇÃO

Não fazer: *Pesquisas, postagens, ou outras atividades em navegadores não-seguros*

Fazer: *Usar o Tor no computador e celular; Usar o Tails em situações mais extremas.*

Vários dos sites que você pode usar – seja para buscar informações, seja para postar atualizações das ações do seu grupo, seja para compartilhar material com outros ativistas – podem ser usados para te localizar fisicamente. Você não precisa usar o Tor pra tudo o que faz na vida, mas tudo aquilo que envolve a terceira camada deve ser feito com navegação segura.

4.1. INSTALE O TOR NO SEU COMPUTADOR

O TOR (The Onion Router) é uma rede aberta, acompanhada de software livre, que te ajuda a se defender da análise de tráfego, uma forma de vigilância de rede que ameaça sua liberdade e privacidade. Ele criptografa sua conexão e depois a passa por uma série de “nós” em diferentes países, colocando diversas camadas entre você e o site que tenta acessar; dessa maneira, não é possível identificar o seu IP a partir do site acessado. Trocando em miúdos, é uma forma de “navegar anonimanente”. Instale o Tor e o Tor Browser no seu computador, e o utilize sempre que for navegar.

4.2. INSTALE O ORBOT NO CELULAR

O Orbot é um aplicativo de celular, com versão para Android ou para iPhone, que usa o Tor como proxy para navegar e usar outros apps. Ele permite navegação anônima, usando o Orfox, e te permite passar alguns aplicativos por essa mesma conexão (“torificar” esses apps). Instale o Orbot e o Orfox no seu celular, e siga os passos abaixo para torificar a conexão de alguns apps:

A) Abra o Orbot no seu celular

B) Na parte de baixo da primeira tela, no campo “Tor-Enabled Apps”, clique na engrenagem

C) Selecione os apps que gostaria de torificar. Sugerimos fortemente que apps de comunicação (Telegram, Whatsapp, Wire, Signal) sejam torificados; esses apps não são seguros, e utilizar o Orbot pode aumentar um pouco a privacidade. Mas não se iluda: não use o Telegram ou o Whatsapp para conversar sobre ações, e nunca faça isso em grupos!

4.3. MUDE HÁBITOS DE NAVEGAÇÃO

A) Sempre use o Tor Browser para navegar no computador, ou o Orfox para navegar no celular. É possível torificar outros aplicativos, mas não é seguro.

B) Não use aplicativos de torrent enquanto estiver usando o Tor. Esses programas podem "furar" as configurações de proxy, enviando seu endereço I.P. real.

C) Não autorize o uso de plugins de navegador. O Tor Browser bloqueia plugins como Flash, RealPlayer, QuickTime, e outros que podem ser utilizados para revelar seu endereço IP, mas permite que você instale plugins (afinal, é uma versão do Firefox). Não ceda à tentação.

D) Sempre use versões HTTPS de websites. O Tor Browser usa uma extensão chamada HTTPS Everywhere para garantir isso, mas é bom ficar esperto: se, na barra de endereços, o site começar com "http://" ao invés de "https://", você não está seguro.

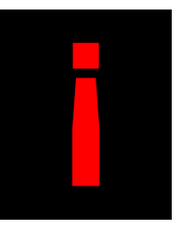
E) Não abra documentos baixados pelo Tor enquanto estiver online. Se precisar ler um PDF ou doc, faça-o com o aplicativo interno do Tor (não é possível fazer isso no celular!). Se não for possível, só abra o arquivo quando desconectar a máquina!

F) Ajude a expandir a rede. Use bridges e convença as pessoas a usar o Tor.

Uma nota: O Tor sempre vai deixar sua conexão mais lenta. Pense que uma conexão criptografada vai viajar o mundo até chegar no site que você deseja; mas é o preço que se paga por privacidade e proteção contra agentes maliciosos e contra o Estado.

4.4. USE O TAILS.

O Tails é um sistema operacional que roda direto de um pen drive ou de um DVD (i.e., é um live OS). Nele, todas as conexões passam pelo Tor, e ferramentas de criptografia de ponta são usadas para criptografar seus arquivos, e-mails, e mensagens instantâneas. Quando precisar tratar de questões de ativismo a partir do seu computador – principalmente se você está organizando uma ação, ou se está divulgando essa ação -, utilize o TAILS. Ele é mais seguro que só utilizar o TOR, já que, além de torificar todas as suas conexões, ele não deixa traços, no seu computador, das atividades que realizou, e roda diretamente do pen drive, sem necessitar de instalação. Ande sempre com um pen drive com o TAILS (instruções aqui). Para comunicações mais cotidianas, usar o Orbot no celular e o TOR no computador pode ser suficiente.



MAIS INFORMAÇÕES:

https://www.apc.org/en/irhr/digital-security-first-aid-kit-7

BUSCADORES

5. BUSCADORES

Não fazer: *Buscar informações sensíveis no Google ou no Bing.*
Fazer: *Usar o Duck Go Go ou o Searx.*

O Google armazena todos seus dados de busca, e você pode ver todas as buscas que você realizou no Google. Todo mundo sabe que esse é o modelo de negócios dos caras. O que isso quer dizer é que mais uma vez, seus dados podem ser acessados em caso de vulnerabilidade ou funcionários mal intencionados.

Use, por padrão, outras ferramentas. Recomendamos o duck go go, mas o Searx também é legal. O duck go go é a ferramenta-padrão de busca dos navegadores dedicados ao TOR, como o Orfox e o Tor Browser, mas você também pode utilizá-lo mesmo em conexões não-privativas e não-anônimas para evitar anúncios direcionados, por exemplo.

MENSAGENS INSTANTÂNEAS

6. MENSAGENS INSTANTÂNEAS

Não fazer: *Usar Whastapp, Facebook Messenger, Google Hangouts, Google Chats, Telegram, Viber, WeChat, ou DMs no Twitter*
Fazer: *Usar Wire ou Signal*

As mensagens instantâneas são fundamentais para organizar um monte de coisas, e os grupos utilizados pelos bolsonaristas para organizar a rede de propaganda (‘fake news’) são exemplo disso. Mas esses caras agiram com a conivência do Estado, que certamente estará mais esperto em relação a esses instrumentos.

No tocante a essas ferramentas, duas coisas são importantes: a primeira é a segurança da ferramente em si; a segunda é a segurança dos seus interlocutores. Lá do “Guia paranóico”:

O Whatsapp dispõe de criptografia ponto-a-ponto, mas é de propriedade do Facebook e não dá pra ter certeza de quantos metadados o Facebook armazena de todas as conversas.
O Messenger dispõe de “chats secretos”, mas o resto das conversas não é encriptada e é armazenada nos servidores do Facebook.

Hangouts e chats não dispõe de comunicação segura e toda a comunicação é armazenada nos servidores do Google.

Viber promete criptografia ponto-a-ponto, mas assim como o Whatsapp, não temos como saber o quão segura é a sua implementação.

Outros aplicativos, tais como WeChat não encriptam suas conversas e devem ser evitados.

O Telegram era minha primeira sugestão durante muito tempo. A interface é a melhor dentre os aplicativos de comunicação, mas o seu design faz com que por padrão as conversas não usem criptografia. Só as conversas criadas como “chat secreto” usam criptografia, o que por consequência faz com que as mensagens de conversas normais sejam todas armazenadas nos servidores do Telegram. Na minha opinião, é melhor do que outros itens dessa lista, mas não é ideal.

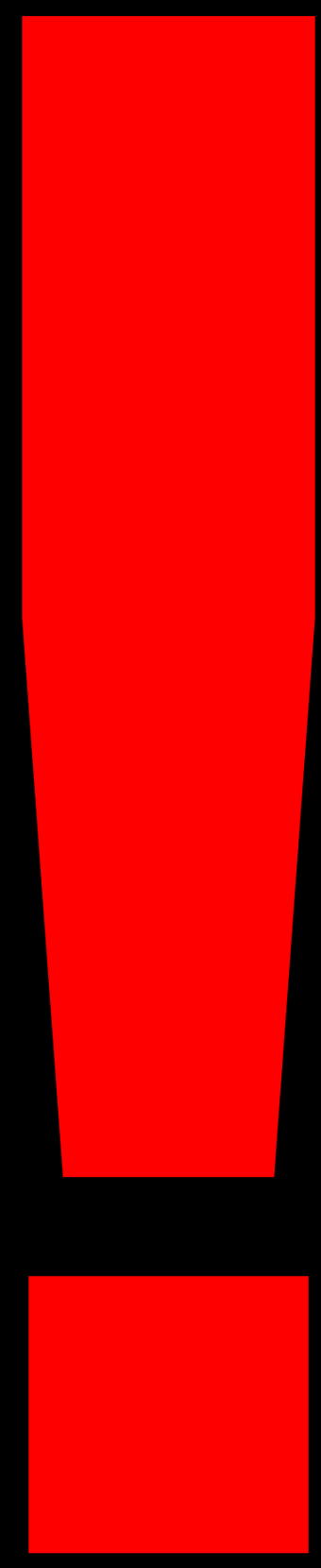
Sobram o Signal e o Wire. Ambos criptografam as mensagens em tempo real, e têm código aberto disponível para inspeção. Sugerimos o Wire, porque tem uma interface mais amigável, permite a verificação do interlocutor através de impressões digitais, e dispensa o número de telefone. De posse do seu e-mail anônimo, instale o Wire no seu celular e no seu computador. Fique longe das plataformas online, por serem menos seguras.

Repetindo o que já dissemos lá em cima:
Não preciso nem falar que não é pra usar seu nome real, ou qualquer nome que possa ser usado para te identificar, nessas contas, né? Não use também pseudônimos que podem ser utilizados para te encontrar em outros espaços (p. ex., não use seu @ do Twitter ou coisa do tipo!)

Outras questões importantes:
Não fale sobre ações específicas ou planos em grupos que não sejam privativos do seu grupo de afinidade
Cuidado com pessoas que se aproximam de você em grupos maiores.
Não se esqueça: mantenha a terceira camada da sua rede de ativismo isolada do resto!

MAIS INFORMAÇÕES:

https://lond.com.br/2018/10/29/o-guia-paran%C3%B3ico-de-seguran%C3%A7a-em-tempos-digitais.html



CELULAR

7. CELULAR

Não fazer: *Navegar sem anonimato; Armazenar mídia não-criptografada; Participar de reuniões presenciais sensíveis com o celular no bolso.*
Fazer: *Proteger suas mídias; Apagar dados sensíveis remotamente; Navegar anonimamente; Criptografar os dados.*

O telefone celular é uma ferramenta importante, e já vimos como podemos melhorar um pouco a segurança dele com Orbot e com mensageiros instantâneos mais seguros. Mas existem diversas outras ameaças à sua privacidade e ao seu ativismo que não só a navegação. Um smartphone é um pequeno computador, construído não para segurança e privacidade, mas para conforto. Uma grande quantidade de informações importantes pode ser encontrada nesses aparelhos: registros de ligações, mensagens, e localização geográfica, que são compartilhados com as teles, e podem ser utilizados por agentes maliciosos ou pelo governo para acessar facilmente informações suas. Algumas dicas para melhorar sua segurança:

Proteja sua mídia, incluindo fotos e vídeos. Não armazene fotos e vídeos sensíveis no seu celular, porque muitos aplicativos comuns podem ganhar acesso a sua galeria. Se necessário, use o app ObscuraCam (só para Android) para criptografar imagens e vídeos.

Se seu celular for comprometido, seja porque foi confiscado pela polícia, seja porque foi roubado, você pode apagar seus dados remotamente com o aplicativo InTheClear (só para Android). Além disso, você pode fazer isso nativamente pelo navegador, no caso do Android ou do iPhone.
Se o seu celular for comprometido, também é importante revocar o acesso dado a aplicativos ou contas, como Facebook, Gmail, e Twitter. Isso pode ser feito por um navegador em qualquer outro aparelho.

Use telas de bloqueio para dificultar que um ladrão oportunista acesse seu conteúdo ou mude o cartão SIM.
Criptografe seu celular. Isso fará com que seus arquivos não sejam facilmente acessíveis por um hacker, e é uma medida complementar ao uso do TOR (que criptografa sua conexão). É muito fácil fazer isso; faça-o no iPhone, ou no Android.

Cuidado com o uso de mensageiros instantâneos; sempre que possível, use o Orbot para torificar as conexões.

Você pode mandar mensagens pelo celular disfarçadas em uma imagem, por técnicas de esteganografia. No Android, use o app Pixelknot para esconder uma mensagem em uma imagem.

Nunca leia e-mails sensíveis no celular.

Se usar seu celular para tirar fotos ou vídeos de uma ação ou de uma manifestação, remova os metadados, que podem ser usados para te localizar. Existem aplicativos que fazem isso no iPhone e no Android.

Você também pode obscurecer rostos e pistas de identificação específicas usando o app ObscuraCam, no Android.

Seu celular pode ser transformado em um aparelho de vigilância, já que o microfone pode ser ligado por diversos aplicativos e serviços. Desligar o telefone também não resolve, já que as fábricas de aparelhos são signatárias de tratados internacionais que permitem que o provedor ative remotamente o aparelho.

Quando estiver falando sobre tópicos sensíveis, retire a bateria, ou mantenha o telefone longe.

Por mais atraentes que sejam do ponto de vista técnico e de controle dos recursos, a maioria dos Custom ROMs (incluindo o LineageOS) são menos seguros do que os sistemas operacionais que já vem com o seu celular. Evite-os.

Faça backups frequentes de dados, como sua lista de contatos.

MAIS INFORMAÇÕES:

https://www.apc.org/es/irhr/digital-security-first-aid-kit-5

ARMAZENANDO E TRANSPORTANDO ARQUIVOS SENSÍVEIS

8. ARMAZENANDO E TRANSPORTANDO ARQUIVOS SENSÍVEIS

Às vezes, produzimos arquivos sensíveis que precisamos armazenar ou transportar (p. ex., fotos, vídeos, material para impressão, etc.). Esses arquivos não devem ser acessados quando nossos computadores ou celulares são confiscados pela polícia. O que fazer para aumentar a segurança nesses casos?

Obscurecer seus dados fisicamente. Ao invés de transportá-los em um laptop ou celular, use cartões de memória ou pen drives. Esses dispositivos podem ser escondidos mais facilmente.
Obscureça seus dados digitalmente. Se você decidiu que é preciso transportar esses dados, eles devem estar criptografados, preferencialmente em um volume oculto. Existem diversas ferramentas para criptografia, como o BitLocker (para Windows). Instruções para como fazer isso no Linux podem ser encontradas aqui. Outra alternativa é usar o VeraCrypt.

Sempre que você quiser armazenar arquivos na nuvem (Google Drive, Dropbox, etc), criptografe-os antes de transferir. Alguns serviços de armazenamento na nuvem oferecem criptografia local (no seu computador) antes de fazer upload, como o SpiderOak, de forma que o conteúdo dos arquivos é inacessível ao provedor do serviço; entretanto, o SpiderOak não é gratuito. Também é possível esconder arquivos dentro de uma imagem, em um método chamado de esteganografia. Após criptografar o arquivo, você pode escondê-lo usando o OpenStego (no Windows e no Linux).

Você também pode criptografar todo o disco. Idealmente, o disco do seu computador deve estar criptografado (links para como fazer isso no Linux e no Windows). As mesmas ferramentas podem ser utilizadas para criptografar uma mídia portátil, como um pen drive ou cartão de memória. Tenha em mente, entretanto, que criptografar toda a mídia pode gerar desconfianças de que você está escondendo algo.

Assim como é importante armazenar arquivos seguramente, é igualmente importante apagar arquivos seguramente sem deixar rastros. Alguns softwares ”picotadores de arquivo” que você pode usar: dban; file shredder; CCleaner.

MAIS INFORMAÇÕES:

https://www.apc.org/en/irhr/digital-security-first-aid-kit-4