MINI GUIA

DE PROTEÇÃO DIGITAL PARA DEFENSORAS E DEFENSORES DE DIREITOS HUMANOS

justiçaglobal

REALIZAÇÃO
Justiça Global

AUTOR
Gabriel Shiozawa Coelho

PROJETO GRÁFICO E DIAGRAMAÇÃO
Rachel Gepp

ANO
2022 - 1ª edição

JUSTIÇA GLOBAL
Equipe: Antonio Neto, Daniela Fichino, Daniele Duarte, Danilo Serejo, Eduardo Baker, Emily Almeida, Francisca Moura, Gizele Martins, Glaucia Marinho, Isabel Lima, Leidiane Moreno, Lourdes Deda, Melisandra Trentin, Monique Cruz, Raoni Dias e Sandra Carvalho.

+55 21 2444 2320
contrato@global.org.br
www.global.org.br

Realização

SUMÁRIO

A proteção é algo sempre relativo. Estar seguro depende de quem é você, o que você faz, tem e com quem lida – e, no caso de defensoras e defensores de direitos humanos, quem você incomoda ou quais interesses contraria. Assim, as medidas de segurança não serão absolutas e é necessário avaliar, em cada caso, as necessidades específicas, por meio de uma avaliação de risco.

Dessa forma, proteção não é apenas uma formação ou trocar um aplicativo. É um processo cotidiano, uma cultura de proteção, considerando sempre quais são os riscos envolvidos em determinada atividade ou luta e quais medidas de proteção deverão ser tomadas, seja pensar no trajeto que se faz até uma reunião ou a escolha do aplicativo de mensagens para se comunicar.

Nunca haverá um estado de "100% proteção". Sempre que se está na luta por direitos, desafiando poderes políticos, econômicos e fáticos, as defensoras e defensores estarão expostas a riscos, por isso é necessário ficar sempre alerta. É importante entender quais são os riscos e se preparar de maneira adequada continuamente.

PROTEÇÃO

PRATICIDADE X SEGURANÇA

Tal adequação é motivada não apenas por causa das ameaças existentes. É preciso considerar o quanto as medidas afetarão o trabalho desenvolvido, equilibrando segurança e privacidade com praticidade e usabilidade. Um aplicativo de mensagens seguro, mas que ninguém tem por ser difícil demais de usar, perde seu objetivo: a comunicação.

Além disso, são observados alguns problemas, como acesso reduzido à internet de qualidade, limitações financeiras para comprar aparelhos, planos de celular que liberam aplicativos como WhatsApp, mas que não incluem outros como o Signal, etc. Então, implantar medidas de segurança coletivamente depende das condições de todas e todos. Por isso, a adaptação é muito importante quando pensamos no contexto das defensoras e defensores de direitos humanos no Brasil.

PROTEÇÃO X PRIVACIDADE

Proteção e privacidade caminham juntas, mas não são sinônimas. Numa simplificação, dados seguros não são roubados por agentes externos, nem dados privados são explorados por quem os hospeda ou transmite.

Isso vale, por exemplo, para mensagens numa grande rede social – seguras (se a empresa protege bem seus servidores) mas não privadas (se a empresa lê as mensagens). O oposto também pode ocorrer: uma alternativa privada, construída pela comunidade, mas com segurança menos robusta.


CONTROLE DAS
INFORMAÇÕES

CONTROLE DAS INFORMAÇÕES E COMPARTIMENTALIZAÇÃO

Muitos dados pessoais hoje estão disponíveis na internet, seja porque foram postados pelas próprias pessoas nas redes sociais, coletados pelas gigantes de tecnologia, cadastrados em sites enganosos ou vazados por crackers (crackers são pessoas que usam seus conhecimentos para violar sistemas ou redes de computadores).

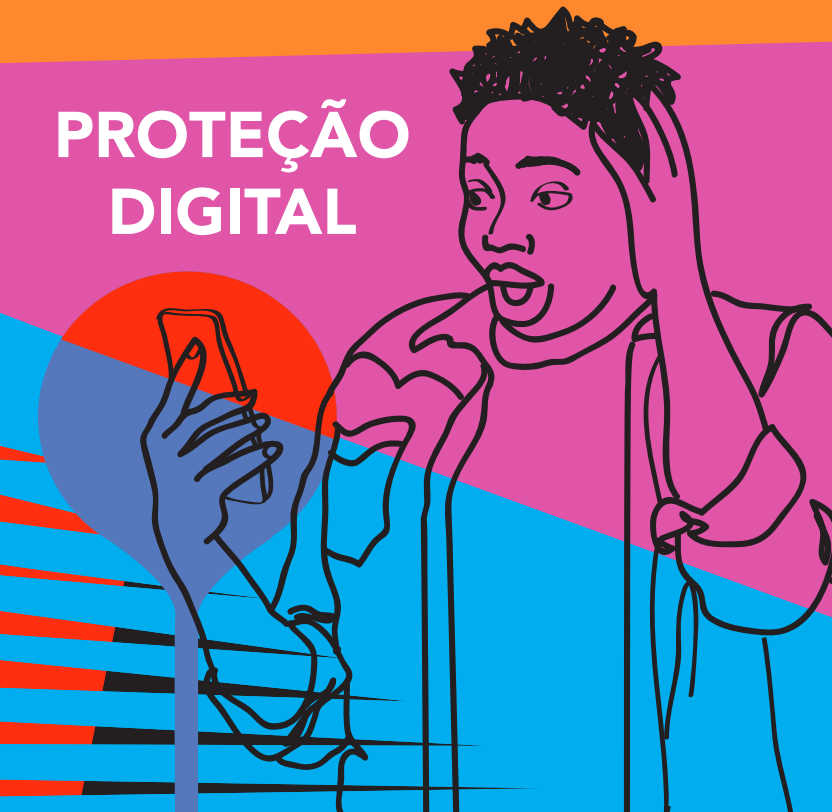
Esses dados podem ser usados de infinitas maneiras para uma porção de fins nefastos: anúncios, repressão, golpes financeiros, roubo de identidade, intimidação, perseguição, vigilância. Assim, tomar controle sobre os próprios dados é fundamental para todo mundo, em especial para quem está na militância.

Para isso, é importante tomar cuidado onde você preenche seus dados, encerrar contas em sites e redes que já não usa, restringir a visibilidade nas redes sociais e refletir

sobre o que vai postar. É recomendável não postar sua própria rotina, endereços e imagens que exponham sua casa.

O controle das informações não é só virtual: serve também para o dia a dia na luta por direitos, evitando a circulação irrestrita de informações sensíveis, reduzindo o risco de vazamentos e mitigando as vulnerabilidades.

PROTEÇÃO DIGITAL



PROTEÇÃO DIGITAL

No meio digital, é importante ter controle sobre o que estão fazendo os aplicativos, sistemas e aparelhos, para que não executem escondidos algo que você não queira.

Para conseguir isso, é bom procurar soluções livres, de código aberto e auditados, ou seja, que tenham compromisso com privacidade e que mostrem como funcionam.

Essa é a orientação deste guia e também de sites voltados para privacidade digital, como o https://prism-break.org/pt/ e o https://www.privacidade.digital/.

Outra máxima que vale em toda proteção digital é sempre manter os sistemas, aplicativos e programas atualizados. Versões ultrapassadas tendem a ser bem mais vulneráveis a ataques.

SISTEMAS OPERACIONAIS

COMPUTADORES
SISTEMAS OPERACIONAIS

Para computador, os sistemas operacionais (SO) que cumprem estes requisitos de segurança e privacidade são, em geral, distribuições GNU/Linux, como Debian e Ubuntu (mais fáceis de usar) ou Qubes (mais seguro). Uma outra alternativa é o Tails, um SO focado em proteção que roda a partir de um dispositivo removível (como um pen drive), utiliza a rede Tor e apaga os registros quando é desligado.

CELULARES
SISTEMAS OPERACIONAIS

Por diversas razões, smartphones são plataformas mais difíceis para que o usuário saiba e controle tudo o que está acontecendo. Alguns sistemas, como LineageOS e GrapheneOS, tentam facilitar esse processo, mas não é toda marca e modelo que suporta a alteração e

trocar o sistema do celular é um processo mais complicado do que do computador. Além disso, alguns desses sistemas podem ter atualizações de segurança menos frequentes que o sistema original, comprometendo a segurança em nome da privacidade.

REQUISITOS MÍNIMOS

Para rodar o Tails, um computador precisa de pelo menos 2 GB de RAM e um processador 64-bit. Para o Debian, o mínimo é mais leve: 512 MB de RAM e 10 GB de espaço no HD. Para celular, os requisitos variam muito de acordo com o fabricante e o sistema, mas o recomendável é ao menos 2 GB e, no caso de um celular Android, um modelo que seja de um sistema que ainda receba atualizações oficiais de segurança – no momento, Android do 8 ao 11.


CRIPTOGRAFIA

CRIPTOGRAFIA DE DISCO

Quando se fala em criptografia no contexto de segurança da informação, geralmente está se referindo a duas formas possíveis: disco e/ou ponta a ponta. A criptografia de disco é basicamente proteger seus dados em um dispositivo: pode ser em computadores, celulares (ainda que neles seja mais frágil), HDs externos, pen drives. É recomendável usar a criptografia de disco em todos os seus dispositivos, pois, ela impede que alguém acesse seus arquivos indevidamente, seja após um furto, uma força de repressão, uma assistência técnica inescrupulosa.

Um programa para criptografia que pode ser usado em vários sistemas é o VeraCrypt, que pode encriptar discos inteiros ou parte deles. O programa é bastante intuitivo e, no dia a dia, a única diferença para quem usa um computador com disco criptografado é precisar digitar uma senha ao ligar o aparelho. Diversos SO Linux/GNU também possibilitam a criptografia de disco no momento em que são instalados.

CRIPTOGRAFIA DE PONTA A PONTA

Criptografia de ponta a ponta é quando os dados são criptografados na hora do envio (uma ponta) e só podem ser abertos pelo destinatário correto (a outra ponta), impedindo que sejam lidos pelo servidor ou caso sejam interceptados no meio do caminho. É um recurso fundamental para a comunicação mais segura, que pode ser usada, por exemplo, em e-mails ou aplicativos de mensagem.

SENHAS

SENHAS

Senhas devem ser únicas. Assim, se algum serviço ou rede tiver os dados vazados, suas outras contas continuam seguras. Senhas fortes podem contar com diferentes conjuntos de caracteres – letras, números, maiúsculas e minúsculas, caracteres especiais (!@#$%) – e devem ser longas. Quanto mais longa, mais difícil será para decifrá-la.

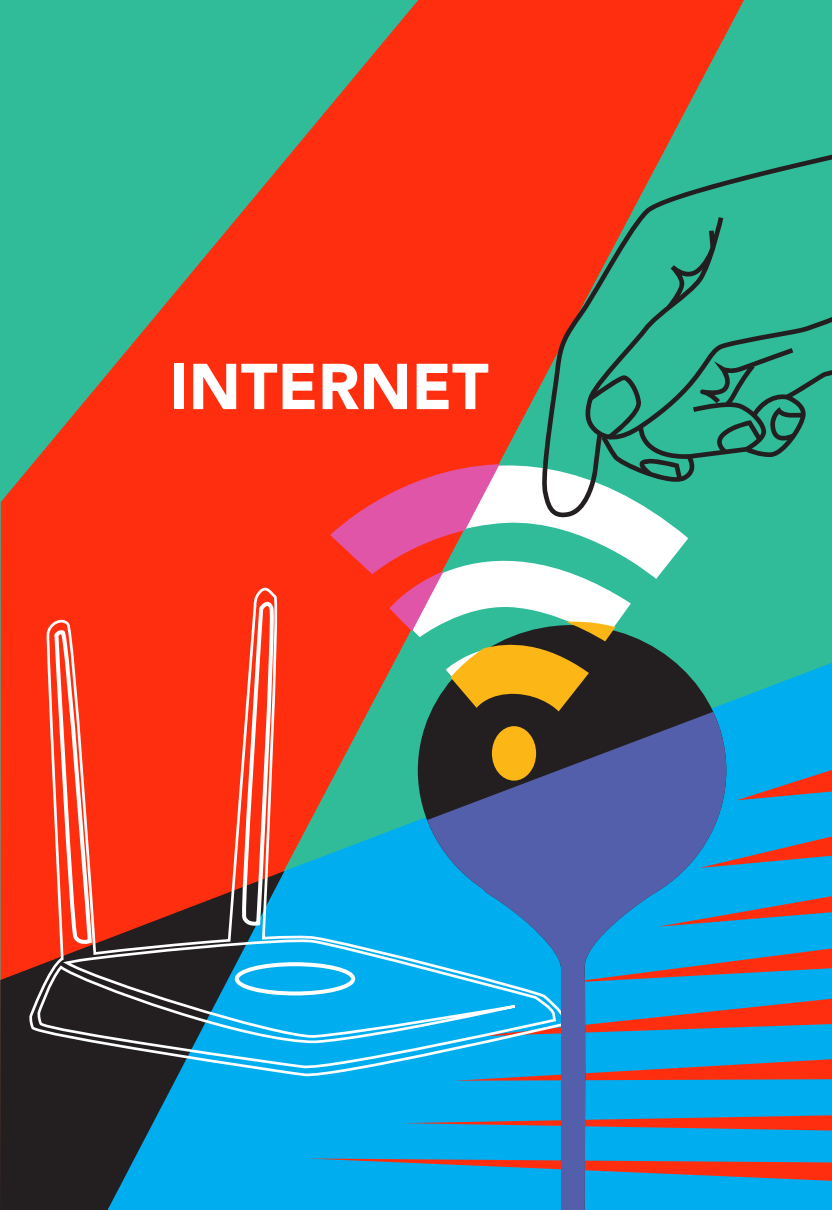
Frases com palavras aleatórias podem ser usadas como senhas difíceis de quebrar, mas fáceis de lembrar. Para ajudar a lembrar várias senhas diferentes e longas, uma dica é usar um gerenciador, como o KeePassXC.

VERIFICAÇÃO EM DUAS ETAPAS

Em diversos serviços, é possível ativar a verificação em duas etapas, que é basicamente a exigência de um código único ou uma

chave específica além da senha para acessar algo. Como SMS são vulneráveis, é mais recomendável usar um aplicativo para gerar esses códigos, como o andOTP e o Aegis.

Lembre-se de fazer o backup de códigos de recuperação de maneira segura, como num gerenciador de senhas.


INTERNET

INTERNET, REDES E TOR

Quando você se conecta à internet, o ideal seria que os dados acessados só fossem vistos por você. No entanto, alguns outros atores podem, de maneira legal ou ilegal, acabar tendo acesso à navegação, como seu provedor de internet (inclusive móvel – 3/4/5G), o administrador da rede Wi-Fi ou alguém que intercepte a comunicação. Para diminuir riscos, o ideal é não confiar em Wi-Fi públicas e usar ferramentas que protejam sua navegação.

Uma das principais medidas é o uso do Tor, uma rede para comunicação segura e privada que busca garantir que a informação que você acessa seja vista apenas por você. Ele evita também que o site que você acessa saiba a sua identidade. O Tor pode ser usado apenas nas conexões do navegador, com o Navegador Tor, ou para todas as conexões do sistema, como no Tails.

Uma alternativa ao Tor são os VPNs que, numa explicação muito simplificada, podem ter o mesmo efeito do Tor. No entanto, o provedor do VPN poderá ver seu tráfego na internet e nem todos os provedores são de confiança – e aí, ao invés do provedor de internet ver tudo, o provedor de VPN vê tudo que você acessa. Além disso, muitos VPNs podem não ter medidas eficazes para proteger sua navegação – é o caso de alguns VPNs usados apenas pra usar serviços de streamings de outro país. O coletivo https://riseup.net/ oferece um serviço gratuito de VPN militante, comprometido com a luta por direitos.

DIMINUA SEUS RISCOS NA INTERNET

É sempre importante repetir algumas recomendações básicas: não clique em links suspeitos, não baixe arquivos desconhecidos, não instale programas que não sejam de confiança. Preste atenção e sempre confira se

o site que você está é o oficial e não um tentando se passar por ele. Navegue desconfiado: não faltam golpistas e agentes de vigilância online.

NAVEGADORES

Os navegadores mais privados e seguros são o Mozilla Firefox e o Tor (que é em si baseado no Firefox) e são as melhores alternativas atuais para navegar na internet.

É uma boa ideia reforçar o navegador com extensões como uBlock Origin, DuckDuckGo Privacy Essentials e HTTPS Everywhere.

REDES SOCIAIS E E-MAILS

REDES SOCIAIS E E-MAILS

Grandes empresas de tecnologia não armazenam uma gigantesca quantidade de dados apenas para fins comerciais, elas têm agendas políticas e podem ter relações com agências de inteligência e vigilância, conforme revelou Snowden.

Assim, é fundamental não usar redes sociais corporativas para se organizar, apenas para divulgação e mobilização. Isso vale também para e-mails, redes, sites para escrever textos, fazer questionários, planilhas, guardar arquivos na nuvem. O PrimsBreak e o Privacidade Digital apresentam algumas alternativas mais privadas e seguras.

O coletivo Riseup tem serviço de e-mail, VPN, lista de e-mails, editor de textos, compartilhamento de arquivos e rede social.

Provedores como ProtonMail, Disroot e Tutatona têm opções gratuitas de e-mail. CryptPad e EtherCalc têm ferramentas de texto e tabelas online (e armazenamento, no caso do CryptPad). Outra ferramenta para compartilhar arquivos é o OnionShare.

Um bom gerenciador de e-mails é o Mozilla Thunderbird, que pode ser configurado para o envio e o recebimento de e-mails com criptografia de ponta a ponta com o protocolo PGP (Privacidade Muito Boa, na sigla em inglês).


REUNIÕES
E LIVES

REUNIÕES E LIVES

O aplicativo mais recomendável para reuniões seguras e privadas é o https://meet.jit.si/.

O serviço, pode ser usado direto no site ou hospedado em um servidor próprio. No entanto, se for pelo site, não aguenta reuniões com um número muito grande de participantes.

Para lives, é importante separar a sala em que estão sendo feitas as apresentações e debates da transmissão, diminuindo as chances de um ataque.

É importante também proteger o link/endereço (e possivelmente senha para entrada) do evento e, em caso de grandes reuniões, destacar pessoas para filtrar quem entra e para retirar sabotadores.

TELEFONES

GRAMPOS
EM LIGAÇÕES E AMBIENTE

No Brasil, grampos – legais e ilegais – são bastante comuns em telefones. Assim, deve-se evitar tratar de assuntos sensíveis por telefone. De maneira geral, é válido trocar ligações normais por ligações via internet, desde que por aplicativos seguros (como o Signal).

Há ainda o risco de grampo ambiental – um microfone no local. São mais raros, mas não fora da realidade. Se o nível de ameaça é tal que essa é uma possibilidade alta, convém vasculhar os ambientes regularmente.

Um celular comprometido também pode servir como grampo ambiental, embora seja algo mais difícil e direcionado; algumas pessoas preferem fazer reuniões com os celulares fora do ambiente, como precaução.

CELULAR
VULNERABILIDADES

Boa parte da vida hoje passa por celulares – conversas, trabalho, atuação política, relacionamentos. Essa concentração é perigosa, pois se o aparelho é comprometido ou extraviado, informações de todas áreas podem ser roubadas e usadas para atacar a defensora ou defensor de direitos humanos.

Por isso, é bom manter o celular criptografado, com uma boa senha e evitando concentrar dados nele. Isso pode ser feito de duas maneiras: não usando o celular para tratar de assuntos sensíveis e rotineiramente limpando os arquivos, mensagens e fotos do aparelho.

Além de concentrar dados, celulares também podem ser usados diretamente na vigilância de alguém – acompanhando a localização, ouvindo indevidamente o microfone, espiando pela câmera – principalmente se tiver sido comprometido.

Utilize bloqueio de tela e uma senha forte, mantenha sempre o sistema atualizado, desative Wi-Fi e Bluetooth quando não estiverem em uso, não baixe arquivos e aplicativos desconhecidos e não conceda permissões desnecessárias para programas – um app para jogar paciência não deve ter acesso ao microfone, por exemplo.

Mesmo com um celular não comprometido e com boas práticas de segurança, os dados dele podem ser usados para apontar sua localização – às vezes convém deixá-lo em casa.

CELULAR
APLICATIVOS DE MENSAGENS

O aplicativo mais adequado hoje para a maior parte das necessidades de segurança e privacidade é o Signal. Convém utilizar mensagens temporárias, deletando automaticamente mensagens antigas.

Em qualquer aplicativo de mensagens, é recomendável usar verificação em duas etapas para reduzir chances de clonagens. Element (antigo Riot) é outra alternativa para troca de mensagens, com a diferença de ser federado e não centralizado (como o caso do Signal).

METADADOS E ARMAZENAMENTO

METADADOS E ARMAZENAMENTO

Os arquivos têm informações que os identificam. São os metadados, dados sobre os dados, como quando ele foi criado, como, em que dispositivo. Programas como o ExifCleaner e o MAT2 buscam deletar estes metadados e preservar sua privacidade ao compartilhar arquivos.

Arquivos deletados no computador não somem completamente e podem ser recuperados. Por isso, é bom apagar arquivos sensíveis de maneiras mais seguras, usando aparelhos como o BleachBit, que fragmenta o arquivo ao deletá-lo.

Isso serve também para registros físicos: deve se ter cuidado ao descartar documentos, agendas, cadernos, atas. Fragmentadoras podem também ser usadas com o papel.

Justiça Global. Mini Guia de Proteção Digital
para defensoras e defensores de direitos humanos.
Rio de Janeiro: Justiça Global, 2022.

Facebook: /justicaglobal
Twitter: @justicaglobal
Instagram: @justicaglobal

www.global.org.br