Segurança Básica

Anonimato

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 e o Google, 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, dependendo das intenções de quem a utiliza, já que esta tecnologia é aberta para qualquer pessoa que queira utilizá-la.

Tor

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.

Tor e a Política

Jacob Appelbaum, funcionario do Tor e voluntario do Wikileaks, rodava o mundo ensinando a ativistas, politicos e espioes 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.

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.

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.

- Tor - https://www.torproject.org/ e https://securityinabox.org/pt/tor_main
- I2P - https://geti2p.net/
- VPN - https://help.riseup.net/en/vpn e https://bitmask.net/
- Android: https://securityinabox.org/pt/Orbot_main
- Tails - https://tails.boum.org/

Ferramentas

Comunicação

- E-mail Seguro – https://mail.riseup.net/ e https://protonmail.com/
- Lista de E-mail Segura - https://lists.riseup.net/
- Videoconferência sem registros - https://meet.jit.si/
- Mensageiro com criptografia – Pidgin - https://securityinabox.org/pt/pidgin_main
- Chat Seguro via Pidgin - https://help.riseup.net/en/chat
- SMS Seguro com Signal- https://whispersystems.org/
- Cliente de Email com Criptografia: https://emailselfdefense.fsf.org/pt-br/ ou https://securityinabox.org/pt/thunderbird_main

Compartilhamento de Informações

- Editor de Texto Colaborativo Online - https://antonieta.vedetas.org/
- Planilha Colaborativa Online - https://eveliyn.vedetas.org/
- Compartilhamento temporário de arquivos - https://share.riseup.net/
- Compartilhamento de texto temporário - http://oneshar.es/

Destruição de Arquivos
- Wipe (Linux)
- CCleaner - https://securityinabox.org/pt/ccleaner_main
- Eraser - http://eraser.heidi.ie/

Identificação
- Apagar Metadados: http://www.sentex.net/~mwandel/jhead/ e http://www.sno.phy.queensu.ca/~phil/exiftool/

Manipulação de Imagem
- PrintScreen Avançado - http://ngwin.com/picpick
- Desfocar – Gimp e Blur Image Background
- Anonimizar Fotos – ObscuraCam: http://bit.ly/1soksgH

Armazenamento:
- Criação, Armazenamento, Compartilhamento de Arquivos e Chat – https://open365.io
- Mega - https://mega.nz/

Proteção:
- Antivírus, localizador e bloqueio de app: http://m.onelink.me/164dce10
- Ocultador de Fotos e Arquivos com Criptografia: http://bit.ly/1TLX0py

Privacidade na Internet
- Forçar HTTPS- https://www.eff.org/https-everywhere
- Bloqueia captura de dados do cliente - https://prism-break.org/en/projects/privacy-badger
- Bloqueia Spams - https://github.com/gorhill/uBlock
- Busca Anonima: https://duckduckgo.com/, https://disconnect.me/search e https://startpage.com/
- Mapas: http://www.openstreetmap.org/
- Meu computador esta sendo espionado? https://resistsurveillance.org/

Criptografia

- GPG4USB - https://securityinabox.org/pt/gpg4usb_portable
- Android: https://prism-break.org/en/projects/openkeychain
- GPG - https://manual.fluxo.info/criptografia/instalando.html#instalando-o-gpg

Senhas

Você pode criar senhas pronunciáveis utilizando palavras que não estejam no dicionário, preferivelmente uma palavra que você mesmo inventou. Misture sempre letras, números e símbolos,

se possível. Quanto maior sua senha, melhor, mas tome cuidado para não esquecê-la!
Você também pode usar palavras conhecidas, mas tome cuidado pois isso em si não é tão seguro quanto palavras imaginárias, então é um método que precisa ser usado com critério.

- http://testedesenha.com.br/
- https://howsecureismypassword.net/

Armazenar Senhas:

- KeePass https://securityinabox.org/pt/keepass_main
- Android: https://securityinabox.org/pt/keepassdroid_basic_use

Link Uteis e Referências:

- https://manual.fluxo.info/
- https://securityinabox.org/pt/
- https://prism-break.org/
- https://ssd.eff.org/pt-br/playlist/ativista-ou-manifestante
- https://ssd.eff.org/pt-br
- https://ativismocibernetico.wordpress.com/
- https://templates.fluxo.info/
- http://www.torproject.org/
- http://www.gta.ufrj.br/grad/11_1/tor/index.php?file=kop1.php
- https://temboinalinha.org/
- https://antivigilancia.org/pt/oficinas-e-ferramentas-beta/
- https://myshadow.org/