HAQUEAR & DESTRUIR

faccaoficticia.noblogs.org

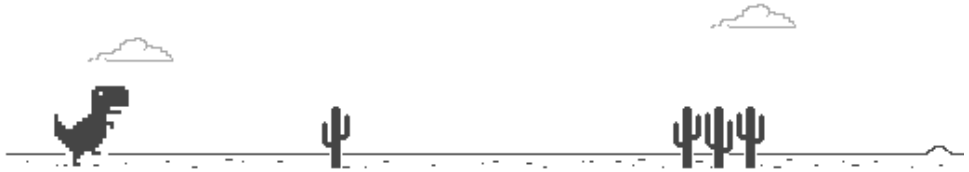
CULTURA DE SEGURANÇA

AUTODEFESA NA ERA DIGITAL

Aviso aos cães:

Esta é uma publicação independente que organiza textos públicos compartilhados em outros meios impressos e na internet. Nosso único propósito é debater e encorajar uma análise crítica sobre seu conteúdo. Não endossamos nem estimulamos qualquer ato de vandalismo, violência contra agentes do Estado, propagação do pânico ou organizações clandestinas, rebeldes, sediciosas, expropriadoras, subversivas, terroristas, criminosas, insurrecionárias nem qualquer outra forma de ação pautada na ilegalidade. Nos enquadramos nessa sociedade, inegavelmente, como parte de uma classe média que se beneficia das desigualdades e injustiças do Capitalismo. Sendo assim, não temos motivos para incentivar o questionamento e o conflito com um sistema que nos garante privilégios tão especiais. É sério.

NA DÚVIDA, MANTENHA INFORMAÇÕES SENSÍVEIS OFFLINE.



BOA SORTE! E LEMBRE-SE:
VOCÊ NÃO OUVIU ISSO DA GENTE!

CHAT:

- Aplicativos de celular de comunicação instantânea em geral usam protocolos privados para comunicação. Isso significa que não podemos saber, mesmo com o WhatsApp alegando criptografia de ponta-a-ponta, como que nossas mensagens trafegam na rede e nos servidores das empresas. Escolha aplicativos com protocolos federados e de código aberto como o XMPP (jabber), que utilizem servidores não comerciais como o riseup.net. Vários dos aplicativos que usam protocolos federados trabalham com a criptografia Off-The-Record (OTR), reconhecida como uma das melhores.
- Entre Telegram, WhatsApp e Signal, prefira o Signal. Em termos de segurança, os critérios mínimos para um software são: ter seu código aberto e usar criptografia bem conhecida. Com base nisso, infelizmente, nenhum desses três são satisfatórios.
- Escolha aplicativos que não usam seu número de celular como usuária. Seu número é um identificador, assim como o de seus contatos. As empresas de telefonias detêm seu nome completo, CPF e endereço. Hoje em dia, celulares são muito mais computadores do que telefones. Utilize-se dessa mudança e use contas com nomes de usuárias. Com esse tipo de aplicativo você pode usar pseudônimos, inclusive de uso único.

CRIPTOGRAFIA:

EMAIL:

No Thunderbird, instale a extensão Enigmail

ARQUIVOS:

LUKS – Para criptografia total de disco, partições e dispositivos USB.

GnuPG – criptografe arquivos ou pastas com a tecnologia OpenPGP.

NAVEGADOR:

- Firefox – Para temas menos sensíveis, onde o anonimato não é vital e que demande mais velocidade de conexão, use o Firefox configurado de acordo com esse manual: myshadow.org/prevent-online-tracking
- TorBrowser – Quando o anonimato é muito importante, use a rede Tor e esconda seu IP para minimizar rastros na internet.

CULTURA DE SEGURANÇA

Tudo sobre cultura de segurança pode ser resumido numa frase: ninguém deve saber de informações que não precisa saber. Quanto mais gente souber de algo que possa colocar pessoas em risco (quem vai fazer o que, quando, ou o local de uma reunião ou ação), mais chances haverá de autoridades terem acesso a essas informações. Isso coloca em risco tanto as pessoas que estão realizando a ação, quanto as pessoas que sabem que existe uma ação. Isso as deixa com a responsabilidade e a tensão de não poderem dar um passo em falso e deixar escapar uma informação. Além de que, se não souberem de fato o que acontece, não precisam mentir caso sejam interrogadas.

Por isso, a cultura de segurança é um conjunto de costumes compartilhados por pessoas ou grupos que podem ser alvos de perseguição ou investigação por parte do governo, empresas ou outros inimigos. Não se trata de regras ou protocolos, mas algo que cultivamos, como hábitos de higiene ou "boas maneiras". Um modo de evitar desentendimentos desnecessários ou conflitos desastrosos. A pessoa que viola a cultura de segurança de suas comunidades não deve ser repreendida duramente na primeira vez. Não é uma questão de ser ativista foda o bastante para participar de panelinhas, mas de estabelecer expectativas coletivas e ajudar as pessoas a entenderem sua importância. É preciso deixar claro imediatamente de que forma as ações de uma pessoa pode colocar todas em risco. Aquelas que não puderem entender isso podem ser excluídas de todas as situações que merecem cuidado.

São coisas que não precisamos pensar e nos forçar como um protocolo, mas práticas e comportamentos que tornamos naturais e cotidianos. Ter uma cultura de segurança nos ajuda a compartilhar habilidades e procedimentos que podem ser acionados a qualquer momento, ao invés de ter que começar do zero toda vez que precisar de agir com sigilo e cautela. Isso ajuda a evitar toda a paranoia e o pânico em situações de estresse. Além de manter as pessoas fora da prisão, é claro.

Para isso, resumiremos algumas dicas, ou passos para compartilharmos um mínimo de segurança e começarmos a construir essa cultura:

- Não pergunte, não diga: você não precisa saber do que não vai participar nem dizer nada a quem não vai fazer algo com você.
- Não comente abertamente com qualquer pessoa sobre ações que você pode ou pretende se envolver em algum momento.
- Diga não a qualquer momento, sobre qualquer coisa: não responda nada do que não queira responder. Faça isso não só quando a polícia te interrogar, mas em conversas com outras pessoas, ativistas ou mesmo com amizades íntimas.
- Não facilite ou deixe rastros para seus inimigos te encontrarem: não seja previsível com métodos de ação, lugares para se reunir ou alvos e momentos para atacar. Evite ambientes monitorados ou próximos do local da ação. Não fique visível ou circule seu nome e informações sobre você em listas de e-mail, compras em lojas, ou redes sociais e contas virtuais. Se for comprar algum material que possa te incriminar, faça-o longe de casa ou do lugar da ação e use dinheiro vivo. Evite cartões ou formas de comprar que salvem seus dados.
- Desenvolva linguagens e códigos para poder se comunicar com seu grupo com segurança mesmo em público. Assim como métodos de estabelecer níveis de segurança para cada situação: numa reunião, as pessoas que se apresentaram devem conhecer pelo menos duas pessoas que têm certeza de que ela não é alguém infiltrado.
- Aprenda e acate as expectativas de segurança de cada pessoa com a qual você interagir e respeite as diferenças de estilo.
- Permita que outras pessoas saibam exatamente quais são suas necessidades com relação à segurança.
- Não use Facebook ou redes sociais: seria suficiente dizer para evitar falar de assuntos subversivos ou criminosos nesses meios, assim como divulgar imagens, marcar eventos ou formar grupos de discussão. Mas dizemos até que publicar dados pessoais ou opiniões em redes sociais é o mesmo que enviar uma carta diretamente para a polícia. Perfis virtuais funcionam como um dossiê que montamos e entregamos de bandeja para nossos inimigos. Nossos gostos, preferências, costumes, onde moramos, onde vamos e com quem nos relacionamos: tudo isso está disponível para facilitar o mapeamento de nossos movimentos e deixar isso salvo permanentemente nos bancos de dados das corporações e

- Mude suas senhas periodicamente.
- Experimente um gerenciador de senhas como o Keepass e proteja seu banco de dados com uma senha mestra forte. Alguns gerenciadores também geram senhas randômicas para você.
- Experimente o sistema Diceware, um modelo para gerar senhas que utiliza um dicionário e dados de seis faces para gerar senhas compostas por várias palavras. É fácil de memorizar e difícil de quebrar.

CONECTANDO-SE:

- 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: 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.
- Antes de compartilhar qualquer imagem, remova GPS/EXIF/metadata com MAT – Metadata Anonymisation Tool.
- Esconda seu IP com uma VPN segura e/ou através da rede Tor
- 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 We.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.

EMAIL:

- Use um e-mail seguro, busque servidores autônomos que usem criptografia de disco e por isso não podem ser intimados pelos órgãos de repressão a fornecer seus dados. Use um cliente de email como o Thunderbird para segurança adicional. Exemplos de servidores de email mais seguros: mail.riseup.net e inventati.org

BÁSICO SOBRE SEGURANÇA NA INTERNET

LEMBRETES GERAIS:

- Não há um jeito totalmente seguro de usar a internet, mas existem formas mais seguras. Nenhuma das ferramentas é por si só uma poção mágica.
- Comunicação é mais segura face-a-face.
- Se seu computador não opera com software livre, então é certo que você está sendo monitorada e por lei a empresa responsável pode entregar seus dados ao governo.
- Quanto mais as pessoas usarem medidas de segurança e criptografia, mais seguro será para todo mundo.
- Comportamentos seguros na internet são mais importantes que qualquer software.
- Tente usar um sistema operacional que seja software livre: linuxmint.com, www.debian.org.
- Tails é um sistema operacional que funciona a partir de um pendrive ou DVD, sem deixar traços no disco rígido, e já vem com diversas ferramentas pré-instaladas com foco em segurança. tails.boum.org/contribute/design/instal...

SENHAS:

- Use senhas com no mínimo 20 caracteres.
- Imagine que seu adversário pode executar milhões de tentativas por minuto.
- Utilize senhas randômicas, que não tenham vínculo algum com sua pessoa. Não use datas de aniversário, nomes de pessoas, frases das suas músicas favoritas, etc.
- Sempre use senhas diferentes para cada login.

acessível para os órgãos repressivos do Estado, agências de segurança privada, grupos fascistas e outros. Se você pretende se envolver em ações políticas ou ilegais, considere redes sociais como um ponto fraco e comprometedor para suas ações e para suas relações.

- Use celular o mínimo possível ou nunca. E jamais em uma reunião: não fale nada de relevante em qualquer ligação, seja por telefone fixo ou celular. Celulares são escutas que podem funcionar mesmo desligados, gravando a conversa em um ambiente. Reuniões ou conversas comprometedoras não devem ser feitas perto de celulares. Desligue-o, tire sua bateria e coloque-o em outro cômodo ou imóvel. Os aparelhos registram com quem você fala numa ligação, a hora e o local. Mas muito mais que isso: também a sua posição exata e seu deslocamento – mesmo os celulares sem GPS! – através da triangulação das antenas mesmo quando você não está ligando. Todos esses dados ficam gravados e podem ser requeridos por um juiz e comprovarão que você e seu grupo se juntaram várias vezes antes da ação ou no mesmo dia e local da ação. Considere deixá-lo em casa ligado quando for se reunir para planejar uma ação ou quando for realizá-la. Se seu uso for importante e garantir a comunicação e a segurança, use um celular barato e um chip com CPF de outra pessoa (pode ser de alguém que já morreu) e destrua-os no fim da ação.
- Não fale nada de relevante ou incriminador por e-mail: toda informação que pode te levar para a cadeia deve ser feita pessoalmente. Emails seguros como o do servido riseup.net podem ser muito úteis e "mais seguros" que os e-mails corporativos. Mas a possibilidade de serem violados ainda é grande. E lembre-se: e-mails são como um cartão postal: a mensagem trafega em texto legível para o seu servidor e para o servidor da pessoa para quem ela está destinada. Criptografia pode ajudar, mas é bom que se estabeleça níveis de segurança para que tipo de informação merece ou não o risco de ser interceptada.
- Não confunda "estou sob vigilância" com "sou mais eficiente ou ofereço mais risco" ao sistema: geralmente as autoridades caem em cima de quem está mais vulnerável. Isto é, as pessoas visíveis e sem apoio o suficiente para mobilizarem e pressionarem o Estado para que as solte. Mesmo quando você age dentro da lei, pode haver motivos para repressão caso achem que você seja inconveniente e precisem de uma prisão que sirva de exemplo.
- Equilibre ser invisível para seus inimigos com ser acessível para pessoas amigas em potenciais: as melhores táticas são as que alcançam as

pessoas sem serem detectadas pelos radares. A longo prazo, apenas estar em segredo não pode nos proteger. Se ninguém souber quem somos ou o que estamos fazendo, poderão nos liquidar e ninguém protestará. Pessoas informadas e solidárias podem nos ajudar. Aquelas que fazem coisas realmente sérias devem manter isso para si, é claro. Mas toda comunidade deve ter uma ou duas pessoas dispostas a defendê-las publicamente e educar as outras sobre ação direta e manter conexões e portas abertas para novos membros.

Se você mantiver informação perigosa fora de circulação e seguir medidas de segurança convenientes para cada projeto, você cumprirá o primeiro dever de uma revolucionária: não ser pega!

TIPO DE SEGURANÇA	O QUE É?	QUANDO É ÚTIL?
Segurança Humana	Pequenas mudanças que você pode fazer nos seus hábitos.	Ajuda a evitar que erros humanos sejam o elo fraco em qualquer sistema de segurança.
Segurança de Dispositivo	Passos para fazer seu computador ou telefone menos vulneráveis a um ataque.	Útil sempre que houver alguma possibilidade de seu dispositivo cair fisicamente nas mãos de um adversário.
Segurança de Comunicação	Meios de criptografar as mensagens individuais que você envia e recebe.	Necessário se você precisa garantir o sigilo de uma mensagem em particular durante o armazenamento e envio.
Segurança de Rede	Bloquear sites que rastreiam você e criptografar seu tráfego na internet.	Ajuda a proteger contra rastreamento comportamental, sequestro de conta, censura, mapeamento de redes de contatos, espionagem e publicidade.