

Cartilha NAVEGAÇÃO SEGURA NA INTERNET





Vai navegar na internet? Então pegue o equipamento de segurança!!!

A Internet é uma ferramenta poderosa, mas também pode ser um ambiente perigoso se não tomarmos as devidas precauções.

O conhecimento é o seu maior aliado, quando se trata de internet, muitas pessoas a utilizam sem prestar atenção, ignorando conceitos básicos, com a desculpa de que não precisam entender desses conceitos, por que não são nerds ou especialistas de informática.

O uso da internet tem que ser racional e responsável, nesta cartilha, abordaremos os principais tópicos para navegar com segurança na internet.

Peguem suas espadas e escudos que vamos começar.

Utilize um navegador seguro:

Mantenha seu navegador sempre atualizado com as versões mais recentes, pois as atualizações frequentes corrigem falhas de segurança. Tenha em mente que ameaças digitais estão em constante evolução e milhares surgem todos os dias.

Utilize navegadores conhecidos e confiáveis, como Google Chrome, Mozilla Firefox, Microsoft Edge, Safari, entre outros. Mas só baixe esses navegadores de seus sites oficiais, em outros sites você corre o risco do instalador vir com vírus.

Ative recursos de segurança, como bloqueadores de pop-ups e notificações, para evitar possíveis golpes.





Não use este navegador, o mesmo é utilizado para acessar camadas inseguras da internet, DeepWeb e DarkWeb.

“Assim como os usuários do Tor, os desenvolvedores, pesquisadores e fundadores que tornaram o Tor possível são um grupo diversificado de pessoas. Mas todas as pessoas que estiveram envolvidas no Tor estão unidas por uma crença comum: os usuários da Internet devem ter acesso privado a uma web sem censura”.Fonte: <https://www.torproject.org/pt-BR/about/history/>

Se a proposta é privacidade, por que não usar o TOR? Porque, assim como outras ideias e tecnologias criadas para internet, tiveram seu propósito desviado, o TOR, seguiu a mesma linha e hoje ele é utilizado pelo submundo digital para cometimento de crimes virtuais.

O que é Deep Web?

A deep web, traduzindo para o Português, seria a web escondida, oculta ou profunda. Ela possui uma quantidade baixa de regulamentação. No caso, você não pode simplesmente pesquisar seu conteúdo no Google ou similar, por exemplo, pois ele não será encontrado por esses motores de busca. No entanto, ela não necessariamente é associada a ações clandestinas.

Fonte: <https://blog.betrybe.com/tecnologia/deep-web-e-dark-web/#1>

Tanto na deep web, quanto a dark web, não existem servidores hospedando paginas e serviços para acesso de todos, a comunicação se dá ponto-a-ponto, ou seja seu computador será um ponto de acesso, onde você pode prover um serviço específico, e só terá acesso ao seu computador, quem tiver conhecimento dele. Assim cibercriminosos e grupos terroristas se utilizam destes recursos, para cometimentos de crimes.

O que é a Dark Web?

A Dark Web seria um nível ainda abaixo da Deep Web e, para ela, precisamos ter um navegador específico para acessar, chamado Tor. Aqui, a fama de algo oculto e clandestino começa a fazer sentido, pois, como há ainda menos supervisão e possibilidade de rastreamento, muitas práticas criminosas surgem nessa camada.

Portanto, a Dark Web fornece um alto nível de privacidade e, com isso, fica quase impossível rastrear as ações que são realizadas por pessoas.

Caso você deseje se aventurar na Dark Web, deverá utilizar softwares poderosos de criptografia para proteção de seus dados, pois todos que estão nessa rede são vulneráveis a todos os tipos de ataques cibernéticos que possam ocorrer.

Fonte: <https://blog.betrybe.com/tecnologia/deep-web-e-dark-web/#1>



Quais as diferenças entre Deep Web, Dark Web e Web de superfície?

As diferenças entre esses conceitos é a seguinte:

Web de superfície: seria, basicamente, a internet visível para todos. A parte da internet onde você realiza suas tarefas como compras online, acessar redes sociais e, até mesmo, ler esse artigo no blog da Trybe. Ou seja, é toda a parte visível da internet que utilizamos;

Deep web: é uma parte escondida da web que pode ter alguns dados comuns nela, como registros de consulta médica, bancos de dados e intranets, redes internas utilizadas pelas empresas para conexões em outros locais.

Dark web: é uma rede que utiliza um navegador em específico para ser utilizado, no caso, o Tor. Ela não deixa rastros em suas ações e garante a privacidade dos usuários ou usuárias que utilizam ela. Mas, ela pode ser facilmente operada por pessoas mal intencionadas.

Fonte: <https://blog.betrybe.com/tecnologia/deep-web-e-dark-web/#1>

Tenha certeza que o site que você navega é seguro

Certifique-se de que o site possui um certificado SSL (Secure Socket Layer), identificado pelo "https://" na barra de endereço e um ícone de cadeado. O HTTPS é um protocolo seguro, que visa garantir a segurança de sua navegação.

Evite clicar em links suspeitos recebidos por e-mail ou mensagem. Em vez disso, digite manualmente o endereço do site que deseja visitar.

Utilize ferramentas de segurança, como extensões de navegador que ajudem a identificar sites maliciosos ou suspeitos.

Acesse a URL

<https://king.host/blog/tecnologia/dicas-de-seguranca/> para conhecer 30 dicas de segurança.



Evite downloads suspeitos

Faça downloads somente de sites confiáveis e oficiais. Evite baixar programas de fontes desconhecidas.

Verifique a autenticidade dos arquivos baixados utilizando um antivírus antes de executá-los.

Evite clicar em anúncios ou links de download suspeitos em sites não confiáveis.

Fuja dos links de casas de apostas e ganhos fáceis, além dos links comerciais e vendas de produtos que apontem para links desconhecidos.



Cuide de suas informações pessoais:

Nunca compartilhe senhas, informações de cartão de crédito ou dados pessoais por e-mail, mensagem ou em sites não seguros.

Utilize senhas fortes, combinando letras maiúsculas, minúsculas, números e caracteres especiais, e evite utilizar a mesma senha para várias contas.

Esteja atento a tentativas de phishing, onde criminosos tentam obter informações pessoais disfarçando-se de empresas ou instituições confiáveis.

Seja responsável das redes sociais:

Revise e ajuste as configurações de privacidade em suas redes sociais para controlar quem pode ver suas informações e postagens.

Tenha cuidado ao aceitar solicitações de amizade ou mensagens de desconhecidos.

Evite compartilhar informações sensíveis publicamente, como endereço, telefone ou detalhes de viagens.

Use antivírus renomados, dê preferência as licenças pagas, para ter direito a suporte.

Mantenha seu antivírus sempre atualizado para garantir a proteção contra as ameaças mais recentes.

Realize varreduras regulares em seu computador para identificar e remover possíveis ameaças.

Não plugue pendrives ou discos externos de desconhecidos, assim como também, não use seus dispositivos de armazenamento em computadores não seguros. Passe sempre o antivírus.



Redes Wi-Fi públicas? CUIDADO

Evite realizar transações financeiras ou acessar informações confidenciais em redes Wi-Fi públicas e não seguras, redes de lojas e instituições públicas. Estas redes não possuem tratamento e nem equipamento de segurança adequado para sua gerência.

Utilize uma rede privada virtual (VPN) ao se conectar a redes Wi-Fi públicas para aumentar a segurança dos seus dados.

Faça uso de seus dados móveis, com os devidos aplicativos de segurança, antivírus, vpn e firewall pessoal.



SEJA PRECAVIDO!!! Faça Backup!

Faça cópias de segurança regularmente de seus arquivos importantes em um dispositivo externo ou serviço de armazenamento na nuvem.

Em caso de ransomware(sequestro de informações por criminosos) ou perda de dados, ter um backup atualizado ajuda a recuperar suas informações.



Se atualize!!!

Esteja sempre atualizado sobre as últimas ameaças e golpes na internet, participando de cursos e lendo notícias confiáveis sobre segurança digital.

Ensine a seus familiares e amigos sobre a importância da navegação segura na internet.

A partir do momento em que você opta por usar a internet, é bom grado que você saiba usá-la com segurança, pois basta apenas um clique para que você perca, dados e quem sabe até mesmo sua identidade.

Fique esperto!!!

Se atualize!!!

Lembre-se de que a segurança na internet é uma responsabilidade compartilhada. Ao seguir essas orientações e manter-se informado, você estará mais preparado para navegar com segurança e proteger suas informações online.



SEJA SEGURO!!!