Integridade Digital

por Celso Bessa

Recomendações e dicas para conquistar **um pouco mais de privacidade, segurança e bem-estar** em espaços digitais.

v0.21.0 (24 de Maio de 2022)

(um projeto permanentemente em progresso)

O que é integridade digital?

- **Segurança e privacidade pessoal**
- **Segurança da informação**
  - Confidencialidade
  - Integridade
  - Disponibilidade
- **Capacidade e resiliência de comunicação**
  - Capacidade
  - Alcance
  - Resistência à censura

Objetivo

O objetivo é mudar nosso modo de pensar sobre nossa privacidade e segurança digital, bem como a integridade e segurança da informação que nós gerenciamos, especialmente informação que possa colocar em risco a nós ou a outras pessoas.

Teremos uma abordagem de redução de danos, adotando algumas ferramentas mais seguras e boas práticas.

Todos e tudo são alvos

- rastreio de atividades para fins financeiros
- vazamento de intimidade e pornô de vingança
- chantagem e ataque à reputação;
- ransomware;
- uso de dados para golpes;
- informação e segredos organizacionais ou pessoais;
- propaganda e manipulação política
- informações de finanças e roubo de dinheiro;
- recurso computacional para ataques;
- censura e repressão;
- guerra e espionagem cibernética;

Todos e tudo são alvos

Não necessariamente um alvo principal. Muitas vezes, um secundário ou acessório para outro ataque.

- **Reunir informação sobre alguém que você conhece**
- **Fingir ser você (ou seu dispositivo)**
- **Grampear seu telefone ou computador para aprender sobre outra pessoa através de suas conversas**

Todos e tudo são alvos

- O famoso príncipe nigeriano;
- O famoso bilhete de loteria;
- Vazamento de fotografias de Caroline Dieckmann;
- Golpe do "sabemos o que você acessou de pornô e vamos divulgar para todos os seus contatos";
- Provas (vídeos e fotos) do abuso do estado contra cidadãos sendo perdidas:
- abuso em manifestações e protestos (e.g. Brasil, Colômbia, América Latina, EUA), abuso policial na periferia;
- Ataque ao sistema do Tribunal Superior Eleitoral;
- VazaJato;

Todos e tudo são alvos

Jornalistas venezuelanos parados por paramilitares em uma estrada na Colômbia perderam seus equipamentos com informações importantes sobre os imigrantes venezuelanos.

Jeff Bezos (Amazon) telefone hackeado usando malware de grupo NSO, uma empresa israelense de tecnologia de espionagem, a fim de permitir o acesso a um terceiro: Jamal Khashoggi, jornalista crítico do regime da Arábia Saudita, que mais tarde foi assassinado por agentes do estado saudita

https://www.wired.com/story/bezos-phone-hack-mbs-saudi-arabia/

É cada vez mais frequente que os aplicativos de banco e finanças nos celulares roubados sejam utilizado para roubar dinheiro e aplicar golpes, com altíssimo prejuízo financeiro para as pessoas.

Todos e tudo são alvos

Ativistas mexicanos infectaram smartphone com spyware após clicarem em phishing bem elaborado em texto SMS:

https://bit.ly/MexicanActivistsScandal

Computadores de escolas públicas de Baltimore alvos de ataque de ransomware durante COVID-19 que impedem as aulas

https://technews.purpee.com/ransomware-attack-forces-baltimore-county-public-schools-to-cancel-classes/

Todos e tudo são alvos

Promotores brasileiros, juiz (ex-ministro da Justiça) e políticos do Telegram contas invadidas por vulnerabilidades na autenticação de dois fatores por SMS ou voz e caixas de correio de voz sem senhas.

https://theintercept.com/series/mensagens-lava-jato/
https://theintercept.com/2019/08/29/deltan-dallagnol-car-wash-leaks-brazil/

Relatórios vazados da Amazon expõem a vigilância que a empresa fez de grupos trabalhistas e ambientais

https://www.vice.com/en/article/5dp3yn/amazon-leaked-reports-expose-spying-warehouse-workers-labor-union-environmental-groups-social-movements

iFood executa campanha de desinformação e esvaziamento de movimento de trabalhadores

https://apublica.org/2022/04/a-maquina-oculta-de-propaganda-do-ifood/?utm_source=celsobessa&utm_medium=twitter&utm_campaign=celsobessa

Devemos pensar em adversários e não apenas hackers

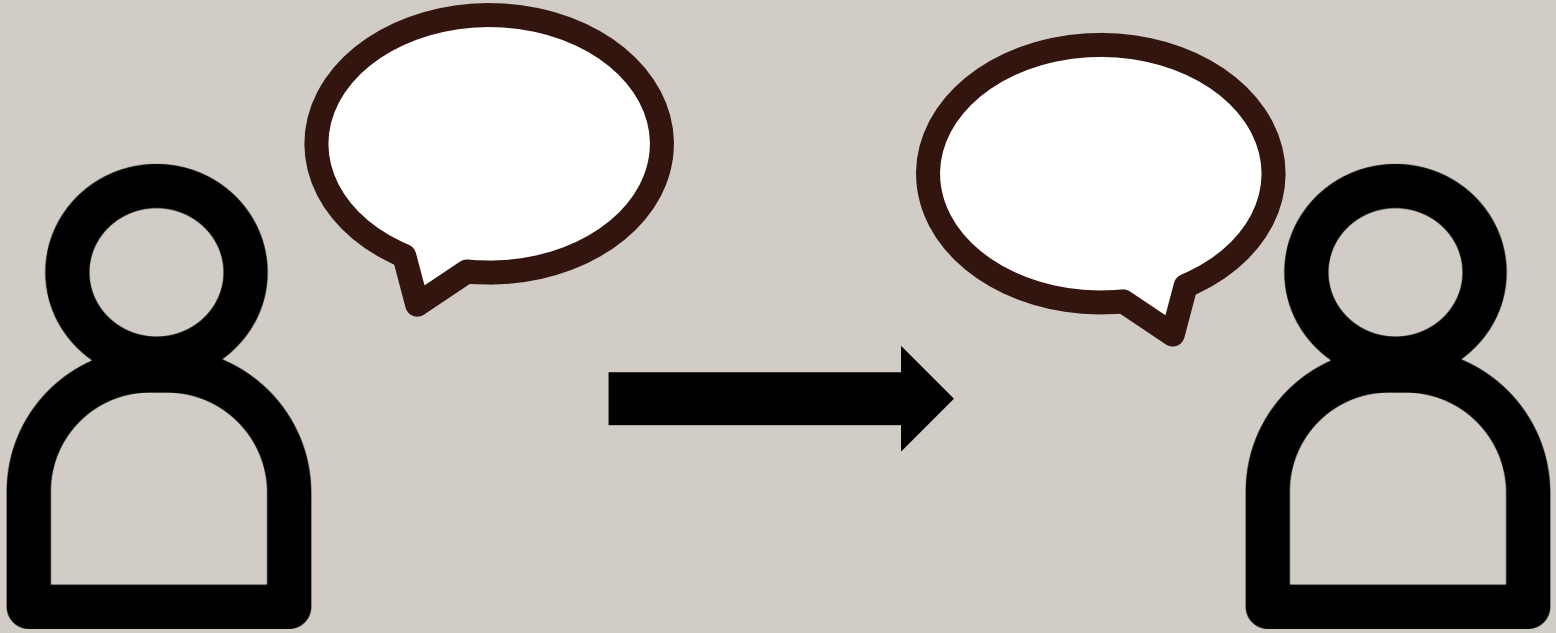
- Ladrões / batedores de carteira comuns
- Agentes do Estado (seja por política estatal ou interesses privados do agente)
- Empresas e grandes interesses econômicos (e.g. Espionagem comercial, desqualificação de trabalhadores e ativistas, chantagem);
- Golpistas, Spammers
- Na Colômbia, por exemplo: paramilitares, guerrilheiros e grandes interesses/grupos econômicos

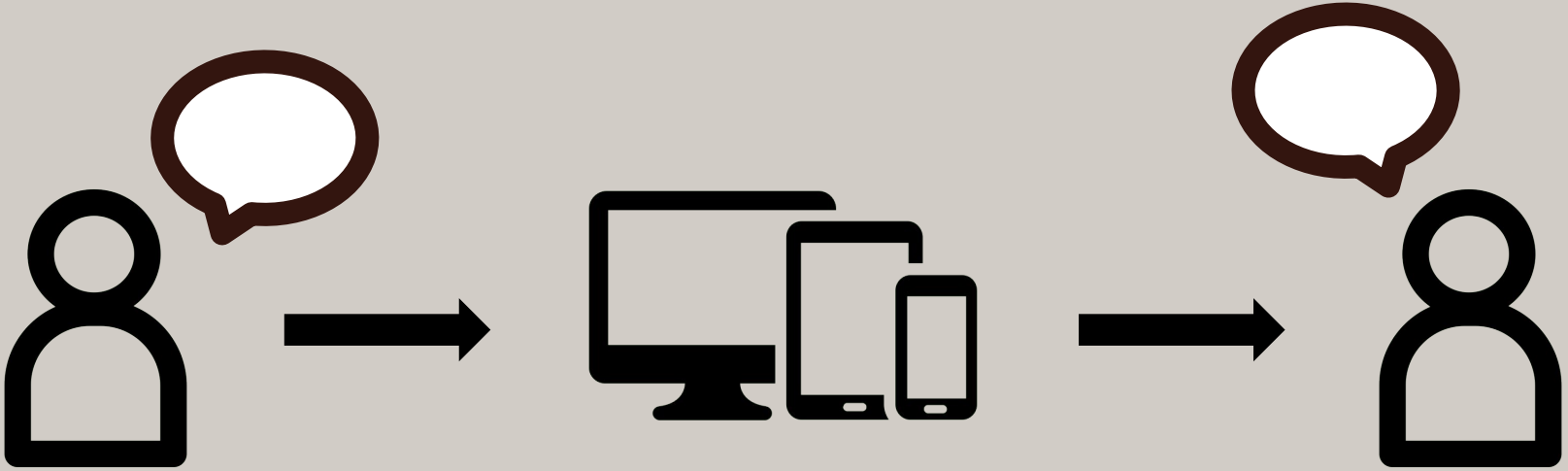
Em resumo

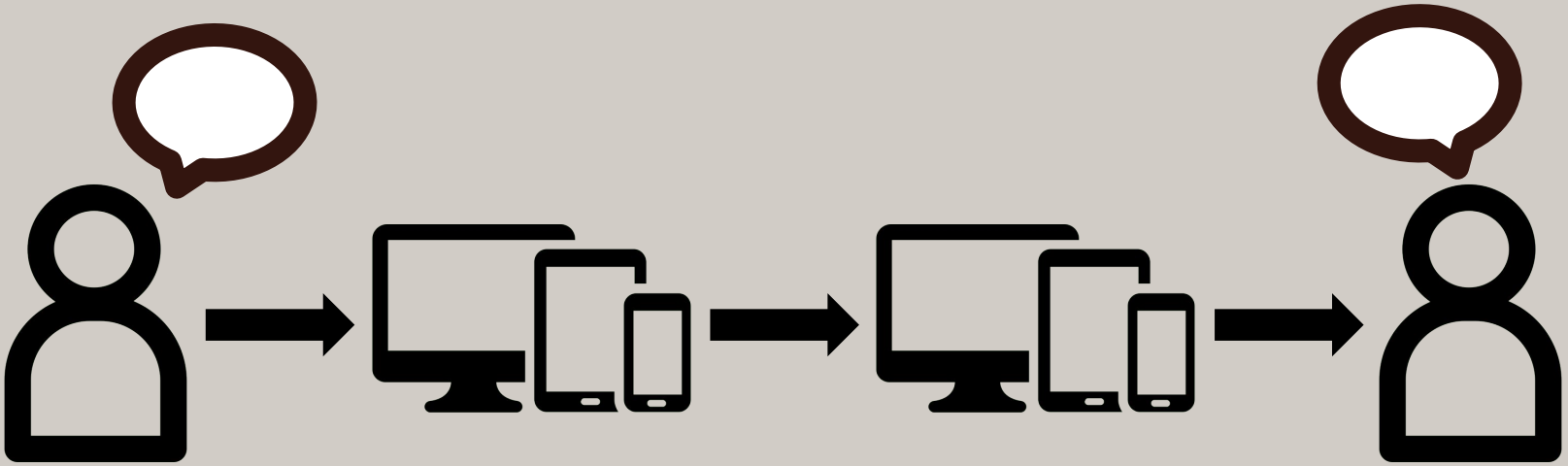
Todo mundo é um alvo

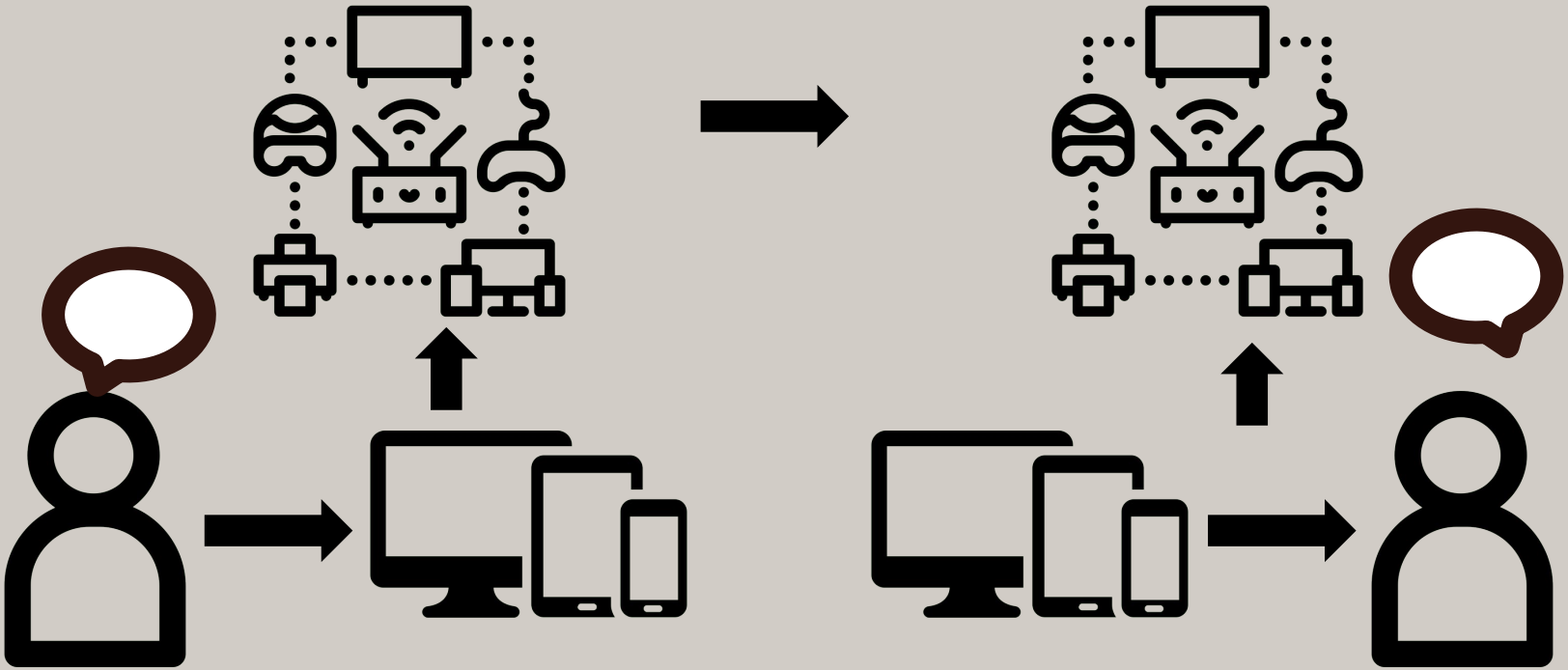
Estamos enfrentando **adversários e não hackers**

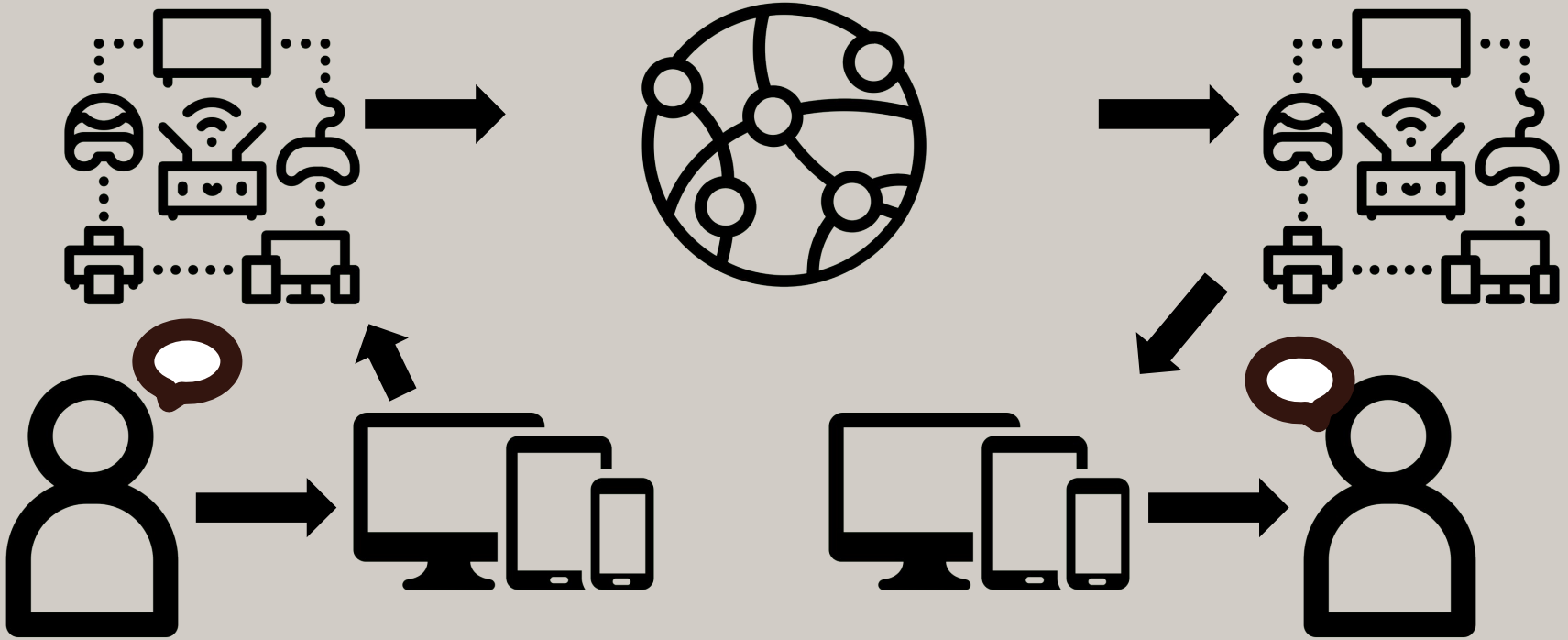
Diferentes contextos significam diferentes ameaças, diferentes desafios, **diferentes práticas** e ferramentas











Vulnerabilidade

Uma fraqueza no sistema de segurança. Por exemplo, na política, no procedimento, no design ou na implementação, que pode ser explorada para causar perda ou dano.

(Pfleeger/Pfleeger)

Superfície de Ataque

Soma das vulnerabilidades em um determinado sistema que são acessíveis a um adversário

Avaliação de riscos (modelo de ameaças)

O que queremos proteger?
De quem?
Quão provável é que necessitemos protegê-lo?
Quais são as consequências se falharmos?
Até onde queremos chegar para protegê-lo?

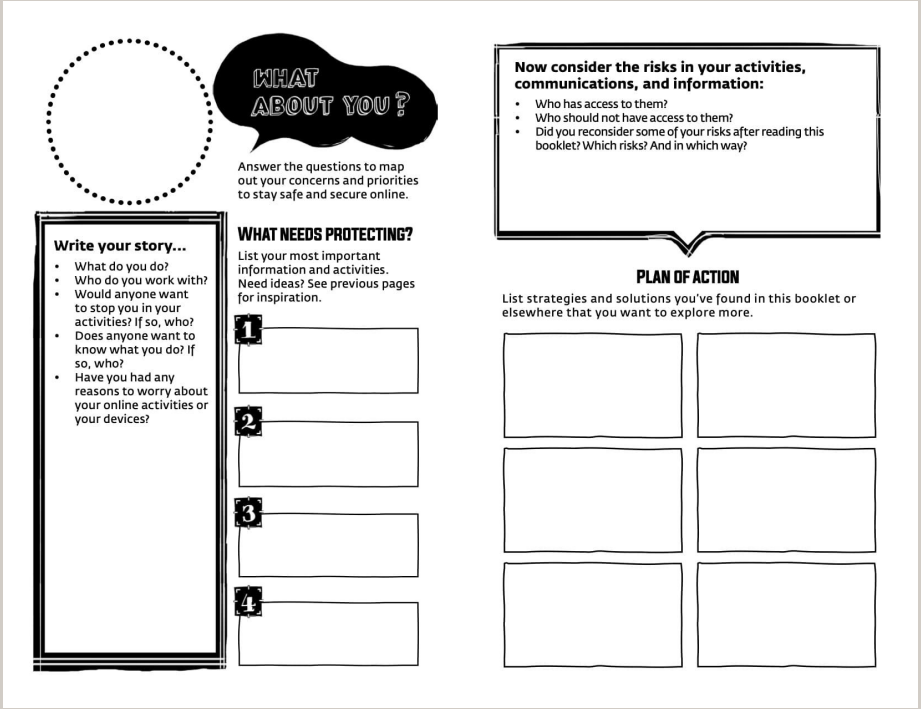
O que queremos proteger?

De **quem**?

Quão provável é que necessitemos protegê-lo?

Quais são as consequências se falharmos?

Até onde queremos chegar para protegê-lo?



https://drive.google.com/file/d/1Gw1tj63d0Zd4c6jW7AEZJJhI1tOw9vvu/view

Não é difícil, se você planejar

- **Respire e evite o pânico**
- **Planeje, se prepare com antecedência**
  - Avalie seus riscos (modelagem de ameaças)
  - Elabore alguns planos
    - Melhor ainda: elabore e documento planos e políticas se você é uma organização ou coletivo
- **Compartimentalize: cada coisa no seu devido lugar!**
  https://youtu.be/VFns39RXPrU?t=572
- **Tenha uma abordagem de segurança multicamadas**

Abordagem de segurança multicamadas

- **Mentalidade de Segurança**
- **Senhas**
- **Autenticação em dois fatores**
- **Criptografia de dados:**
  - em repouso
  - em trânsito
- **Confie, mas verifique**

Conveniência X Segurança/Privacidade

Conveniente

Padrões de bloqueio de tela
Impressões digitais
PINS
Senhas fáceis
Senhas com alguns caracteres
1 única senha
Dispositivos, aplicativos, sites e serviços gratuitos e / ou baratos
Fácil ou divertido de usar

Mais Seguro
(nada é 100% seguro)

Senhas longas
Senhas difíceis de adivinhar
Encriptação
VPNs
TOR
Serviços Pagos
Dispositivos mais caros
Aplicativos sem graçaaaa (mas mais seguros)

Comparando apps de mensagem

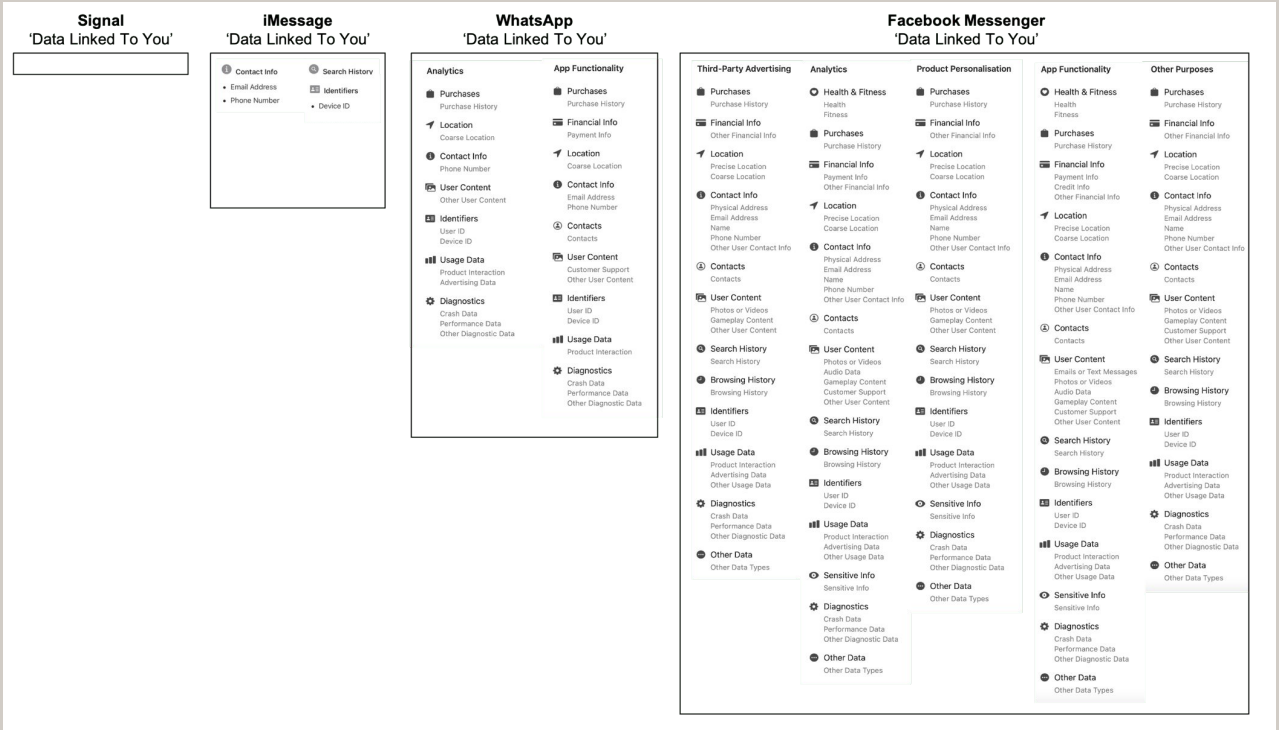
Whatsapp

- **Vantagens:**
  - Todo mundo usa
- **Desvantagens:**
  - Captura muitos metadados, que fornece muitas das informações sobre seus hábitos de uso e comunicação.
  - **Integrado ao Facebook e outros serviços que o FB é proprietários, juntando um número absurdo de informações sobre você**
  - **Conecta seu número de telefone à conta (identifica o usuário)**

Signal

- **Vantagens:**
  - **Melhor implementação de criptografia**
  - **Gera menos metadados**
  - NÃO conectado ao Facebook e outros negócios FB
  - Modelo de negócios não baseado em dados ou Publicidade (*)
  - **Autodestruição de mensagem**
- **Desvantagens:**
  - Nem todo mundo está lá
  - Conecta seu número de telefone à conta

Comparando apps de mensagem



Fonte: Forbes, based on Apple privacy "nutritional labels" Jan/2020

https://bit.ly/394d29d

Cheque suas senhas. Agora!

Verifique se sua senha foi exposta ou vazada de um site invadido com os seguintes links:

Have I Been Pwned?

https://haveibeenpwned.com

Have I Been Pwned? Password check

https://haveibeenpwned.com/Passwords

Tipos de ataque (pins / senhas)

Força bruta: tenta todas as combinações possíveis (geralmente usando um software simples)

Padrões mais comuns e prováveis, listas de combinações de pins e senhas
https://bit.ly/dejus0005

Ataque direcionado usando informações que o invasor aprende sobre o alvo

Pegue o dispositivo da vítima e instale um software malicioso

Engenharia Social / Phishing

Tipo de Ataque: Dicionário de PIN

Datas importantes: nascimento, morte, casamento, divórcio, formatura, etc.

Placas do carro, endereço, códigos postais, número do prédio.

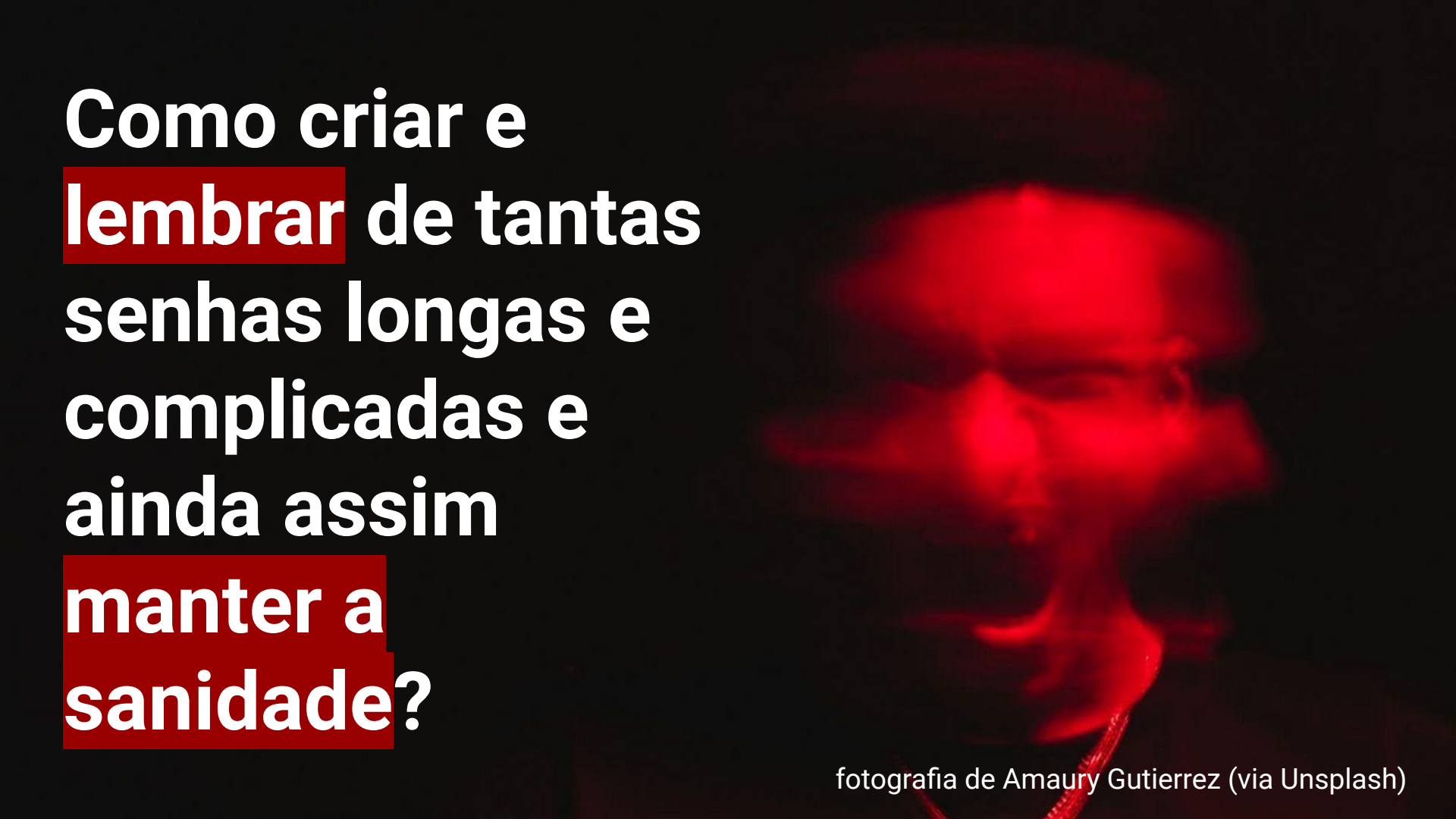
	PIN	Freq
#1	1234	10.713%
#2	1111	6.016%
#3	0000	1.881%
#4	1212	1.197%
#5	7777	0.745%
#6	1004	0.616%
#7	2000	0.613%
#8	4444	0.526%
#9	2222	0.516%
#10	6969	0.512%
#11	9999	0.451%
#12	3333	0.419%
#13	5555	0.395%
#14	6666	0.391%
#15	1122	0.366%
#16	1313	0.304%
#17	8888	0.303%
#18	4321	0.293%
#19	2001	0.290%
#20	1010	0.285%

Tipo de Ataque: Dicionário de Senhas

Palavras comuns;
Times esportivos;
Nomes comuns;
Nomes de familiares e pessoas significativas: pais, filhos, irmãos, esposa, marido, companheiros, namorado, namorada, animais de estimação, etc;
Políticos;
Títulos de filmes, canções, personagens populares;

Senhas segur… oops, melhores

Elas são grandes.
Elas são diferentes para cada dispositivo.
São difíceis de adivinhar.



fotografia de Amaury Gutierrez (via Unsplash)

Gerenciadores de Senha

Nos seus dispositivos:

KeePassXC (site em inglês, aplicação em português)

https://keepassxc.org/

basicamente um arquivo de banco de dados / planilha de senhas, criptografado, no seu dispositivo

Gerenciadores de Senha

Serviços na nuvem, que podem ser usados/sincronizados entre diversos dispositivos:

BitWarden

versões grátis e pagas, app pode ser configurado para português

https://bitwarden.com/

1Password

pago, site e app podem ser configurados para português

https://1password.com/pt/

LastPass

versões grátis e pagas, app pode ser configurado para português

https://www.lastpass.com/pt

Gerenciadores de Senha

Tome cuidado: todos os ovos numa cesta

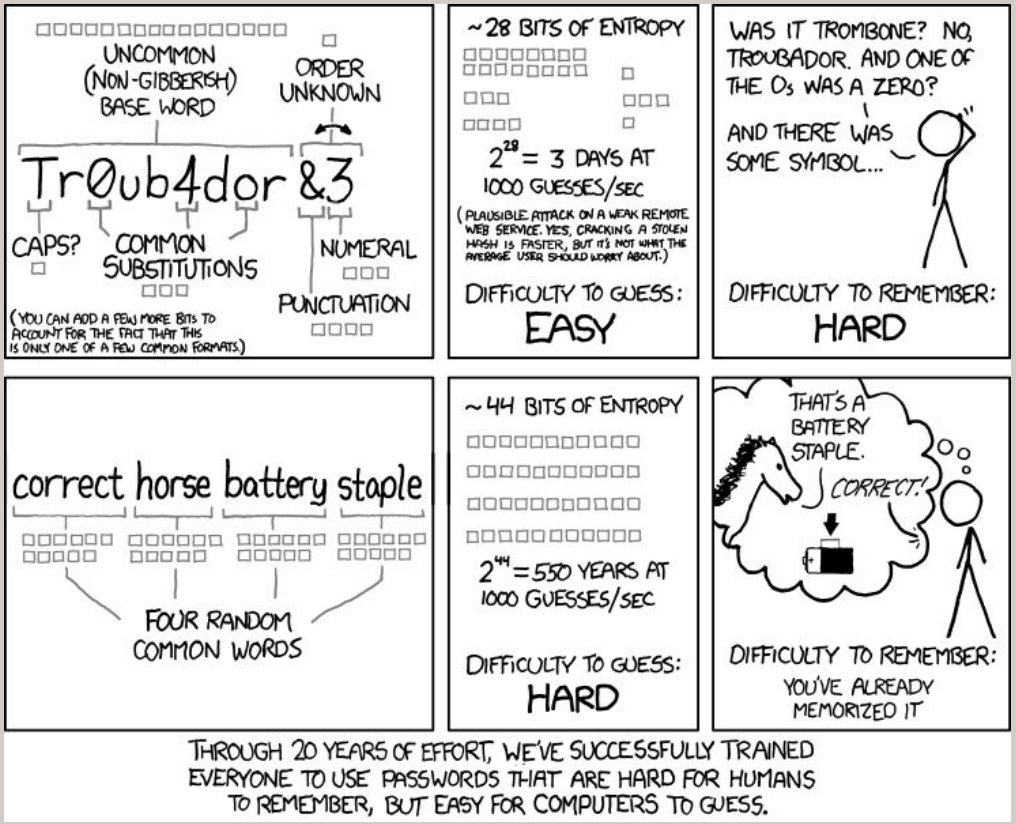
Considere não usá-lo para coisas realmente importantes:

A senha do próprio gerendiador
Seu email
Seu e-mail de trabalho
Computador pessoal
Telefone
Google, Facebook, iCloud, etc
Banco
Sistema/Plano de saúde

Frases-chaves

Grandes,
difíceis de adivinhar e
fáceis de lembrar.

Quanto mais absurdas ou inusitadas, mais fácil de lembrar.



Técnica 1: frases absurdas

melaodancante **(fácil de lembrar, porém frágil)**

MangasSaltitantesMelãoDançante

(*relativamente fácil de lembrar,* mais longa, mistura maiúsculas, minúsculas, acentos e sinais ortográficos)

JumpingsMangosMelãoDançante!

(além dos fatores da senha anterior, utilizada 2 idiomas)

2JumpingMangos1MelãoDançante!

(*igual anterior, mas acrescenta números e sinais de pontuação,* muito difícil de adivinhar, mas já começa a ficar difícil. Use com parcimônia)

Frases-chaves

2JumpingMangos!1MelãoDançante!And0Bananas:(

longa, tem diversos números e sinais de pontuação e utiliza 3 idiomas. O que a torna-a **muito difícil de adivinhar, muito difícil de lembrar e deixa seus amigos e parentes preocupados com sua sanidade. Pega leve e volte uma casa!**

Frases-chaves

- **Estes exemplos são claramente exagerados (mas não muito)**
- **Se você sabe mais que um idioma, mescle palavras em cada idioma.**
- **Listas de palavras ajudam a treinar a técnica no começo. Se possível, uma lista mental, não física. E evite coisas que as pessoas sabem que você gosta muito.**

Frases-chaves

- **Verifique se o site ou aplicação aceita emoji na senha pois, em teoria, são considerados textos. Muitos são, tecnicamente, 2 caracteres.**
- **Você pode utilizar um emoji no lugar de um caracteres especial (evite utilizar como substituto a palavras).**
- **Evite utilizar um emoji que você use com frequência em conversas. Escolha um bem inusitado e que dificilmente utilizará em conversas.**
- **Exemplos:**
  - 2JumpingMangos1MelãoDançante😆
  - 2JumpingMangos1MelãoDançante🔚
  - 2JumpingMangos🔶1MelãoDançante🔚

Técnica 2: mesclando listas de palavras

(explicado apenas em oficinas e treinamentos. Mais informação no penúltimo slide ou via contrate@celsobessa.com.br)

Autenticação com múltiplos fatores

Também conhecido como autenticação de 2 fatores, 2FA ou token.

SMS, Google Authenticator, Authy, códigos de backup, biometria quando acompanhada de senha ou outro fator.

Google Authenticator: https://www.google.com/landing/2step/?hl=en

Autenticação com múltiplos fatores

Evite usar SMS, é fácil de ser interceptado.

Use SMS para a configuração inicial e, em seguida, configure o aplicativo Google Authenticator ou Authy em seu telefone celular, imprima ou anote os códigos de backup e remova a opção de SMS.

Criptografia

Dados em trânsito:

dados sendo transmitidos, por exemplo, pela Internet, de seu navegador em um computador, seu e-mail ou um aplicativo em um telefone.

dados em repouso:

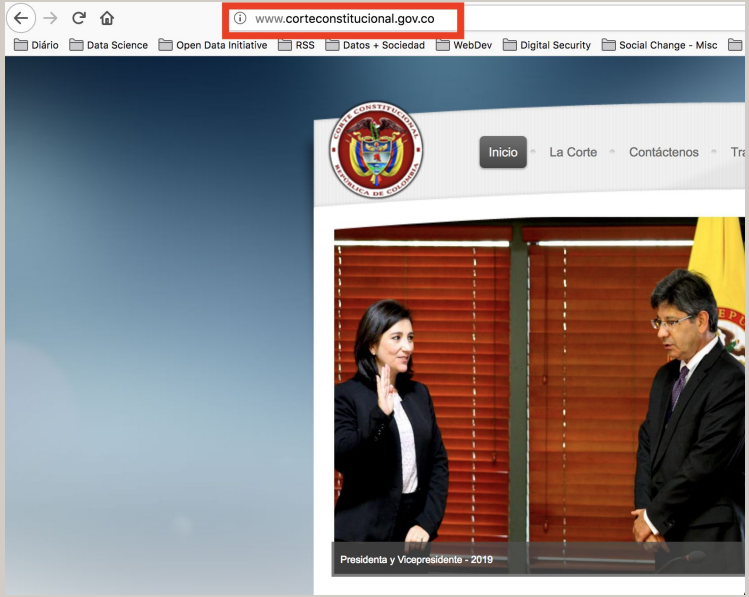
dados armazenados em um smartphone ou o disco/HD do computador.

Criptografia em trânsito - Transmissão de dados na web

Certifique-se que o endereço seja HTTPS e não HTTP.

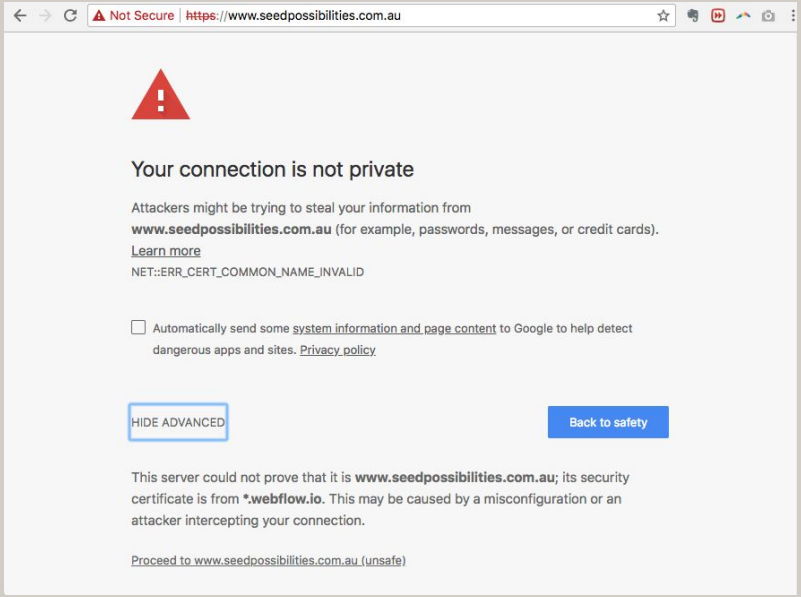
O cadeado verde indica o uso de HTTPS.

Criptografia em trânsito - Transmissão de dados na web



Tenha certeza que o endereço é **HTTPS** e não HTTP.

Criptografia em trânsito - Transmissão de dados na web



Se você vir uma tela e um aviso como este, saia correndo.

Criptografia de dados em trânsito - navegador

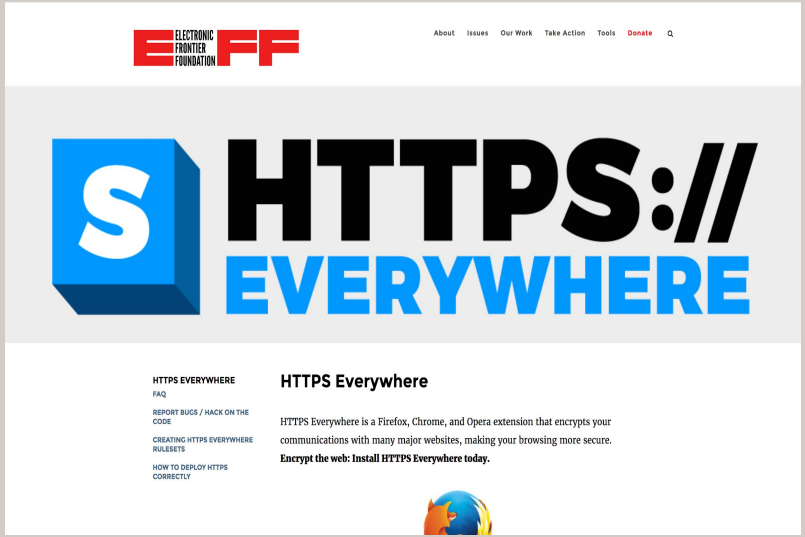
HTTPS Everywhere (Windows, MacOs)

https://www.eff.org/https-everywhere

para smartphones, disponível apenas para Firefox no Android.

Extensão HTTPS Everywhere

Força a versão HTTPS, se disponível. Se não, interrompe a conexão.

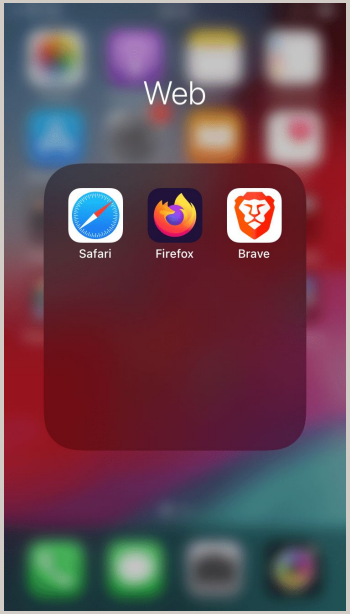


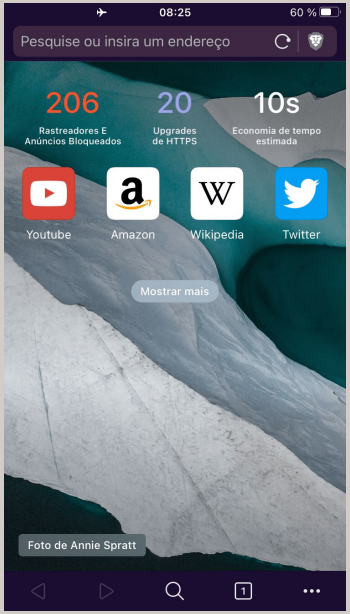
Criptografia de dados em trânsito - navegador

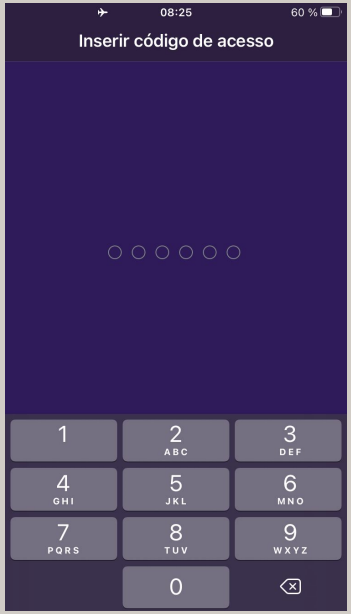
Brave browser (Windows, MacOs, Android and iOS)

https://brave.com/

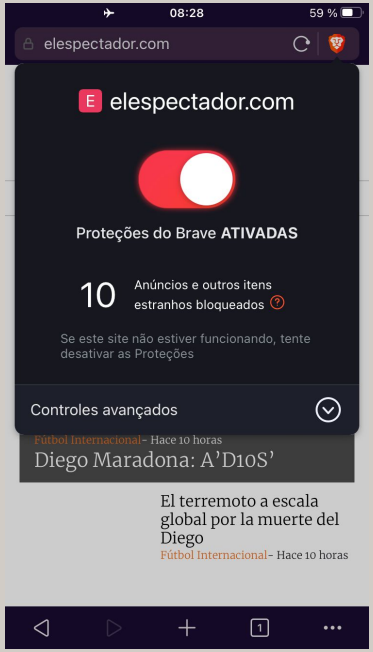
Possui HTTPS Everywhere integrado, disponível tanto para computadores quanto para smartphones.

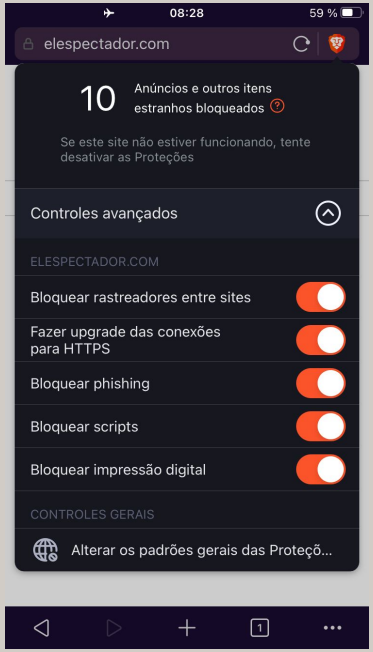

Web
Safari
Firefox
Brave


08:25
60 %
Pesquise ou insira um endereço
206
Rastreadores E Anúncios Bloqueados
20
Upgrades de HTTPS
10s
Economia de tempo estimada
Youtube
Amazon
Wikipedia
Twitter
Mostrar mais
Foto de Annie Spratt


08:25
60 %
Inserir código de acesso
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0


08:26
60 %
elespectador.com
EL ESPECTADOR
Jueves 26 De Noviembre
Fútbol Internacional- Hace 9 horas
Diego Maradona: A'D10S'
El terremoto a escala global por la muerte del Diego
Fútbol Internacional- Hace 10 horas


08:28
59 %
elespectador.com
elespectador.com
Proteções do Brave ATIVADAS
10
Anúncios e outros itens estranhos bloqueados
Se este site não estiver funcionando, tente desativar as Proteções
Controles avançados
Fútbol Internacional- Hace 10 horas
Diego Maradona: A'D10S'
El terremoto a escala global por la muerte del Diego
Fútbol Internacional- Hace 10 horas


08:28
59 %
elespectador.com
10
Anúncios e outros itens estranhos bloqueados
Se este site não estiver funcionando, tente desativar as Proteções
Controles avançados
ELESPECTADOR.COM
Bloquear rastreadores entre sites
Fazer upgrade das conexões para HTTPS
Bloquear phishing
Bloquear scripts
Bloquear impressão digital
CONTROLES GERAIS
Alterar os padrões gerais das Proteçõ...


08:27
59 %
elespectador.com
EL ESPECTADOR
Jueves 26 De Noviembre
Suscríbete
Iniciar Sesión
Fútbol Internacional- 25 nov. 2020 - 10:25 p. m.
Diego Maradona: A'D10S'
Al continuar navegando el usuario acepta que el portal web, propiedad de Comunican S.A. en el que se encuentra navegando, haga uso de Cookies de acuerdo con esta Política
Entendido

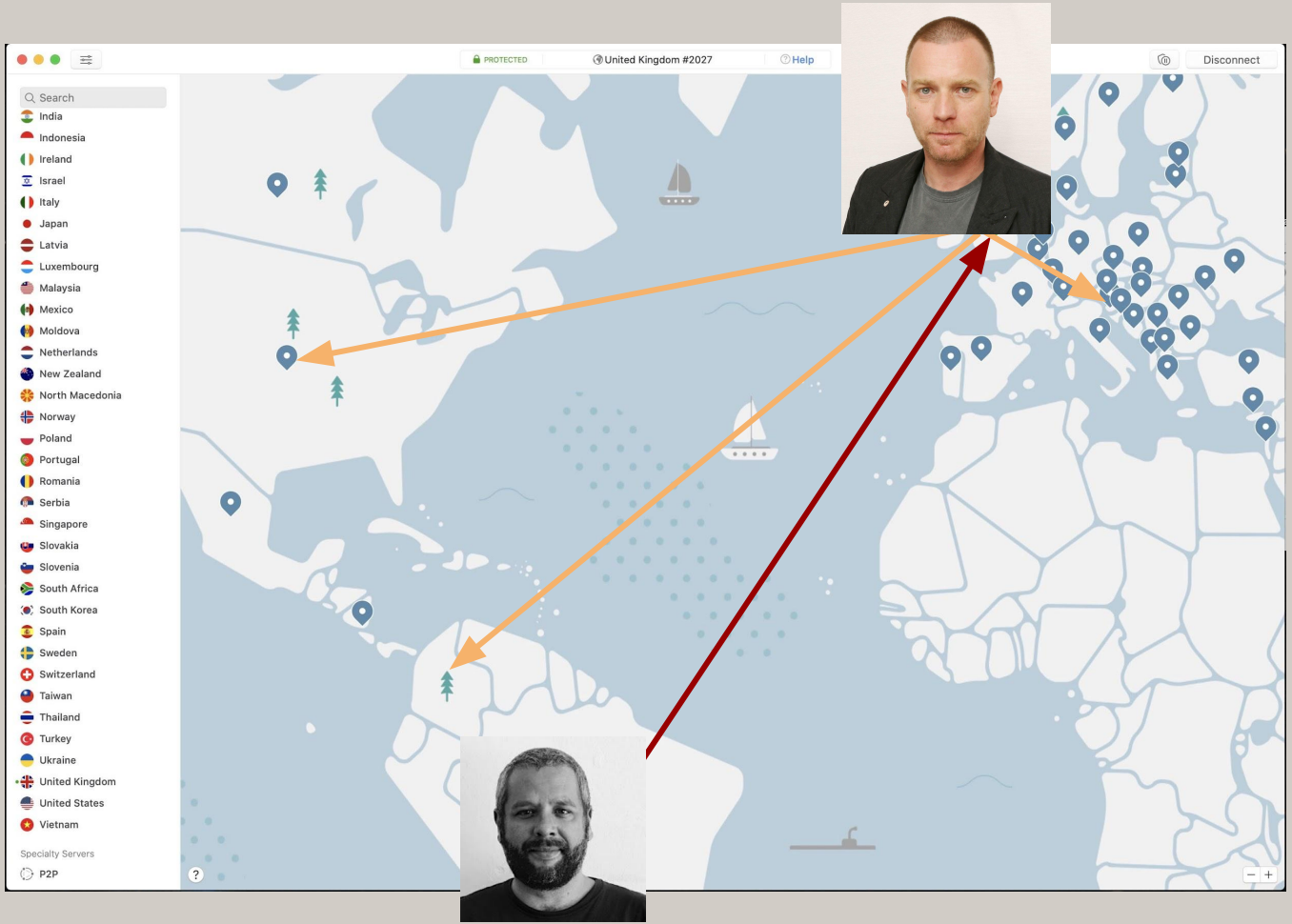
Criptografia de dados em trânsito - todos os programas no dispositivo

Para mascarar seu IP e criptografar todos os dados que fluem de e para o seu dispositivo, utilize uma boa VPN (Virtual Private Network).

VPNs


PROTECTED
United Kingdom #2027
Help
Disconnect
Search
India
Indonesia
Ireland
Israel
Italy
Japan
Latvia
Luxembourg
Malaysia
Mexico
Moldova
Netherlands
New Zealand
North Macedonia
Norway
Poland
Portugal
Romania
Serbia
Singapore
Slovakia
Slovenia
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Turkey
Ukraine
United Kingdom
United States
Vietnam
Specialty Servers
P2P

VPNs


PROTECTED
United Kingdom #2027
Help
Disconnect
Search
India
Indonesia
Ireland
Israel
Italy
Japan
Latvia
Luxembourg
Malaysia
Mexico
Moldova
Netherlands
New Zealand
North Macedonia
Norway
Poland
Portugal
Romania
Serbia
Singapore
Slovakia
Slovenia
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Turkey
Ukraine
United Kingdom
United States
Vietnam
Specialty Servers
P2P

VPN para mascarar IPs e criptografar toda a conexão

Basicamente, você se conecta aos servidores VPN e seus servidores se conectam aos sites e serviços que você deseja. Dessa forma, seu endereço IP é mascarado.

VPN para mascarar IPs e criptografar toda a conexão

Boas VPNs criptografam todos os seus dados e não mantém nenhum registro (ou quase todos os registros) de metadados que podem identificar você.

VPN para mascarar IPs e criptografar toda a conexão

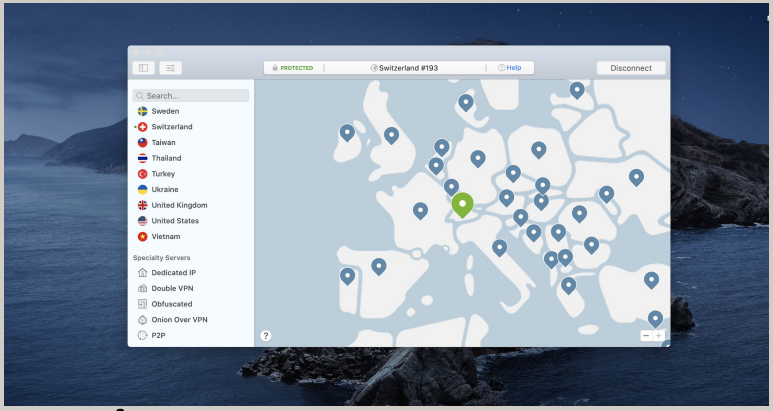
As melhores VPNs não pedem informações identificáveis como e-mail para inscrição, aceitam Bitcoin ou dinheiro vivo para pagamentos e não estão em jurisdições do chamado 5 eyes (5 olhos):

https://www.oficinadanet.com.br/seguranca/24804-o-que-e-a-vigilancia-five-eyes-usuarios-de-vpn-cuidado

https://web.archive.org/web/20220407172712/https://www.oficinadanet.com.br/seguranca/24804-o-que-e-a-vigilancia-five-eyes-usuarios-de-vpn-cuidado

Mullvad

Servidores rápidos e confiáveis ao redor do mundo.
Até seis dispositivos.
Mantém quase nenhum metadato.
Fundadores/executivos manjam dos paranauê*.

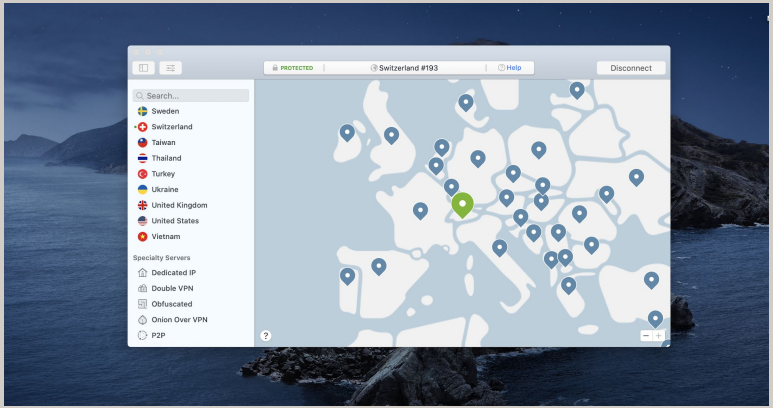


Não precisa de email e nem exige email para criar conta.
Mais caro, mas aceita bitcoin e pagamento em dinheiro, que facilita o anonimato.

* https://www.qualeagiria.com.br/giria/manjar-dos-paranaue/

NordVPN

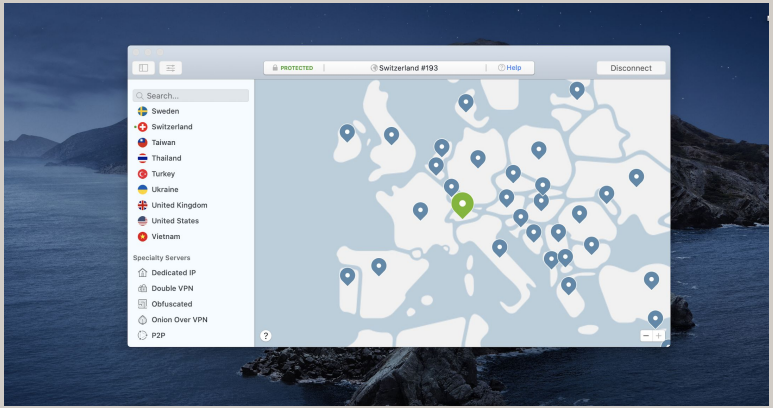
Servidores rápidos e confiáveis ao redor do mundo.
Você pode usar até seis dispositivos, incluindo telefone.
Mantém poucos metadatos.



Pago (mas relativamente acessível);
Usa informação de email e cartão de crédito para criação da conta, o que serve para te identificar, por exemplo, num processo.

ProtonVPN

Servidores rápidos e confiáveis ao redor do mundo.
Até seis dispositivos
Mantém poucos metadatos.
Jurisdição: Suíça, que valoriza privacidade e estado de direito.



Pago (mas relativamente acessível);
Usa informação de email e cartão de crédito para criação da conta, o que serve para te identificar.

Criptografia de e-mail

Criptografa apenas o conteúdo de uma mensagem, os metadados ainda são vísiveis: remetente, destinatário, horário, endereço IP, assunto, etc, é público.

Utiliza duas chaves criptográficas, uma pública usado para criptografar a mensagem e verificar a identidade, e uma privada, usado para descriptografar a mensagem e que deve ser compartilhada apenas com a pessoa que você deseja que leia a mensagem.

Protonmail

Orientado ao consumidor serviço de e-mail criptografado, usado principalmente no navegador, cuida de todos os aspectos técnicos de gerar e gerenciar chaves de criptografia. Eles não podem ler suas mensagens (dados criptografados em servidores). Empresa e servidores na Suíça, protegidos por rígidas leis de privacidade suíças.

Para usuários pagos, oferece um programa que permite seu uso com um cliente de e-mail como outlook, mail ou thunderbird.

Protonmail

Gratuito

- **Espaço máximo de 500mb;**
- **Endereços com o sufixo @protonmail.com ou @pm.me**

Plano pago (5-30 USD / usuário / mês)

- **Mais espaço;**
- **múltiplos endereços;**
- **suporte a domínios customizados (E.g. @celsobessa.com.br)**

Protonmail

Se você não pode pagar por uma conta, abra uma conta gratuita e a use apenas para as conversas mais importantes e confidenciais.

https://protonmail.com
https://pr.tn/ref/HTQ3VDHEFNEG (link de afiliado)

Criptografia de dados do telefone

Celulares Apple (iOS):

Ativado por padrão ao usar senhas

Android:

Depende do fabricante e da versão Android. Habilitado por padrão em telefones mais novos e mais sofisticados. Caso contrário, precisa ser ativado nas configurações (criptografar disco e inicialização segura)

Criptografia de dados de disco MacOs

MacOS:

A criptografia pode ser feita em todo o disco ativando o FileVault em Configurações do sistema> Segurança.

Use VeraCrypt para criar volumes encriptados no disco do dispositivo ou um Memory Stick USB.

https://support.apple.com/en-us/HT204837
https://www.veracrypt.fr
https://www.veracrypt.fr/en/Documentation.html
https://www.veracrypt.fr/en/Creating%20New%20Volumes.html

Criptografia de dados de disco do Windows

Use VeraCrypt para criar uma partição ou disco criptografado do sistema, para criar volumes criptografados no dispositivo ou em um stick de memória USB.

https://www.veracrypt.fr
https://www.veracrypt.fr/en/System%20Encryption.html
https://www.veracrypt.fr/en/Creating%20New%20Volumes.html
https://www.veracrypt.fr/en/Documentation.html

obrigado!
gracias!
thanks!
شكرًا
תודה!
danke!
merci!
arigato!
go raibh maith agat!

Obrigado também a Ewan McGregor pela participação!

Perguntas?

Fim!

Ma é o fim memu?

Para acessar a fase bônus e conteúdos extras, repitam:

cima, cima;
baixo, baixo;
esquerda, direita;
esquerda, direita;
B,A;
start!

https://pt.wikipedia.org/wiki/C%C3%B3digo_Konami


MARIO
003250
×09
WORLD
1-1
TIME
308
★BONUS★

Bônus: recursos sobre integridade digital

https://www.frontlinedefenders.org/pt/manual-de-seguran%C3%A7a

https://ssd.eff.org/pt-br

https://securitycheckli.st/

Bônus: recursos sobre integridade digital

https://securityinabox.org/pt/

https://www.privacidade.digital/

Bônus: vitórias rápidas

Navegadores orientados à privacidade (ordenados por recursos de privacidade)

Brave: https://brave.com/

Firefox: https://www.mozilla.org/en-US/firefox/new/

(good option, not as private as the two above, but less broken sites)

Mecanismos de pesquisa alternativos:

SearchEncrypt: https://www.searchencrypt.com (extremo)

DuckDuckGo: https://duckduckgo.com/ (minha opção pessoal)

Ferramentas de bloqueio de publicidade e rastreamento (Chrome e Firefox Desktop)

Ghostery: https://www.ghostery.com/

Privacy Badger: https://www.eff.org/privacybadger

DuckDuckGo Privacy Essentials: https://duckduckgo.com/app

Bônus: vitórias rápidas

Tampa da câmera / bloqueador de áudio

Bloqueia a gravação de vídeo e áudio de seus dispositivos

https://j.mp/CameraCoverAmazon
https://j.mp/AudioJackBlocker

Gaiola de Faraday

Um invólucro usado para bloquear campos eletromagnéticos como wi-fi, rede celular, ondas de rádio, etc.

Se você estiver em uma reunião confidencial e quiser ter certeza de que os celulares dos participantes não estão transmitindo, você pode usar seu microondas como uma gaiola de faraday!

https://pt.wikipedia.org/wiki/Gaiola_de_Faraday
https://youtu.be/VFns39RXPrU?t=561

Bônus: informação extra

VPNs:

NordVPN (pago): https://go.nordvpn.net/SH2gx
ProtonVPN (pago e versão grátis limitada): https://protonvpn.com/pt_br/
Mullvad: https://mullvad.net/pt/

Use navegador TOR para coisas realmente sensíveis.
É mais lento, porém mais seguro. Como uma VPN com esteróides.
https://www.torproject.org/pt-BR/

Guias sobre TOR:

https://ssd.eff.org/pt-br/module/como-utilizar-o-tor-para-windows
https://ssd.eff.org/pt-br/module/tutorial-como-usar-o-tor-no-macos
https://ssd.eff.org/pt-br/module/tutorial-como-usar-o-tor-no-linux

TOR

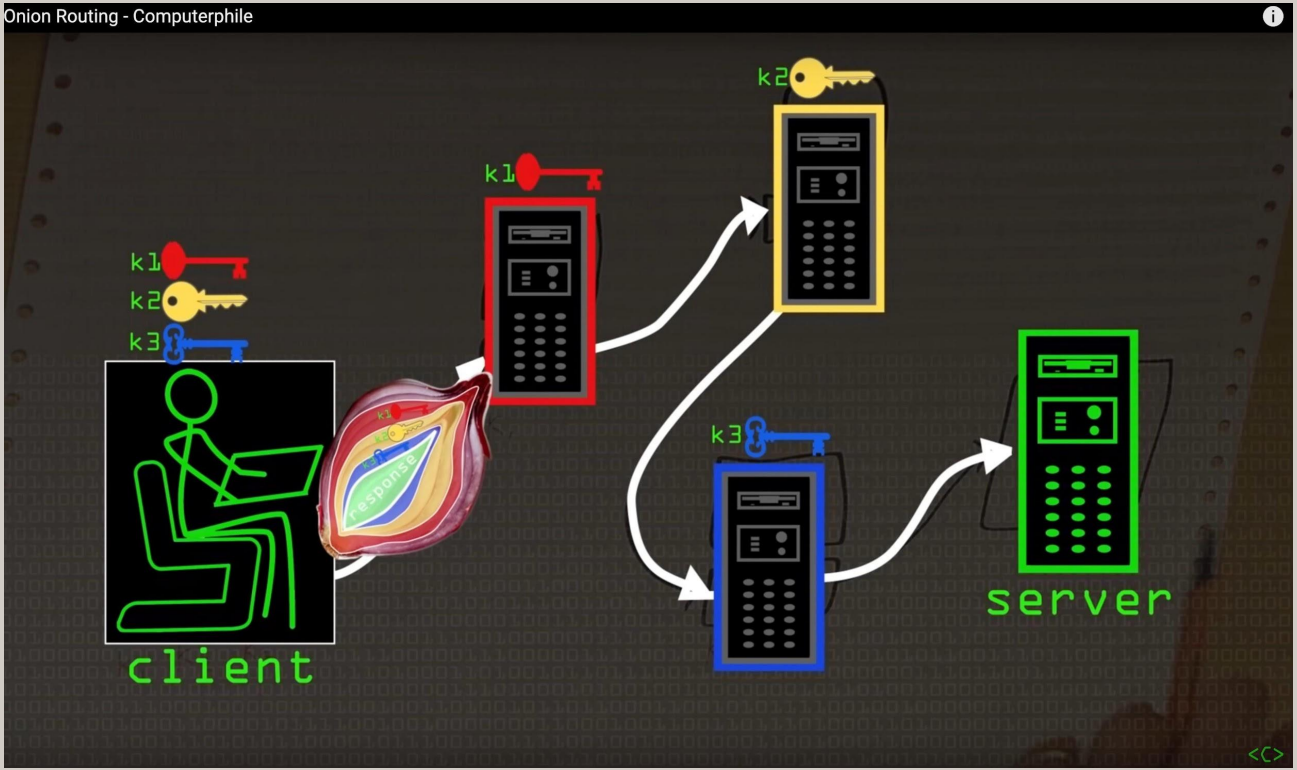
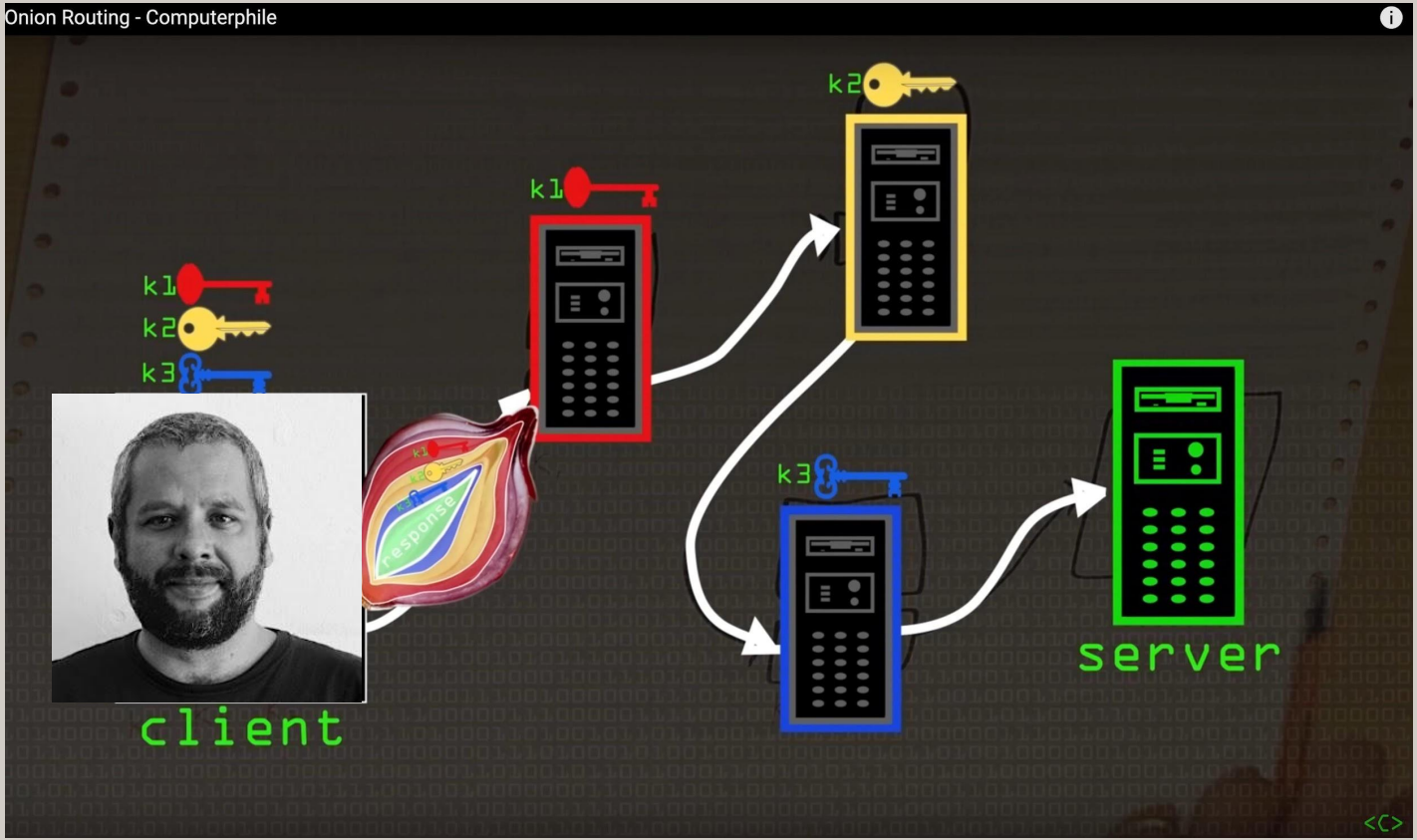
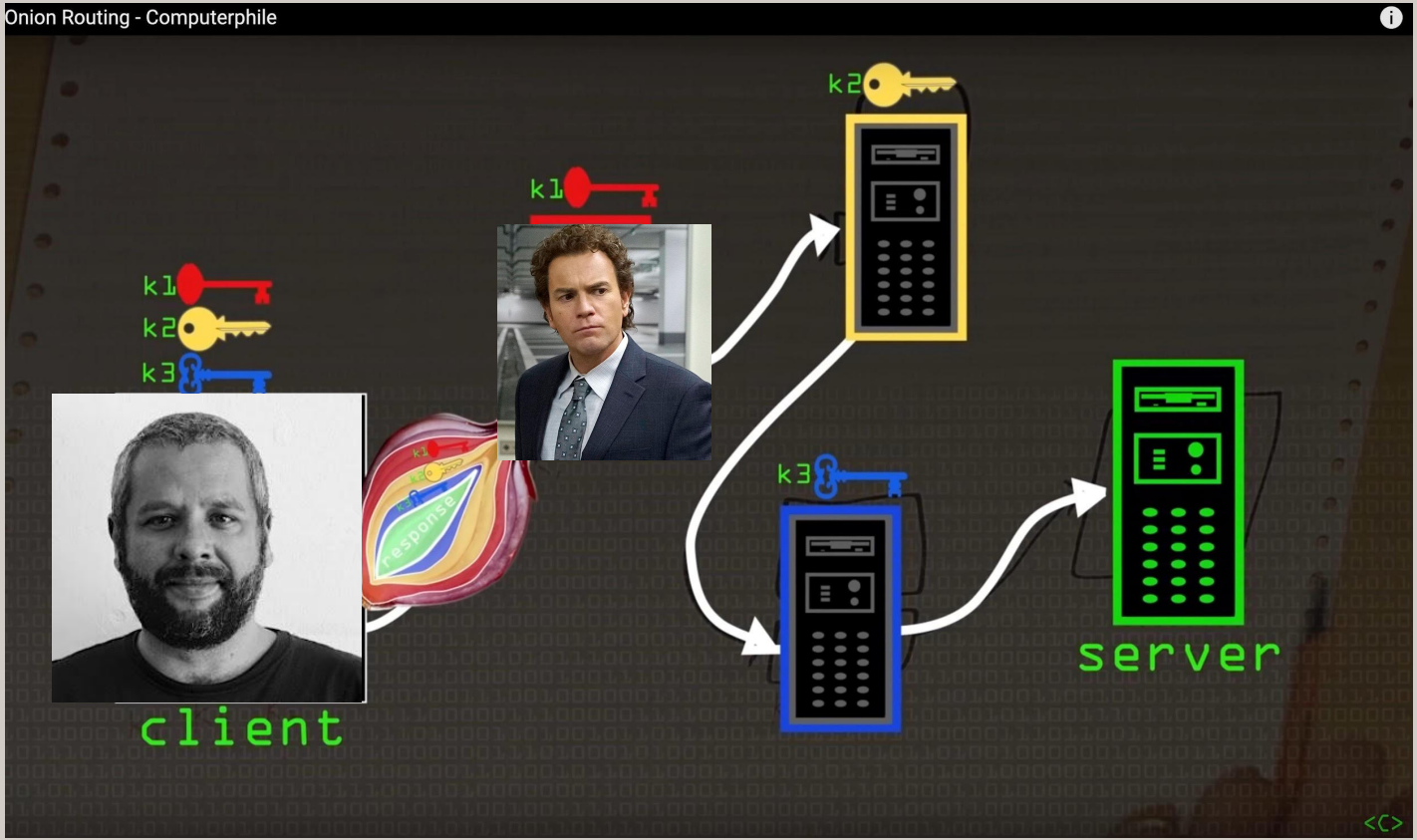


Diagrama mostrado no vídeo sobre TOR do ótimo canal de YouTube Computerphile (em inglês):
https://www.youtube.com/watch?v=QRYzre4bf7I

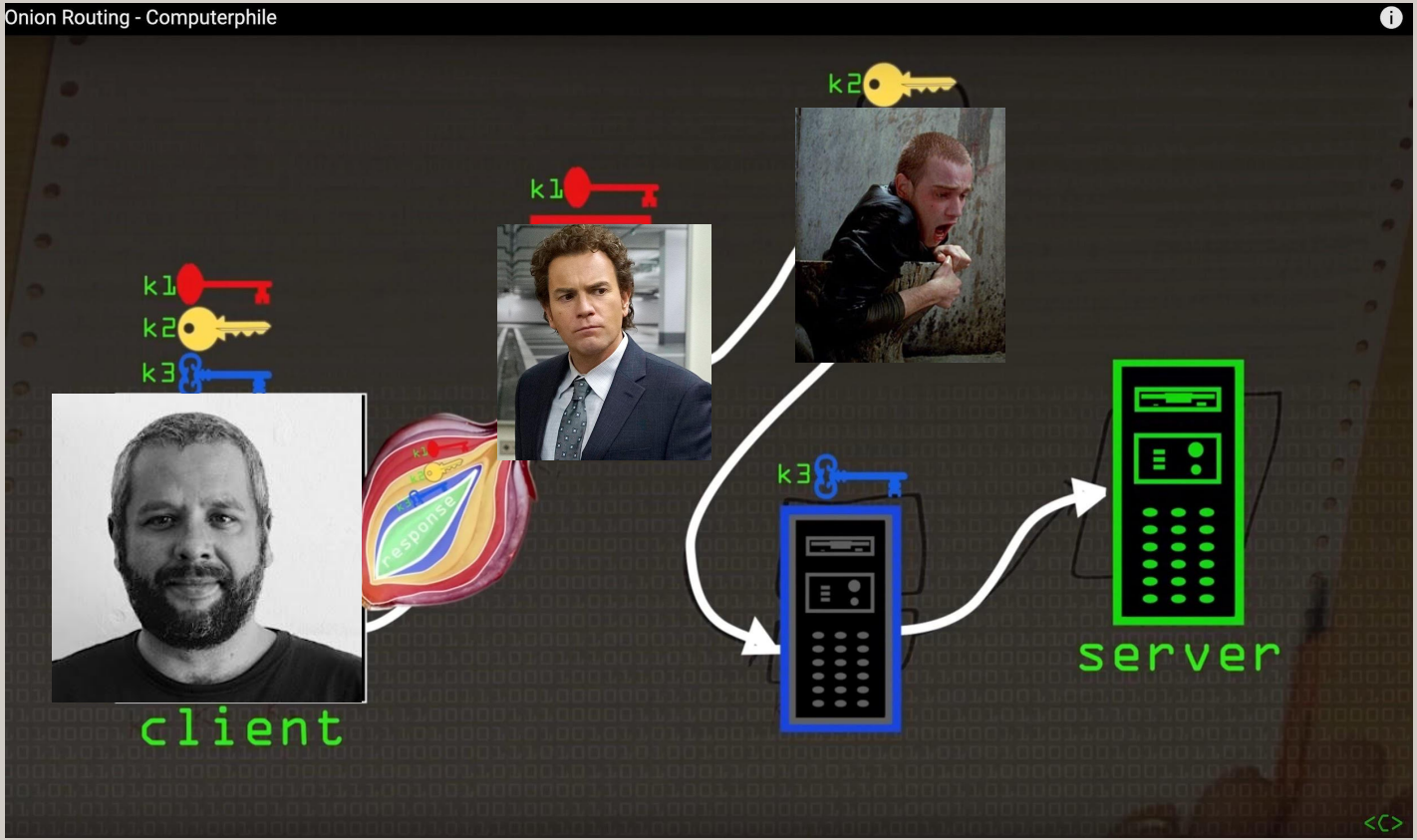
TOR


Onion Routing - Computerphile
k1
k2
k3
k1
k2
k3
response
client
server

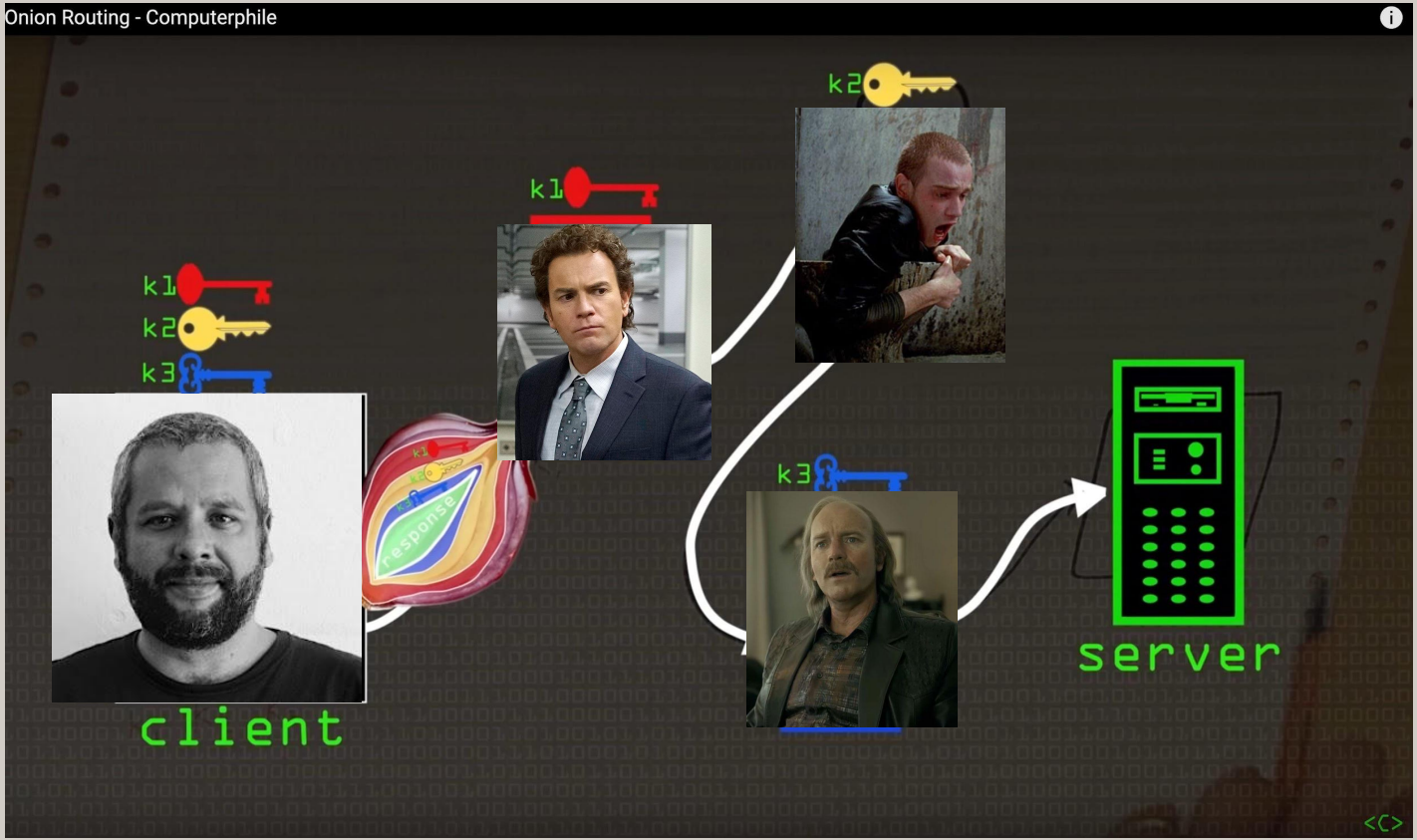
TOR


Onion Routing - Computerphile
k1
k2
k3
k1
k2
k3
response
client
server

TOR


Onion Routing - Computerphile
k1
k2
k3
k1
k2
k3
response
client
server

TOR

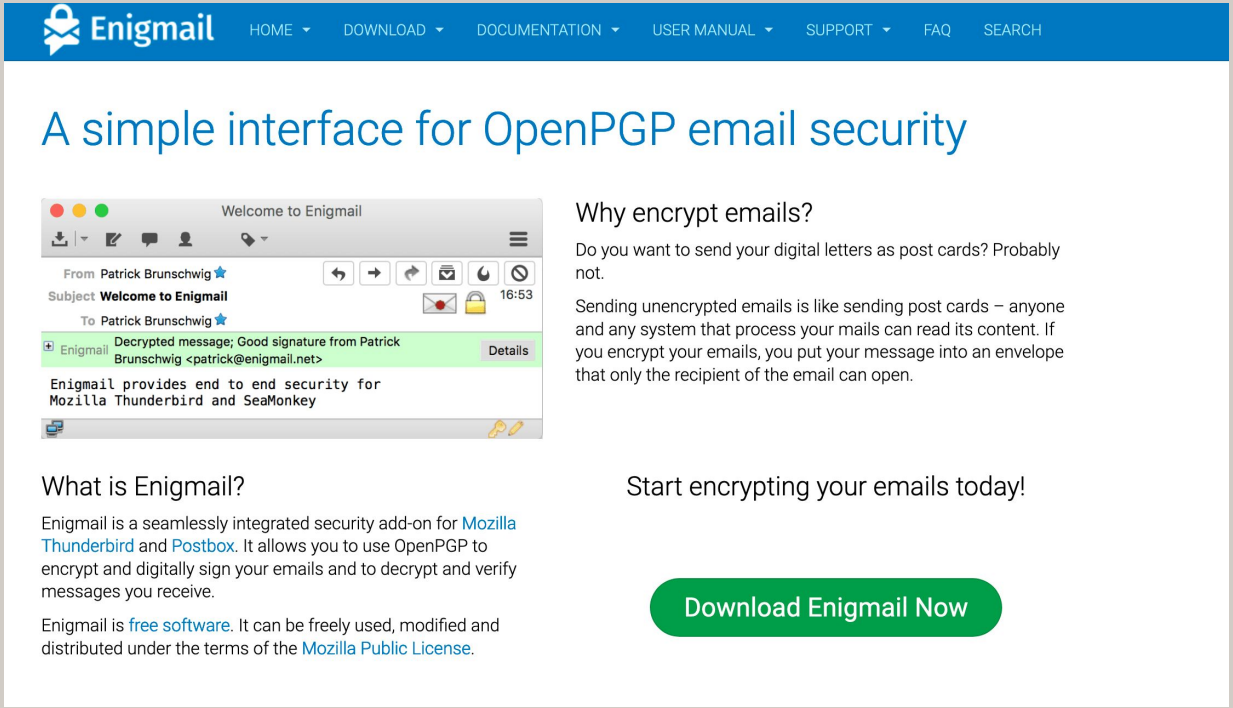

Onion Routing - Computerphile
k1
k2
k3
k1
k2
k3
response
client
server

Thunderbird + Enigmail PGP

Thunderbird é um cliente de e-mail, alternativa aos programas como o Outlook. Enigmail PGP é um plugin para Thunderbird que torna mais fácil criar e gerenciar chaves de criptografia e enviar e receber e-mail criptografado.

https://ssd.eff.org/en/module/how-use-pgp-windows
https://ssd.eff.org/en/module/how-use-pgp-mac-os-x
https://ssd.eff.org/en/module/how-use-pgp-linux

Thunderbird + Enigmail PGP



Veracrypt

(sessão prática disponível apenas em treinamentos e oficinas)

Site oficial do Veracrypt:
https://www.veracrypt.fr

Mais perguntas?

Treinamentos em segurança digital

Se desejar uma oficina de segurança digital para um grupo ou sessões 1:1, entre em contato via contrate@celsobessa.com.br .

Treinamentos e sessões para ativistas de direitos humanos, jornalistas, coletivos e veículos de mídia independente são gratuitos[1] ou com valor simbólico.

1: a depender de agenda ou patrocínio

Celso Bessa

contrate@celsobessa.com.br
PGP Fingerprint
96efd952eeab8a87084d04aa8c77bda00e204995

*transparência: alguns dos links mencionados na apresentação são links de afiliados. O que significa que se você contratar o serviço através deles, eu posso vir a ganhar uma comissão, um bônus em minha assinatura, etc.