PEQUENO MANUAL DE SEGURANÇA DIGITAL

Pequeno manual de segurança digital

PV

Contents

1 Computador pessoal

1.1 Sistema operacional

Um sistema operacional (SO) é um software que inicializa um computador e o mantém funcionando e respondendo aos seus comandos. Os sistemas operacionais desempenham várias tarefas importantes, como executar aplicativos, manter interface de usuário, controlar armazenamento de arquivos, etc. Os sistemas operacionais mais seguros são os de código aberto da família Linux 🐧 (Ubuntu, Linux Mint, Arch Linux, Fedora, Debian, etc). Eles requerem um pouco de prática e habituacão, porém são inquestionavelmente melhores. Isso não quer dizer que são imunes a ataques (especialmente a ataques direcionados, ou seja, aqueles em que você pessoalmente é a vítima pretendida). Mas como a esmagadora maioria de ataques não-direcionados (aqueles em que as vítimas são de oportunidade) tem como alvo usuários de Windows, usuários de Linux se encontram, por definição, fora da mira. Se você tem um sistema operacional Linux 🐧 munido de um anti-vírus e um *root kit hunter* você está bastante seguro.

Sistemas operacionais da Apple tem um bom custo-benefício em termos de usabilidade e segurança, porém são menos seguros que Linux 🐧. Por último, sistemas operacionais Windows são os mais fáceis para o usuário, porém são os menos seguros. Torna-se então necessário tomar várias precaucões e medidas adicionais.

1.2 Sistemas seguros

1.2.1 Ubuntu 🐧

Para instalar Ubuntu, visite https://www.ubuntu.com/download/desktop e faça download do arquivo ISO (a versão mais atual é a 18.04.1 LTS). Lembre-se de optar por criptografar o disco rígido na instalação do Ubuntu! Essa opção é oferecida durante a instalação.

Siga o tutorial de instalação em inglês (https://tutorials.ubuntu.com/tutorial/tutorial-install-ubuntu-desktop) ou em português (http://ubuntu-manual.org/?lang=pt_BR). Se precisar, o YouTube tem tutoriais de instalação em português.
Mais instrucões em inglês sobre como migrar de MacOS (https://tutorials.ubuntu.com/tutorial/tutorial-create-a-usb-stick-on-macos#0) e Windows (https://tutorials.ubuntu.com/tutorial/tutorial-create-a-usb-stick-on-windows#0) para Ubuntu.

Antivírus: Comodo - gratuito https://www.comodo.com/home/internet-security/antivirus-for-linux.php

Root kit hunter: Para instalar, digite no Terminal:

```
sudo apt install chkrootkit
```

Atualize seu Ubuntu com frequência. Digite no Terminal:

```
sudo apt-get update
sudo apt-get upgrade
```

1.2.2 TAILS 🐧 - máxima segurança e anonimidade

Com o sistema operacional TAILS, você pode criar um espaço digital anônimo, amnésico e seguro. E você nem precisa ter um computador próprio para usá-lo. O TAILS é um sistema operacional portátil baseado em Linux, projetado especificamente para privacidade pessoal. Você o instala em um DVD ou em um pendrive e pode inicializá-lo a partir de qualquer computador que desejar – seja Windows, Apple ou outro Linux.

- O TAILS é um sistema *amnésico*, o que significa que nenhum dado é armazenado entre as sessões: toda vez que você o usa, você tem um ambiente digital totalmente novo, sem informações de identificação

pessoal, independentemente de qual computador você está usando.

- Todas as conexões de internet usadas pelo TAILS são roteadas pela Tor Network, portanto, seu endereço de IP, localização e atividade não podem ser monitorados por terceiros (seu provedor de internet pode ver que você está usando o Tor, mas não consegue ver como você está usando.
- O endereço MAC do seu computador é falsificado, o que significa que sua conexão com a internet não possui um identificador de hardware reconhecível e exclusivo.
- Extensões de privacidade, como o HTTPS Everywhere, já vem pré-instaladas no Firefox para o TAILS.
- O TAILS vem com software de privacidade pré-instalado, como um cliente de e-mail PGP para enviar e-mails criptografados.
- O modo "Camuflagem" faz com que sua área de trabalho se pareça com uma área de trabalho do Windows, caso você não queira despertar suspeitas.

Para instalar o TAILS, visite https://tails.boum.org/install/ e faça download do arquivo ISO. A instalação é um processo longo, e instruções confiáveis existem no site oficial do TAILS em inglês, espanhol ou português (as instruções em português estão, atualmente, incompletas).

1.2.3 Segurança para Windows

Apesar de não ser recomendável usar Windows, nem sempre se tem a opção de abdicar desse SO.

- Criptografar disco rígido: instalar VeraCrypt (https://www.veracrypt.fr/en/Home.html), instruções de uso: https://pplware.sapo.pt/software/veracrypt-aprenda-a-criar-uma-zona-segura-no-seu-pc/
- Tornar extensões de arquivos visíveis para evitar ser infectado por programas maliciosos (https://br.ccm.net/faq/35304-como-exibir-a-extensao-oculta-de-arquivos-no-windows-10)
- Ativar Firewall
- Desinstalar bloatware (programas pré-instalados do Windows, raramente úteis)
- Ativar SmartScreen (programa nativo que previne contra infecções de programas maliciosos e tentativas de phishing online)
- Escanear sistema frequentemente com Windows Defender para detectar e remover programas maliciosos
- Desabilitar AutoPlay para evitar instalação automática de programas

2 Armazenamento de arquivos seguro

2.1 VeraCrypt

VeraCrypt é um aplicativo gratuito que permite salvar e armazenar seus arquivos através de criptografia, e o acesso a esses arquivos é restringido por meio de uma senha.

O VeraCrypt cria uma área segura, chamada de volume, em seu computador ou HD externo. Este volume inteiro fica em um arquivo chamado *recipiente*, que você pode abrir (montar) e fechar (desmontar) usando o VeraCrypt. Você pode guardar seus arquivos com segurança dentro deste *recipiente*. VeraCrypt também pode criar e gerenciar volumes criptografados que equivalem a todo o espaço de um disco específico.

VeraCrypt aceita tanto volumes criptografados padrão quanto volumes ocultos. Ambos

manterão seus arquivos confidenciais, mas volumes ocultos permitem a você esconder suas informações importantes por trás de dados menos sensíveis para protegê-los mesmo quando você é forçado a revelar sua senha do VeraCrypt.

VeraCrypt
para instalar, visite https://www.veracrypt.fr

2.2 Armazenamento na nuvem

Sempre que quiser armazenar arquivos na nuvem (Google Drive, Dropbox, etc), é importante criptografá-los com VeraCrypt antes de fazer upload. Alguns serviços de armazenamento na nuvem oferecem criptografia local (no seu computador) antes de fazer upload, como SpiderOak (https://spideroak.com/), de forma que o conteúdo dos arquivos é inacessível ao provedor do serviço.

2.3 Apagar arquivos

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:

http://www.dban.org/
http://www.fileshredder.org/
https://www.piriform.com/ccleaner

3 Acesso à internet

3.1 Tor

Tor direciona seu tráfego de internet por meio de uma rede internacional de computadores de voluntários que atuam como redes de retransmissão chamadas *nós* (*nodes*). Suas informações são criptografadas e enviadas entre esses nós, antes de chegar a um "nó de saída" que se comunica entre a rede Tor e o resto da internet. Dessa forma, a sua identidade é ocultada dos sites que você visita e seu histórico de navegação é inacessível ao seu provedor de internet. As maiores desvantagens são redução na velocidade da conexão e vulnerabilidade caso configurado incorretamente.

Tor
https://www.torproject.org/download/download

3.2 Mozilla Firefox

É um navegador gratuito e de código aberto que tem privacidade e segurança como foco - porém não é tão seguro e privado quanto Tor.

Para usar Mozilla Firefox seguramente, algumas extensões são essenciais: HTTPS Everywhere, Disconnect.me e uBlock Origin. Você pode instalar essas extensões na página de Complementos do Mozilla Firefox, que você acessa no canto superior direito clicando no ícone ☰.

Mozilla Firefox
https://www.mozilla.org

Após instalar, modifique as configurações de privacidade do navegador para bloquear *cookies*. Clique no menu ☰ no canto superior direito > *Preferências* > *Privacidade e Segurança* > *Cookies e Dados de Sites*. Marque a opção *Bloquear cookies e dados de sites*.

3.3 VPN

VPN cria um "túnel" criptografado entre o seu PC e a rede de computadores do provedor de VPN. Sua rede, em seguida, se comunica com o resto da internet, mascarando sua identidade e atividades.

VPNs de confianca

Bitmask (grátis)
https://bitmask.net/en/install

TunnelBear (grátis e pago)
https://www.tunnelbear.com/

Get a VPN (pago, porém barato)
https://www.getavpn.org/

Nota importante

O uso de Tor + VPN é controverso e um pouco complicado (https://www.techradar.com/news/tor-and-vpn-how-well-do-they-mix).

Use Mozilla Firefox com VPN.

Evite navegadores como Google Chrome, Internet Explorer, ou Safari.

4 Contas de e-mail

Crie uma nova conta de e-mail usando um dos servicos abaixo. Não use nomes de usuário fáceis de identificar (seu nome, apelido, etc).

https://riseup.net

https://aktivix.org/

https://protonmail.com

Os provedores acima oferecem servicos de e-mail com criptografia ponta-a-ponta que preservam sua anonimidade e privacidade.

4.1 Criptografia de ponta-a-ponta

Criptografia de ponta-a-ponta garante que ninguém, nem mesmo quem monitora a rede de comunicação, pode ver o conteúdo de sua mensagem - nem hackers, nem o governo, nem mesmo o provedor de e-mails.

4.2 E-mails no desktop

4.2.1 Usando Thunderbird + GnuPG + Enigmail

O Thunderbird é um cliente de e-mail, ou seja, um software que permite ao usuário acessar várias contas de e-mail a partir de um só programa. Para garantir que suas mensagens serão lidas apenas pelo destinatário pretendido, criptografe suas mensagens usando GNU Privacy Guard (GnuPG ou GPG). GnuPG é um software de criptografia livre e de código aberto desenvolvido pelo Projeto GNU. O Enigmail é uma extensão do Thunderbird que permite que você acesse os recursos de criptografia do GnuPG a partir do Thunderbird. O GnuPG gera uma chave privada e uma chave pública, permitindo assim a troca segura de mensagens.

4.2.2 Thunderbird

Para instalar, visite https://www.thunderbird.net/

Configurações de segurança e Privacidade no Thunderbird

- Desabilitar exibição de mensagens com HTML: Clique no ícone no canto direito superior do Thunderbird para abrir o menu. Clique em *Exibir* > *Formatação da mensagem como* > *Sem formatação*.
- Desabilitar escrita de mensagens com HTML: Clique no ícone no canto direito superior do Thunderbird. Clique em *Preferências* > *Configurações de conta* > *Editar e Endereçar*. Desmarque a opção *Usar formatacão HTML*.
- Configure segurança: Clique no ícone no canto direito superior do Thunderbird. Clique em *Preferências* > *Preferências* e depois na aba *segurança*. Clique na aba *Senhas* e ative o campo *Usar uma senha mestra*. Escolha uma senha forte com

ajuda do KeePassXC (https://www.keepassxc.org/)

- Configure privacidade: Clique no ícone ☰ no canto direito superior do Thunderbird. Clique em *Preferências* > *Preferências* e depois na aba *Privacidade*. Desmarque os seguintes campos: *Permitir conteúdo remoto nas mensagens* (você ainda pode habilitar conteúdos remotos em mensagens individuais), *Lembrar sites e links que eu visitei* e *Aceitar cookies dos sites*

4.2.3 GnuPG

🐧 Para instalar, digite no Terminal
`sudo apt install gpa`
 Para instalar, acesse https://gpgtools.org/gpgsuite.html
 Para instalar, acesse https://www.gpg4win.org/

4.2.4 Enigmail 🐧

Abra o Thunderbird e, em seguida, o Menu ☰ localizado no canto superior à direita). Clique em *Complementos* e, na barra de busca, procure *Enigmail*. Clique no ícone + *Instalar*. Para acessar e configurar o Enigmail, clique em ☰ > *Enigmail*.

5 Celular

Comece desativando serviços de localização no seu celular.

5.1 Desbloqueio

Primeiramente, você deve desativar o desbloqueio com impressão digital ou qualquer tipo de identificação biométrica. Ao invés disso, use a senha de acesso para desbloquear o celular. Outra boa medida é ativar o recurso de apagar os dados do celular caso a senha seja digitada incorretamente x número de vezes. Assim você se protege e protege suas companheiras e companheiros caso seu telefone seja apreendido.

5.2 Criptografia

Criptografe seu celular. Os telefones da Apple já são encriptografados de fábrica, portanto basta configurar a senha de desbloqueio do aparelho para proteger suas informacões. Se você tem um Android, você deve tomar algumas medidas adicionais para criptografar seu aparelho. Vá em *Configuracões* > *segurança* > *Codificar aparelho* (o caminho pode variar um pouco dependendo do seu aparelho).

5.3 Aplicativos de mensagem

Os aplicativos de mensagem abaixo estão disponíveis para iOS e Android, possuem criptografia ponta-a-ponta e outras funcões de segurança que os tornam confiáveis:

Signal
Telegram

Sobre o WhatsApp : o fato de ser propriedade do Facebook torna o WhatsApp menos seguro, pois a corporação pode cooperar com governos.

É possível usar o Signal, Telegram e WhatsApp sem um número de telefone associado. O aplicativo TextNow, disponível para iOS e Android, fornece um número de telefone exclusivo que você pode inserir em um aplicativo de mensagens e usar para verificar sua conta. Para mais detalhes, veja o guia https://www.techbout.com/whatsapp-without-phone-number-sim-5365/

5.4 VPN

Assim como é importante manter segurança e anonimidade usando a internet no computador, o mesmo se estende para

uso de internet no celular. Abaixo, alguns servicos de VPN gratuitos para iOS e Android:

TunnelBear
FreeVPN
Bitmask

5.5 Navegadores

Alguns navegadaores seguros para celular são:

Onion
Equivalente do Tor para celular

Firefox Focus
Uma versão do Firefox que bloqueia anúncios e protege contra rastreamento. É equivalente a usar o Firefox em modo Privado, mas com o Firefox Focus essas proteções são o padrão.

6 Senhas

Senhas são extremamente importantes para segurança e proteção. Porém, usar a mesma senha para mais de um serviço/site é muito arriscado. Por outro lado, lembrar dezenas de senhas é praticamente impossível. Daí a importância de um administrador de senhas para gerar senhas seguras e gerir o armazenamento das mesmas. Assim, a única senha que você deve se lembrar é a senha-mestra do administrador de senhas.

O KeePassXC é uma ferramenta fácil de usar que te ajuda a armazenar e gerenciar múltiplas senhas dentro de um arquivo de banco de dados criptografado. Esse arquivo é criptografado com uma senha-mestra que você mesmo cria. O KeePassXC também pode ser usado para gerar senhas fortes para suas contas.

Como esse banco de dados é criptografado, você pode armazenar cópias em vários lugares, o que torna o seu backup relativamente simples. Não é recomendável enviar o seu banco de dados por e-mail ou armazená-lo online onde outras pessoas podem ter acesso. Muitos usuários do KeePassXC mantém uma cópia em um dispositivo USB e uma cópia em um disco de backup.

KeePassXC
https://keepassxc.org/

Para a senha mestra, não use nenhuma referência pessoal (aniversários, nomes, datas especiais, bandas, etc). Caso prefira, decore uma senha complexa (com caracteres alfanuméricos e pontuação).

7 Redes sociais

Redes sociais são ubíquas hoje em dia, de forma que prescrever o abandono total do seu uso é contra-producente. No entanto, redes sociais são uma das maiores ameaças à segurança e integridade de militantes e ativistas. Evite ao máximo que puder usar redes sociais como Facebook, Twitter, Instagram, Google Plus, etc. Evite especialmente postar informações pessoais como endereço, telefone, aniversário, emprego, detalhes de familiares e amigos. Altere as configurações das suas contas para maior privacidade possível. Há vários tutoriais na internet sobre como configurar privacidade nas diferentes redes sociais.

Evite se comunicar por Facebook Messenger, GChat, ou qualquer serviço de mensagem de grandes corporacões. Use os aplicativos mencionados na seção **Aplicativos de Mensagem**.

Evite organizar atividades, protestos, eventos, etc, por meio de Facebook. Evite também usar grupos de Facebook para discussão, pois eles são alvo fácil de infiltradores.

8 Boas práticas

- Não use sua conta Google, Facebook, ou Twitter pra registrar em outros servicos.

Registre-se do zero, com sua conta de e-mail e uma senha específica gerada pelo KeePassXC.

- Troque suas senhas periodicamente com ajuda do KeePassXC.
- Não use a ferramenta de busca do Google. O Google rastreia seus passos e coleta informações do seu uso de internet. Use DuckDuckGo: https://duckduckgo.com/.
- Sempre faça logout de todos os sites que você fizer login, incluindo e-mail e redes sociais, mesmo no seu próprio computador.
- Somente acesse Wi-Fi público com seu VPN ativado, seja no computador, seja no celular.
- Nunca digite nomes de usuário e senhas em sites cujo acesso se deu por meio de um link em um e-mail ou mensagem de celular. Sempre que fizer login em qualquer site, digite você mesmo o endereço do site na barra de endereços do navegador.
- Instale atualizações de softwares e sistemas operacionais com frequência (semanalmente, de preferência).
- Nunca forneça informações pessoais por meio de e-mail ou mensagens de celular, independente de quão "sério" o e-mail ou mensagem pareça.
- Sempre que possível, evite fornecer informações pessoais. Forneça apenas quando absolutamente necessário. Seja criativo, invente pseudônimos, contas falsas, etc.
- Evite ao máximo usar seu nome, imagem e identidade pessoal, especialmente em contas ligadas com sua militância.
- Sempre que possível, use autenticaçao em dois passos (2 Factor Authentication). O aplicativo Authy, disponível em iOS e Android, gera tokens seguros de autenticação em dois passos.
- Faça back-ups semanais do computador e celular.
- Criptografe *tudo* que for possível.
- Sempre apague histórico e cookies dos navegadores, especialmente se usar computadores públicos ou de outras pessoas.
- Sempre que puder, use computadores de terceiros com o sistema operacional portátil TAILS.
- Evite comunicar informações potencialmente sensíveis por meio de Gmail, Hotmail, Yahoo, Facebook, Instagram, etc.
- Não permita marcação de rosto em fotos nas redes sociais.
- Remova metadados de arquivos como imagens, PDFs e documentos Word antes de compartilhá-los por e-mail ou postar em redes sociais. Para remover metadados de várias imagens simultaneamente, use http://www.exifpurge.com/ gratuitamente. Para remover metadados de PDFs, use https://pdfcandy.com/edit-pdf-meta.html
- Reduza o número de aplicativos no seu celular. Mantenha apenas o essencial.

9 Lembre-se

Finalmente, um aviso importante: segurança, privacidade e anonimato são *processos contínuos e coletivos*. É preciso sempre manter-se atualizado, pois o que é seguro hoje pode não ser amanhã. É também preciso educar nossas companheiras e companheiros sobre o assunto

para que o maior número de pessoas em um grupo pratiquem boas medidas de segurança. Quando um membro está exposto, os demais também correm risco.

10 Recursos adicionais

Esse manual tem como objetivo apresentar o básico de segurança digital. Há vários recursos adicionais na internet e é importante que você sempre busque mais informações. Abaixo segue uma pequena lista:

- Surveillance Self-Defense
  https://ssd.eff.org
- Digital Defenders
  https://www.digitaldefenders.org/
- Info-Activism How-To Guide
  https://howto.informationactivism.org/
- Front Line Defenders
  https://www.frontlinedefenders.org
- Security in a Box
  https://securityinabox.org/pt
- Hack Blossom
  https://hackblossom.org
- Anarchist Black Cross Dresden
  https://abcdd.org/en/security-guide-2/
- Bristol Anarchist Federation
  https://bristolaf.wordpress.com/2017/05/31/essential-online-security-an-anarchists-guide-for-everyone/
- Neighborhood Anarchist Collective
  https://neighborhoodanarchists.org/security-tools/
- Rise Up
  https://riseup.net/