Muito se fala sobre anonimato, porém muita gente vacila na hora de aplicar e aí acaba aparecendo no fantástico, então aqui será um guia completo sobre anonimato

Vamos começar com o número que vocês utilizam no telegram e whatsapp

Aconselho utilizarem o app eSIM PLUS, com ele vocês podem receber SMS sempre que precisarem, porém é pago

Já para utilizar um número descartável, vocês podem utilizar o bot de SMS : @NotzSMSBot

Mas ele só funciona 1 vez, ou seja, número descartável, por isso é tão baratinho

Ou vocês podem optar em comprar um chip da Tim nas americanas (custa só 10 reais), aí cadastra com os dados de algum grupo de puxadas, assim não saberão quem é você.

Lembrando que quando se fala em anonimato, a coisa mais importante é não deixar rastros em nada que faz na internet, então nunca usem seus dados em nada na internet.

Isso é importante tanto para não serem pegos, tanto para a própria segurança, dados são vazados todos os dias de diversas pessoas, porém não conseguiram vazar os seus caso você não use eles em nenhum lugar.

4G/5G - O básico da utilização do 4G e 5G será explicado aqui. Saiba que ele não te garante anonimato.

O 4G (quarta geração) é uma tecnologia de comunicação móvel que representa uma evolução significativa em relação às gerações anteriores.

O 4G utiliza protocolos de comunicação avançados, incluindo o Protocolo de Controle de Transmissão (TCP) e o Protocolo de Internet (IP)

O 5G (quinta geração) utiliza uma variedade de frequências de onda, incluindo ondas milimétricas.

O 5G permite a criação de redes LAN virtuais, que são redes privadas independentes da infraestrutura principal da operadora.

Por que utilizam 4G/5G para o 7?

Em casos como esses é muito comum as pessoas ligarem os dados móveis, realizarem algumas tarefas ilícitas e posteriormente ligarem o Modo Avião...

Bom... Se fosse simples assim, todo mundo faria né

Na realidade, ao ligar o 5G para sua operação, basicamente você está desvinculando sua atividade via Wi-Fi. Fazendo com que o acesso seja mais difícil, mas não impossível, principalmente em uma investigação.

Quando você faz o 7 pelo seu Wi-Fi, caso o invasor consiga invadir, ele terá acesso a todos que estão conectados a aquela rede em específico.

Devo utilizar apenas o 4G/5G em minha operação?

Óbvio que não. Não seja idiota, quanto mais camadas de proteção, melhor fica.

Precisa, e sempre vai precisar se camuflar, e essa é uma técnica simples mas que já ajuda você que está iniciando nesse mercado.

Dicas Para Sua Segurança 2024

📚 Passo 1 - Ocultar informações: Se você quiser alguma informação online ou se quiser abrir uma conta em algum lugar, use informações falsas.

📚 Passo 2 - Máquina Virtual: Trabalhar virtualmente pode ser um tanto seguro. Porque as máquinas virtuais têm endereços MAC virtuais diferentes dos endereços MAC reais. Além disso, mesmo que a máquina virtual seja invadida, seu PC principal está protegido.

📚 Passo 3 - Cuidado com a VPN: Muitas VPNs mantêm todos os seus logs. Ou seja, o histórico de tudo, incluindo seu IP e o que você está usando com a VPN ligada. Portanto, use VPNs que não possuem logs. por exemplo: ExpressVPN, CyberGhost, VyprVPN, IPVanish e por aí vai né camarada

📚 Passo 4 - Navegador anônimo: Quando você navega em algo, seus dados são armazenados em seus cookies. Esses cookies pode facilmente torná-lo vítima, ative o modo de navegação anônima ao usar o navegador. Ou você pode usar navegadores que não salvam seus dados. ex: Brave, Tor

📚 Passo 5 - E-mail anônimo: Hoje em dia o e-mail é necessário em qualquer lugar da internet. Muitos usam e-mail falso ou e-mail temporário. Mas você pode usar o e-mail anônimo para comunicação permanentemente segura, bem como usar em qualquer lugar. Um deles é o Proton Mail mas utilize qual adaptar melhor

📚 Passo 6 - ISO anônimo: Todos nós estamos acostumados a usar o Windows. O Windows é o sistema operacional menos seguro entre todos os sistemas operacionais populares disponíveis atualmente. Muito mais seguro, por exemplo: Tail OS

📚 Passo 7 - PC remoto: Usar seu próprio PC é mais seguro se você alugar o PC de outra pessoa. Se você fizer algo usando RDP, não terá nenhuma informação. Além

disso, mesmo que haja um ataque de vírus em seu RDP, seu PC principal não será prejudicado. Mesmo que o RDP esteja danificado, você pode substituí-lo.

Afinal, você não está 100% seguro. Quanto mais consciente você estiver, mais seguro estará