7 PASSOS para aumentar sua SEGURANÇA digital

1 SENHAS

Você acha que sua senha é segura porque é muito grande - mas você usa a mesma senha em todos os serviços? Teste seus e-mails usados em serviços online:

`https://haveibeenpwned.com/`

Esse site vai mostrar se sua senha já vazou na internet, através de grandes vazamentos de bancos de dados de sites. Mude sua senha caso já tenha sido vazada.

Você usa senhas diferentes, mas são simples pra você se lembrar? Há programas gratuitos que testam combinações de senhas (usando dicionários, números e caracteres disponíveis). Esses programas chegam a uma senha simples em segundos, por isso use senhas diferentes e longas para cada serviço, especialmente em redes sociais, e-mails e dispositivos que armazenam documentos sigilosos.

Recomendamos o uso de frases-senha. Uma frase, com dígitos e caracteres especiais, é mais fácil de lembrar. Você também pode usar um gerenciador de senhas, como o Bitwarden e o KeepassXC.

2 VERIFICAÇÃO EM DUAS ETAPAS

A verificação em duas etapas é um processo que adiciona, por meio de um código (PIN ou código aleatório), uma camada de segurança às suas contas. Isso evitará que suas contas de comunicação (WhatsApp, Telegram, Signal, Messenger), de e-mail, de redes sociais, e outras sejam roubadas - e no caso das mensagerias (WhatsApp), "clonadas"/sequestradas.

Ative a verificação de duas etapas com o uso de PIN ou de aplicativo (como o DuoMobile ou TOTPAuth). Evite usar SMS para a verificação de 2 etapas. SMS é inseguro e fácil de ser interceptado.

PROTEJA SEU NÚMERO DE CELULAR 3

SIM Swap é a clonagem ou roubo do seu chip de celular, para acessar e/ou roubar as suas informações pessoais. Isso foi muito usado no período eleitoral de 2018, contra ativistas feministas do #EleNão. Ainda que não envolva necessariamente o roubo do seu celular ou do seu chip físico, essa prática permite fraudar os seus dados pessoais nas operadoras de telefonia. Verifique se seu número de telefone está público na internet (muito comum com PJ/MEI) ou em redes sociais.

Além disso, saiba que podem ocorrer vazamentos de dados que expõem números de telefone.

Procure evitar ao máximo que seu número fique público, pois um atacante pode solicitá-lo a uma operadora telefônica. Caso seu número seja público, proteja com verificação de duas etapas todas as contas que ficam no seu celular. Nas redes sociais, coloque seu número como privado.

4 MINIMIZE SEUS RASTROS ONLINE

OSINT, Inteligência de código aberto

Open Source Intelligence é rastrear todas as informações públicas de alguém, como redes sociais, postagens de foto ou vídeo, publicações, blogs antigos, etc.

Doxxing

Exposição de dados pessoais de pessoas ou organizações, com o objetivo de descredibilizá-las, atacá-las ou fragilizá-las. Exemplos: endereço pessoal, dados pessoais de familiares - como nome de escola infantil -, telefones, etc.

Através do OSINT, faça uma pesquisa sobre você mesmo e veja quais são os seus dados públicos. Caso esteja sendo vítima de doxxing, torne privada as suas contas em redes sociais; nas plataformas que publicam fotos e dados pessoais, adicione apenas pessoas que você conhece e confia; evite confirmar online a sua presença em eventos (opte pela opção "salvar"); bloqueie marcações de fotos em redes sociais.

No caso de figuras públicas que precisam de exposição, é necessário fazer uma análise de risco mais apurada e específica.

5 MANTENHA SEUS SISTEMAS ATUALIZADOS

Muitos ataques online acontecem em sistemas operacionais desatualizados! Em seus computadores e celulares, habilite a atualização automática. Essa dica também é válida para roteadores, modems, impressoras e outros dispositivos eletrônicos conectados à internet.

6 BLOQUEIO DE TELA

Ative bloqueio de tela com senha, e não use padrões (desenhos). Habilite nas configurações, tanto do seu celular quanto do seu computador, o bloqueio de tela por tempo de inatividade, evitando assim pessoas oportunistas.

* Uso de padrões ou reconhecimento facial ou fingerprint não são recomendados.

7 NAVEGAÇÃO SEGURA

Use o navegador Tor para realizar de maneira segura suas atividades e pesquisas. Ele anonimiza sua conexão e localização, evitando que qualquer pessoa possa espionar e rastrear sua atividade online, inclusive o histórico de buscas.

Através do navegador Tor, é possível driblar a censura, o que possibilita um acesso livre e seguro à informação.

Para o uso de redes sociais e e-mails, você precisará ter ativado a verificação em duas etapas (como vimos no passo 2).

Não use o navegador Tor para acessar bancos ou entidades financeiras, pois estes limitam o acesso de acordo com a sua localização.

ALERTA: O modo incógnito e privado dos navegadores tradicionais não é anônimo.

Dispositivos protegidos

Ative a criptografia de seu celular ou computador. No Windows 10 essa opção é ativada pelo programa Bitlocker, já no macOS, pelo fileVault. Guarde bem a senha de criptografia, pois caso a esqueça, perderá todos os seus dados.
Não entregue seu celular ou seu computador a pessoas nas quais não confia. Em caso de reuniões sigilosas, tenha sua própria bolsa que bloqueia sinais de celulares, como a bolsa de faraday. No caso de uma organização, tenha uma caixa de faraday para a sala de reuniões.
Protetores de tela de privacidade para notebooks e celulares restringem a visibilidade periférica das telas e evitam que o seu trabalho seja vigiado e espiado por terceiros.

Comunicação protegida

Não use SMS ou ligações comuns para comunicar informações sensíveis, pois estes meios são interceptados mais facilmente. Ligações de WhatsApp são mais seguras do que ligações comuns, e ligações e mensagens de Signal são mais seguras do que WhatsApp.
No aplicativo Signal, ative o temporizador de mensagens, o qual destrói, após um tempo predefinido, as mensagens de todos os envolvidos na conversa. Além disso, ao enviar uma imagem o aplicativo remove metadados do arquivo. Com o Signal também é possível fazer videochamada no celular ou no computador, tanto individual, como em grupo.

Alguns cuidados extras

Em caso de exposição pública, é importante construir sua própria análise de risco. Mas deixamos aqui algumas dicas que você pode implementar, caso ache necessário.
Faça uma busca na Internet e verifique os seus rastros digitais (ver passo 4, OSINT). Veja quais são suas redes sociais abertas ao público.

* Avalie restringir o acesso às suas contas públicas de redes sociais;
* Em perfis públicos, limite as postagens da sua vida pessoal;
* Verifique seus e-mails de recuperação de contas e ative a verificação em duas etapas;
* Verifique o backup (cópia de segurança) de seus computadores e celulares, e de outros dados. Mantenha-os seguros e protegidos por senha e, se possível, por criptografia também.
* Atualize seus contatos de emergência e mantenha uma pessoa avisada de seu status.
* Esteja sempre atualizado sobre as leis que regem a proteção de seus dados na internet, assim como seu direito e direito de outras pessoas sobre eles.

Um contato de emergência é uma pessoa de sua confiança que estará disponível e saberá onde e como procurar ajuda caso você precise. Mantenha essa pessoa atualizada e não entre em pânico. Tenha um acordo com seus pares, no caso de precisar de ajuda emergencial.

GLOSSÁRIO

Atacante: pessoa que pretende atacar você online (hacker, alguém vigiando sua conexão em casa, um inimigo, etc)
Sistema operacional: o programa que faz o seu dispositivo eletrônico (computador, celular) funcionar. Exemplo: Linux, Windows, iOS.
Backup: também conhecido como "cópia de segurança". É o ato de copiar arquivos, pastas ou discos inteiros (físicos ou virtuais) para sistemas de armazenamento secundário (hd externo, pen drive, e-mail, etc).
Faraday: a gaiola de Faraday permite criar uma barreira de isolamento em dispositivos elétricos e eletrônicos, de forma que o campo elétrico ou magnético gerado no interior de um dispositivo não cause interferência em dispositivos próximos a ele.
Metadado: são dados sobre os seus dados transmitidos. Por exemplo, quando você envia um e-mail, o seu endereço de e-mail, o endereço da pessoa que vai recebê-lo, o horário, o cliente de email, o tipo de navegador usado e a quantidade de dados (por exemplo, 3MB) são metadados desse e-mail.

* Revisão técnica: Gustavo Gus
* Revisão textual: Bruno Rigonato Mundim

Esse material foi produzido como parte da Bertha Fellowship 2020-2021, com o apoio de The Tor Project e financiamento da Bertha Foundation.

Acesse o site para mais informações:
https://acaravana.tech