Um guia de segurança e privacidade dos mochileiros das interwebs

Caio Volpato (caioau) (@caioauv) https://caioau.keybase.pub
210B C5A4 14FD 9274 6B6A 250E **EFF5 B2E1 80F2 94CE**

Casa Hacker – Festival – 17 Ago 2019

Resumo:

- OPSEC - Modelagem de ameaças.
- Tudo sobre senhas.
- Navegando com privacidade.
- Privacidade e boas praticas de segurança para todos dispositivos.
- Alternativas livres que respeitam privacidade.

OPSEC

A segurança digital é o oposto da paranoia

OPSEC

O que é OPSEC?

Segurança operacional – OPSEC se trata de minimizar superfície de ataque e pontos críticos de falha através de hábitos e políticas apropriados. é um processo sistemático e provado que podemos usar para negar informações aos adversários que eles precisam para nos causar mal ou interromper nossos planos.

OPSEC

O processo OPSEC

1. Identificar a informação que precisa proteger.
2. Analisar as ameaças.
3. Analisar suas vulnerabilidades.
4. Avalie seus riscos.
5. Aplique as contra medidas

- Entender seus próprios riscos/modelagem de ameaças: Quem é seu adversário ? O que necessita de proteção ?
- Os dois passos do OPSEC: Saber o que precisa proteger e como proteger la?

OPSEC

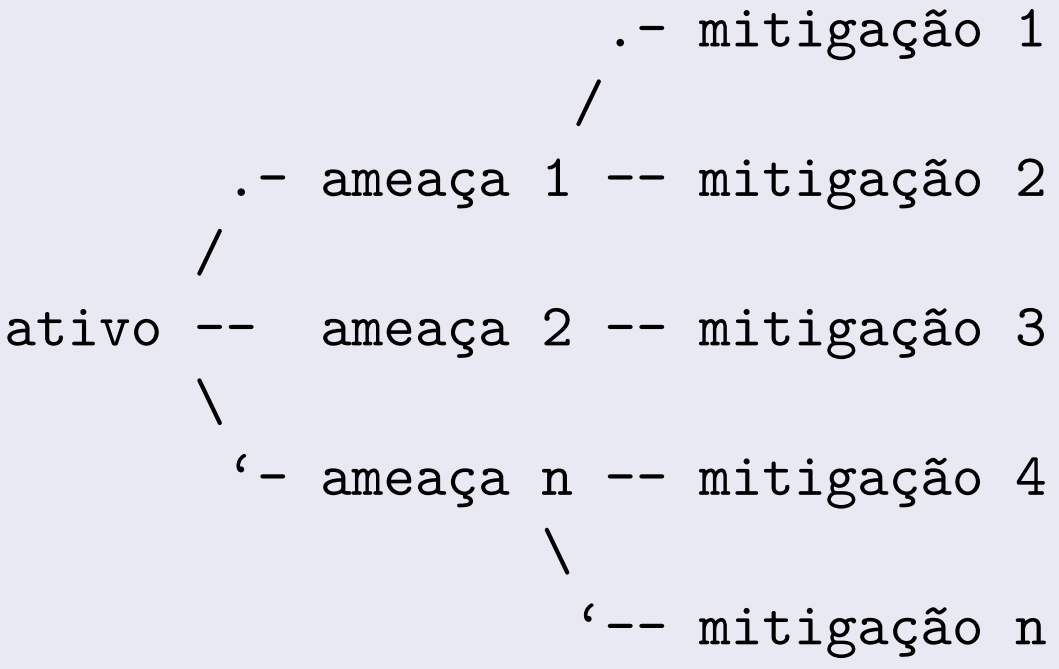
Glossário: Definições importantes:

- Entidade: O principal ator do modelo, pode ser um indivíduo ou uma organização.
- Ameaça: Qualquer forma de ataque contra a entidade.
- Ativo: Qualquer coisa que pertence a entidade.
- Mitigação : Uma maneira para dispersar uma ameaça.
- Adversário: Um ator que promove ameaças e é definido como tendo conflito de interesses com outros atores.
- Risco: A possibilidade de uma ameaça acontecer.

Propriedades desses elementos:

- Ativo:
  - tipo.
  - histórico.
  - quantidade.
  - importância.
  - ameaças.
- Ameaça:
  - probabilidade de ocorrer: P$\{0,1\}$.
  - severidade: quantos ativos essa ameaça compromete ativos.
  - mitigações.
- Mitigação:
  - custo.
  - eficácia: P$\{0,1\}$.
  - ameaças.

Relação entre esses elementos:



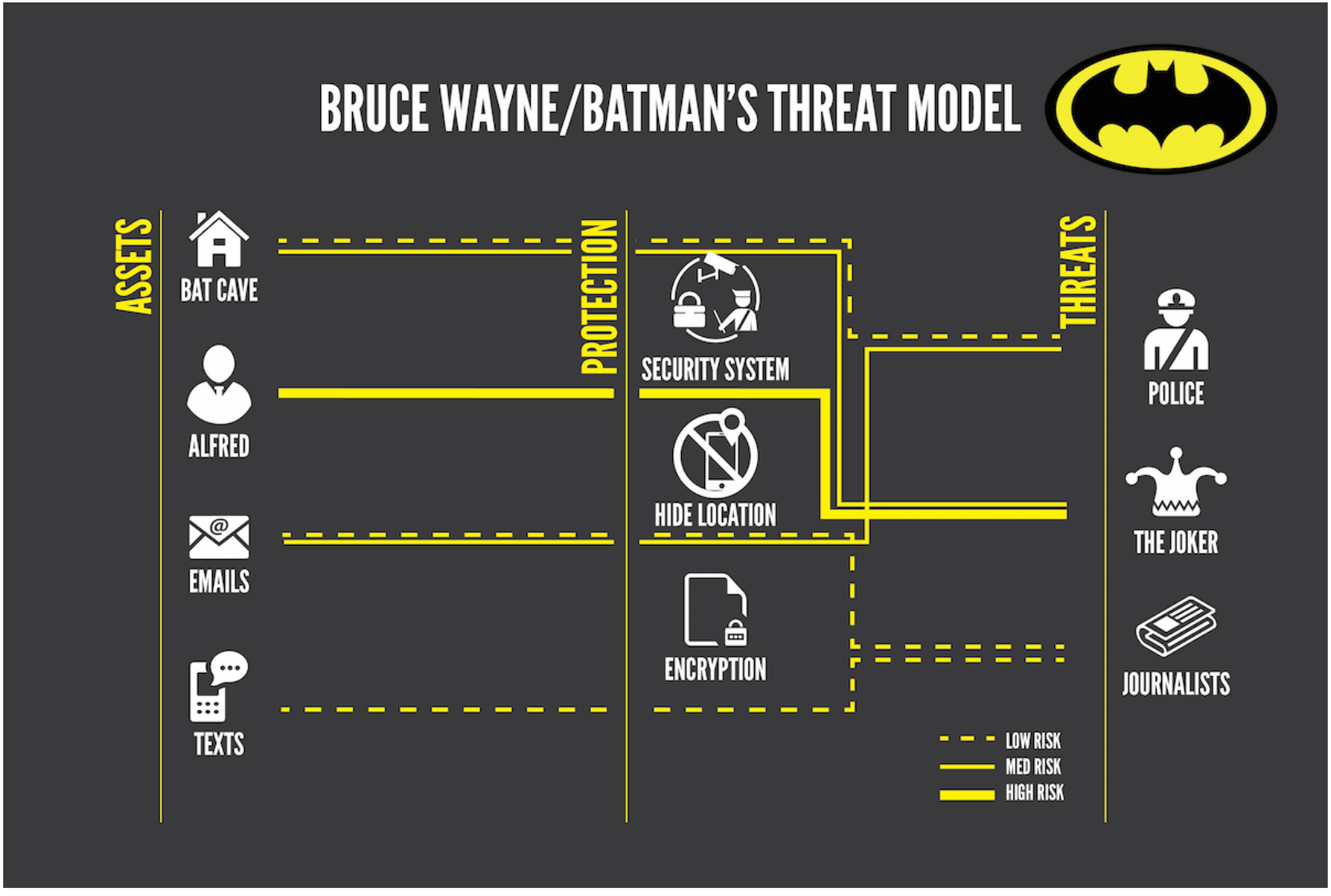


Figure 1: modelo de ameaças do Batman

Cinco perguntas da EFF – Electronic Frontier Foundation:

1. Que coisas eu quero proteger?
   - Os dados, as comunicações e outras coisas que podem causar problemas para você se mal utilizados.
2. De quem você quer proteger?
   - As pessoas, organizações, ou atores criminosos que podem tentar acessar essas coisas.
3. O quão provável é que eu precise protegê-las?
   - Seu nível pessoal de exposição a essas ameaças.
4. O quão graves serão as consequências caso eu falhe?
5. Até onde eu estou disposto a ir para tentar evitar potenciais consequências?
   - O dinheiro, tempo e conveniências que estou disposto a investir para proteger essas coisas.

OPSEC

Leituras complementares:

- plano.autodefesa.org
- (en) EFF – Surveillance Self-Defense
- (en) How I learned to stop worrying (mostly) and love my threat model

Podcasts:

- The Privacy, Security, & OSINT Show – 079-Revisit Your Threat Model
- Reply all – #130 The Snapchat Thief

Tudo sobre senhas

Uma senha segura deve demorar seculos para ser quebrada mesmo se todos os computadores do mundo são utilizados, mas em 2016 as senhas do LinkeDin vazaram eram **61 milhões de senhas únicas** e tomou **apenas 2 horas para quebrar 65% delas.**

Tudo sobre senhas

Security

Mark Zuckerberg's Twitter and Pinterest password was 'dadada'

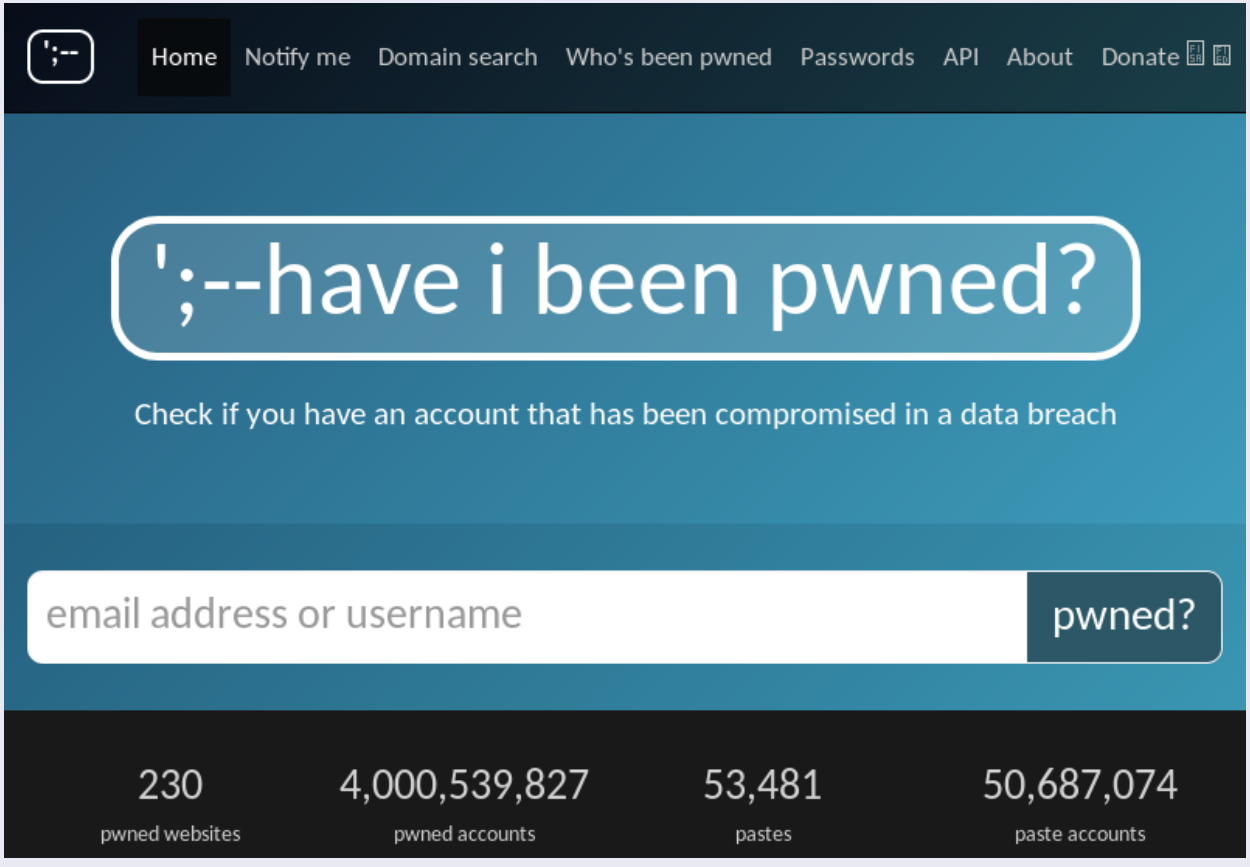
'Idiotic' doesn't even come close to describing this

By John Leyden 6 Jun 2016 at 11:27 SHARE

Tudo sobre senhas

Verifique se suas senhas foram comprometidas

haveibeenpwned.com



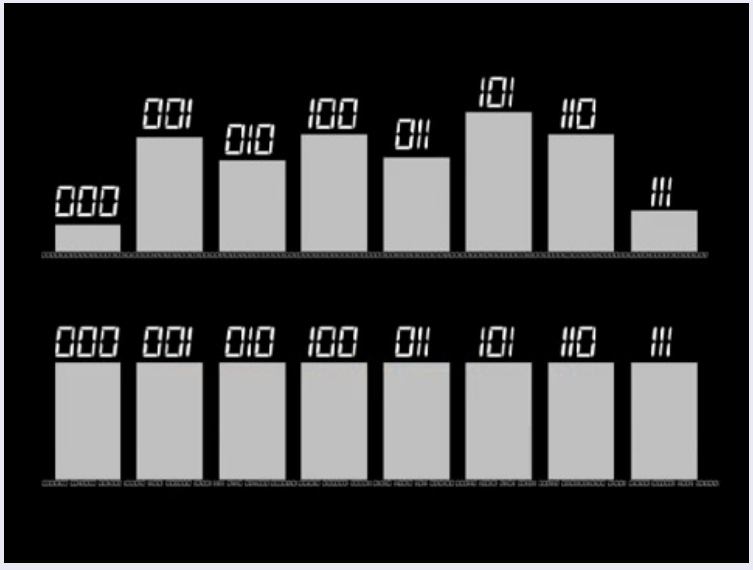
Tudo sobre senhas

Distinguindo verdadeiramente aleatório de gerado por humanos

Imagine que duas pessoas estão ligando e desligando uma lâmpada, uma baseada no lançamento de uma moeda e outra tentando simular aleatoriedade.
será que conseguimos determinar qual lâmpada está sendo baseada na moeda?

Tudo sobre senhas

Distinguindo verdadeiramente aleatório de gerado por humanos



A abordagem é contar sequências de números, como sequências de lançamentos com comprimento 3: Uma sequência verdadeiramente aleatória terá será igualmente provável de conter todas sequências de qualquer comprimento (Propriedade de estabilidade de frequência).

Tudo sobre senhas

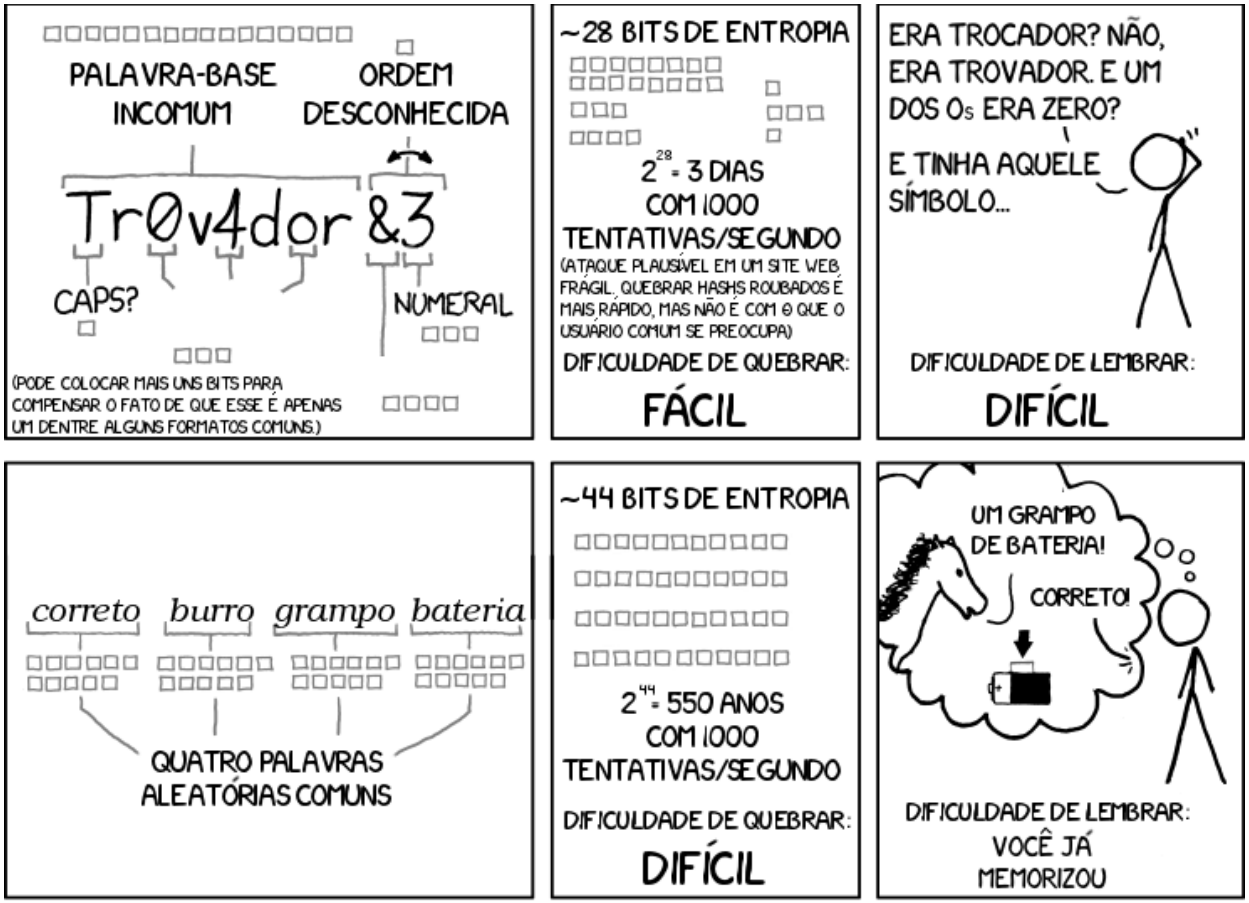


Figure 2: xkcd 936 : Password Strength

Tudo sobre senhas

Humanos favorecem certas sequências quando pensam suas senhas, uma razão disso acontecer é porque erroneamente pensamos que certos resultados são menos aleatórios que outros.

Esse comportamento de manada resulta em senhas mais previsíveis.

Tudo sobre senhas

Método Dadoware (Diceware) de gerar senhas seguras

Então nossas senhas são horríveis, precisamos criar senhas que são:

- Fácil de lembrar.
- Verdadeiramente aleatória.
- Longa o suficiente.

O dadoware é um método de gerar senhas seguras: Consiste em lançar um dado para selecionar palavras de uma lista.

lista PT_BR lista EN

Tudo sobre senhas

Método Dadoware completo:

1. Baixe o livreto com a lista de palavras: livreto
2. Tenha certeza que você esteja sozinho no quarto e feche a porta e janelas e escreva em cima de superfície dura.
3. Jogue o dado 5 vezes por palavra, exemplo: 2-6-5-1-3 : vá na pagina 2,6 do livreto e procure a palavra 513 = egípcio.
4. repita o 3o passo 6 vezes.
5. Jogue 1~3 para sortear a palavra vai ficar em maiúscula.
6. Jogue o dado 2 vezes por simbolo/numero.
7. faça o 6o passo 3~7 vezes.
8. Escreva a senha final algumas vezes, e digite-a para ajudar na memorização.
9. Depois de memorizar a senha, bote jogo no papel e jogue as cinzas no vazo sanitário.

Método Diceware :

Exemplos de senhas geradas:

1. Simples:
   conhecer origem estrago maldade farra copa

Entropia=77 bits (1T/s = 2.4 mil anos,100T/s=24 anos)

2. Reduzida:**wordlist completa (270 mil palavras)**
   recupereis flagelo passagens ancestralidade

Entropia=72 bits (1T/s = 150 anos, **100T/s = 1,5 anos**)

Atenção: Esse tempo é o pior caso: o tempo de percorrer todas as combinações, o tempo real será menor (na media metade)

Método Diceware :

Em suma, o diceware é um método de gerar senhas que é:

- Harder: as senhas geradas são verdadeiramente aleatórias as tornando bem mais difíceis de quebrar.
- Better: são melhores para lembrar.
- Faster: é mais rápido de pensar numa senha, basta jogar o dado (ou fazer no computador).
- Stronger: As senhas geradas são fortes, pois tem mais entropia.

Gerenciadores de senhas (Password Manager)

Agora que sabemos como avaliar se uma senha é boa e como gerar boas senhas, ainda precisamos resolver o seguinte problema: precisamos ter uma senha para cada serviço.

Uma solução para isso é um password manager (gerenciador de senhas), é um programa que cria boas senhas aleatórias automaticamente, para cada site individualmente, guardando todas essas senhas trancadas com apenas uma senha mestra.

Recomendações de gerenciadores de senhas livres:

- KeePassXC Armazena arquivo **(mude para argon2)**.
- LessPass sem estádo (não armazena nada).
- Bitwarden baseado na nuvem.

Gerenciadores de senhas (Password Manager)

No Android:

- **Atenção: Não utilize a área de transferência para acessar suas entradas**, é compartilhada entre todos aplicativos.
- Use o KeePass DX, tem teclado de autocompletar (e sincronize com syncthing).

Autenticação em duas etapas (2FA)

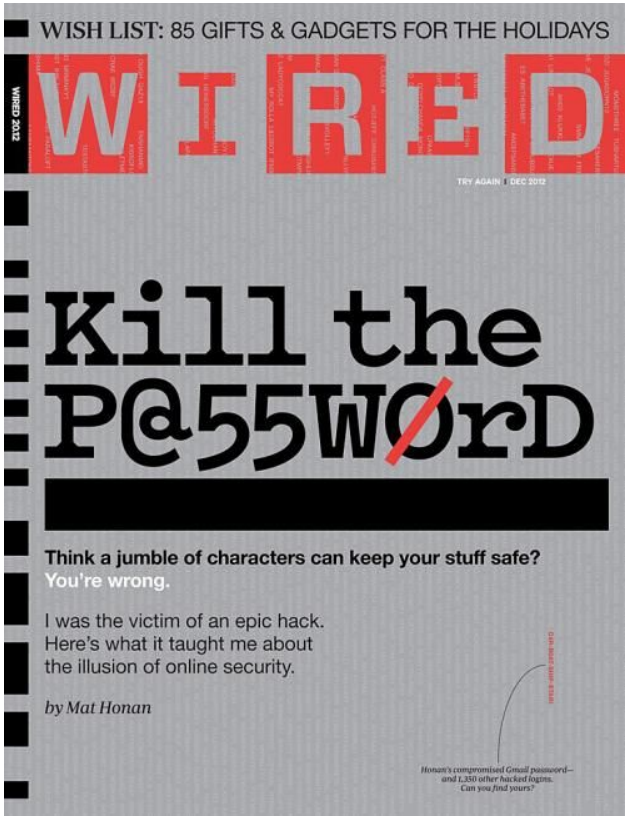
A ideia por trás da autenticação em duas etapas (2FA – 2 factor authentication) é que para entrar na sua conta além da senha (que uma coisa que só você sabe), precisa de uma coisa que só você tem, no caso um app no celular.

turnon2fa.com mostra como habilitar para cada serviço.

Normalmente consiste em escanear um QR code com um app, recomendo o andOTP.

Autenticação em duas etapas (2FA)

Kill the Password: A String of Characters Won't Protect You.



Autenticação em duas etapas (2FA)

Autenticação em duas etapas com SMS:

Usar SMS para autenticação é péssimo, pois:

1. Pode comprometer sua privacidade (como o facebook fez)
2. Pode ser interceptado por torres espias.
3. Seu SIM card pode ser "clonado" (SIM swapping)
   - Dez2018:Golpe com número clonado usa WhatsApp
   - **habilite a verificação em dois passos em seus mensageiros**
4. Pode ser espiada com celular travado.
   - **desabilite notificações na tela de bloqueio**

Tokens de segurança (yubikey)

2FA é susceptível a ataques phishing

Mesmo que usar 2FA seja um método robusto para proteger suas contas, mas infelizmente é susceptível a ataques phishing (no qual o atacante cria um pagina de login idêntica do serviço original e redireciona a vítima e a faz entrar suas credenciais e o código 2FA, dando acesso ao atacante a conta da vítima).

Tokens de segurança:

Os tokens de segurança são uma maneira mais segura de autenticação em duas etapas, utilizam o padrão Universal 2nd Factor – U2F que usa criptografia de chave pública e privada para assinar um desafio enviado pelo serviço e como o domínio é enviado para o token dessa forma a pagina falsa não consegue acessar a chave do serviço legitimo. Toda vez que o token é utilizado é necessário tocar fisicamente ele.

PinCodes:

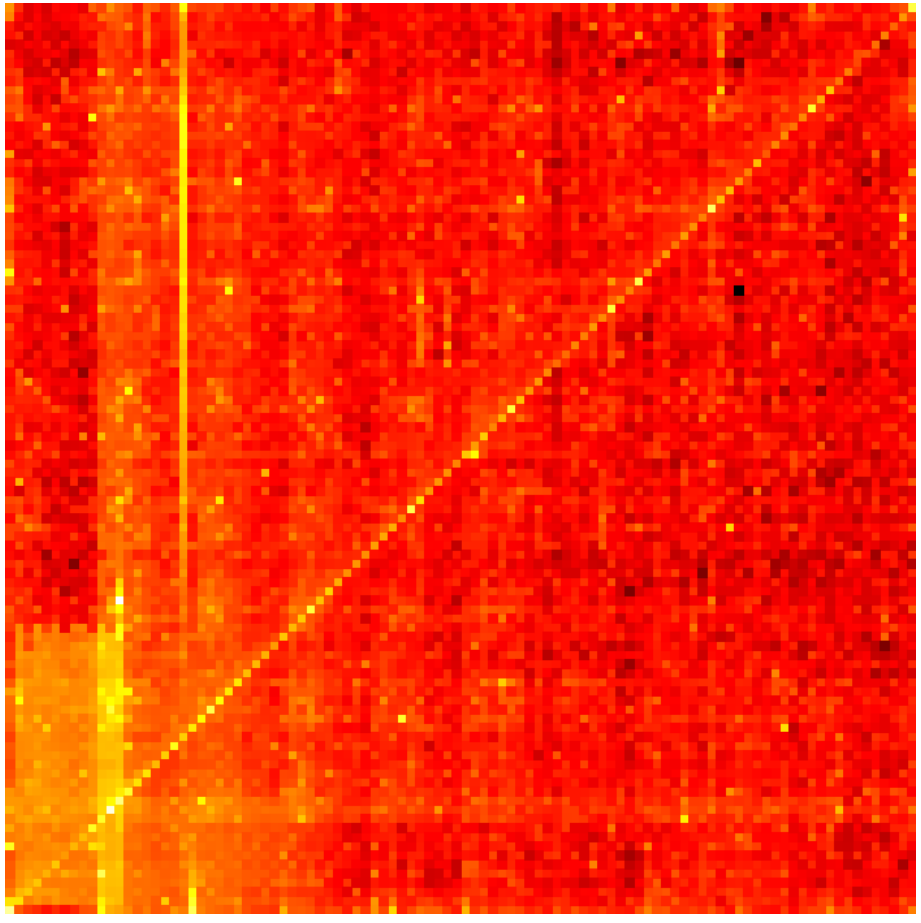


Figure 3: PIN analysis

Pincodes

Em excelente seu post (PIN analysis), Nick Berry analisou 3.4 milhões de PinCodes de 4 dígitos (10 mil combinações). E constatou:

- Os top 20 pincodes são responsáveis por 27% do total.
- estatisticamente 1/3 de todos os PinCodes podem ser adivinhados apenas testando 61 combinações.
  - 50% pode ser adivinhado testando apenas 426 combinações (muito menos que 5000).
- PinCodes contendo Anos (19XX) e datas (MMDD) são muito frequentes.

Padrão de desbloqueio do Android

Se você usa o padrão do Android (aquela gradezinha 3x3): existem 389112 possibilidades que podem ser usadas (ou seja **usar um PinCode verdadeiramente aleatório de 6 dígitos é um pouco melhor**).

Uma pesquisadora norueguesa chamada Marte Løge em sua tese de mestrado mostrou que mais de 10% dos padrões analisados, usa como padrão de desbloqueio uma "letra" que é a inicial do companheiro, filho, ou algo parecido.

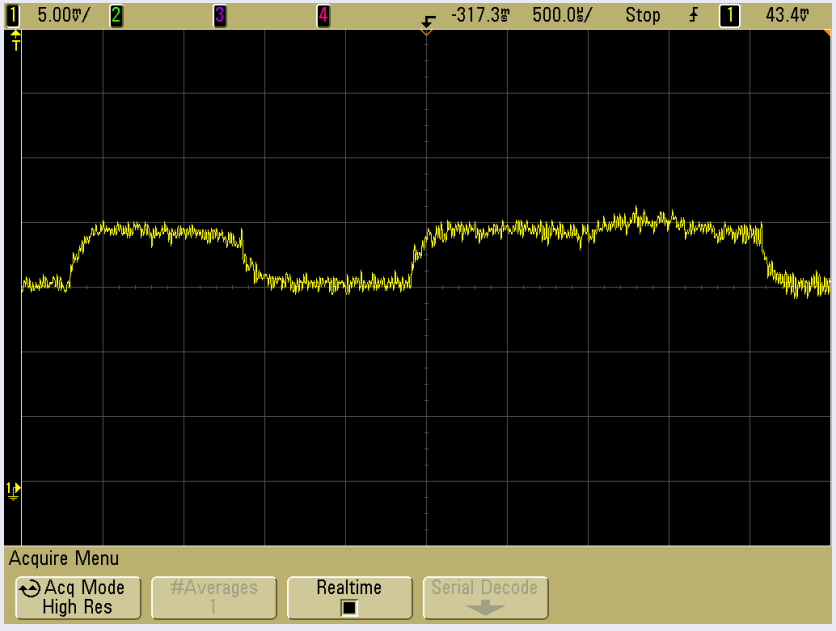
veja o artigo na arstechnica falando sobre o assunto: New data uncovers the surprising predictability of Android lock patterns

Ataques de canal lateral

Definição: Ataques de canal lateral

Ataques da canal lateral são aqueles que se concentram na forma que o sistema é implementado, se ela vaza alguma informação sensível que pode ser monitorada pelo atacante.

- exemplo: análise de potencia usada para vazar a chave privada de um smartcard



Ataques de canal lateral

Uso do acelerômetro para descobrir o pincode

Nesse paper: Stealing PINs via Mobile Sensors: Actual Risk versus User Perception os pesquisadores conseguiram descobrir 80% dos pincodes digitados no celular através de um script js no navegador que monitora o movimento através do acelerômetro.

Ataques de canal lateral

Câmera térmica

Nesse video : iPhone ATM PIN code hack- HOW TO PREVENT ele mostra um "case" para iPhone que é uma câmera térmica e através do calor dos dedos é possível descobrir o pincode digitado, conforme a foto abaixo:

Ataques de canal lateral

note que as teclas que estão com uma coloração mais clara estão mais quentes, ou seja foram digitadas por ultimo: ou seja o pincode digitado foi 12345.

Ataques de canal lateral

para prevenir desse ataque ele sugere que enquanto digita o pincode mantenha os dedos sobre todas as outras teclas, assim todas as teclas ficaram com uma coloração mais clara.

resultado:

Navegando com privacidade

Como somos rastreados enquanto navegamos:

- Browser fingerprint (qual navegador e versão, tamanho da tela, fontes, plugins e extensões)
- pixel tags
- super cookies.
- cookies
- web beacons.

Navegando com privacidade

A aba privativa não é anonima

visite nothingprivate.ml coloque seu nome na caixa, feche o navegador e abra novemente na abra privada, ira lembrar você, mesmo usando VPN.

leitura complementar:

- Mãe é quem clica: estámos parindo crias do chupadados

Navegando com privacidade

navegue com privacidade: o jeito mais fácil: Brave Browser

Brave Browser é um navegador software livre que automaticamente bloqueia propagandas e rastreadores com proteção contra fingerprint.

Navegando com privacidade

navegue com privacidade: abordagem mais completa: Firefox hardenizado

Siga as instruções em: 0xacab.org/caioau/firefox-hardening

Navegando com privacidade

Quando acessando a internet sua operadora sabe quais sites você está acessando (mas não sabe o que você está fazendo neles, a maioria dos sites tem https) e o site sabe o seu IP real (logo sua localização), as VPNs tentam resolver isso.

VPNs

VPN – Virtual Private network (rede privada virtual), é um tunnel que conecta duas redes, dessa forma sua operadora não sabe quais sites está acessando e os sites não sabem seu IP real.

Navegando com privacidade

VPN - a Very Precarious Narrative

VPNs não são uma solução completa para o anonimato pois:

- Apenas move a completa e total confiança da operadora para o provedor da VPN (não reduz a informação).
- Agindo como elas fazem, promover provedores comerciais de VPN como solução para possíveis problemas faz mais mal do que bem.
- Na maioria das circunstancias, VPNs fazem quase nada para melhoram sua segurança e privacidade a menos de combinada com outras mudanças.

Tor

Tor – The onion router (roteamento cebola), enquanto VPNs movem toda a confiança do sua operadora para a VPN, o Tor distribui a confiança.

Tor

Dismistificando o Tor: Mitos

- Deep web? Dark web? Hackers? Ilegalidade?

Tor

Dismistificando o Tor: Mitos

- Deep web? Dark web? Hackers? Ilegalidade?
- Deep dark web é bem maior que Google, Youtube, Facebook?

Tor

Dismistificando o Tor: Mitos

- Deep web? Dark web? Hackers? Ilegalidade?
- Deep dark web é bem maior que Google, Youtube, Facebook?
- Quando você usa o Tor podem acontecer coisas estranhas como ficar na mira do FBI?

Tor

Dismistificando o Tor: Mitos

- Deep web? Dark web? Hackers? Ilegalidade?
- Deep dark web é bem maior que Google, Youtube, Facebook?
- Quando você usa o Tor podem acontecer coisas estranhas como ficar na mira do FBI?
- Usar Tor é entrar em sites duvidosos?

Dismistificando o Tor: Fatos

Então o que de fato é esse tal de Tor?

- Um software livre usado para contornar a censura, vigilância e o rastreamento na web.

Dismistificando o Tor: Fatos

Então o que de fato é esse tal de Tor?

- Um software livre usado para contornar a censura, vigilância e o rastreamento na web.
- Quem apoia e usa o Tor?

Dismistificando o Tor: Fatos

Então o que de fato é esse tal de Tor?

- Um software livre usado para contornar a censura, vigilância e o rastreamento na web.
- Quem apoia e usa o Tor?
  - Ongs de Privacidade: Como a EFF

Dismistificando o Tor: Fatos

Então o que de fato é esse tal de Tor?

- Um software livre usado para contornar a censura, vigilância e o rastreamento na web.
- Quem apoia e usa o Tor?
  - Ongs de Privacidade: Como a EFF
  - Defensores de direitos humanos e LGBTQIA+: Como a Human Rights Watch

Dismistificando o Tor: Fatos

Então o que de fato é esse tal de Tor?

- Um software livre usado para contornar a censura, vigilância e o rastreamento na web.
- Quem apoia e usa o Tor?
  - Ongs de Privacidade: Como a EFF
  - Defensores de direitos humanos e LGBTQIA+: Como a Human Rights Watch
  - jornalistas: Como BuzzFeed, Huffington Post

Dismistificando o Tor: Fatos

Então o que de fato é esse tal de Tor?

- Um software livre usado para contornar a censura, vigilância e o rastreamento na web.
- Quem apoia e usa o Tor?
  - Ongs de Privacidade: Como a EFF
  - Defensores de direitos humanos e LGBTQIA+: Como a Human Rights Watch
  - jornalistas: Como BuzzFeed, Huffington Post
  - diversas empresas como facebook e cloudflare

Dismistificando o Tor: Fatos

Então o que de fato é esse tal de Tor?

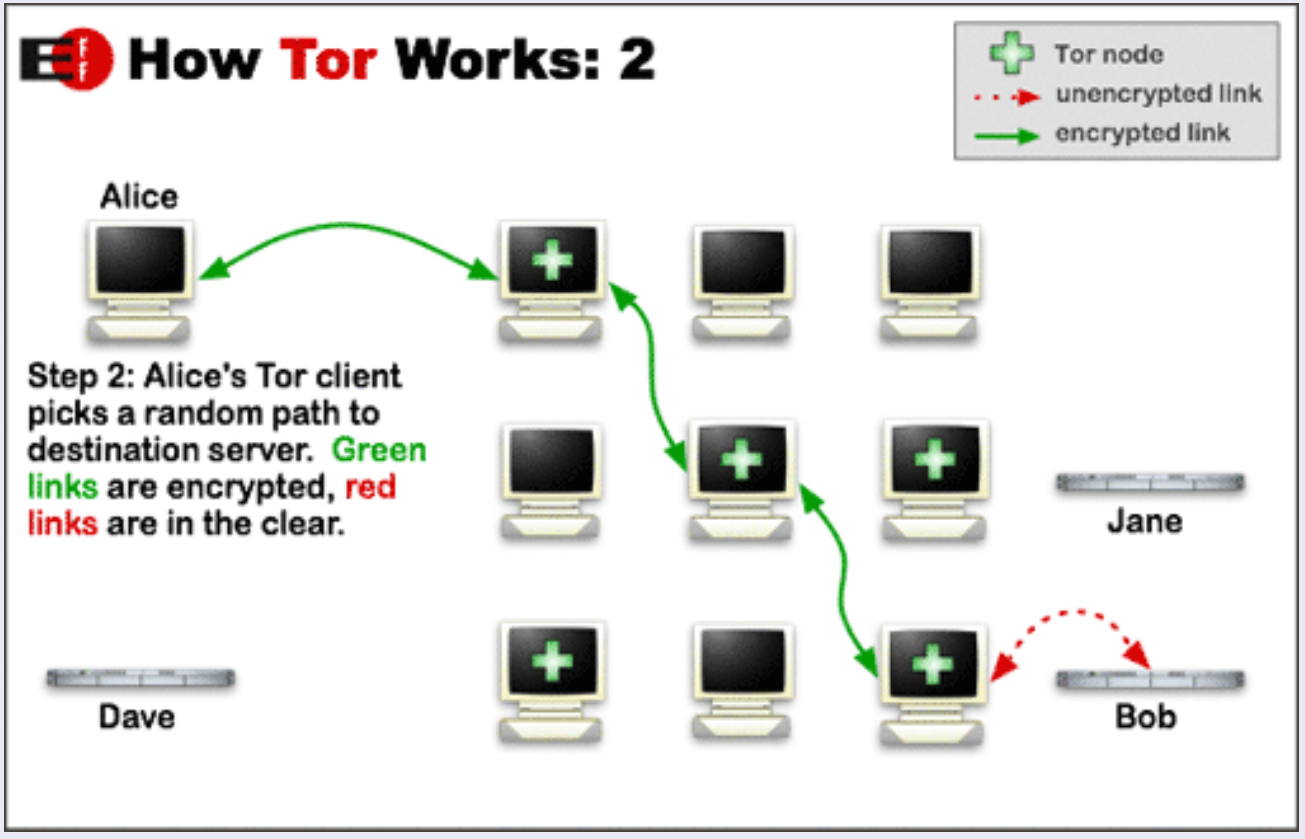
- Um software livre usado para contornar a censura, vigilância e o rastreamento na web.
- Quem apoia e usa o Tor?
  - Ongs de Privacidade: Como a EFF
  - Defensores de direitos humanos e LGBTQIA+: Como a Human Rights Watch
  - jornalistas: Como BuzzFeed, Huffington Post
  - diversas empresas como facebook e cloudflare
  - A própria polícia

Dismistificando o Tor: Fatos

Qual é a missão do Tor?

Proteger os direitos humanos e liberdades por meio da criação e implementação de tecnologias de anonimato e privacidade livres e de código aberto, provendo apoio a seu uso e disponibilidade irrestritos. Ao mesmo tempo, contribuímos para o avanço de sua compreensão científica e popular.

Como o Tor funciona:



O que cada relay da rede Tor sabe?

- Bridge/guard (entrada)
  - sabe:
    - O IP/localizacao do usuario e do relay middle
  - não sabe:
    - IP/localizacao do relay de saída
    - a mensagem do relay middle e exit
- Middle node (meio)
  - sabe:
    - O IP/localizacao of bridge/guard e exit
  - não sabe:
    - IP/localizacao do usuario
    - a mensagem do relay guard e exit

O que cada relay da rede Tor sabe?

- Relay de saída (exit node)
  - sabe:
    - O IP/localizacao do usuario e guard/bridge
    - O conteudo da mensagem do usuario
  - não sabe:
    - IP/localizacao do usuario e da bridge/guard
    - a mensagem do relay middle e guard

tor and https

Enquanto usando o Tor e importante sabe:

- Sua operadora (**apenas**) sabe* que está usando Tor.
- Use o Tor Browser.
- Não baixe torrent via Tor.
- **Não instale plugins ou add-ons no Tor Browser**
- Não maximize a janela do Tor Browser.
- Evite ao maximo abrir anexos baixados via Tor (use o Tails).

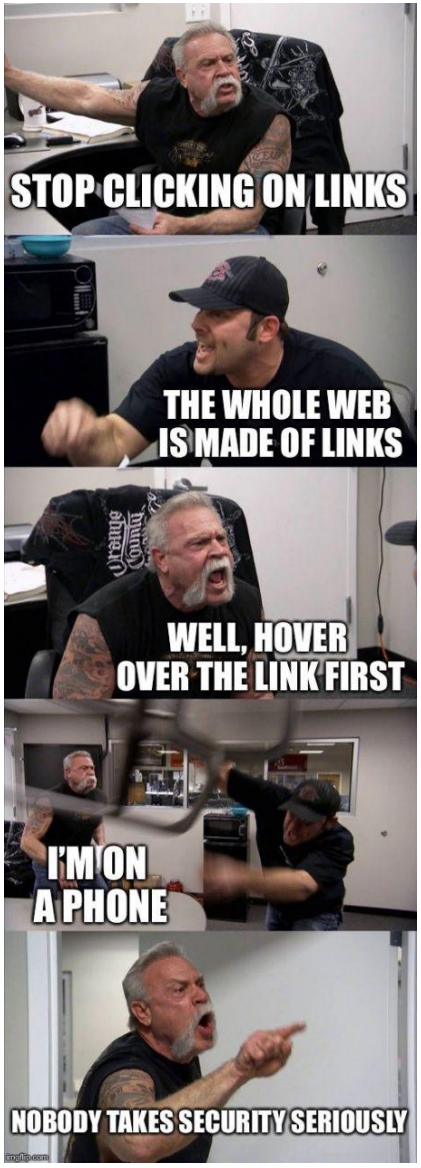
Servicos cebola do Tor (Tor onion services)

Quando usando o Tor, a conexão tem que sair da rede Tor, talvez deixando aquela conexão exposta para o relay de saída, além disso o Tor só protege o cliente, não o serviço.
Como funciona: Quando usando serviços cebola (domínios .onion) o cliente e o serviço cada um constrói um circuito para um ponto de encontro.

Propriedades dos serviços cebola:

- Auto autenticado.
- Criptografado fim a fim.
- "Perfuração" de NAT integrada.
- Não "sai" da rede Tor

Boas praticas de segurança



Boas praticas de segurança

Como manter seu PC seguro

- mantenha seu windows e programas (principalmente navegadores) atualizados.
- desinstale completamente flash.
- faça backups.
  - Backup não é uma copia simples, ou seja o backup deve ser feito em outra mídia.
  - deve ser automático e periódico, porém não confie cegamente no automático: certifique-se que está sendo feito.
- baixe apenas programas confiáveis de fontes confiáveis (tente ao máximo só utilizar os repos oficiais de sua distro).

Boas praticas de segurança

proteja seu wifi:

- use uma senha forte.
  - dica: como passar sua senha forte: visite qrstuff.com selecione a opção Wifi Login e gere seu qr code e use o app Barcode Scanner para escanear o qr e salvar a rede no android.
- troque a senha padrão da administração e desabilite o acesso remoto.
- desabilite o UPnP e o WPS.
- mantenha o firmware do seu roteador atualizado (e se possível procure alternativas livres como librewrt)

Boas praticas de segurança

Boas Praticas de Segurança: Android:

- The Privacy Enthusiast's Guide to Using Android:
  - Use PinCode ou senha Forte (6+ dígitos **VERDADEIRAMENTE ALEATÓRIOS**).
  - tenha consciência que se você usa a digital para desbloquear seu aparelho podem te forçar você a colocar seu dedo.
  - "Esconda" notificações sensíveis da tela de bloqueio.
  - Desative "minhas atividades" do Google (histórico de buscas, localização, etc . . .): myactivity.google.com/myactivity
  - Desative (ou não) o find my phone
  - Desative Backup do Google: histórico de chamadas, senhas do Wifi e Apps são salvos no Google.
  - Desative permissões desnecessárias.
  - Vá no app de Câmera e desabilite a opção de Geolocalização.

Boas Praticas de Segurança: Android:

- Use o app chamado Send Reduced que além de tirar metadados de fotos, reduz seu tamanho, fdroid
- Tem android 9 (P) ? **Criptografe seu DNS** (DNS over TLS) usando CloudFlare ou nextdns (permite bloquear propagandas e rastreadores)

Isole Apps sensíveis:

Recomendo o app shelter (fdroid): ele cria um perfil isolado e permite usar apps de maneira isolada e permite "congelar" apps preservando sua privacidade.

Boas Praticas de Segurança: Android:

Bloqueie uso indevido do seu microfone:

Recomendo o app PilferShush Jammer (fdroid): ele bloqueia apps de usarem seu microfone.

Leituras complementares:

- (PT) Cartilhas de segurança para internet – CERT.br.
- The Motherboard Guide to Not Getting Hacked pt-br
- The WIRED Guide to Digital Security
- Device Privacy Tips - DuckDuckGo
- (PT) Meu celular sem Google!? – Oficina Antivigilância
- Wolfgang's Channel – Privacy on Android: A Definitive Guide

Alternativas livres que respeitam privacidade.

Ferramentas de produtividade:

- etherpad Editor online colaborativo.
- ethercalc Planilhas online.
- cryptpad Serviço colaborativo criptografado.
- Standard Notes Notas criptografadas.

Motores de busca:

- DuckDuckGo
- startpage
- Qwant
- searX

Alternativas livres que respeitam privacidade.

Mensageiros:

- Signal/Wire Mensageiros privados com ligação (Wire não precisa de numero de telefone).
- Briar: Mensageiro descentralizado.
- Jitsi Meet site e app que permite ligações.

compartilhamento de arquivos:

- firefox send/Up1 – share.riseup
- OnionShare Permite compartilhar arquivos de maneiro segura e anonima.

Armazenamento na nuvem:

- Syncthing sincronize seus arquivo entre seus dispositivos.
- Nextcloud alternativa livre ao dropbox.

Alternativas livres que respeitam privacidade.

Software de criptografia:

- VeraCrypt Criptografia de disco.
- Cryptomator Criptografe seus arquivos para sincronizar com a nuvem.

Plataforma de vídeos:

- PeerTube Plataforma descentralizada
- libreflix Streaming
- invidio.us Uma “interface” do youtube

misc

- OpenStretMap mapas livres

Aplicativos livres que respeitam a privacidade

Fdroid

Fdroid é uma loja de aplicativos que respeitam a liberdade e privacidade, contem apenas apps livres.

Alguns apps da Fdroid

- Jogos: 1010! Klooni and 2048 and so on ...
- Simple Mobile tools (gallery, calendar, file manager ...)
- Navegadores: Fennec, Klar, PrivacyBrowser, Tor Browser for Android.
- Redes sociais: Twidere (twitter), Slide (reddit), Febilab (Fediverse), Telegram
- Compartilhamento de arquivos: NextCloud, Syncthing
- K9Mail, OpenKeyChain (PGP)
- OpenVPN for android, Orbot (Connects to Tor), Netguard (firewall and adblocker), shelter
- AnySoftKeyboard, Markor (text editor), Gadgetbridge (smart watches)
- Media: NewPipe (youtube), AntennaPod (podcasts), Vinyl (music player), DroidShows (tv shows manager)

Alguns apps da Fdroid

- Gerenciadores de senhas: lesspass, keepassdx; andOTP (2FA).
- Osmand~ (navigation), Transportr (public transport)
- termux (terminal with packages), yalp store (downloads apk from play store)
- Contacts and calendar sync: DAVx5, DesyncCC
- barcode scanner (qr reader), document viewer (PDF)

Obrigado!