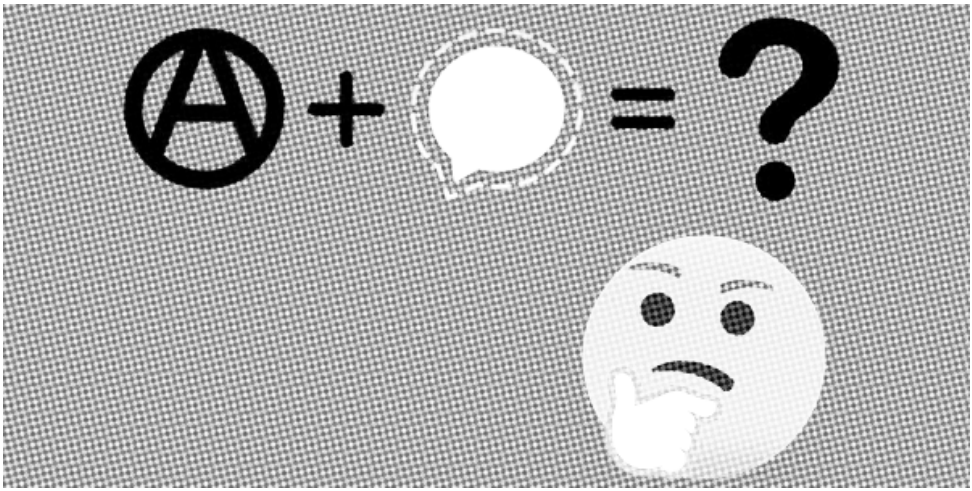
Quando o Signal não dá conta



Quando o Signal não dá conta

Texto original em Inglês
Signal Fails
2019
north-shore.info/2019/06/02/signal-fails

Tradução para o português
saltamontes.noblogs.org/post/2019/09/02/quando-o-signal-nao-da-conta

Layout
No Trace Project
notrace.how/resources/#signal-nao-da-conta

Introdução

O Signal[1] é um serviço de mensagens criptografadas que existe em diferentes formas há cerca de 10 anos. Desde então, tenho visto o software ser amplamente adotado por redes anarquistas no Canadá e nos Estados Unidos. Cada vez mais, para melhor e pior, nossas conversas interpessoais e em grupo passaram para a plataforma do Signal, na medida em que se tornou a maneira dominante pela qual anarquistas se comunicam neste continente, com muito pouco debate público sobre as implicações.

O Signal é apenas um aplicativo para espertofone. A mudança real de paradigma que está acontecendo é para uma vida cada vez mais mediada por telas de espertofones e mídias sociais. Levou apenas alguns anos para que os espertofones se tornassem obrigatórios para quem quer amigos ou precisa de trabalho, fora alguns bolsos perdidos. Até recentemente, a subcultura anarquista era um desses bolsos, onde você poderia se recusar a carregar um espertofone e ainda existir socialmente. Agora tenho menos certeza, e isso é deprimente. Então, vou teimosamente insistir ao longo deste texto que não há substituto para as relações face a face do mundo real, com toda a riqueza e complexidade da linguagem corporal, emoção e contexto físico, e elas continuam a ser a maneira mais segura de ter uma conversa privada. Então, por favor, vamos deixar nossos telefones em casa, nos encontrar em uma rua ou floresta, conspirar juntos, fazer música, construir alguma merda, quebrar alguma merda e nutrir a vida off-line juntos. Acho que isso é muito mais importante do que usar o Signal corretamente.

A ideia desse zine surgiu há um ano, quando eu estava visitando amigos em outra cidade e brincando sobre como as conversas do Signal lá onde moro viraram grandes tretas. Os padrões foram imediatamente reconhecidos e passei a perceber que essa conversa estava acontecendo em muitos lugares. Quando comecei a perguntar, todos tinham reclamações e opiniões, mas muito poucas práticas compartilhadas haviam surgido. Então, fiz uma lista de perguntas e botei-as para circular. Fiquei agradavelmente surpreso ao receber mais de uma dúzia de respostas detalhadas, que, combinadas com

[1] https://signal.org

várias conversas informais, são a base para a maior parte deste texto.[2]

Não sou especialista—não estudei criptografia e não sei programar. Sou um anarquista com interesse em segurança holística e um cético com relação à tecnologia. Meu objetivo com este artigo é refletir sobre como o Signal se tornou tão central na comunicação anarquista em nosso contexto, avaliar as implicações em nossa segurança coletiva e organização social e lançar algumas propostas preliminares para o desenvolvimento de práticas compartilhadas.

Uma breve história do Signal

Há 25 anos, aqueles entre nós que eram otimistas com a tecnologia viram um enorme potencial na Internet que surgia: ela seria uma ferramenta libertadora. Lembra daquele velho segmento da CBC[3] que elogiou "uma rede de computadores chamada Internet" como "anarquia modulada?" E embora ainda existam formas poderosas de se comunicar, coordenar e disseminar ideias online com segurança, fica claro que as entidades estatais e corporativas estão gradualmente capturando cada vez mais o espaço online e usando-o para nos sujeitar a formas cada vez mais intensas de vigilância e controle social.[4]

A internet sempre foi uma corrida armamentista. Em 1991, o criptógrafo, libertário e ativista da paz[5] Phil Zimmerman criou o Pretty Good Privacy[6] (PGP), um aplicativo de código aberto para criptografia de arquivos e criptografia de ponta a ponta para e-mail. Estou evitando detalhes técnicos, mas basicamente a importância de ser de ponta a ponta é que você

[2]Muito obrigado a todos que me escreveram! Roubei muitas de suas ideias.

[3]https://www.youtube.com/watch?v=bl0wS1304jo

[4]Os modos de governança da era da Internet variam de lugar para lugar—Estados mais autoritários podem preferir filtragem e censura, enquanto Estados democráticos produzem uma espécie de "cidadania digital"—mas a vigilância em massa e a guerra cibernética estão se tornando a norma.

[5]Ironicamente, o governo dos EUA mais tarde tentou acusar Zimmerman de publicar livremente o código-fonte do PGP, argumentando que ele estava "exportando armas". Então, ele publicou o código-fonte em livros de capa dura e enviou-os pelo mundo. O motivo é que a exportação de livros está protegida pela Constituição dos EUA.

[6]https://openpgp.org

pode se comunicar de forma segura diretamente com outra pessoa, e seu serviço de e-mail não pode ver a mensagem, seja o Google ou o Riseup. Até hoje, até onde sabemos, a criptografia PGP nunca foi quebrada.[7]

Durante anos, técnicos e nerds de segurança em certos círculos—anarquistas, jornalistas, criminosos, etc.—tentaram espalhar o PGP para suas redes como uma espécie de infraestrutura de comunicações seguras, com algum sucesso. Como em tudo, havia limitações. Minha maior preocupação de segurança com o PGP é a falta de Sigilo Direto, o que significa que, se uma chave de criptografia privada for comprometida, todos os e-mails enviados com essa chave poderão ser descriptografados por um invasor. Esta é uma preocupação real, dado que a NSA quase certamente está armazenando todos os seus e-mails criptografados em algum lugar, e um dia computadores quânticos poderão ser capazes de quebrar o PGP. Não me pergunte como funcionam os computadores quânticos—até onde sei, é pura mágica do mal.

O grande problema social com o PGP, um dos que mais influenciaram o projeto Signal, é o fato de que nunca foi amplamente adotado fora de um pequeno nicho. Na minha experiência, foi até difícil trazer anarquistas para o PGP e fazê-los usá-lo apropriadamente. Houve oficinas, muitas pessoas foram instruídas, mas assim que um computador caiu ou uma senha foi perdida, tudo voltava à estaca zero. Simplesmente não colou.

Por volta de 2010, os espertofones começaram a se popularizar e tudo mudou. A onipresença das mídias sociais, as mensagens instantâneas constantes e a capacidade das empresas de telecomunicações (e, portanto, do governo) de rastrear todos os movimentos dos usuários[8] transformaram completamente o modelo de ameaças. Todo o trabalho que as pessoas dedicam à segurança de computadores teve que voltar décadas para trás: os espertofones contam com uma arquitetura completamente diferente dos PCs, resultando em muito menos controle do usuário, e o advento

[7]Processos judiciais contra as Brigadas Vermelhas na Itália (2003) e pornógrafos infantis nos EUA (2006) mostraram que as agências policiais federais não conseguiram entrar em dispositivos e comunicações protegidos por PGP. Em vez disso, os agentes recorreram a dispositivos de escuta, passando leis que exigiam que você entregasse senhas e, é claro, informantes.

[8]Quer ler algo assustador? Procure o Sensorvault da Google.

de permissões de aplicativos completamente livres tornou quase ridícula a ideia de privacidade dos espertofones.

Este é o contexto em que o Signal apareceu. O anarquista "cypherpunk" Moxie Marlinspike[9] começou a trabalhar num software para levar criptografia de ponta a ponta para smartphones, com a propriedade de Segredo Futuro, trabalhando na ideia de que a vigilância em massa deveria ser combatida com criptografia em massa. O signal foi projetado para ser utilizável, bonito e seguro. Moxie concordou em juntar-se aos gigantes da tecnologia WhatsApp, Facebook, Google e Skype para implementar o protocolo de criptografia do Signal em suas plataformas também.

> "É uma grande vitória para nós quando um bilhão de pessoas estão usando o WhatsApp e nem sequer sabem que ele está criptografado."
>
> — *Moxie Marlinspike*

Compreensivelmente, os anarquistas são mais propensos a confiar suas comunicações ao Signal—uma fundação sem fins lucrativos dirigida por um anarquista—do que a confiar numa grande empresa de tecnologia, cujo principal modelo de negócio é colher e revender dados de usuários. E o Signal tem algumas vantagens sobre essas outras plataformas: é de código aberto (e, portanto, sujeito a revisão por pares), criptografa a maioria dos metadados, armazena o mínimo possível de dados do usuário e oferece alguns recursos úteis, como o desaparecimento de mensagens e a verificação do número de segurança para proteger contra intercepções.

O Signal conquistou elogios quase universais de especialistas em segurança, incluindo endossos do delator da NSA, Edward Snowden,[10] e as melhores pontuações da respeitada Electronic Frontier Foundation.[11] Em 2014, documentos vazados da NSA descreveram o Signal como uma "grande ameaça" à sua missão (de saber tudo sobre todos). Pessoalmente, confio na criptografia.

Mas o Signal realmente protege apenas uma coisa, e essa coisa é a sua comunicação enquanto viaja entre o seu dispositivo e outro dispositivo.

---

[9] https://moxie.org

[10] https://web.archive.org/web/20220119200511/https://twitter.com/Snowden/status/661313394906161152

[11] https://eff.org

Isso é ótimo, mas é apenas uma parte de uma estratégia de segurança. É por isso que é importante, quando falamos de segurança, começar com um Modelo de Ameaças.[12] As primeiras perguntas para qualquer estratégia de segurança são quem é o seu adversário esperado, o que ele está tentando capturar e como é provável que o faça. A ideia básica é que as coisas e práticas são apenas seguras ou inseguras em relação ao tipo de ataque que você está esperando se defender. Por exemplo, você pode ter seus dados fechados com criptografia sólida e a melhor senha, mas se o invasor estiver disposto a torturá-lo até que você entregue os dados, tudo aquilo realmente não importa.

Para o propósito deste texto, eu proporia um modelo de ameaças de trabalho que se preocupa principalmente com dois tipos de adversários. O primeiro é agências de inteligência globais ou hackers poderosos que se envolvem em vigilância em massa e interceptam comunicações. A segunda são as agências policiais, operando em território controlado pelo governo canadense ou estadunidense, engajados numa vigilância direcionada a anarquistas. Para a polícia, as técnicas básicas de investigação incluem monitoramento de listas de e-mail e mídias sociais, envio de policiais à paisana (p2) para eventos e informantes casuais. Às vezes, quando eles têm mais recursos, ou nossas redes se tornam uma prioridade maior, eles recorrem a técnicas mais avançadas, incluindo infiltração de longo prazo, vigilância física frequente ou contínua (incluindo tentativas de capturar senhas), escuta de dispositivos, interceptação de comunicações e invasões domésticas, onde os dispositivos são apreendidos e submetidos a análise forense.

Devo salientar que muitas jurisdições europeias estão implementando leis de quebra de sigilo importantes[13] que obrigam legalmente os indivíduos a dar suas senhas às autoridades sob certas condições ou ir pra cadeia.[14] Talvez seja apenas uma questão de tempo, mas, por enquanto, no Canadá e nos EUA, não somos legalmente obrigados a divulgar senhas para as

[12] https://en.wikipedia.org/wiki/Threat_model

[13] https://en.wikipedia.org/wiki/Key_disclosure_law

[14] Negação plausível, sigilo antecipado e destruição segura de dados são projetados em algumas ferramentas de privacidade para tentar conter essa ameaça ou pelo menos minimizar seus danos.

autoridades, com a notável exceção de quando estamos atravessando a fronteira.[15]

Se o seu dispositivo estiver comprometido com um gravador de digitação (keylogger) ou outro software malicioso, não importa quão seguras sejam as suas comunicações. Se você está saindo com um informante ou policial, não importa se você tira a bateria do telefone e fala em um parque. Cultura de segurança e segurança de dispositivos são dois conceitos não cobertos por este texto mas que devem ser considerados para nos proteger contra essas ameaças muito reais. Incluí algumas sugestões na seção "Outras leituras", p. 16.

Também vale mencionar que o Signal não foi projetado para anonimato. Sua conta do Signal é registrada com um número de telefone, portanto, a menos que você se registre usando um telefone descartável comprado em dinheiro ou um número descartável on-line, você não está anônimo. Se você perder o controle do número de telefone usado para registrar sua conta, outra pessoa poderá roubar sua conta. É por isso que é muito importante, se você usar um número anônimo para registrar sua conta, ativar o recurso "bloqueio de registro".

Principalmente por razões de segurança, o Signal se tornou o meio de comunicação padrão nos círculos anarquistas nos últimos 4 anos, ofuscando todo o resto. Mas assim como "o meio é a mensagem", o Signal está tendo efeitos profundos sobre como os anarquistas se relacionam e se organizam, que muitas vezes são negligenciados.

[15] As impressões digitais (e outros dados biométricos) não são consideradas senhas em muitas jurisdições, o que significa que as impressões digitais não estão sujeitas às mesmas proteções legais.

O lado social do Signal

> "O Signal é útil na medida em que substitui formas menos seguras de comunicação eletrônica, mas se torna prejudicial […] quando substitui a comunicação face a face."
>
> — *Participante da minha pesquisa*

A maioria das implicações sociais do Signal não tem a ver especificamente com o aplicativo. São as implicações de mover cada vez mais nossas comunicações, expressão pessoal, esforços de organização e tudo o mais para plataformas virtuais e mediá-las com telas. Mas algo que me ocorreu quando comecei a analisar as respostas aos questionários que enviei é que, antes do Signal, conheci várias pessoas que rejeitaram os espertofones por razões de segurança e sociais. Quando o Signal surgiu com respostas para a maioria das preocupações de segurança, a posição de recusa foi significativamente corroída. Hoje, a maioria das pessoas que querem estar fora tem espertofones, seja porque elas foram convencidas a usar o Signal ou ele se tornou efetivamente obrigatório se elas quisessem se continuar envolvidas. O Signal atuou como uma porta de entrada no mundo dos espertofones para alguns anarquistas.

Por outro lado, já que o Signal é uma redução de danos para aqueles de nós que já estamos presos em espertofones, isso é uma coisa boa. Fico feliz que as pessoas que estavam principalmente socializando e fazendo organização política em canais não criptografados como o Facebook, mudaram para o Signal. Na minha vida, o bate-papo em grupo substituiu

a "pequena lista de e-mails" e é bastante útil para fazer planos com amigos ou compartilhar links. Nas respostas que coletei, os grupos de signal que eram mais valiosos para as pessoas, ou talvez os menos irritantes, eram os que eram pequenos, focados e pragmáticos. O Signal também pode ser uma ferramenta poderosa para divulgar de maneira rápida e segura um assunto urgente que requer uma resposta rápida. Se a organização baseada no Facebook levou muitos anarquistas a acreditar que a organização com qualquer elemento de surpresa é impossível, o Signal salvou parcialmente essa ideia, e sou grato por isso.

O Signal não dá conta

Inicialmente, imaginei este projeto como uma pequena série de vinhetas de quadrinhos que eu planejava chamar de "O Signal não Dá Conta", vagamente inspirado no livro "Come Hell or High Water: A Handbook on Collective Process Gone Awry"[16] ("Come Hell ou High Water: um manual sobre processo coletivo cheio de percalços"). Acontece que é difícil fazer desenhos interessantes representando as conversas do Signal e eu sou uma droga no desenho. Foi mal se eu prometi a alguém que, talvez na segunda edição… De qualquer forma, ainda quero incluir alguns desenhos de "O Signal não dá conta", como uma maneira de tirar sarro de nós (e eu me incluo nisso!) e talvez para cutucar gentilmente todo mundo para que deixem de ser tão chatos.

Bond, James Bond. Ter Sinal não te torna intocável. Dê um pouco de criptografia a algumas pessoas e elas imediatamente aporrinharão toda a sua lista de contatos. Seu telefone ainda é um dispositivo de rastreamento e a confiança ainda é algo que se constroí. Converse com a sua galera sobre os tipos de coisas que vocês se sentem à vontade de falar ao telefone e o que não.

Silêncio não é consentimento. Você já foi numa reunião, fez planos com outros, montou um grupo de Signal para coordenar a logística, e então uma ou duas pessoas rapidamente mudaram os planos coletivos através de

[16]https://web.archive.org/web/20240308061230/https://www.akpress.org/comehellorhighwater.html

uma série rápida de mensagens que ninguém teve tempo de responder? Pois é, não é legal.

Uma reunião interminável é um inferno. Um grupo de Signal não é uma reunião em andamento. Como já estou muito grudado ao meu telefone, não gosto quando um assunto está explodindo no chat do telefone e na real é apenas uma longa conversa entre duas pessoas ou o fluxo de consciência de alguém que não está relacionado com o propósito do grupo. Aprecio quando conversas têm começos e fins.

"Me dá mais!" Esse é um que particularmente odeio. Provavelmente por causa do comportamento em redes sociais, alguns de nós estão acostumados a receber informações escolhidas para nós por uma plataforma. Porém, o Signal não é rede social, ainda bem! Então, fique ligado porque quando um grande grupo no Signal começa a se tornar um mural de notícias (feed), você está com problemas. Isso significa que, se você não estiver envolvido e prestando atenção, perderá todos os tipos de informações importantes, sejam eventos futuros, pessoas mudando seus pronomes ou conversas inflamadas que levam a rachas. As pessoas começam a esquecer que você existe e, eventualmente, você literalmente desaparece. Mate o FEED.

Incêndio num teatro lotado. Também conhecido como o problema do botão de pânico. Você está de boa em um grande grupo do Signal com todos os seus pseudo amigos e todos os seus números de telefone reais, aí alguém é pego por tentar roubar numa loja ou algo assim, e ta-dan, o telefone daquela pessoa não é criptografado! Todo mundo se assusta e pula do navio, mas é tarde demais, porque se os policiais estão vistoriando esse telefone agora, eles podem ver todos que saíram e o mapeamento social está feito. Sinto muito.

História sem fim. Alguém criou um grupo no Signal para coordenar um evento específico que aconteceria uma vez só. Rolou, mas ninguém quer sair do grupo. De alguma forma, essa formação ad hoc muito específica é agora A ORGANIZAÇÃO PERMANENTE que se encarregou de decidir tudo sobre todas as coisas—indefinidamente.

Em busca de práticas compartilhadas

Se você achava que esse era um guia de boas práticas de Signal ou como se comportar num chat, foi mal ter te trazido tão longe sem ter deixado claro que não era. Esse texto é muito mais algo como "temos que falar sobre Signal". Acredito de verdade no desenvolvimento de práticas compartilhadas dentro de contextos sociais específicos, e recomendo que comecemos tendo essa conversa de maneira explícita nas suas redes. Para isso, tenho algumas propostas.

Existem alguns obstáculos para a adoção de práticas compartilhadas. Algumas pessoas não possuem o Signal. Se isso acontece porque elas estão construindo relações sem espertofones, tudo que posso dizer é: elas têm o meu respeito. Se é porque elas passam o dia inteiro no Facebook, mas o Signal é "muito difícil", aí é difícil de engolir. De resto, o Signal é fácil de instalar e de usar para qualquer pessoas que tenha um espertofone e uma conexão de internet.

Também discordo da perspectiva orwelliana que vê a criptografia como inútil: "A polícia já sabe de tudo!" É muito desempoderador pensar o governo dessa forma, e felizmente isso não é verdade—resistir ainda não é infrutífero. As agências de segurança possuem capacidade fodásticas, incluindo algumas que a gente nem sabe ainda. Mas existe ampla evidência de que a criptografia vem frustrado investigações policiais e é por isso que o governo está passando leis que impeçam o uso dessas ferramentas.

Talvez o maior obstáculo para as práticas compartilhadas é a falta generalizada de um "nós"—em que medida temos responsabilidades com alguém,

e se temos, com quem? Como estamos construindo eticamente normas sociais compartilhadas? A maioria das anarquistas concordam que é errado dedurar, por exemplo, mas como podemos chegar lá? Eu realmente acredito que um tipo de individualismo liberal barato está influenciando o anarquismo e tornando a própria questão das "expectativas" quase um tabu de ser discutido. Mas esse seria um texto para outro dia.

Algumas propostas de Boas Práticas

1. **Mantenha as coisas no mundo real**. Como uma pessoa disse, "a comunicação não apenas compartilhar informação." A comunicação cara a cara constrói relações completas, incluindo confiança, e continua sendo a forma mais seguras de se comunicar.
2. **Deixe os seus aparelhos em casa**. Quem sabe às vezes? Especialmente se você vai atravessar a fronteira, onde podem te forçar a descriptografar seus dados. Se você vai precisar de um telefone durante uma viagem, compre um telefone de viagem com suas amizades que não tenha nenhuma informação sensível nele, como sua lista de contatos.
3. **Torne seus aparelhos seguros**. A maioria dos aparelhos (telefones e computadores) já possuem a opção de criptografia total de disco. A criptografia é tão boa quanto a sua senha e protege seus dados "em descanso", ou seja, quando ele está desligado ou os dados não estão sendo usados por algum programa. O bloqueio de tela fornece alguma proteção enquanto seu aparelho está ligado, mas pode ser desviada por um atacante sofisticado. Alguns sistemas operacionais obrigam a usar a mesma senha para a criptografia de disco e para o bloqueio de tela, o que é uma pena pois não é prático escrever uma senha longa 25 vezes por dia (às vezes na presença do zóião ou de câmeras de vigilância).
4. **Desligue seus aparelhos**. Se você não está de olho neles, ou se for dormir, desligue-os. Compre um despertador barato. Caso sua casa seja invadida pela polícia durante a noite, você ficará bem feliz de ter feito isso. Quando o aparelho está desligado e criptografado com uma senha forte quando for apreendido, a polícia terá muito

menos chances de "quebrá-lo". Caso você queira ir ainda mais longe, compre um bom cofre e tranque seus aparelhos lá dentro quando não estiver usando-os. Isso reduzirá o risco de que eles sejam adulterados fisicamente sem que você perceba.

5. **Estabeleça limites**. Temos noções diferentes sobre o que é seguro falar no telefone e o que não é. Discuta e crie limites coletivos sobre isso, e onde houver desacordo, respeite os limites das pessoas mesmo se você acha que está seguro.
6. **Combine um sistema de entrada no grupo**. Se você está discutindo assuntos sensíveis no coletivo, crie uma compreensão coletiva sobre o que seria um sistema de entrada de novas pessoas. Numa época em que anarquistas são acusados de conspiração, a falta de comunicação sobre isso pode mandar pessoas para a cadeia.
7. **Pergunte primeiro**. Se você vai adicionar alguém num assunto, fazendo assim com que os números de telefone do grupo todo sejam revelados, antes de tudo peça o consentimento do grupo.
8. **Minimize as tomadas de decisão online**. Considere deixar as decisões que não sejam de sim/não para reuniões presenciais, se possível. Pela minha experiência. o Signal empobrece os processos de tomada de decisão.
9. **Objetivo definido**. Idealmente, um grupo no Signal tem um objetivo específico. Cada pessoa que for adicionada a esse grupo deveria ser devidamente apresentada sobre esse objetivo. Caso ele seja alcançado, saia do grupo e delete-o.
10. **Mensagens Temporárias**. Isso é bem útil para manter a casa em ordem. Indo de 5 segundos a uma semana, as Mensagens Temporárias podem ser configuradas ao clicar no ícone do cronômetro na barra superior de uma conversa. Muitas pessoas usam o padrão de 1 semana para todas as suas mensagens, sejam as conversas sensíveis ou não. Escolha o tempo de expiração com base no seu modelo de ameaças. Isso também te protege, de alguma forma, caso a pessoa com que você está se comunicando esteja usando práticas de segurança fracas.
11. **Verifique os números de segurança**. Esta é a sua melhor proteção contra ataques de homem-no-meio. É bem simples e fácil de fazer

isso ao vivo—abra sua conversa com a pessoa e vá até as "Configurações da Conversa > Ver o número de segurança" e escaneie o código QR ou compare os números. A maioria das pessoas que me responderam disseram que "eu deveria fazer isso, mas não faço". Aproveita suas reuniões para verificar seus contatos. Tudo bem ser nerd!

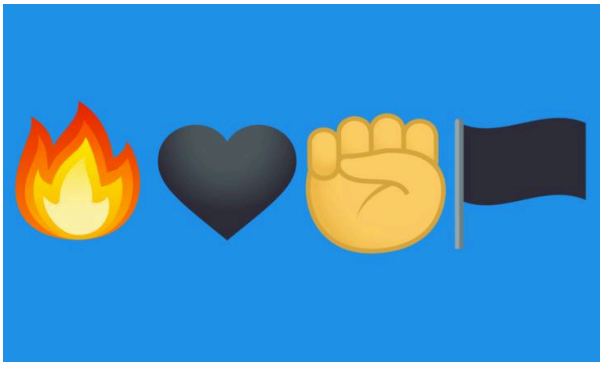
12. **Habilite o Bloqueio de Registro**. Habilite essa opção nas configurações de privacidade do Signal, para o caso de se alguém conseguir hackear seu número de telefone usado para registrar sua conta, ele ainda precisará obter seu PIN para roubar sua identidade. Isso é especialmente importante para contas do Signal anônimas registradas com números descartáveis, já que alguém certamente usará esse número novamente.
13. **Desativar a visualização de mensagens**. Impeça que as mensagens apareçam na sua tela de bloqueio. No meu dispositivo, tive que definir isso nas configurações do dispositivo (não configurações do Signal) em "Bloquear Preferências de tela > Ocultar conteúdo sensível".
14. **Excluir mensagens antigas**. Seja ativando o número máximo mensagens por conversa ou excluindo manualmente as conversas concluídas, não guarde as mensagens que você não precisa mais.

Conclusão

Embarquei neste projeto para refletir e reunir feedbacks sobre o impacto que o Signal teve em redes anarquistas nos EUA e no Canadá, do ponto de vista da segurança e da organização social. Ao fazê-lo, acho que esbarrei com algumas frustrações comuns que as pessoas têm, especialmente com grandes grupos de Signal, e reuni algumas propostas para fazê-las circular. Continuo insistindo que os espertofones estão causando mais danos do que benefícios às nossas vidas e lutas. Digo isso porque elas são importantes para mim. Precisamos preservar e construir outras formas de nos organizar, especialmente offline, tanto para nossa qualidade de vida quanto para a segurança do movimento. Mesmo se continuarmos usando espertofones, é perigoso quando nossas comunicações são centralizadas. Se os

servidores do Signal caírem hoje à noite, ou Riseup,[17] ou Protonmail,[18] imagine como isso seria devastador para nossas redes. Se anarquistas alguma vez representarem uma grande ameaça à ordem estabelecida, eles virão atrás de nós e de nossa infraestrutura sem piedade, inclusive suspendendo as "proteções legais" das quais poderemos estar dependendo. Para melhor e pior, acredito que este cenário seja possível enquanto ainda estivermos vivos, e por isso devemos planejar pensando em resiliência.

A galera tech entre nós deve continuar a experimentar outros protocolos, softwares e sistemas operacionais,[19] compartilhando-os se forem úteis. Quem decidiu ficar fora deve continuar resistindo fora e encontrar maneiras de seguir lutando offline. Para o resto de nós, vamos minimizar o grau em que somos capturados pelos espertofones. Juntamente com a capacidade de lutar, devemos construir vidas que valham a pena, com uma qualidade de relacionamento que os potenciais amigos e co-conspiradores considerem irresistivelmente atraente. Pode ser a única esperança que temos.



[17]https://riseup.net

[18]https://protonmail.com

[19]No meu telefone, recentemente substituí o Android pelo LineageOS, que é um sistema operacional desgooglezado, direcionado para a privacidade, baseado no código Android. Ele é ótimo, mas é feito apenas para determinados dispositivos, você anula a garantia do telefone e definitivamente há uma curva de aprendizado quando se trata de configurá-lo, mantê-lo atualizado e mudar para um software de código aberto.

Outras leituras

Este zine foi publicado em maio de 2019. O Signal atualiza periodicamente seus recursos. Para obter as informações mais atualizadas sobre assuntos técnicos, acesse signal.org, community.signalusers.org, e /r/signal[20] no Reddit.

- Seu telefone é um policial.[21]
- Escolhendo a ferramenta apropriada para a tarefa.[22]
- Guias de ferramentas da EFF para autodefesa de vigilância (incluindo Signal).[23]
- Para uma cultura de segurança coletiva.[24]
- Guia de segurança do Riseup.[25]
- Grupo Principal de Conspiração do Toronto G20: as acusações e como elas surgiram.[26]

[20]https://reddit.com/r/signal

[21]https://itsgoingdown.org/phone-cop-opsecinfosec-primer-dystopian-present

[22]https://crimethinc.com/2017/03/21/choosing-the-proper-tool-for-the-task--assessing-your-encryption-options

[23]https://ssd.eff.org/en/module-categories/tool-guides

[24]https://crimethinc.com/2009/06/25/towards-a-collective-security-culture

[25]https://riseup.net/security

[26]https://notrace.how/resources/#toronto-g20-main-conspiracy-group

O Signal é um serviço de mensagens criptografadas que existe em diferentes formas há cerca de 10 anos. Desde então, tenho visto o software ser amplamente adotado por redes anarquistas no Canadá e nos Estados Unidos. Cada vez mais, para melhor e pior, nossas conversas interpessoais e em grupo passaram para a plataforma do Signal, na medida em que se tornou a maneira dominante pela qual anarquistas se comunicam neste continente, com muito pouco debate público sobre as implicações.

No Trace Project / No trace, no case. Um coleção de ferramentas para auxiliar anarquistas e outros rebeldes a **entender** as capacidades de seus inimigos, **minar** tentativas de vigilância, e principalmente **agir** sem ser pego.

Dependendo do seu contexto, a posse de certos documentos pode ser criminalizada ou acabar por atrair atenção indesejada; seja cuidadoso com quais zines você imprime e onde você os guarda.