PROTOCOLO DE SEGURANÇA DIGITAL

Um guia básico de segurança para todos

internationalistcommune.com

Protocolo de Segurança Digital

Um guia básico de segurança para todos

internationalistcommune.com

Protocolo Informativo de Segurança Digital

Usamos nossos telefones, tablets ou smartphones, bem como nossos computadores e nossas câmeras todos os dias. Portanto, nossa segurança ao usá-los é um tópico muito importante com o qual temos que nos confrontar. Especialmente para as pessoas que se organizam e lutam contra o sistema capitalista, a segurança e a autodefesa são tópicos essenciais que devem ser levados em consideração tambem no ambiente digital. Com o uso de tais dispositivos diariamente, podemos nos tornar vulneráveis ao estado ou a qualquer pessoa que queira nos prejudicar. Quando recebemos uma ligação, quando usamos a internet, quando enviamos mensagens, deixamos rastros digitais que o inimigo pode usar contra nós. Este protocolo tem como objetivo apresentar as principais ameaças e propor soluções e recursos para se adaptar e se proteger de boas maneiras.

Segurança digital para quê?

INo tópico de segurança digital, é importante fazer algumas perguntas para que possamos entender o motivo pelo qual certas medidas devem ser tomadas para nossa proteção e qual o impacto que elas têm. Dessa forma, podemos evitar que nos tornemos paranóicos ou um alvo fácil para o inimigo. As perguntas a seguir são, portanto, importantes para nós.

Por que é importante cuidar da nossa segurança?

Proteger a si mesmo, seus dispositivos, telefone e computadores significa ao mesmo tempo proteger seus companheiros, seu coletivo ou sua organização. A segurança cibernética não é uma questão individual e somos responsáveis não apenas por nossa segurança, mas também pela de nossos companheiros e companheiras.

Quais informações eu quero proteger?

Minha identidade, minha pesquisa na Internet, minha atividade nas redes sociais, localização ou minha presença em um determinado lugar, minhas comunicações, canais de informação, publicações na internet...

De quem quero me proteger, de quais inimigos?

Pessoas desconhecidas, serviços de inteligência do estado, outros estados, banqueiros, hackers, serviços de polícia judiciária, golpistas, minha operadora de celular ou meu provedor de serviços de internet, etc.

Que tipos de ataque?

Quando a policia tem acesso ao meu telefone após ser apreendido, quando estão me procurando na Internet, quando tentam hackear meu computador, quando o Estado solicita informações à minha operadora de telefonia ...

Precisamos iniciar entendendo quais são os rastros que deixamos em nossos dispositivos (telefone/computador) que podem ser vazados quando fazemos uma pesquisa, quando publicamos uma foto, etc. Por esse motivo, veremos como deixamos rastros nos computadores e que tipo de sistemas operacionais (software que gerencia o hardware e os aplicativos de um computador) existem e como eles são diferentes uns dos outros em questões de segurança e uso. Faremos o mesmo com os telefones e veremos os motivos pelos quais e como usar a VPN (Virtual Private Network). Vamos entender que tipos de ataques do inimigo existem e como podemos nos proteger contra eles também. Isso significa que também apresentaremos formas de uso seguro e boas práticas para os dispositivos com os quais trabalhamos diariamente.

Computadores

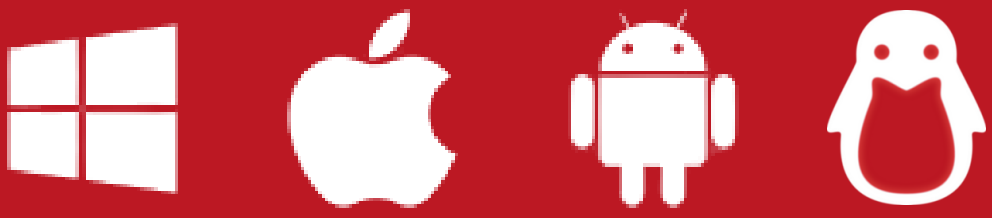
Em computadores, deixamos rastros utilizáveis quando:

- Armazenamos arquivos (vídeos/ fotos/ audios/ documentos ...) em um disco rígido (interno ou externo), em Pendrive USB e em cartões SD.

- Nós nos conectamos à Internet para acessar sites, usar aplicativos (mensagens, e-mails, aplicativos de jogos e aplicativos de mídia digital como Instagram etc.), baixar arquivos (foto/ vídeo/ audio/documento, etc.)

Sistemas operacionais

Um sistema operacional desempenha um papel muito importante, é o responsável por fazer com que todas as partes do computador, como memória, processador, armazenamento, funcionem juntas. Além disso, o Sistema Operacional é quem traduzirá a linguagem do computador para uma linguagem que possamos entender. Um computador sem sistema operacional é inútil. Softwares podem ser entendidos como um facilitador para realizar uma tarefa no computador. Então, por exemplo, se você precisar enviar uma mensagem, poderá instalar um aplicativo que envia mensagens. O software é este aplicativo. O termo software é usado para diferenciá-lo do hardware, ou seja, os componentes físicos de um sistema de computador. Mas existem diferentes sistemas operacionais, nem todos permitem as mesmas possibilidades. Alguns desses sistemas operacionais são sistemas operacionais de código aberto. Isso significa que é um sistema operacional ou um software desenvolvido de forma colaborativa e que também está aberto para qualquer pessoa usá-lo, alterá-lo e distribuí-lo.



- Windows:

É um sistema operacional desenvolvido pela empresa Microsoft que colabora com serviços estatais em todo o mundo. Pode ser útil para usar software de criação de conteúdo privado (como Adobe Photo-shop, Adobe Premiere, Sony Vegas Pro, etc.). Mas é impossível saber como os dados do computador são processados pela empresa. Ele não fornece seus algoritmos, como seus dados serão utilizados, além de não permitir que você tome iniciativa de proteger suas informações, é muito fácil quebrar a senha e invadir seus dados. Como uma empresa capitalista, ela pode vender informações de seus usuários para estados (como a Turquia) em troca de tornar seus serviços autorizados para operar naquele país.

- macOS:

É um sistema operacional desenvolvido pela empresa Apple Inc. Assim como o Windows, é impossível saber como os dados do seu computador são processados pela empresa. Mas também é útil para usar software de criação de conteúdo privado (Adobe Photo-shop, Adobe Premiere, Sony Vegas Pro, etc.). Ele não fornece seus algoritmos e não permite que o disco rígido seja protegido. É difícil quebrar a senha e invadir seus dados. A Apple afirma que não vende dados pessoais a terceiros. Como forças anticapitalistas, ainda temos que tomar precauções e não devemos acreditar em nenhuma dessas empresas.

- Linux:

É um sistema operacional de código aberto que possui várias versões disponíveis (por exemplo Debian, Ubuntu, etc).

Foi desenvolvido por Linus Torvalds e é baseado em sistemas operacionais Unix.

Não é compatível com o uso de software de criação de conteúdo privado (Adobe Photo-shop, Adobe Premiere, Sony Vegas Pro ...). No Linux existem todos os tipos de aplicativos de código aberto que podem ser usados para criação de conteúdo, uma alternativa a softwares geridos pelas grandes empresas capitalistas. Todos os algoritmos são acessíveis e verificados regularmente por pessoas ao redor do mundo. É possível criptografar com segurança o disco rígido e qualquer outro sistema de armazenamento. Com uma boa senha, é (muito) difícil quebrar a senha. Isso significa que é muito caro em tempo e energia. Além disso, muitos aplicativos úteis para limpeza e navegação de dados (detalhados posteriormente) são pré-instalados. É o mais eficaz dos sistemas para evitar malware e vírus. Por esses motivos, é recomendável usá-los em vez do Windows/MacOS.

Sabia mais:
https://ubuntu.com/download/desktop
https://www.linux.org/pages/download/

- TAILS (O Sistema de Viver Incógnito Amnésico):

Este é um **sistema operacional que foi desenvolvido para garantir um alto nível de segurança e anonimato** ao navegar na Internet e arquivar fotos, documentos, etc. Esse sistema funciona de uma forma independente, isso significa que você pode instalá-lo em um Pendriv eUSB ou cartão SD e usá-lo em todos os computadores (mas não em Macbooks), sem usar o sistema de computador original (Windows/Linux...). Sua função amnésica (perde toda a memória) permite que você não mantenha nada no computador. Ele se conecta à internet pelo navegador Tor. É recomendado pela maioria dos Whistle Blowers (uma pessoa que revela informações sobre a atividade dentro de uma organização) e foi financiado pelo Projeto Tor (https://www.torproject.org/). Com base em uma estrutura Linux, com uma boa senha, é (muito) difícil quebrar a senha.

Aqui está sua documentação e o tutorial para sua instalação: https://tails.net/

Telefones

Em um telefone/ tablet, deixamos rastros utilizáveis quando:

- Comunicamos por SMS/chamada (através de uma operadora de telefonia)
- Tiramos fotos ou gravamos videos e audios
- Aplicativos que usam localização
- Armazenamos arquivos (vídeos / fotos / documentos) no telefone ou no cartão mini SD
- Conectamo-nos à internet para acessar sites, usar aplicativos (mensagens, e-mails, etc.) ou baixamos arquivos

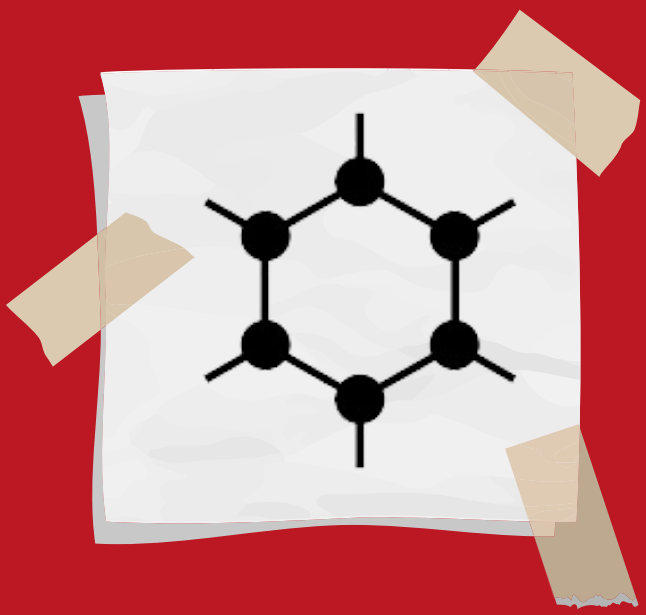
Existem diferentes sistemas operacionais de telefone, nem todos permitem as mesmas possibilidades:

- iOS:
É um sistema operacional móvel para iPhone desenvolvido pela Apple Inc. É impossível saber como os dados telefônicos são processados pela empresa.

- Android:
É um sistema operacional móvel de código aberto usado na maioria dos telefones (Samsung, Huawei, Redmi, etc.). Não oferece boa segurança contra hackers. É impossível saber como os dados do telefone são processados.

- GrapheneOS:

É um sistema operacional móvel de código aberto que suporta apenas telefones Google Pixel. Recomenda-se usar as novas versões do Pixel, já que as séries Pixels mais antigas não são mais suportadas pelo GrapheneOS. **Ele permite que você evite a vigilância do Google e criptografe o conteúdo do seu telefone usando um sistema desenvolvido por companheiras.** É compatível com a maioria dos aplicativos Android e também oferece alternativas de código aberto. **Foi desenvolvido como um projeto alternativo sem fins lucrativos.**

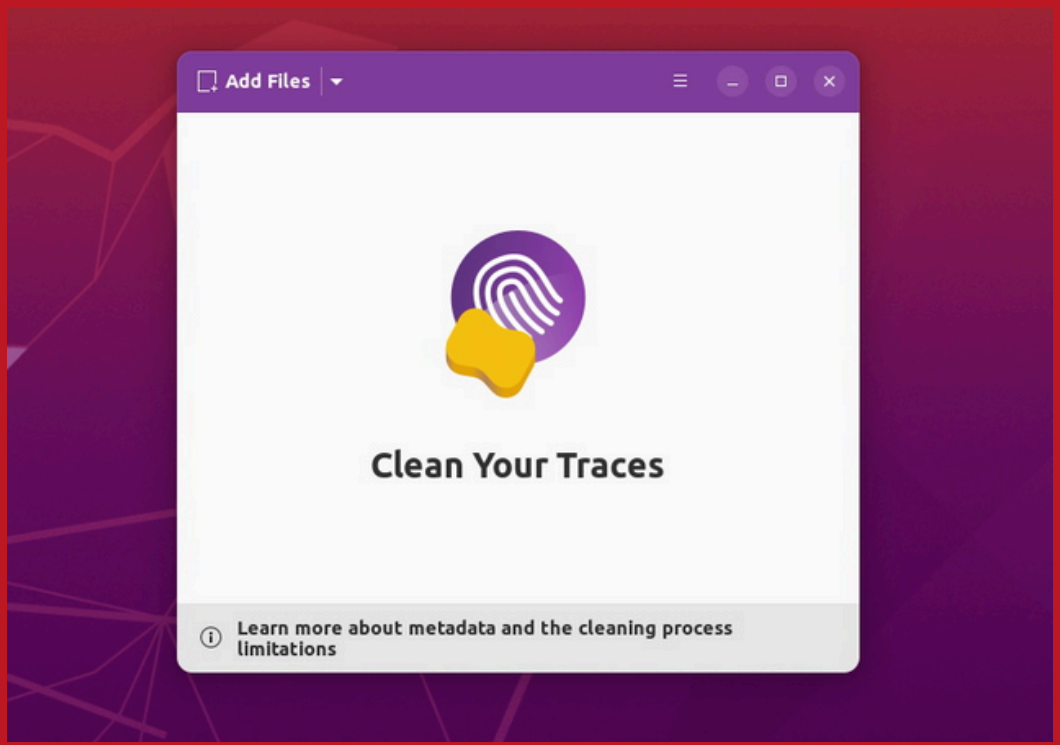


Devido à privacidade e segurança que oferece, torna a exploração das fontes mais comuns de vulnerabilidades substancialmente mais difícil. **Ele melhora a segurança do sistema operacional e dos aplicativos executados nele.**

O GrapheneOS adiciona várias configurações para recursos como permissão de rede, permissão de sensores (microfone, câmera etc.), restrições quando o dispositivo está bloqueado (pinos USB-C, câmera, configurações, etc.), juntamente com recursos de privacidade e segurança mais complexos voltados para o usuário. Recomenda-se instalar o GrapheneOS para o uso seguro de telefones.

Sobre armazenamento

Cada arquivo (vídeo, foto, pdf etc.) contém metadados que são informações sobre sua data de criação, modificação, tamanho, câmera, formato, aplicativo usado para criá-lo e modificá-lo. Sua localização geográfica também é um metadado. Os metadados fornecem informações sobre onde um dispositivo está localizado, geralmente expressas em coordenadas ou em um endereço físico. Para evitar esse tipo de rastro de ser criado, é recomendado revisar a configuração do seu dispositivo. Existe o perigo constante de espalhar metadados por e-mail/ SMS/ redes sociais dos arquivos. É desejável removê-los, especialmente em caso de publicação na Internet ou compartilhamento (por mensagem ou e-mail). Existe o aplicativo Metadata Cleaner no Tails/Debian/Linux ou, em smartphones, o aplicativo Image Pipe pode ser usado para isso.



1. Como evitar que as informações se espalhem na internet?

Ao usar a Internet, muitas informações circulam e são salvas por vários anos. Eles variam de qual site visitamos, de qual telefone, qual rede Wi-Fi, qual compartilhamento de conexão com a Internet, etc. Existem algumas soluções para reduzir a espionagem e a identificação durante a navegação na Internet.

VPN

A função da VPN (Virtual Private Network) é ocultar a localização da sua conexão e também garantir que suas informações sejam mais protegidas. **O VPN estabelece uma conexão segura e confiável sobreposta a uma rede insegura, protegendo sua atividade, localização e identidade online.**

Como isso funciona?
Quando você se conecta à internet, cada conexão tem um endereço atribuído, por exemplo, se você estiver conectado à internet na sua casa, essa conexão tem um endereço, um código, qualquer pessoa que se conectar será identificada como presente nesse endereço. Esse endereço é chamado de endereço IP. Este é o perigo, se o inimigo souber qual é o seu dispositivo e se ele estiver espionando você, sua localização real será facilmente identificada, quando você se conectar a uma rede sem usar uma VPN, expondo sua localização e que este é um lugar onde você, seus amigos ou familiares vivem.

A função da VPN é alterar esse endereço e também ocultar as informações enviadas, tornando o trabalho de espionagem praticamente impossível. A VPN colocará suas informações em uma caixa protegida por uma chave, se alguém tentar interceptar suas informações por meio de espionagem digital, ele não poderá abrir esta caixa.

Existem alguns provedores de VPN pelos quais você não precisa pagar e que são completamente anônimos, como a RiseUp VPN, que pode ser instalada em qualquer dispositivo. A VPN RiseUp não é compatível com dispositivos iOS da Apple. O Proton VPN funciona bem em sua versão grátis, sendo compatível também com dispositivos OS, mas requer login para funcionar. Alguns outros provedores que são seguros, como Mullvad, PIA etc, porém esses provedores não oferecem versões gratuitas, porém são bons e seguros.

Quando usar uma VPN

Tor Browser

O Navegador TOR é a melhor solução para fazer pesquisas, assistir vídeos ou publicar na internet de forma segura e simples. Não há histórico de navegação, nem registro de senha e permite o usuário locultar sua identidade da operadora de Internet e dos sites visitados. Ele usa vários pontos de retransmissão que permitem anonimizar nossas conexões e nosso trabalho. Está disponível em todos os telefones e computadores.

https://www.torproject.org/

2. Do que se proteger?

É difícil verificar se um componente de um telefone foi ou não fisicamente modificado e/ou corrompido pelo Estado. Ao nosso redor temos milhares de dispositivos eletrônicos, como telefones, computadores, etc. Muito mais do que isso, a maioria das nossas comunicações é feita utilizando esses dispositivos. Isso torna ainda mais necessário usá-lo de forma segura e consciente para se defender de ameaças online. Ameaças online são conjuntos de práticas e técnicas para invadir dispositivos, espionar, coletar e alterar dados. Para combater isso, a segurança digital são técnicas e práticas que tornam o uso da tecnologia mais seguro.

Tipos de ataques

Malware

"Malware" é qualquer tipo de software projetado para danificar um computador. O malware pode roubar informações confidenciais do seu computador, desacelerar gradualmente o computador ou até mesmo enviar e-mails falsos de sua conta de e-mail sem o seu conhecimento.

Aqui estão alguns tipos comuns de malware sobre os quais você já deve ter ouvido falar:

- **Vírus:** Um programa de computador nocivo que pode copiar a si mesmo e infectar um computador.
- **Worm:** Um programa de computador malicioso que envia cópias de si mesmo para outros computadores por meio de uma rede.
- **Spyware:** Malware que coleta informações de pessoas sem o seu conhecimento.
- **Adware:** Software que reproduz, exibe ou baixa automaticamente anúncios em um computador.
- **Cavalo de Tróia:** Um programa destrutivo que finge ser um aplicativo útil, mas danifica seu computador ou rouba suas informações após a instalação.

Como o malware se espalha:

- Baixando programas da Internet que contêm malware secretamente
- Visitando um site infectado com malware
- Clicando em uma mensagem de erro falsa ou janela pop-up que inicia um download de malware
- Abrindo um anexo de e-mail que contém malware
- através de unidades USB e discos rígidos

Existem muitas maneiras diferentes pelas quais o malware pode se espalhar, mas isso não significa que você seja impotente para detê-lo. Agora que você sabe o que é malware e o que ele pode fazer, vamos examinar algumas etapas práticas que você pode seguir para se proteger.

Como evitar malware:

- Mantenha seu computador e software atualizados
- Não conecte flashes USB que não sejam confiáveis
- Use o Linux → para melhor segurança, o malware geralmente só funciona no Windows
- Pense duas vezes antes de clicar em links ou baixar qualquer coisa

Phishing

Usado para roubar informações, incluindo logins, acessos, dados. Executado principalmente via e-mail, mensagens e telefonemas.

Como se proteger:

- Verifique se a origem da mensagem de e-mail é confiável.
- Se tiver endereços de sites suspeitos.
- Se possível, verifique sempre a confiabilidade da mensagem com a pessoa que a enviou.

Ataque "Man-in-the-middle"

Quando o inimigo se conecta às nossas redes, ele pode espionar as informações que um dispositivo envia via internet. Este ataque pode ser realizado por malware de forma remota, ou por meio de ataques físicos e assim obter informações confidenciais.

Como se proteger:

- Evitar conexões Wi-Fi que não sejam protegidas por senha.
- Prestar atenção às notificações do navegador relatando que um site não é seguro.
- Não utilizar redes públicas (por exemplo, cafés, hotéis) ao realizar transações sensíveis.
- Use o TOR ou VPN se precisar navegar em redes inseguras.

3. Guerra cibernética

Com o desenvolvimento de todas essas tecnologias, ficou claro que os estados usariam essas ferramentas e técnicas para atacar, espionar e coletar informações. Outros estados como EUA, Rússia, Ucrânia, Israel e Irã também estão se tornando cada vez mais profissionais na realização de ataques. A OTAN tem vindo a realizar cada vez mais ataques e treinos nesta área.

Isso podemos ver muito no exemplo do malware **Stuxnet**. O Stuxnet é um worm de computador malicioso descoberto pela primeira vez em 2010 e acredita-se que esteja em desenvolvimento desde pelo menos 2005. O Stuxnet tem como alvo sistemas de controle em computadores e software e acredita-se que seja responsável por causar danos substanciais ao programa nuclear iraniano. Embora nem os EUA nem Israel tenham admitido abertamente a responsabilidade, várias organizações de notícias independentes afirmam que o Stuxnet é um worm cibernético construído pelos dois países de forma colaborativa. O Stuxnet funciona visando máquinas que usam o sistema operacional e as redes Windows e, em seguida, procurando o software Siemens Step7, que é o programa usado no programa nuclear. O Stuxnet supostamente comprometeu os sistemas de controle iranianos, coletando informações sobre sistemas industriais e fazendo com que as centrífugas de rotação rápida colapsassem. O Stuxnet supostamente destruiu quase um quinto das centrífugas nucleares do Irã. Visando sistemas de controle industrial, o worm infectou mais de 200.000 computadores e fez com que 1.000 máquinas se degradassem fisicamente.

Isso não está tão longe da nossa realidade. A França criou malware para espionar arquivos, informações, locais, especialmente na Síria. Até hoje vemos esse vírus infectando dispositivos e circulando em computadores da região. Aqui, o malware **Babar** é um bom exemplo que vazou pelo denunciante Edward Snowden. O spyware Babar é capaz de registrar pressionamentos de tecla, registro da área de transferência, fazer capturas de tela e até mesmo registrar conversas de áudio através do Skype e do Yahoo. Ele pode injetar códigos e roubar arquivos. Ele também usa uma rede Tor para se comunicar secretamente. Este spyware certamente é uma ferramenta de espionagem e pode ter sido usado por vários motivos políticos.

A Turquia, apesar de muitas fraquezas, tem planos de se tornar uma potência em ataques e espionagem digital. Em termos de controle digital, existe atualmente uma lei na Turquia que para que o Google, Meta (Facebook, Whatsapp, Instagram) operem dentro de seu território, essas empresas devem fornecer todos os dados que o Estado solicitar, como localização, mensagens, acesso às suas fotos, etc., bem como quase qualquer conta em plataformas de mídia digital solicitada por eles. Especialmente antes de ataques e operações do Estado turco as mídia digital, como a Meta, bloqueia contas que compartilham conteúdo político como método de censura. Por exemplo, antes que os ataques do Estado turco em Rojava comecem a acontecer, geralmente as contas em plataformas de mídia digital como Instagram, Twitter etc. que poderiam se mobilizar contra esses ataques são bloqueadas e fechadas.

As capacidades de ação dos serviços de inteligência digital são usadas principalmente para vigilância doméstica e espionagem contra seus adversários políticos, usando programas de vigilância de potencias como Israel. Além disso, a espionagem de serviços telefônicos em outros países, como Armênia, Grécia, Israel e Síria, já foi comprovada. A organização de inteligência do estado turco, MIT, também afirma que está trabalhando em segurança digital, satélites e interceptação de sinais em todo o mundo

Nessa realidade, temos que nos conscientizar do uso de tecnologias, principalmente com a especialização de nosso inimigo, também precisamos nos profissionalizar, nos conscientizar e nos preparar para uma guerra que já se tornou real. Esta guerra precisa seguir nossos princípios de Guerra Popular Revolucionária, pois uma pessoa desprotegida, uma pessoa que não é cuidadosa, pode colocar em perigo dezenas de companheiros e companheiras. Temos que fazer deste tópico um tema comum para todos nós e para toda a sociedade. Todos nós temos que trabalhar juntos para proteger nossas identidades, nossas localizações, nossas mensagens e informações.

4. Segurança da câmera e do microfone

lSe o inimigo quiser tirar vantagem de você por meio da vigilância por câmeras e microfones, ele terá que invadir seu dispositivo. **Quase todos os hacks são causados por malware.** Abrir anexos de e-mail desconhecidos, baixar de fontes desconhecidas e visitar sites não confiáveis são como cerca de 98% dos malwares acabam em nossos dispositivos. Depois que o malware é instalado, seu computador ou telefone fica totalmente aberto a hackers. Simplesmente evitar malware e certificar-se de que seu software antivírus esteja ativado e atualizado pode evitar isso. Mas uma vez que o malware é instalado em seu computador, o atacante pode ter acesso ao seu microfone e câmera. A maioria dos computadores tem microfones e câmeras embutidos. O mesmo se aplica aos telefones.

Portanto, é recomendável cobrir todas as câmeras em seus dispositivos. Como especialmente as câmeras e microfones embutidos estão diretamente conectados à Internet, eles são facilmente hackeados. Nesse caso, o inimigo pode facilmente assumir a funcionalidade da câmera e ligá-la ou desligá-la como desejar, além de desativar a luz LED para evitar a detecção. Claro que é possível bloquear todas as permissões e acessos ao microfone e à câmera também. Na maioria dos casos, a proteção de software é mais conveniente do que a proteção física, mas nem sempre tão confiável. Existem inúmeros softwares com acesso a esta função.

Especialmente o GrapheneOS está dando essa opção para o dispositivo desde o setup inicial e também a capacidade de sempre verificar se o acesso ao microfone e à câmera é permitido ou não.

Mesmo que cobrir sua câmera com fita adesiva não impeça alguém de ouvir pelo microfone, ainda é uma boa proteção para o seu anonimato. Claro, isso impedirá a vigilância por vídeo, mas o som do microfone ainda pode ser captado. Os laptops modernos geralmente têm vários microfones para melhorar a qualidade do som, e cobrir todos eles será difícil. Em alguns modelos, os microfones embutidos são desativados quando você conecta um microfone externo. Uma solução para isso é conectar um plug sem microfone. Seu laptop pensará que um microfone externo está conectado e desligará todos os integrados.

Porque na maioria dos casos, a proteção de software é mais conveniente do que a física – mas nem sempre tão confiável. Sempre temos que ter cuidado quando falamos para não expor nenhuma informação ao inimigo enquanto estivermos perto de nossos dispositivos.

5. Como se comunicar com segurança

Signal

Para se comunicar com segurança, é bom saber se a empresa que desenvolve o aplicativo do serviço de mensagens colabora com a polícia, estados, se vende dados etc. ou não. Existem vários aplicativos que não são seguros, como o Whatsapp, mas alguns aplicativos de comunicação fornecem criptografia. É claro que, com o tempo, melhores aplicativos serão desenvolvidos ou sempre haverá a possibilidade de que os aplicativos usados comecem a coloborar com o inimigo. Portanto, em geral, é recomendável ter cuidado na questão da comunicação em quaisquer dispositivos para não expor informações nessas plataformas e aplicativos.

Para se comunicar por mensagens/chamadas, o aplicativo SIGNAL fornece criptografia de comunicação muito alta contra hackers. Está disponível em todos os telefones e também em computadores. É possível configurar mensagens que se auto-deletam e diversas opções para mais segurança.

Como mencionamos anteriormente, o uso de aplicativos como o Whatsapp não é seguro, além de fornecer informações ao estado turco, o Whatsapp tem uma segurança muito fraca contra ataques, é muito fácil descobrir informações por meio de tecnologias de espionagem.

Outro aspecto muito perigoso do Whatsapp é que todas as mensagens, mesmo as excluídas, são armazenadas em arquivos do Whatsapp. Se o Estado turco solicitar suas mensagens, localização, todas as suas informações serão repassadas. Nesse caso, nem mesmo usar uma VPN seria uma solução completa, pois apenas suas informações estariam protegidas, mas todas as mensagens e fotos ainda seriam compartilhadas mesmo vários meses após o envio.

Tails

Além do Signal, o TAILS oferece muitas opções de comunicação criptografada. Dessa forma, grande parte da comunicação pode ser feita pelos serviços que estão disponíveis nele. Isso pode melhorar nossa privacidade online.

Tails inclui:

- Tor Browser com uBlock, um navegador seguro e um bloqueador de anúncios
- Thunderbird, para e-mails criptografados
- KeePassXC, para criar e armazenar senhas fortes
- OnionShare, para compartilhar arquivos, sites e mensagens pelo Tor
- Limpador de Metadados, para remover metadados de arquivos

6. Boas Práticas

- **Use senhas diferentes dependendo das contas e aplicações.** A força de uma senha está no seu comprimento; se possivel use até uma “frase-senha” para mais segurança. O uso de caracteres especiais já não aumenta a segurança de uma senaha. Recomenda-se criar uma senha composta por várias palavras aleatórias para um aplicativo ou computador, e uma senha de 12 caracteres para um telefone.

- **Use aplicativos seguros** recomendados por companheiros e companheiras. Instale aplicativos de fontes confiáveis. Esses aplicativos passam por verificações de segurança, reduzindo o risco de atividades maliciosas relacionadas ao microfone ou outros recursos confidenciais.

- **Não responda a mensagens de contatos desconhecidos ou estranhos** e não abra links que são enviados a você possivelmente por estes, pois estes visam obter sua localização

- **Mantenha a localização (GPS) desativada**, sendo a melhor prática deixar o celular sempre no modo avião. O modo avião pode ser ativado enquanto a conexão Wi-Fi está operando.

- **Não viaje com o celular ligado**, se possível retire o SIM Card antes de viajar para outros locais, isso também evita que sua localização seja decifrada via satélite.

- **Organize a compra de embalagens de segurança** que cortam o sinal (**como uma bolsa de Faraday)**. Isso evita que qualquer sinal seja enviado do seu celular, tornando-o a melhor opção para viagens e transporte.

- **Não envie mensagens com seu nome, localização, onde você está, para onde está indo.** As mensagens, especialmente no Whatsapp, podem ser interceptadas e usadas pela inteligência do inimigo.

- **Use uma solução antivírus/ antimalware.** É um software ou serviço essencial que protege os sistemas de computador contra software malicioso. Esses programas fazem isso detectando possíveis ameaças de malware, bloqueando ameaças antes que elas acessem o sistema e eliminando ameaças existentes para que não causem mais danos ao sistema. Para isso, existem vários softwares que você pode baixar em seus dispositivos. Isso se aplica a todos os tipos de dispositivos, como computadores, telefones de todos os sistemas operacionais e até telefones com GrapheneOS.

- **Mantenha seu dispositivo atualizado.** Certifique-se de que seu dispositivo esteja executando o sistema operacional e os patches de segurança mais recentes disponíveis. As atualizações regulares geralmente incluem correções de bugs e aprimoramentos de segurança que abordam possíveis vulnerabilidades. Não atualizar para garantir a segurança é um pensamento comum e falso. É melhor atualizar para garantir a segurança de um dispositivo que tenha acesso à Internet.

Conclusão

Com este pequeno protocolo de segurança digital, queríamos compartilhar algumas informações básicas sobre como se proteger em nível digital. Como os ataques cibernéticos estão aumentando e o uso de comunicações e plataformas digitais se torna cada vez mais presente, é importante sabermos como podemos usá-los de forma segura e como nos manter protegidos ou prevenir quaisquer ataques do Estado ou de outros inimigos contra nós. Como somos a parte anticapitalista da sociedade que luta contra esse sistema, temos que sempre nos lembrar de que podemos nos tornar alvos de tais ataques. Portanto, levar nossa segurança a sério é uma questão muito importante e essencial para todos nós na vida cotidiana.

internationalistcommune.com