TREINAMENTO DE SEGURAÇA DIGITAL

DEFENDDEFENDERS

East and Horn of Africa Human Rights Defenders Project

SOBRE ESTE GUIA

DefendDefenders apresenta: Um guia simples para melhorar a sua segurança digital com ferramentas grátis e acções simples.

DefendDefenders é um projecto de defensores de direitos humanos do Este e Corno de África.

Procuramos fortalecer os esforços dos defensores de direitos humanos por toda região reduzindo a sua vulnerabilidade em relação ao risco de perseguição e **melhorando a sua capacidade de efectivamente defender os direitos humanos**.

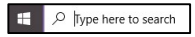
DefendDefenders trabalham em Burundi, Djibouti, Eritrea, Etiópia, Kenya, Ruanda, Somália (conjuntamente com a Somalilândia), Sudão do Sul, Sudão, Tanzânia, e Uganda.

Para **Ajuda urgente** Por favor veja: https://www.defenddefenders.org/get-help/ ou ligue para nossa linha de emergência 24/7 pelo +256-783-027611, mande mensagem para linha de ajuda em TICs/Signal/WhatsApp on +256-787-556560

SEGURANÇA DE DISPOSITIVOS

Vamos guia-lo por algumas áreas onde deverá verificar seus dispositivos e contas de acesso para a sua segurança e dos seus dados.

Windows

A maioria destes parâmetros podem ser facilmente encontrados no menu start. Para aceder, pressione a tecla Windows > Na caixa de pesquisa 

> Escreva Control Panel > Clique em Systems and Security > Verifique o estado da segurança da firewall do Window Defender, encriptação do disco Bitlocker para assegurar que estão ligados.

Mac

Vá ao menu Apple () > System Preferences, clique em Security & Privacy, depois clique em General. Para mais detalhes, navegue para: https://apple.co/365i2KA

Android

Vá para 'Settings'. Habilite parâmetros como password/ biometric. Desabilte rastreio de localização. Para mais detalhes, navegue para: https://nr.tn/3fIBQ9J

iPhone

Vá para Settings > Touch ID & Passcode e escreva sua passcode. De seguida, desça e garanta que acessórios de USB não são permitidos na tela de bloqueio. Para mais detalhes, navegue para: https://zd.net/3nXf94p, e https://apple.co/2J1bc03

BACKUP

O backup é a cópia dos seus ficheiros, mantidos num local diferente dos originais. Isto significa que se você perder seus ficheiros, porque seu dispositivo avariou or foi roubado por exemplo, você terá perdido somente seu dispositivo e não sua informação.

Para Windows & Mac:

Google Drive Sync é uma óptima opção com pelo menos 15GB de armazenamento sem custo.

Microsoft OneDrive também oferece 5GB de armazenamento sem custo, e uma ferramenta de sincronização fácil de usar – útil, se usar maioritariamente ferramentas Microsoft **Office**, porque integra-se com muita facilidade.

Dropbox, **Degoo**, e **Sync.com** ambos oferecem aramazenamento limitado sem custo e fácil de configurar. Recomendamos que escolha a ferramenta que satisfaça suas necessidades (se está indeciso, comece com Google Drive!) e certifique-se que que os dados são **sincronizados automaticamente quando estiver online**.

Para dispositivos móveis:

iPhone / iPad: Settings > Apple ID (Opção no topo) > Escolha seu dispositivo > iCloud Backup

Android: varia consoante a marca e modelo, mas normalmente integra-se com sua conta Google usada para configurar o celular. abra settings > clique em System > Backup > active o serviço de backup. Para mais detalhes, navegue para: https://bit.ly/3nXhHQ1

SEGURANÇA ONLINE

Phishing

É a tentiva fraudulenta de obter informação previlegiada.

Preocupe-se com emails com:

- Anexos suspeitos
- Erros gramaticais
- Cumprimentos em linguagem estranha
- Solicitação de resposta imediata

Para mais detalhes, navegue para: https://bit.ly/3666qqI e https://bit.ly/3q5EIT1

Vishing

Engenharia social por telefone (Voice-Phishing = Vishing) Para mais detalhes, navegue para: https://nr.tn/3q3hnkN

Para ver o que outros podem saber sobre sí, use sites como ThreatCrowd.org, HaveIBeenPwnded.com, e OSINTFramework.com para pesquisa de nomes de utilizadores, endereços de email, números de email, e seu nome. Você se surpreenderá com os resultados!

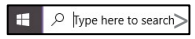
Se encontrar alguma coisa que não quer que seja pública:

- Troque as difinições da rede social para o serviço onde encontrou a exposição de seus dados.
- Preste atenção ao que publica no futuro, porque as informações são dificeis de iliminar quando estão na internet.

ENCRIPTAÇÃO

Garanta sempre que o seu dispositivo está encriptado:

Windows:

Pressione a tecla Windows > na caixa de pesquisa 

escreva Bitlocker > Clique Manage Bitlocker > Turn on Bitlocker. Guarde a chave de recuperação no seu gestor de passwords (abordado na página a seguir) caso precise a posterior!
Se usar uma versão do Windows que não tenha a função Bitlocker, pode usar VeraCrypt, uma ferramenta de encriptação sem custos e com excenteles recursos de ajuda. Visite: https://bit.ly/3q2Ndho.

Mac:

Vá ao menu Apple ( ) > System Preferences, depois clique em Security & Privacy > Clique no tab FileVault > Turn on FileVault. Para mais detalhes navegue para: https://apple.co/39ir7ld

Android:

Vá para Settings > Security > Encryption > Clique Encrypt Phone. Para mais detalhes navegue para: https://bit.ly/39isi47

iPhone:

Vá para Settings > FaceID/Touch ID Passcode > Turn Passcode On > Introduza seu passcode colocando qualquer passcode / password automaticamente encripta seu dispositivo – funcionalidade muito boa!

PASSWORDS & AUNTENTICAÇÂO "2 FACTOR"

Um gestor de passwords guarda e lhe assiste no processo de criação de passwords novas para todas suas contas (online/offline). Isto significa que pode usar passwords diferentes longas e seguras para cada website, sem a necessidade de se lembrar delas!

Recomendamos **LastPass** ou **Bitwarden** como gestor de passwords, ambas possuem óptimas funcionalidades sem custos, e estão disponíveis para uma variedade de plataformas. Outras alternativas offline incluem **PasswordSafe** ou **KeePass**.

bitwarden KeePass passbolt

Multi Factor Authentication (MFA) comummente conhecido como autenticação de dois factores (2FA) é uma mêtodo de autenticação que requer que se providencie dois ou mais factores de verificação para se ter acesso a recursos como aplicações e contas online. Use aplicações de autenticação commo **Authy** ou **Google Authenticator** ao invês de receber códigos por SMS. Pode instalar **Authy** em vários dispositivos activando a opção 'Allow Multi Devices' – isto significa que, diferente das aplicações de autenticação da Google ou Microsoft, pode ter certeza que os códigos estarão disponíveis no seu laptop, celular, tablet, etc. – Todos dispositivos que usa.

Configure o maior número possível de contas no seu gestor de passwords e active autenticação de 2 factores – Entretanto, se tiver que fazer escolhas rápidas, priorize suas contas de email e qualquer local onde informação sensível que diga respeito a direitos humanos esteja guarada.

Mensagens instantâneas

Whatsapp , Signal e Telegram todos providenciam encriptação ponta-a-ponta e devem ser considerados como canais de comunicação seguros.

Alguns consideram WhatsApp menos seguro, mas isto não tem que ver com a segurança do canal de comunicação (é seguro), mas sim com 3 factores-chave em como as aplicações são usadas pelas pessoas:

- Não mande mensagens a grupos com mebros que desconhece e não confia – sempre mantenha comunicações sigilosas a uma audiência reduzida.
- Outras aplicações permitem configurar um período para que as mensagens desapareçam.
- Outras aplicações como **Wire** permitem falar com contactos sem que se saiba seus números de contacto reais.

O mais importante, é usar uma destas ferramentas e evitar o uso de SMS sempre que possível - especialmente se você achar que possa ser alvo, não seja seguro, e seja fácil apara seu provedor de telefonia móvel ou entidades relacionadas interceptar suas comuniões.

Existem também versões instaláveis e web de todos estes aplicativos, portanto, pode facilmente usa-las em substituição a emails se for necessáriio.

Email:

Emails são inseguros por omissão, portanto, seja cauteloso ao usar para situações que requerem segurança a não ser que tenha feito algumas das configurações abaixo.

PGP é um mêtodo comum para assegurar emails mas, a sua configuração é notavelmente complexa para utilizadores sem experiência - Sugerimos que que ignore este guia se souber como configurar suas chaves PGP, este guia não se recomenda a si!

Não obstante, recentemente, tem se feito esforços para tornar o PGP mais usável com ferramentas como Mailvelope and FlowCrypt.

Mailvelope

Mailvelope é usado em todos sistemas de email tais como gmail and yahoo. Guia passo-a-passo: https://bit.ly/3fDBiBX

FlowCrypt

Um mêtodo comum que sugerimos aos utilizadores do Gmail é uma extensão de navegador chamada FlowCrypt. Visite FlowCrypt.com e siga as instruções simples e veja como poderá usar email seguro em menos de 5 minutos!

PLANEAMENTO

Dedique 1 hora ou 2 para se sentar ao seu laptop e telemóvel, e revisitar as configurações e contas. Poderá ver que é útil, praticularmente se for responsável por fazer isto em sua organização, fazer um aplano de acção "SMART".

Online poderá encontrar vários artigos explicando o que são objctivos/metas "SMART", mas todos focam-se numa ideia similar: objectivos/metas SMART são so que facilmente pode rastrear, provar a pessoas chaves que há progresso e judará a todos a estarem envolvidos no que é preciso fazer, quando e de quem é a responsabilidade.

Check https://www.projectsmart.co.uk/smart-goals.php for further ideas and information.

Obrigado e Boa Sorte com a protecção de seus dispositivos e o seu trabalho!