Navegação Segura na Web

Para uma navegação mais segura na web, vejam abordagens abaixo.

A forma como navegamos na www, os conteúdos a que acedemos, quem tem acesso a esse histórico de navegação e como é usado, é motor que gera anualmente biliões.

Gestão de Credenciais

Verifiquem se os endereços de e-mail que usam estão comprometidos em

https://haveibeenpwned.com/

Usem um gestor de credenciais,Proton Pass, Bitwarden ou 1Password (uso Proton Pass, que faz também a gestão 2FA), explicado mais abaixo), e definam credenciais de login específicas para cada website, em vez de usarem as API de autenticação Google, Facebook, etc).

Para gerar boas passwords, uso a função do Proton Pass sendo que tendo a criar passwords com um mínimo de 21 caracteres (minúsculas, maiúsculas, números e caracteres expeciais).

Como solução local em ambientes segregados (também funciona com integração com browser), o KeePassXC é excelente.

Favoritos

Salvaguardem os vossos favoritos com Raindrop.

Redes Sociais

Comecem a equacionar se pretendem continuar reféns de plataformas como Facebook, Twitter e Youtube, etc, onde a liberdade de expressão é inexistente e toda a informação lá colocada é capitalizada (Big Data) e usada contra nós.

Como alternativas, têm Nostr, Mastodon, Gab, Gettr, MeWe, Brighteon, BitChute e BrandNewTube.

Smartphones

Nos telemóveis é comum o uso de PIN com 4 dígitos. Se possível, usem mais complexo, com bloqueio automático não superior a 1 minuto.
Se não estão a precisar, desativem o Bluetooth e Localização. Revejam também que aplicações têm autorização para usar as mesmas.
As fotos que tiram com o smartphone, e se o acima estiver ativo, ficam com informação sensível disponível para o mundo quando as publicam nas redes sociais.

Se conseguirem usar GrapheneOS ou LineageOS, tanto melhor.
Mais, podem sempre obter um número que não vos caracteriza para usar em todo o lado, como por exemplo, Hushed.

Substituam o Google Maps por Organic Maps.

Mensagens (SMS)

O WhatsApp não é seguro (o Facebook tem acesso ao que lá é escrito. O Telegram é mais seguro mas prefiro o Signal. Mais seguro é o Session, que nem o número de telemóvel se tem de declarar pois usa o conceito de chave pública/privada e assenta na rede OXEN.

Outras excelentes opções: Wire, Threema

Blocos de Notas

Apesar de usar prolificamente o Evernote há mais de uma década, existem plataformas que já trazem encriptação ponto-a-ponto e fazem essencialmente o mesmo. São exemplos: Obsidian, Notesnook, Skiff, Standard Notes e Anytype. Uso o Notesnook para o efeito, e estou a descontinuar o Evernote.

Clientes de E-mail

Grande parte usa o Gmail para troca de correio eletrónico. Como deverão saber, o facto de ser livre quer dizer que ao usarmos estamos a ser o produto, ou seja, a Google vê tudo o que lá escrevemos e usa isso para nos apresentar publicidade direcionada.
Temos excelentes alternativas como o Skiff, Protonmail, LedgerMail (assenta na blockchain XDC mas só permite troca de correio eletrónico entre endereços LedgerMail) ou Mailchain (e-mail a usar as chaves públicas de wallet pessoal sendo que só o destinatário - que tem a chave privada - consegue abrir o mesmo).

Mantenham a privacidade do vosso endereço de correio eletrónico com aliases gerados para cada situação com Anonaddy ou SimpleLogin.

Autenticação

Implementem autenticação de dois factores (Two-factor authentication (2FA)).
Aegis, FreeOTP (para iPhone), Authy, Google Authenticator, Yubikey e OnlyKey. Uso Aegis para geração TOTP e várias Yubikey.

Pagamentos Online

Protejam os vossos cartões de crédito com cartões virtuais - Privacy.

DNS

Alterem os DNS's para providers seguros e rápidos:
Cloudflare ou Quad9

Notas: Se usarem o Portmaster (abaixo), com DNS roteado para Cloudflare com Filtro Malware, já estarão muito bem.

Nos smartphones, como não têm o Portmaster disponível, considerem usar **NextDNS**. Se bem configudado, um teste aqui, devolverá os três primeiros bem sucedidos.

Firewall e Antivírus

Tenham todas as funcionalidades do Windows Defender ativas e no smartphone o Sophos Intercept X for Mobile.

Como firewall, usem Portmaster (se pagarem, terão disponível SPN (Safing Privacy Network) activo) e Glasswire

Atualizações

Mantenham atualizados os Drivers, Sistema Operativo e Aplicações.

Armazenamento

Façam backup do que têm na Cloud (Google Drive, OneDrive, Box, etc) para um disco externo vosso e deixem de usar as online que são livres.Para acrescida segurança, podem encriptar o conteúdo com VeraCrypt e usem Free File Sync para estabelecer rotina de backup para o mesmo.

Se são livres, vocês são o produto e a qualquer momento podem ser impedidos de aceder ao conteúdo e não existe garantia de que só vocês acedem ao mesmo.

São bons exemplos de armazenamento seguro, ProtonDrive, Skiff ou StorX, se pretendem ter os vossos ficheiros online.

Cripto moedas

Se possuem moeda digital, adquiram uma carteira física (por ex.: D'Cent, Trezor, Ledger) ou lógicas (D'Cent, XUMM, Zelcore, Metamask) e transfiram para lá os vossos assets. Guardem as chaves privadas, credenciais, frases de recuperação, QRCodes, etc, em local seguro.

Navegadores Web

Usem como navegadores web, LibreWolf, Brave e o Tor ou, no mínimo, o Firefox (se num Android, experimentem Carbon).

Torrents (Downloads)

Para download de torrents, o qBitTorrent (com as definições a forçar a ligação encriptada).
Nota muito importante: *Não façam download de torrents sem uma VPN ativa*.

Motor de busca

Elejam como motor de busca (a definir nos browsers acima), o PreSearch (têm extensão disponível).

Correio Eletrónico

Quanto a correio electrónico, o ProtonMail (Correio eletrónico, Contactos, Calendário, Drive), Skiff (Correio eletrónico, Notas, Drive e Calendário) ou LedgerMail (Correio eletrónico na blockchain XDC).

Vídeo e Áudio

Cubram a câmara do laptop, se não a estão a usar e, se a trabalhar em locais públicos, estejam conscientes do que vos rodeia e se têm privacidade. Lembrem-se que o microfone do vosso smartphone e laptop, estão 24/7 ativos.

Se codecs de vídeo ou áudio precisarem, instalem K-Lite.

Videoconferência

Se precisam de efetuar videoconferências, usem Jitsi Meet ou Jitsi Desktop e se as mesmas são particularmente sensíveis, configurem o vosso servidor com o mesmo e usem-no como host.

VPN / DPN

Usem ProtonVPN, Deeper Network (Pico e Mini) ou Lokinet. Sem tal, o vosso provedor de internet vê tudo o que na web estão a fazer.

Sistema Operativo

Se quiserem elevar a segurança a outro nível, quando precisam fazer algo que de tal careça, usem Tails como sistema operativo (numa Pen USB, e arranquem o PC a partir da mesma), QubesOS ou ZorinOS.

E já está, com o acima implementado já usufruirão de uma navegação mais segura na web.

Doação

Se o acima te trouxe valor, aceito com gratidão uma doação

CoinRequest button

Image not found or type unknown

Revision #36
Created 8 November 2022 20:13:36 by MoldedLight
Updated 22 October 2023 21:08:03 by MoldedLight